SIEMENS

SIMATIC

S7-1200 Programmable controller

System Manual

Introduction 1

Product overview 2

New features 3

STEP 7 programming software 4

Installation 5

PLC concepts 6

Device configuration 7

Programming concepts 8

Basic instructions 9

Extended instructions 10

Technology instructions 11

Communication 12

Web server 13

Communication processor and Modbus TCP 14

Online and diagnostic tools 15

V4.7 12/2024

A5E02486680-AQ

Continued on next page

Continued

Technical specifications A

Calculating a power budget B

Ordering Information C

Device exchange and spare parts compatibility D

S7-1200 Programmable controller

System Manual

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E02486680-AQ
Ⓟ 11/2024 Subject to change

Copyright © Siemens 2024.
All rights reserved

Table of contents

1 Introduction ... 24

1.1 General information ... 24

1.2 Maintaining operational safety of your plant ... 26

1.3 S7-1200 documentation guide ... 27

1.4 SIMATIC Technical Documentation ... 27

1.5 Tool support ... 29

1.6 Cybersecurity information ... 31

2 Product overview ... 32

2.1 Introducing the S7-1200 PLC ... 32

2.2 Expansion capability of the CPU ... 35

2.3 HMI panels ... 36

3 New features ... 37

4 STEP 7 programming software ... 38

4.1 Different views to make the work easier ... 38

4.2 Compatibility between STEP 7 and the S7-1200 ... 39

5 Installation ... 41

5.1 Guidelines for installing S7-1200 devices ... 41

5.2 Power budget ... 42

5.3 Installation and removal procedures ... 44

5.3.1 Mounting dimensions for the S7-1200 devices ... 44

5.3.2 Installing and removing the CPU ... 47

5.3.3 Installing and removing an SB, CB, or BB ... 49

5.3.4 Installing and removing an SM ... 50

5.3.5 Installing and removing a CM or CP ... 51

5.3.6 Removing and reinstalling the S7-1200 terminal block connector ... 52

5.3.7 Installing and removing the expansion cable ... 53

5.4 Wiring guidelines ... 55

5.5 Maintenance and repair ... 60

6 PLC concepts ... 61

6.1 Execution of the user program ... 61

6.1.1 Startup configuration and processing ... 64

6.1.2 Processing the scan cycle in RUN mode ... 66

6.1.3 Organization blocks (OBs) ... 66

6.1.3.1 Organization blocks (OBs) ... 66

6.1.3.2 Program cycle OB ... 67
6.1.3.3 Startup OB ... 67
6.1.3.4 Time delay interrupt OB ... 68
6.1.3.5 Cyclic interrupt OB ... 68
6.1.3.6 Hardware interrupt OB ... 69
6.1.3.7 Time error interrupt OB ... 70
6.1.3.8 Diagnostic error interrupt OB ... 71
6.1.3.9 Pull or plug of modules OB ... 72
6.1.3.10 Rack or station failure OB ... 73
6.1.3.11 Time of day OB ... 73
6.1.3.12 Status OB ... 74
6.1.3.13 Update OB ... 74
6.1.3.14 Profile OB ... 75
6.1.3.15 MC-Servo and MC-Interpolator OB ... 75
6.1.3.16 MC-PreServo ... 76
6.1.3.17 MC-PostServo ... 77
6.1.3.18 Event execution priorities and queuing ... 77
6.1.4 Monitoring and configuring the cycle time ... 81
6.1.5 CPU memory ... 83
6.1.5.1 Notes about retentive memory ... 84
6.1.5.2 System and clock memory ... 84
6.1.6 Diagnostics buffer ... 86
6.1.7 Time of day clock ... 87
6.1.8 Configuring the outputs on a RUN-to-STOP transition ... 88

6.2 Data storage, memory areas, I/O, and addressing ... 89
6.2.1 Accessing the data of the CPU ... 89

6.3 Processing of analog values ... 94

6.4 Data types ... 95
6.4.1 Bool, Byte, Word, and DWord data types ... 96
6.4.2 Integer data types ... 97
6.4.3 Floating-point real data types ... 97
6.4.4 Time and Date data types ... 98
6.4.5 Character and String data types ... 99
6.4.6 Array data type ... 101
6.4.7 Data structure data type ... 102
6.4.8 PLC data type ... 102
6.4.9 Variant pointer data type ... 103
6.4.10 Accessing a "slice" of a tagged data type ... 103
6.4.11 Accessing a tag with an AT overlay ... 104

6.5 Using a memory card ... 106
6.5.1 Inserting a memory card in the CPU ... 106
6.5.2 Configuring the startup parameter of the CPU before copying the project to the memory card ... 109
6.5.3 Transfer card ... 109
6.5.4 Program card ... 112
6.5.5 Using a memory card for protecting confidential PLC configuration data ... 115
6.5.6 Firmware update ... 117

6.6 Recovery from a lost password ... 119

7 Device configuration ... 121

7.1 Inserting a CPU ... 122

7.2 Uploading the configuration of a connected CPU ... 124

7.3 Adding modules to the configuration ... 126

7.4 Configuration control ... 127
7.4.1 Advantages and applications of configuration control ... 127
7.4.2 Configuring the central installation and optional modules ... 128
7.4.3 Example of configuration control ... 133

7.5 Changing a device ... 136

7.6 Configuring the operation of the CPU ... 136
7.6.1 CPU properties ... 136
7.6.2 Configuring the onboard I/O ... 138
7.6.3 Configuring digital input filter times ... 139
7.6.4 Pulse catch ... 140

7.7 Configuring multilingual support ... 142

7.8 Protection & security ... 144
7.8.1 Using the security wizard to set PLC security settings ... 144
7.8.2 Protection of confidential PLC configuration data ... 145
7.8.3 User Management & Access Control (UMAC) ... 147
7.8.4 Access control for the S7-1200 CPU ... 151
7.8.5 Configuring connection mechanisms ... 154
7.8.5.1 Setting access mechanism for remote partners ... 154
7.8.5.2 Enabling secure PG/PC and HMI communication and creating certificates ... 155
7.8.6 Syslog server ... 156
7.8.7 External load memory ... 159
7.8.8 Know-how protection ... 159
7.8.9 Write protection ... 160
7.8.10 Copy protection ... 160

7.9 Configuring the parameters of the modules ... 162

7.10 Configuring the CPU for communication ... 163

7.11 Time synchronization ... 165

8 Programming concepts ... 167

8.1 Guidelines for designing a PLC system ... 167

8.2 Structuring your user program ... 168

8.3 Using blocks to structure your program ... 169
8.3.1 Organization block (OB) ... 170
8.3.2 Function (FC) ... 172
8.3.3 Function block (FB) ... 172
8.3.4 Data block (DB) ... 174
8.3.5 Creating reusable code blocks ... 175
8.3.6 Passing parameters to blocks ... 176

8.4 Understanding data consistency ... 178

8.5 Programming language ... 179
8.5.1 Ladder logic (LAD) ... 179
8.5.2 Function Block Diagram (FBD) ... 180
8.5.3 SCL ... 181
8.5.3.1 SCL program editor ... 181
8.5.3.2 SCL expressions and operations ... 182
8.5.3.3 Indexed addressing with PEEK and POKE instructions ... 185
8.5.4 EN and ENO for LAD, FBD and SCL ... 187

8.6 Downloading the elements of your program ... 189

8.7 Synchronizing the online CPU and offline project ... 192

8.8 Uploading from the online CPU ... 193
8.8.1 Comparing the online CPU to the offline CPU ... 194

8.9 Debugging and testing the program ... 194
8.9.1 Monitor and modify data in the CPU ... 194
8.9.2 Watch tables and force tables ... 194
8.9.3 Cross reference to show usage ... 195
8.9.4 Call structure to examine the calling hierarchy ... 196

9 Basic instructions ... 197

9.1 Bit logic operations ... 197
9.1.1 Bit logic instructions ... 197
9.1.2 Set and reset instructions ... 200
9.1.3 Positive and negative edge instructions ... 202

9.2 Timer operations ... 204

9.3 Counter operations ... 211

9.4 Comparator operations ... 215
9.4.1 Compare values instructions ... 215
9.4.2 IN_Range (Value within range) and OUT_Range (Value outside range) ... 216
9.4.3 OK (Check validity) and NOT_OK (Check invalidity) ... 217
9.4.4 Variant and array comparison instructions ... 217
9.4.4.1 Equality and non-equality comparison instructions ... 217
9.4.4.2 Null comparision instructions ... 218
9.4.4.3 IS_ARRAY (Check for ARRAY) ... 219

9.5 Math functions ... 219
9.5.1 CALCULATE (Calculate) ... 219
9.5.2 Add, subtract, multiply and divide instructions ... 220
9.5.3 MOD (return remainder of division) ... 221
9.5.4 NEG (Create twos complement) ... 222
9.5.5 INC (Increment) and DEC (Decrement) ... 222
9.5.6 ABS (Form absolute value) ... 223
9.5.7 MIN (Get minimum) and MAX (Get maximum) ... 223
9.5.8 LIMIT (Set limit value) ... 224
9.5.9 Exponent, logarithm, and trigonometry instructions ... 225

9.6 Move operations ... 226
9.6.1 MOVE (Move value), MOVE_BLK (Move block), UMOVE_BLK (Move block uninterruptible), and MOVE_BLK_VARIANT (Move block) ... 226

9.6.2 Deserialize ... 229
9.6.3 Serialize ... 232
9.6.4 FILL_BLK (Fill block) and UFILL_BLK (Fill block uninterruptible) ... 234
9.6.5 SCATTER ... 235
9.6.6 SCATTER_BLK ... 238
9.6.7 GATHER ... 241
9.6.8 GATHER_BLK ... 245
9.6.9 SWAP (Swap bytes) ... 248
9.6.10 Read / Write memory instructions ... 249
9.6.10.1 PEEK and POKE (SCL only) ... 249
9.6.10.2 Read and write big and little Endian instructions (SCL) ... 250
9.6.11 Variant instructions ... 252
9.6.11.1 VariantGet (Read VARIANT tag value) ... 252
9.6.11.2 VariantPut (Write VARIANT tag value) ... 252
9.6.11.3 CountOfElements (Get number of ARRAY elements) ... 253
9.6.12 Array instructions ... 254
9.6.12.1 LOWER_BOUND: (Read out ARRAY low limit) ... 254
9.6.12.2 UPPER_BOUND: (Read out ARRAY high limit) ... 255
9.6.13 Legacy instructions ... 257
9.6.13.1 FieldRead (Read field) and FieldWrite (Write field) instructions ... 257

9.7 Conversion operations ... 258
9.7.1 CONV (Convert value) ... 258
9.7.2 Conversion instructions for SCL ... 259
9.7.3 ROUND (Round numerical value) and TRUNC (Truncate numerical value) ... 262
9.7.4 CEIL and FLOOR (Generate next higher and lower integer from floating-point number) ... 263
9.7.5 SCALE_X (Scale) and NORM_X (Normalize) ... 263
9.7.6 Variant conversion instructions ... 266
9.7.6.1 VARIANT_TO_DB_ANY (Convert VARIANT to DB_ANY) ... 266
9.7.6.2 DB_ANY_TO_VARIANT (Convert DB_ANY to VARIANT) ... 267

9.8 Program control operations ... 268
9.8.1 JMP (Jump if RLO = 1), JMPN (Jump if RLO = 0), and Label (Jump label) instructions ... 268
9.8.2 JMP_LIST (Define jump list) ... 269
9.8.3 SWITCH (Jump distributor) ... 269
9.8.4 RET (Return) ... 271
9.8.5 ENDIS_PW (Enable/disable CPU passwords) ... 272
9.8.6 RE_TRIGR (Restart cycle monitoring time) ... 274
9.8.7 STP (Exit program) ... 275
9.8.8 GET_ERROR and GET_ERROR_ID (Get error and error ID locally) instructions ... 276
9.8.9 RUNTIME (Measure program runtime) ... 279
9.8.10 SCL program control statements ... 280
9.8.10.1 IF-THEN ... 281
9.8.10.2 CASE ... 282
9.8.10.3 FOR ... 283
9.8.10.4 WHILE-DO ... 284
9.8.10.5 REPEAT-UNTIL ... 284
9.8.10.6 CONTINUE ... 285
9.8.10.7 EXIT ... 286
9.8.10.8 GOTO ... 286
9.8.10.9 RETURN ... 287

9.9 Word logic operations ... 287

9.9.1 AND, OR, and XOR logic operation instructions ... 287
9.9.2 INV (Create ones complement) ... 288
9.9.3 DECO (Decode) and ENCO (Encode) instructions ... 288
9.9.4 SEL (Select), MUX (Multiplex), and DEMUX (Demultiplex) instructions ... 289

9.10 Shift and rotate ... 291
9.10.1 SHR (Shift right) and SHL (Shift left) instructions ... 291
9.10.2 ROR (Rotate right) and ROL (Rotate left) instructions ... 292

10 Extended instructions ... 293

10.1 Date, time-of-day, and clock functions ... 293
10.1.1 Date and time-of-day instructions ... 293
10.1.2 Clock functions ... 295
10.1.3 SET_TIMEZONE (Set timezone) ... 297
10.1.4 RTM (Runtime meters) ... 299

10.2 String and character ... 301
10.2.1 String data overview ... 301
10.2.2 S_MOVE (Move character string) ... 301
10.2.3 String conversion instructions ... 302
10.2.3.1 S_CONV, STRG_VAL, and VAL_STRG (Convert to/from character string and number) instructions ... 302
10.2.3.2 Strg_TO_Chars and Chars_TO_Strg (Convert to/from character string and array of CHAR) instructions ... 310
10.2.3.3 ATH and HTA (Convert to/from ASCII string and hexadecimal number) instructions ... 311
10.2.4 String operation instructions ... 313
10.2.4.1 MAX_LEN (Maximum length of a character string) ... 313
10.2.4.2 LEN (Determine the length of a character string) ... 313
10.2.4.3 CONCAT (Combine character strings) ... 314
10.2.4.4 LEFT, RIGHT, and MID (Read substrings in a character string) instructions ... 315
10.2.4.5 DELETE (Delete characters in a character string) ... 316
10.2.4.6 INSERT (Insert characters in a character string) ... 317
10.2.4.7 REPLACE (Replace characters in a character string) ... 318
10.2.4.8 FIND (Find characters in a character string) ... 319
10.2.5 Runtime information ... 319
10.2.5.1 GetSymbolName (Read out a tag on the input parameter) ... 319
10.2.5.2 GetSymbolPath (Query composite global name of the input parameter assignment) ... 322
10.2.5.3 GetInstanceName (Read out name of the block instance) ... 324
10.2.5.4 GetInstancePath (Query composite global name of the block instance) ... 326
10.2.5.5 GetBlockName (Read out name of the block) ... 328

10.3 Distributed I/O (PROFINET, PROFIBUS, or AS-i) ... 330
10.3.1 RDREC and WRREC (Read/write data record) ... 330
10.3.2 GETIO (Read process image) ... 333
10.3.3 SETIO (Transfer process image) ... 334
10.3.4 GETIO_PART (Read process image area) ... 335
10.3.5 SETIO_PART (Transfer process image area) ... 336
10.3.6 RALRM (Receive interrupt) ... 337
10.3.7 D_ACT_DP (Enable/disable PROFINET IO devices) ... 340
10.3.8 STATUS parameter for RDREC, WRREC, and RALRM ... 345
10.3.9 Others ... 348
10.3.9.1 DPRD_DAT and DPWR_DAT (Read/write consistent data) ... 348
10.3.9.2 RCVREC (Receive data record) ... 351

10.3.9.3 PRVREC (Make data record available) ... 353
10.3.9.4 DPNRM_DG (Read diagnostic data from a PROFIBUS DP slave) ... 355

10.4 PROFIenergy ... 357

10.5 Interrupts ... 358
10.5.1 ATTACH and DETACH (Attach/detach an OB and an interrupt event) instructions ... 358
10.5.2 Cyclic interrupts ... 361
10.5.2.1 SET_CINT (Set cyclic interrupt parameters) ... 361
10.5.2.2 QRY_CINT (Query cyclic interrupt parameters) ... 363
10.5.3 Time of day interrupts ... 364
10.5.3.1 SET_TINTL (Set time of day interrupt) ... 364
10.5.3.2 CAN_TINT (Cancel time of day interrupt) ... 366
10.5.3.3 ACT_TINT (Activate time of day interrupt) ... 366
10.5.3.4 QRY_TINT (Query status of time of day interrupt) ... 367
10.5.4 Time delay interrupts ... 368
10.5.5 DIS_AIRT and EN_AIRT (Delay/enable execution of higher priority interrupts and asynchronous error events) instructions ... 370

10.6 Alarms ... 371
10.6.1 Gen_UsrMsg (Generate user diagnostic alarms) ... 371

10.7 Diagnostics (PROFINET or PROFIBUS) ... 373
10.7.1 RD_SINFO (Read current OB start information) ... 373
10.7.2 LED (Read LED status) ... 382
10.7.3 Get_IM_Data (Read the identification and maintenance data) ... 383
10.7.4 Get_Name (Read the name of a PROFINET IO device) ... 384
10.7.5 GetStationInfo (Read the IP or MAC address of a PROFINET IO device) ... 390
10.7.6 DeviceStates instruction ... 397
10.7.6.1 DeviceStates example configurations ... 398
10.7.7 ModuleStates instruction ... 402
10.7.7.1 ModuleStates example configurations ... 403
10.7.8 GET_DIAG (Read diagnostic information) ... 406
10.7.9 GetSMCInfo (Reading out information about the memory card) ... 412

10.8 Pulse ... 415
10.8.1 CTRL_PWM (Pulse width modulation) ... 415
10.8.2 CTRL_PTO (Pulse train output) ... 416
10.8.3 Operation of the pulse outputs ... 419
10.8.4 Configuring a pulse channel for PWM or PTO ... 421

10.9 Recipes and Data logs ... 425
10.9.1 Recipes ... 425
10.9.1.1 Recipe overview ... 425
10.9.1.2 Recipe example ... 426
10.9.1.3 Program instructions that transfer recipe data ... 429
10.9.1.3.1 RecipeExport (Recipe export) ... 429
10.9.1.3.2 RecipeImport (Recipe import) ... 431
10.9.1.4 Recipe example program ... 432
10.9.2 Data logs ... 435
10.9.2.1 Data log record structure ... 435
10.9.2.2 Program instructions that control data logs ... 436
10.9.2.2.1 DataLogCreate (Create data log) ... 436
10.9.2.2.2 DataLogOpen (Open data log) ... 440
10.9.2.2.3 DataLogWrite (Write data log) ... 441

10.9.2.2.4 DataLogClear (Empty data log) 443
10.9.2.2.5 DataLogClose (Close data log) 445
10.9.2.2.6 DataLogDelete (Delete data log) 446
10.9.2.2.7 DataLogNewFile (Data log in new file) 447
10.9.2.3 Working with data logs 449
10.9.2.4 Limit to the size of data log files 451
10.9.2.5 Data log example program 453

10.10 Data block control 459
10.10.1 CREATE_DB (Create data block) 459
10.10.2 READ_DBL and WRIT_DBL (Read/write a data block in load memory) instructions 462
10.10.3 ATTR_DB (Read data block attribute) 464
10.10.4 DELETE_DB (Delete data block) 466

10.11 Address handling 467
10.11.1 GEO2LOG (Determine the hardware identifier from the slot) 467
10.11.2 LOG2GEO (Determine the slot from the hardware identifier) 469
10.11.3 IO2MOD (Determine the hardware identifier from an I/O address) 470
10.11.4 RD_ADDR (Determine the IO addresses from the hardware identifier) 471
10.11.5 GEOADDR system data type 472

10.12 Common error codes for the Extended instructions 473

10.13 File handling 473
10.13.1 FileReadC: Read file from the memory card 473
10.13.2 FileWriteC: Write file on the memory card 476
10.13.3 FileDelete: Delete file on the memory card 478

11 Technology instructions 480

11.1 Counting (High-speed counters) 480
11.1.1 CTRL_HSC_EXT (Control high-speed counter, extended) 481
11.1.1.1 CTRL_HSC_EXT example 482
11.1.1.2 CTRL_HSC_EXT Instruction System Data Types (SDT) 485
11.1.1.2.1 SDT: HSC_Count 485
11.1.1.2.2 SDT: HSC_Period 487
11.1.1.2.3 SDT: HSC_Frequency 488
11.1.2 Operating the high-speed counter 489
11.1.2.1 Synchronization function 489
11.1.2.2 Gate function 490
11.1.2.3 Capture function 491
11.1.2.4 Compare function 493
11.1.2.5 Application 493
11.1.3 Configuring a high-speed counter 494
11.1.3.1 Type of Counting 496
11.1.3.2 Operating phase 497
11.1.3.3 Initial values 500
11.1.3.4 Input functions 500
11.1.3.5 Output function 501
11.1.3.5.1 Compare output 501
11.1.3.6 Interrupt events 501
11.1.3.7 Hardware input pin assignment 502
11.1.3.8 Hardware output pin assignment 503
11.1.3.9 HSC input memory addresses 504
11.1.3.10 Hardware identifier 504

11.1.4 Legacy CTRL_HSC (Control high-speed counter) instruction ... 504
11.1.4.1 CTRL_HSC (Control high-speed counter) ... 504
11.1.4.2 Using CTRL_HSC ... 506
11.1.4.3 HSC current count value ... 506

11.2 Motion control ... 507
11.2.1 Motion control overview ... 507
11.2.2 Hardware components for motion control ... 507
11.2.3 Motion control instructions ... 509
11.2.3.1 MC instruction overview ... 509
11.2.3.2 MC_Power (Release/block axis) ... 510
11.2.3.3 MC_Reset (Confirm error) ... 511
11.2.3.4 MC_Home (Home axis) ... 511
11.2.3.5 MC_Halt (Pause axis) ... 512
11.2.3.6 MC_MoveAbsolute (Position axis absolutely) ... 512
11.2.3.7 MC_MoveRelative (Position axis relatively) ... 513
11.2.3.8 MC_MoveVelocity (Move axis at predefined velocity) ... 513
11.2.3.9 MC_MoveJog (Move axis in jog mode) ... 514
11.2.3.10 MC_CommandTable (Run axis command as movement sequence) ... 514
11.2.3.11 MC_WriteParam (write parameters of a technology object) ... 515
11.2.3.12 MC_ReadParam instruction (read parameters of a technology object) ... 515
11.2.3.13 MC_ChangeDynamic (Change dynamic settings for the axis) ... 516

11.3 PID control ... 516
11.3.1 PID functionality ... 516
11.3.2 PID instructions ... 517
11.3.2.1 PID_Compact instruction ... 517
11.3.2.2 PID_3Step instruction ... 518
11.3.2.3 PID_Temp instruction ... 519

12 Communication ... 520

12.1 Overview ... 520

12.2 Secure vs. legacy communication ... 521

12.3 Communication protocols and ports used by Ethernet communication ... 524

12.4 Asynchronous communication connections ... 526

12.5 Supported certificates ... 529

12.6 PROFINET ... 530
12.6.1 Creating a network connection ... 531
12.6.2 Configuring the Local/Partner connection path ... 532
12.6.3 Assigning Internet Protocol (IP) addresses ... 535
12.6.3.1 Assigning IP addresses to programming and network devices ... 535
12.6.3.2 Checking the IP address and MAC address of your network interface ... 537
12.6.3.3 Assigning an IP address to a CPU online ... 537
12.6.3.4 Configuring an IP address for a CPU in your project ... 538
12.6.4 Testing the PROFINET network ... 542
12.6.5 Locating the Ethernet (MAC) address on the CPU ... 543
12.6.6 Configuring Network Time Protocol (NTP) synchronization ... 544
12.6.7 PROFINET device start-up time, naming, and address assignment ... 545
12.6.8 Open user communication ... 546
12.6.8.1 Protocols ... 546

12.6.8.2 TCP and ISO on TCP.... 547
12.6.8.3 Ad hoc mode.... 548
12.6.8.4 Communication services and used port numbers.... 548
12.6.8.5 Connection IDs for the Open user communication instructions.... 549
12.6.8.6 Parameters for the PROFINET connection.... 551
12.6.8.7 Supported TLS versions.... 557
12.6.8.8 Configuring DNS.... 558
12.6.8.9 Configuring an OUC connection in the TIA Portal.... 558
12.6.8.10 TSEND_C and TRCV_C instructions.... 562
12.6.8.10.1 TSEND_C and TRCV_C (Send and receive data using Ethernet).... 562
12.6.8.11 Legacy TSEND_C and TRCV_C instructions.... 571
12.6.8.11.1 Legacy TSEND_C and TRCV_C (Send and receive data using Ethernet).... 572
12.6.8.12 TCON, TDISCON, TSEND, and TRCV instructions.... 577
12.6.8.12.1 TCON, TDISCON, TSEND, and TRCV (TCP communication) instructions.... 578
12.6.8.13 TCONSettings.... 586
12.6.8.14 Legacy TCON, TDISCON, TSEND, and TRCV instructions.... 591
12.6.8.14.1 Legacy TCON, TDISCON, TSEND, and TRCV (TCP communication) instructions.... 592
12.6.8.15 T_RESET (Terminate and re-establish an existing connection) instruction.... 599
12.6.8.16 T_DIAG (Checks the status of connection and reads information) instruction.... 601
12.6.8.17 TMAIL_C (Send an email using the Ethernet interface of the CPU) instruction.... 604
12.6.8.17.1 Overview.... 604
12.6.8.17.2 MAIL_ADDR_PARAM parameter.... 609
12.6.8.17.3 TO_S and CC parameters.... 615
12.6.8.17.4 DONE, BUSY and ERROR parameters.... 616
12.6.8.17.5 Sending data logs, recipes, and user files using email attachments.... 616
12.6.8.17.6 Error condition codes.... 618
12.6.8.18 UDP.... 623
12.6.8.19 TUSEND and TURCV.... 623
12.6.8.20 T_CONFIG.... 629
12.6.8.20.1 CONF_DATA Data block.... 632
12.6.8.20.2 Example: Using the T_CONFIG instruction to change IP parameters.... 635
12.6.8.20.3 Example: Using the T_CONFIG instruction to change IP parameters and PROFINET IO device names.... 636
12.6.8.20.4 Example: Using the T_CONFIG instruction to change IP addresses in the NTP servers.... 638
12.6.8.21 Common parameters for instructions.... 639
12.6.9 Communication with a programming device.... 640
12.6.9.1 Establishing the hardware communications connection.... 640
12.6.9.2 Configuring the devices.... 641
12.6.9.3 Assigning Internet Protocol (IP) addresses.... 642
12.6.9.4 Testing your PROFINET network.... 642
12.6.10 HMI-to-PLC communication.... 642
12.6.10.1 Configuring logical network connections between two devices.... 643
12.6.11 PLC-to-PLC communication.... 644
12.6.11.1 Configuring logical network connections between two devices.... 645
12.6.11.2 Configuring the Local/Partner connection path between two devices.... 645
12.6.11.3 Configuring transmit (send) and receive parameters.... 645
12.6.11.3.1 Configuring the TSEND_C instruction transmit (send) parameters.... 645
12.6.11.3.2 Configuring the TRCV_C instruction receive parameters.... 647
12.6.12 Configuring a CPU and PROFINET IO device.... 648
12.6.12.1 Adding a PROFINET IO device.... 648
12.6.12.2 Assigning CPUs and device names.... 648
12.6.12.3 Assigning Internet Protocol (IP) addresses.... 649

12.6.12.4 Configuring the IO cycle time ... 649
12.6.13 Configuring a CPU and PROFINET I-device ... 650
12.6.13.1 I-device functionality ... 650
12.6.13.2 Properties and advantages of the I-device ... 651
12.6.13.3 Characteristics of an I-device ... 652
12.6.13.4 Data exchange between higher- and lower-level IO system ... 654
12.6.13.5 Configuring the I-device ... 657
12.6.14 Shared devices ... 659
12.6.14.1 Shared device functionality ... 659
12.6.14.2 Example: Configuring a shared device (GSD configuration) ... 662
12.6.14.3 Example: Configuring an I-device as a shared device ... 667
12.6.15 Media Redundancy Protocol (MRP) ... 675
12.6.15.1 Media redundancy with ring topologies ... 677
12.6.15.2 Using Media Redundancy Protocol (MRP) ... 678
12.6.15.3 Configuring media redundancy ... 681
12.6.16 S7 routing ... 684
12.6.16.1 S7 routing between CPU and CP interfaces ... 685
12.6.16.2 S7 routing between two CP interfaces ... 686
12.6.17 SNMP ... 686
12.6.18 Diagnostics ... 691
12.6.19 Distributed I/O and diagnostic instructions ... 691

12.7 PROFIBUS ... 691
12.7.1 Communications services of the PROFIBUS CMs ... 693
12.7.2 Reference to the PROFIBUS CM user manuals ... 693
12.7.3 Configuring a DP master and slave device ... 694
12.7.3.1 Adding the CM 1243-5 (DP master) module and a DP slave ... 694
12.7.3.2 Configuring logical network connections between two PROFIBUS devices ... 694
12.7.3.3 Assigning PROFIBUS addresses to the CM 1243-5 module and DP slave ... 695
12.7.4 Distributed I/O and diagnostic instructions ... 696

12.8 AS-i ... 696
12.8.1 Configuring an AS-i master and slave device ... 697
12.8.1.1 Adding the AS-i master CM 1243-2 and AS-i slave ... 698
12.8.1.2 Configuring logical network connections between two AS-i devices ... 698
12.8.1.3 Configuring the properties of the AS-i master CM1243-2 ... 699
12.8.1.4 Assigning an AS-i address to an AS-i slave ... 699
12.8.2 Exchanging data between the user program and AS-i slaves ... 702
12.8.2.1 STEP 7 configuration ... 702
12.8.2.2 Configuring AS-i slaves with STEP 7 ... 703
12.8.3 Distributed I/O instructions ... 705
12.8.4 Working with AS-i online tools ... 705

12.9 S7 communication ... 706
12.9.1 GET and PUT (Read and write from a remote CPU) ... 706
12.9.2 Creating an S7 connection ... 709
12.9.3 Configuring the Local/Partner connection path between two devices ... 710
12.9.4 GET/PUT connection parameter assignment ... 711
12.9.4.1 Connection parameters ... 711
12.9.4.1.1 Connection ID parameter ... 713
12.9.4.1.2 Connection name parameter ... 713
12.9.4.2 Configuring a CPU-to-CPU S7 connection ... 714
12.9.4.2.1 Configuring a PROFINET S7 connection ... 715

12.9.4.2.2 Configuring a PROFIBUS S7 connection ... 716
12.10 Diagnostic events for distributed I/O ... 718
12.11 What to do when you cannot access the CPU by the IP address ... 719
12.12 OPC UA Server ... 720
12.12.1 OPC UA server configuration ... 720
12.12.1.1 Activating the OPC UA server ... 720
12.12.1.2 Behavior of the OPC UA server in operation ... 721
12.12.1.3 Settings for the OPC UA server ... 723
12.12.1.4 Limitations of the OPC UA server ... 724
12.12.2 OPC UA server security ... 725
12.12.2.1 Supported security policies ... 726
12.12.2.2 Trusted clients ... 727
12.12.2.3 Assigning OPC UA user rights for V4.7 configured CPUs ... 728
12.12.2.4 Authenticating OPC UA users for CPUs with project configurations earlier than V4.7 ... 730
12.12.2.5 OPC UA user compatibility ... 732
12.12.3 OPC UA server interface ... 734
12.12.3.1 Supported data types ... 734
12.12.3.2 PLC representation ... 735
12.12.3.3 Downloadable server interfaces ... 736
12.12.4 OPC UA Diagnostics Buffer ... 738
12.12.4.1 OPC UA Limits reached ... 739
12.12.4.2 OPC UA Security events ... 740
12.12.4.3 OPC UA Wrong usage ... 747
12.12.4.4 Summary messages for OPC UA ... 748
12.12.5 OPC UA Method calls ... 748
12.12.5.1 Boundary conditions for using server methods ... 752

13 Web server ... 753

13.1 Enabling the Web server ... 755
13.2 Web server user management ... 757
13.2.1 Assigning Web server user privileges for V4.7 configured CPUs ... 757
13.2.2 Assigning Web server user privileges for CPU project configurations earlier than V4.7 ... 760
13.2.3 User configuration compatibility ... 762
13.3 Accessing the Web pages from a PC ... 764
13.4 Accessing the Web pages from a mobile device ... 765
13.5 Using a CP module to access Web pages ... 766
13.6 Web server security certificates ... 767
13.7 Standard Web pages ... 768
13.7.1 Layout of the standard Web pages ... 768
13.7.2 Basic pages ... 769
13.7.3 Logging in and user privileges ... 769
13.7.4 Introduction ... 772
13.7.5 Start ... 773
13.7.6 Diagnostics ... 773
13.7.7 Diagnostics Buffer ... 776
13.7.8 Module Information ... 777
13.7.9 Communication ... 781

13.7.10 Tag status ... 784
13.7.11 Watch tables ... 786
13.7.12 Online backup ... 787
13.7.13 Data Logs ... 789
13.7.14 User Files ... 792
13.7.15 Data Log UserFiles API ... 794
13.7.16 File Browser ... 794

13.8 User-defined Web pages ... 796
13.8.1 Creating HTML pages ... 797
13.8.2 AWP commands supported by the S7-1200 Web server ... 798
13.8.2.1 Reading variables ... 799
13.8.2.2 Writing variables ... 800
13.8.2.3 Reading special variables ... 802
13.8.2.4 Writing special variables ... 803
13.8.2.5 Using an alias for a variable reference ... 804
13.8.2.6 Defining enum types ... 805
13.8.2.7 Referencing CPU variables with an enum type ... 806
13.8.2.8 Creating fragments ... 807
13.8.2.9 Importing fragments ... 808
13.8.2.10 Combining definitions ... 809
13.8.2.11 Handling tag names that contain special characters ... 809
13.8.3 Configuring use of user-defined Web pages ... 811
13.8.4 Configuring the entry page ... 812
13.8.5 Programming the WWW instruction for user-defined web pages ... 812
13.8.6 Downloading the program blocks to the CPU ... 814
13.8.7 Accessing the user-defined Web pages ... 814
13.8.8 Constraints specific to user-defined Web pages ... 814
13.8.9 Example of a user-defined web page ... 816
13.8.9.1 Web page for monitoring and controlling a wind turbine ... 816
13.8.9.2 Reading and displaying controller data ... 818
13.8.9.3 Using an enum type ... 818
13.8.9.4 Writing user input to the controller ... 819
13.8.9.5 Writing a special variable ... 820
13.8.9.6 Reference: HTML listing of remote wind turbine monitor Web page ... 820
13.8.9.7 Configuration in STEP 7 of the example Web page ... 825
13.8.10 Setting up user-defined Web pages in multiple languages ... 826
13.8.10.1 Creating the folder structure ... 826
13.8.10.2 Programming the language switch ... 826
13.8.10.3 Configuring STEP 7 to use a multi-language page structure ... 829
13.8.11 Advanced user-defined Web page control ... 829
13.8.12 Web API ... 833

13.9 Constraints ... 834
13.9.1 Use of JavaScript ... 835
13.9.2 Feature restrictions when the Internet options do not allow cookies ... 835
13.9.3 Rules for entering tag names and values ... 835
13.9.4 Importing CSV format data logs to non-USA/UK versions of Microsoft Excel ... 836

14 Communication processor and Modbus TCP ... 837

14.1 Using the serial communication interfaces ... 837

14.2 Biasing and terminating an RS485 network connector ... 838

14.3 Point-to-point (PtP) communication ... 839
14.3.1 PtP, Freeport communication ... 840
14.3.2 3964(R) communication ... 841
14.3.3 Configuring the PtP Freeport communication ... 842
14.3.3.1 Managing flow control ... 844
14.3.3.2 Configuring transmit (send) parameters ... 846
14.3.3.3 Configuring receive parameters ... 847
14.3.4 Configuring 3964(R) communication ... 854
14.3.4.1 Configuring the 3964(R) communication ports ... 854
14.3.4.2 Configuring the 3964(R) priority and protocol parameters ... 855
14.3.5 Point-to-point instructions ... 857
14.3.5.1 Common parameters for Point-to-Point instructions ... 857
14.3.5.2 Port_Config (Configure communication parameters dynamically) ... 859
14.3.5.3 Send_Config (Configure serial transmission parameters dynamically) ... 861
14.3.5.4 Receive_Config (Configure serial receive parameters dynamically) ... 863
14.3.5.5 P3964_Config (Configuring the 3964(R) protocol) ... 868
14.3.5.6 Send_P2P (Transmit send buffer data) ... 870
14.3.5.7 Receive_P2P (Enable receive messages) ... 873
14.3.5.8 Receive_Reset (Delete receive buffer) ... 875
14.3.5.9 Signal_Get (Query RS-232 signals) ... 876
14.3.5.10 Signal_Set (Set RS-232 signals) ... 877
14.3.5.11 Get_Features ... 878
14.3.5.12 Set_Features ... 879
14.3.6 Programming the PtP communications ... 880
14.3.6.1 Polling architecture ... 881
14.3.7 Example: Point-to-Point communication ... 882
14.3.7.1 Configuring the communication module ... 882
14.3.7.2 RS422 and RS485 operating modes ... 885
14.3.7.3 Programming the STEP 7 program ... 887
14.3.7.4 Configuring the terminal emulator ... 889
14.3.7.5 Running the example program ... 889

14.4 Universal serial interface (USS) communication ... 889
14.4.1 USS instructions ... 892
14.4.1.1 USS_Port_Scan (Edit communication using USS network) ... 892
14.4.1.2 USS_Drive_Control (Swap data with drive) ... 893
14.4.1.3 USS_Read_Param (Readout parameters from the drive) ... 895
14.4.1.4 USS_Write_Param (Change parameters in the drive) ... 896
14.4.2 USS status codes ... 898
14.4.3 USS general drive setup requirements ... 899
14.4.4 Example: USS general drive connection and setup ... 900

14.5 Modbus communication ... 902
14.5.1 Overview of Modbus TCP and Modbus RTU communication ... 902
14.5.2 Modbus TCP ... 904
14.5.2.1 Overview ... 904
14.5.2.2 Modbus TCP instructions ... 906
14.5.2.2.1 MB_CLIENT (Communicate using PROFINET as Modbus TCP client) instruction ... 906
14.5.2.2.2 MB_SERVER (Communicate using PROFINET as Modbus TCP server) instruction ... 914
14.5.2.2.3 MB_RED_CLIENT (Redundant communication over PROFINET as a Modbus TCP client) ... 924
14.5.2.2.4 MB_RED_SERVER (Communicating over PROFINET as a Modbus TCP server) ... 942
14.5.2.3 Modbus TCP examples ... 962
14.5.2.3.1 Example: MB_SERVER Multiple TCP connections ... 962

14.5.2.3.2 Example: MB_CLIENT 1: Multiple requests with common TCP connection ... 963
14.5.2.3.3 Example: MB_CLIENT 2: Multiple requests with different TCP connections ... 964
14.5.2.3.4 Example: MB_CLIENT 3: Output image write request ... 965
14.5.2.3.5 Example: MB_CLIENT 4: Coordinating multiple requests ... 965
14.5.3 Modbus RTU ... 966
14.5.3.1 Overview ... 966
14.5.3.2 Maximum number of supported Modbus slaves ... 968
14.5.3.3 Modbus RTU instructions ... 968
14.5.3.3.1 Modbus_Comm_Load (Configure SIPLUS I/O or port on the PtP module for Modbus RTU) instruction ... 968
14.5.3.3.2 Modbus_Master (Communicate using SIPLUS I/O or the PtP port as Modbus RTU master) instruction ... 972
14.5.3.3.3 Modbus_Slave (Communicate using SIPLUS I/O or the PtP port as Modbus RTU slave) instruction ... 978
14.5.3.4 Modbus RTU examples ... 987
14.5.3.4.1 Example: Modbus RTU master program ... 987
14.5.3.4.2 Example: Modbus RTU slave program ... 989

14.6 Legacy PtP communication (CM/CB 1241 only) ... 990
14.6.1 Legacy point-to-point instructions ... 990
14.6.1.1 PORT_CFG (Configure communication parameters dynamically) ... 990
14.6.1.2 SEND_CFG (Configure serial transmission parameters dynamically) ... 992
14.6.1.3 RCV_CFG (Configure serial receive parameters dynamically) ... 993
14.6.1.4 SEND_PTP (Transmit send buffer data) ... 997
14.6.1.5 RCV_PTP (Enable receive messages) ... 999
14.6.1.6 RCV_RST (Delete receive buffer) ... 1001
14.6.1.7 SGN_GET (Query RS-232 signals) ... 1002
14.6.1.8 SGN_SET (Set RS-232 signals) ... 1003

14.7 Legacy USS communication (CM/CB 1241 only) ... 1004
14.7.1 Legacy USS instructions ... 1005
14.7.1.1 USS_PORT (Edit communication using USS network) instruction ... 1005
14.7.1.2 USS_DRV (Swap data with drive) instruction ... 1006
14.7.1.3 USS_RPM (Readout parameters from the drive) instruction ... 1008
14.7.1.4 USS_WPM (Change parameters in the drive) instruction ... 1009
14.7.2 Legacy USS status codes ... 1011
14.7.3 Legacy USS general drive setup requirements ... 1012

14.8 Legacy Modbus TCP communication ... 1013
14.8.1 Overview ... 1013
14.8.2 Legacy Modbus TCP instructions ... 1013
14.8.2.1 MB_CLIENT (Communicate using PROFINET as Modbus TCP client) ... 1013
14.8.2.2 MB_SERVER (Communicate using PROFINET as Modbus TCP server) ... 1019
14.8.3 Legacy Modbus TCP examples ... 1024
14.8.3.1 Example: Legacy MB_SERVER Multiple TCP connections ... 1024
14.8.3.2 Example: Legacy MB_CLIENT 1: Multiple requests with common TCP connection ... 1024
14.8.3.3 Example: Legacy MB_CLIENT 2: Multiple requests with different TCP connections ... 1025
14.8.3.4 Example: Legacy MB_CLIENT 3: Output image write request ... 1027
14.8.3.5 Example: Legacy MB_CLIENT 4: Coordinating multiple requests ... 1027

14.9 Legacy Modbus RTU communication (CM/CB 1241 only) ... 1028
14.9.1 Overview ... 1028
14.9.2 Legacy Modbus RTU instructions ... 1028
14.9.2.1 MB_COMM_LOAD (Configure port on the PtP module for Modbus RTU) ... 1028
14.9.2.2 MB_MASTER (Communicate using the PtP port as Modbus RTU master) ... 1031

14.9.2.3 MB_SLAVE (Communicate using the PtP port as Modbus RTU slave) 1036
14.9.3 Legacy Modbus RTU examples 1042
14.9.3.1 Example: Legacy Modbus RTU master program 1042
14.9.3.2 Example: Legacy Modbus RTU slave program 1044

14.10 Industrial Remote Communication (IRC) 1044
14.10.1 Telecontrol CPs overview 1044
14.10.2 Further information 1046

15 Online and diagnostic tools 1047

15.1 Status LEDs 1047

15.2 Analog module diagnostics 1049

15.3 CPU error behavior 1050

15.4 Going online and connecting to a CPU 1051

15.5 Assigning a name to a PROFINET IO device online 1053

15.6 Setting the IP address and time of day 1054

15.7 Updating firmware 1055

15.8 Setting or deleting the password for protection of confidential PLC configuration data 1056

15.9 Resetting to factory settings 1057

15.10 Checking a module for defects (saving service data) 1058

15.11 Formatting a SIMATIC memory card from STEP 7 1060

15.12 CPU operator panel for the online CPU 1061

15.13 Monitoring the cycle time and memory usage 1061

15.14 Displaying diagnostic events in the CPU 1062

15.15 Comparing offline and online CPUs 1063

15.16 Performing an online/offline topology comparison 1064

15.17 Monitoring and modifying values in the CPU 1065
15.17.1 Going online to monitor the values in the CPU 1065
15.17.2 Displaying status in the program editor 1066
15.17.3 Capturing a snapshot of the online values of a DB for restoring values 1066
15.17.4 Using a watch table to monitor and modify values in the CPU 1068
15.17.4.1 Using a trigger when monitoring or modifying PLC tags 1069
15.17.4.2 Enabling outputs in STOP mode 1070
15.17.5 Forcing values in the CPU 1070
15.17.5.1 Using the force table 1070
15.17.5.2 Operation of the Force function 1071

15.18 Downloading in RUN mode 1072
15.18.1 Prerequisites for "Download in RUN mode" 1073
15.18.2 Changing your program in RUN mode 1074
15.18.3 Downloading selected blocks 1075
15.18.4 Downloading a single selected block with a compile error in another block 1076
15.18.5 Modifying and downloading existing tags in RUN mode 1077

15.18.6 System reaction if the download process fails ... 1079
15.18.7 Considerations when downloading in RUN mode ... 1080

15.19 Tracing and recording CPU data on trigger conditions ... 1081

15.20 Determining the type of wire break condition from an SM 1231 module ... 1083

15.21 Backing up and restoring a CPU ... 1085
15.21.1 Backup and restore options ... 1085
15.21.2 Backing up an online CPU ... 1086
15.21.3 Restoring a CPU ... 1088

A Technical specifications ... 1090

A.1 Siemens Online Support Web site ... 1090

A.2 General technical specifications ... 1090

A.3 Altitude specifications ... 1100

A.4 PROFINET interface X1 port pinouts ... 1103

A.5 CPU 1211C ... 1105
A.5.1 General specifications and features ... 1105
A.5.2 Timers, counters, and code blocks supported by CPU 1211C ... 1106
A.5.3 Communications CPU 1211C ... 1107
A.5.4 Power supply and sensor power ... 1109
A.5.5 Digital inputs and outputs ... 1110
A.5.6 Analog inputs ... 1111
A.5.6.1 Step response of the built-in analog inputs of the CPU ... 1112
A.5.6.2 Sample time for the built-in analog ports of the CPU ... 1112
A.5.6.3 Measurement ranges of the analog inputs for voltage (CPUs) ... 1112
A.5.7 CPU 1211C wiring diagrams ... 1113

A.6 CPU 1212C ... 1116
A.6.1 General specifications and features ... 1116
A.6.2 Timers, counters, and code blocks supported by CPU 1212C ... 1117
A.6.3 Communications CPU 1212C ... 1118
A.6.4 Power supply and sensor power ... 1120
A.6.5 Digital inputs and outputs ... 1121
A.6.6 Analog inputs ... 1123
A.6.6.1 Step response of the built-in analog inputs of the CPU ... 1123
A.6.6.2 Sample time for the built-in analog ports of the CPU ... 1123
A.6.6.3 Measurement ranges of the analog inputs for voltage (CPUs) ... 1124
A.6.7 CPU 1212C wiring diagrams ... 1124

A.7 CPU 1214C ... 1127
A.7.1 General specifications and features ... 1127
A.7.2 Timers, counters and code blocks supported by CPU 1214C ... 1129
A.7.3 Communications CPU 1214C ... 1130
A.7.4 Power supply and power sensor ... 1132
A.7.5 Digital inputs and outputs ... 1133
A.7.6 Analog inputs ... 1134
A.7.6.1 Step response of the built-in analog inputs of the CPU ... 1135
A.7.6.2 Sample time for the built-in analog ports of the CPU ... 1135
A.7.6.3 Measurement ranges of the analog inputs for voltage (CPUs) ... 1135
A.7.7 CPU 1214C wiring diagrams ... 1136

A.8 CPU 1215C ... 1139
A.8.1 General specifications and features ... 1139
A.8.2 Timers, counters and code blocks supported by CPU 1215C ... 1141
A.8.3 Communications CPU 1215C ... 1142
A.8.4 Power supply and sensor power (CPU 1215C) ... 1144
A.8.5 Digital inputs and outputs ... 1145
A.8.6 Analog inputs and outputs ... 1146
A.8.6.1 Step response of built-in analog inputs of the CPU ... 1147
A.8.6.2 Sample time for the built-in analog ports of the CPU ... 1147
A.8.6.3 Measurement ranges of the analog inputs for voltage (CPUs) ... 1147
A.8.6.4 Analog output specifications ... 1148
A.8.7 CPU 1215C wiring diagrams ... 1149

A.9 CPU 1217C ... 1153
A.9.1 General specifications and features ... 1153
A.9.2 Timers, counters and code blocks supported by CPU 1217C ... 1155
A.9.3 Communications CPU 1217C ... 1156
A.9.4 Power supply and sensor power (CPU 1217C) ... 1158
A.9.5 Digital inputs and outputs ... 1159
A.9.6 Analog inputs and outputs ... 1162
A.9.6.1 Analog input specifications ... 1162
A.9.6.2 Step response of built-in analog inputs of the CPU ... 1163
A.9.6.3 Sample time for the built-in analog ports of the CPU ... 1163
A.9.6.4 Measurement ranges of the analog inputs for voltage (CPUs) ... 1163
A.9.6.5 Analog output specifications ... 1164
A.9.7 CPU 1217C wiring diagrams ... 1165
A.9.8 CPU 1217C Differential Input (DI) detail and application example ... 1167
A.9.9 CPU 1217C Differential Output (DQ) detail and application example ... 1168

A.10 Digital signal modules (SMs) ... 1169
A.10.1 SM 1221 digital input specifications ... 1169
A.10.2 SM 1222 8-point digital output specifications ... 1171
A.10.3 SM 1222 16-point digital output specifications ... 1172
A.10.4 SM 1223 digital input/output V DC specifications ... 1177
A.10.5 SM 1223 digital input/output V AC specifications ... 1184

A.11 Analog signal modules (SMs) ... 1186
A.11.1 SM 1231 analog input module specifications ... 1186
A.11.2 SM 1232 analog output module specifications ... 1190
A.11.3 SM 1234 analog input/output module specifications ... 1192
A.11.4 Step response of the analog inputs ... 1195
A.11.5 Sample time and update times for the analog inputs ... 1195
A.11.6 Measurement ranges of the analog inputs for voltage and current (SB and SM) ... 1195
A.11.7 Measurement ranges of the analog outputs for voltage and current (SB and SM) ... 1196

A.12 Thermocouple and RTD signal modules (SMs) ... 1197
A.12.1 SM 1231 Thermocouple ... 1197
A.12.1.1 Basic operation for a thermocouple ... 1200
A.12.1.2 Selection tables for the SM 1231 thermocouple ... 1201
A.12.2 SM 1231 RTD ... 1203
A.12.2.1 Selection tables for the SM 1231 RTD ... 1206

A.13 Technology modules ... 1209
A.13.1 SM 1278 4xIO-Link Master SM ... 1209

A.13.1.1 SM 1278 4xIO-Link Master overview ... 1212
A.13.1.2 Connecting ... 1214
A.13.1.3 Parameters/address space ... 1217
A.13.1.3.1 Parameter data record ... 1217
A.13.1.4 Interrupt, error, and system alarms ... 1219

A.14 Digital signal boards (SBs) ... 1222
A.14.1 SB 1221 200 kHz digital input specifications ... 1222
A.14.2 SB 1222 200 kHz digital output specifications ... 1224
A.14.3 SB 1223 200 kHz digital input / output specifications ... 1226
A.14.4 SB 1223 2 X 24 V DC input / 2 X 24 V DC output specifications ... 1230

A.15 Analog signal boards (SBs) ... 1232
A.15.1 SB 1231 1 analog input specifications ... 1232
A.15.2 SB 1232 1 analog output specifications ... 1235
A.15.3 Measurement ranges for analog inputs and outputs ... 1236
A.15.3.1 Step response of the analog inputs ... 1236
A.15.3.2 Sample time and update times for the analog inputs ... 1237
A.15.3.3 Measurement ranges of the analog inputs for voltage and current (SB and SM) ... 1237
A.15.3.4 Measurement ranges of the analog outputs for voltage and current (SB and SM) ... 1238
A.15.4 Thermocouple signal boards (SBs) ... 1239
A.15.4.1 SB 1231 1 analog thermocouple input specifications ... 1239
A.15.4.2 Basic operation for a thermocouple ... 1240
A.15.5 RTD signal boards (SBs) ... 1244
A.15.5.1 SB 1231 1 analog RTD input specifications ... 1244
A.15.5.2 Selection tables for the SB 1231 RTD ... 1246

A.16 BB 1297 Battery board ... 1248

A.17 Communication interfaces ... 1250
A.17.1 PROFIBUS ... 1250
A.17.1.1 CM 1242-5 PROFIBUS DP SLAVE ... 1250
A.17.1.2 Pinout of the D-sub socket of the CM 1242-5 ... 1251
A.17.1.3 CM 1243-5 PROFIBUS DP Master ... 1251
A.17.1.4 Pinout of the D-sub socket of the CM 1243-5 ... 1253
A.17.2 CP 1243-7 LTE ... 1253
A.17.3 CM 1243-2 AS-i master ... 1257
A.17.3.1 Technical data for the AS-i master CM 1243-2 ... 1257
A.17.3.2 Electrical connections of the AS-i master ... 1258
A.17.4 RS232, RS422, and RS485 ... 1259
A.17.4.1 CB 1241 RS485 specifications ... 1259
A.17.4.2 CM 1241 RS232 specifications ... 1261
A.17.4.3 CM 1241 RS422/485 specifications ... 1262

A.18 SIMATIC memory cards ... 1263

A.19 Input simulators ... 1264

A.20 S7-1200 Potentiometer module ... 1265

A.21 I/O expansion cable ... 1266

A.22 Companion products ... 1267
A.22.1 PM 1207 power module ... 1267

A.22.2 CSM 1277 compact switch module 1267
A.22.3 CM CANopen module 1267
A.22.4 RF120C communications module 1268
A.22.5 SM 1238 Energy meter module 1268
A.22.6 SIWAREX electronic weighing systems 1269

B Calculating a power budget 1270

C Ordering Information 1274

C.1 CPU modules 1274
C.2 Signal modules (SMs), signal boards (SBs), and battery boards (BBs) 1274
C.3 Communication 1276
C.4 Fail-safe CPUs and signal modules 1276
C.5 Other modules 1277
C.6 Memory cards 1277
C.7 Spare parts and other hardware 1277
C.8 Programming software 1283
C.9 OPC UA Licenses 1283

D Device exchange and spare parts compatibility 1284

D.1 Replacing a CPU that has protection of confidential configuration data 1284
D.2 Exchanging a V3.0 CPU for a V4.x CPU 1285
D.3 S7-1200 V3.0 and earlier terminal block spare kits 1290

Index 1292

Introduction 1

1.1 General information

Purpose of the documentation

The S7-1200 programmable logic controllers (PLCs) can control a variety of automation applications. Compact design, affordable price, and a powerful instruction set make the S7-1200 CPU and modules a perfect solution for controlling a wide variety of applications. Together with the STEP 7 configuration and programming tool (Page 38), you have the flexibility you need to design your automation solutions.

This documentation provides information about the S7-1200 CPU and modules. It contains information for engineers, programmers, installers, and electricians.

Required basic knowledge

To understand this documentationl, you need a general knowledge of automation and programmable logic controllers.

Validity of the documentation

This documentation applies to the S7-1200 CPU family and modules.

Refer to the technical specifications (Page 1090) for each CPU and module in the S7-1200 family.

Conventions

STEP 7: In this documentation, "STEP 7" is used as a synonym for all versions of the configuration and programming software "STEP 7 (TIA Portal)".

Also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product, or on the section of the documentation to which particular attention should be paid.

ID link for the digital nameplate

The ID link is a globally unique identifier according to IEC 61406-1, which you will find as a QR code on your product.

The figure shows an example of an ID link for the CPU 1211C AC/DC/RLY.

You can recognize the ID link by the frame with a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product.

Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Access the ID link.

In the digital nameplate, you can find product data, manuals, declarations of conformity, certificates and other helpful information about your product.

Industry Mall

The Industry Mall is the catalog and order system of Siemens AG for automation and drive solutions on the basis of Totally Integrated Automation (TIA) and Totally Integrated Power (TIP).

You can find catalogs for all automation and drive products on the Internet (https://mall.industry.siemens.com).

Certifications and approvals

Refer to the technical specifications (Page 1090) for details on certifications and approvals.

Glossary

The definitions in the glossary provide an easy first reference for understanding the terms in this documentation.

1.2 Maintaining operational safety of your plant

NOTE

Operators of plants with safety-related features must meet operational safety requirements. Suppliers must also take measures when monitoring products.

To stay up-to-date on the latest operational safety requirements, visit the Siemens Industry Online Support (http://support.industry.siemens.com) site and subscribe to email notifications:

1. Follow one of the links below:
   - SIMATIC S7-1200/SIMATIC S7-1200F (https://support.industry.siemens.com/cs/ww/en/ps/13683)
   - Distributed I/O (https://support.industry.siemens.com/cs/ww/en/ps/14029)
   - STEP 7 TIA Portal (https://support.industry.siemens.com/cs/ww/en/ps/14667)
2. To subscribe to notifications, select "email on update".

NOTE

To reduce the risks associated with malicious or counterfeit CPUs and modules, use only official sales channels, such as the following:

- Siemens Industry Mall
- Official Siemens distributors
- Country-specific official Siemens sales and distribution channels

NOTE

To reduce the risks associated with compromised CPU or module firmware, only download firmware from the Siemens Industry Online Support website and verify the file integrity against the associated published SHA checksum.

NOTE

To reduce the risk of physical tampering with critical industrial equipment, implement the measures defined in the Operational guidelines (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity/downloads.html).

1.3 S7-1200 documentation guide

The S7-1200 and the TIA Portal provide a variety of documentation and other resources for finding the technical information that you require.

- The S7-1200 Programmable Logic Controller System Manual provides specific information about the operation, programming, and the specifications for the complete S7-1200 product family.
  The system manual is available on Siemens Industry Online Support (https://support.industry.siemens.com/) in multiple display formats and languages.
- The TIA Portal Information System provides access to the conceptual information and specific instructions that describe the operation and functionality of the programming package and basic operation of SIMATIC CPUs.
- You can also follow or join product discussions on the Service & Support technical forum (https://support.industry.siemens.com/tf/ww/en/?Language=en&siteid=csius&treeLang=en&groupid=4000002&extranet=standard&viewreg=WW&nodeid0=34612486). These forums allow you to interact with various product experts.
  - Forum for S7-1200 (https://support.industry.siemens.com/tf/ww/en/threads/237?title=simatic-s7-1200&skip=0&take=10&orderBy=LastPostDate+desc)
  - Forum for TIA Portal (https://support.industry.siemens.com/tf/ww/en/threads/243?title=step-7-tia-portal&skip=0&take=10&orderBy=LastPostDate+desc)
- The SIMATIC Industrial Software SIMATIC Safety - Configuring and Programming Manual (http://support.automation.siemens.com/WW/view/en/54110126/0/en) provides information about configuring and programming fail-safe PLCs.

Contact your Siemens distributor or sales office for assistance in answering any technical questions, for training, or for ordering S7 products. Because sales representatives are technically trained and have knowledge about your operations, process and industry, as well as about the Siemens products that you are using, they can provide efficient answers to problems you might encounter.

System manual updates

When needed, changes and supplements to released system manuals are available in a system manual update document. These updates take precedence over the system manual. You can find the latest system manual updates on Siemens Industry Online Support (https://support.industry.siemens.com/)

1.4 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International
(https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.
For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)
     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:
     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.
You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

1.5 Tool support

Tools

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.
You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/us/en/view/109767888)

SIMATIC Automation Tool

You can use the SIMATIC Automation Tool to perform commissioning and maintenance activities on various SIMATIC S7 stations as bulk operations independent of TIA Portal.
The SIMATIC Automation Tool offers a wide range of functions:

- Scanning of a PROFINET/Ethernet system network and identification of all connected CPUs
- Assignment of addresses (IP, subnet, Gateway) and device name (PROFINET device) to a CPU
- Transfer of the date and the programming device/PC time converted to UTC time to the module
- Program download to CPU
- RUN/STOP mode switchover
- CPU localization through LED flashing
- Reading out of CPU error information
- Reading the CPU diagnostic buffer
- Reset to factory settings
- Firmware update of the CPU and connected modules

You can find the SIMATIC Automation Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/98161300)

PRONETA

SIEMENS PRONETA (PROFINET network analysis) is a commissioning and diagnostic tool for PROFINET networks. PRONETA Basic has two core functions:

- In the network analysis, you get an overview of the PROFINET topology. Compare a real configuration with a reference installation or make simple parameter changes, e.g. to the names and IP addresses of the devices.
- The "IO test" is a simple and rapid test of the wiring and the module configuration of a plant, including documentation of the test results.

You can find SIEMENS PRONETA Basic on the Internet:
(https://support.industry.siemens.com/cs/ww/en/view/67460624)

SIEMENS PRONETA Professional is a licensed product that offers you additional functions. It offers you simple asset management in PROFINET networks and supports operators of automation systems in automatic data collection/acquisition of the components used through various functions:

- The user interface (API) offers an access point to the automation cell to automate the scan functions using MQTT or a command line.
- With PROFIenergy diagnostics, you can quickly detect the current pause mode or the readiness for operation of devices that support PROFIenergy and change these as needed.
- The data record wizard supports PROFINET developers in reading and writing acyclic PROFINET data records quickly and easily without PLC and engineering.

You can find SIEMENS PRONETA Professional on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109781283)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of

your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

1.6 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

Product overview 2

2.1 Introducing the S7-1200 PLC

The S7-1200 controller provides the flexibility and power to control a wide variety of devices in support of your automation needs. The compact structure, flexible configuration, and powerful instruction set combine to make the S7-1200 CPUs and modules ideal for controlling a wide variety of applications.

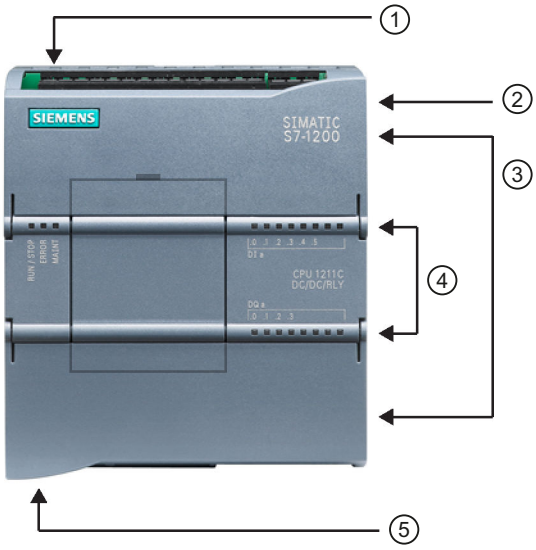
The CPU combines the following elements and more in a compact housing to create a powerful controller:

- A microprocessor
- An integrated power supply
- Input and output circuits
- Built-in PROFINET
- High-speed counters
- Basic Motion Control

After you download your program, the CPU contains the logic required to monitor and control the devices in your application. The CPU monitors the inputs and changes the outputs according to the logic of your user program, which can include Boolean logic, counting, timing, complex math operations, motion control, and communications with other intelligent devices.

The CPUs provide PROFINET ports for communication over a PROFINET network. Additional modules are available for communicating over networks and protocols such as the following:

- PROFIBUS
- Mobile communication (LTE and UMTS)
- Ethernet
  - Security
  - Firewall
  - VPN
  - IEC 60870
  - DNP3
- RS422/485
- RS232
- USS
- MODBUS



① Power connector
② Memory card slot under top door
③ Removable user wiring connectors (behind the doors)
④ Status LEDs for the on-board I/O
⑤ One or two PROFINET connectors (on the bottom of the CPU)

The following security features help protect access to both the CPU and the control program:

- User management access control (UMAC) (Page 147) to restrict PLC access to specific users
- Password protection (Page 151) that allows you to configure access levels for the CPU functions
- "know-how protection" (Page 159) to hide the code within a specific block
- Copy protection (Page 160) to bind your program to a specific memory card or CPU
- Protection of confidential PLC configuration data (Page 145) that allows the use of passwords to protect data such as private keys
- Secure PG/PC and HMI communication (Page 155) to ensure the integrity and confidentiality of sensitive data

Table 2-1 Comparing the CPU models

Feature		CPU 1211C	CPU 1212C	CPU 1214C	CPU 1215C	CPU 1217C
Physical size (mm)		90 x 100 x 75		110 x 100 x 75	130 x 100 x 75	150 x 100 x 75
User memory	Work	75 Kbytes	100 Kbytes	150 Kbytes	200 Kbytes	250 Kbytes
	Load	1 Mbyte	2 Mbytes	4 Mbytes		
	Retentive	14 Kbytes				
Local onboard I/O	Digital	6 inputs/ 4 outputs	8 inputs/ 6 outputs	14 inputs/ 10 outputs		
	Analog	2 inputs			2 inputs/2 outputs	
Process image size	Inputs (I)	1024 bytes				

[1] The slower speed is applicable when the HSC is configured for quadrature mode of operation.

[2] For CPU models with relay outputs, you must install a digital signal (SB) to use the pulse outputs.

[3] Up to 200 kHz are available with the SB 1221 DI x 24 V DC 200 kHz and SB 1221 DI 4 x 5 V DC 200 kHz.

Feature		CPU 1211C	CPU 1212C	CPU 1214C	CPU 1215C	CPU 1217C
Process image size	Outputs (Q)	1024 bytes				
Bit memory (M)		4096 bytes		8192 bytes		
Signal module (SM) expansion		None	2	8		
Signal board (SB), Battery board (BB), or communication board (CB)		1				
Communication module (CM) (left-side expansion)		3				
High-speed counters	Total	Up to 6 configured to use any built-in or SB inputs				
	1 MHz	-				Ib.2 to Ib.5
	100/[1]80 kHz	Ia.0 to Ia.5				
	30/[1]20 kHz	--	Ia.6 to Ia.7	Ia.6 to Ib.5		Ia.6 to Ib.1
	200 kHz[3]					
Pulse outputs[2]	Total	Up to 4 configured to use any built-in or SB outputs				
	1 MHz	--				Qa.0 to Qa.3
	100 kHz	Qa.0 to Qa.3				Qa.4 to Qb.1
	20 kHz	--	Qa.4 to Qa.5	Qa.4 to Qb.1		--
Memory card		SIMATIC memory card (optional)				
Data logs	Number	Maximum 8 open at one time				
	Size	500 MB per data log or as limited by maximum available load memory				
Real time clock retention time		20 days, typ./12 day min. at 40 degrees C (maintenance-free Super Capacitor)				
PROFINET Ethernet communication port		1			2	
Real math execution speed		2.3 µs/instruction				
Boolean execution speed		0.08 µs/instruction				

1 The slower speed is applicable when the HSC is configured for quadrature mode of operation.

2 For CPU models with relay outputs, you must install a digital signal (SB) to use the pulse outputs.

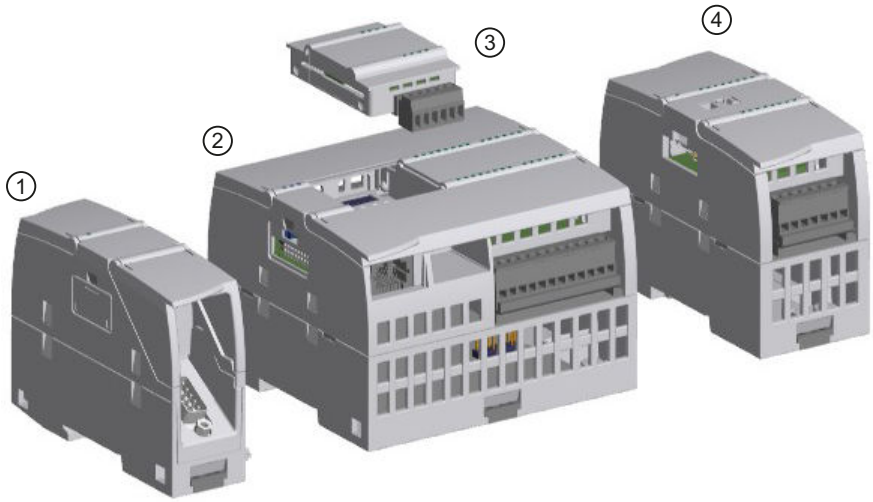
3 Up to 200 kHz are available with the SB 1221 DI x 24 V DC 200 kHz and SB 1221 DI 4 x 5 V DC 200 kHz.

The CPU and modules have a scannable ID Link. You can scan this lasered image with a smartphone to access information about the product.

The different CPU models provide a diversity of features and capabilities that help you create effective solutions for your varied applications. For detailed information about a specific CPU, see the technical specifications (Page 1090).

2.2 Expansion capability of the CPU

The S7-1200 family provides a variety of modules and plug-in boards for expanding the capabilities of the CPU with additional I/O or other communication protocols. For detailed information about a specific module, see the technical specifications (Page 1090).



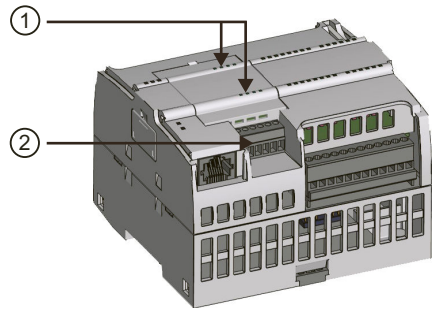
① Communication module (CM) or communication processor (CP) (Page 1250)

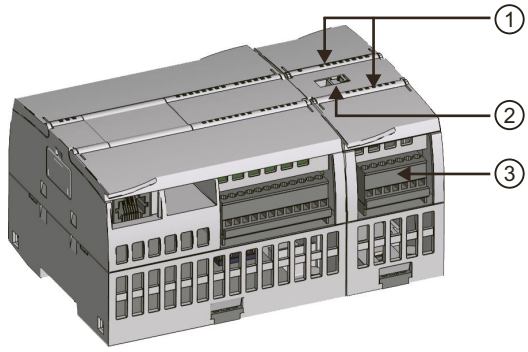
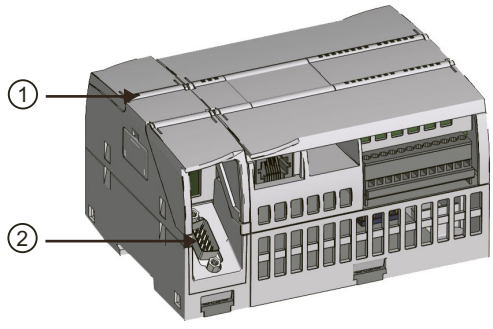
② CPU (CPU 1211C (Page 1105), CPU 1212C (Page 1116), CPU 1214C (Page 1127), CPU 1215C (Page 1139), CPU 1217C (Page 1153))

③ Signal board (SB) (digital SB (Page 1222), analog SB (Page 1232)), communication board (CB) (Page 1259), or Battery Board (BB) CPU (CPU 1211C, CPU 1212C, CPU 1214C, CPU 1215C, CPU 1217C) (Page 1248)

④ Signal module (SM) (digital SM (Page 1169), analog SM (Page 1186), thermocouple SM (Page 1197), RTD SM (Page 1203), technology SM) (Page 1209)

Table 2-2 S7-1200 expansion modules

Type of module	Description
The CPU supports one plug-in expansion board: • A signal board (SB) provides additional I/O for your CPU. The SB connects on the front of the CPU. • A communication board (CB) allows you to add another communication port to your CPU. • A battery board (BB) allows you to provide long term backup of the real-time clock.	
	① Status LEDs on the SB
	② Removable user wiring connector

Type of module	Description
Signal modules (SMs) add additional functionality to the CPU. SMs connect to the right side of the CPU. • Digital I/O • Analog I/O • RTD and thermocouple • SM 1278 IO-Link Master • SM 1238 Energy Meter (https://support.industry.siemens.com/cs/ww/en/view/109483435)	
	① Status LEDs
	② Bus connector slide tab
	③ Removable user wiring connector
Communication modules (CMs) and communications processors (CPs) add communication options to the CPU, such as for PROFIBUS or RS232/RS485 connectivity (for PtP, Modbus or USS), or the AS-i master. A CP provides capabilities for other types of communication, such as connecting to the CPU over a LTE, IEC, DNP3, or WDC network. • The CPU supports up to three CMs or CPs • Each CM or CP connects to the left side of the CPU (or to the left side of another CM or CP)	
	① Status LEDs
	② Communication connector

2.3 HMI panels

The SIMATIC HMI panels provide touch-screen devices for basic operator control and monitoring tasks. All panels have a protection rating for IP65 and have CE, UL, cULus, and NEMA 4x certification. You add an HMI device to your project the same way that you insert a CPU (Page 122).

Contact your distributor to order HMI panels.

New features

3

The following features are new in the V4.7 release:

- User management access control (UMAC) (Page 147)
- System logging (Syslog) (Page 156)
- Ability to set names of SNMP (Page 686) read and read/write Community strings
- Disabling of SNMP (Page 686) by default

STEP 7 programming software

4

The Totally Integrated Automation Portal (TIA Portal) is an engineering framework for implementing automation solutions. The TIA Portal includes STEP 7 for PLC programming and configuration. You use STEP 7 to configure CPUs and modules (Page 128) and for programming your application logic (Page 179).
TIA Portal provides an extensive information system.

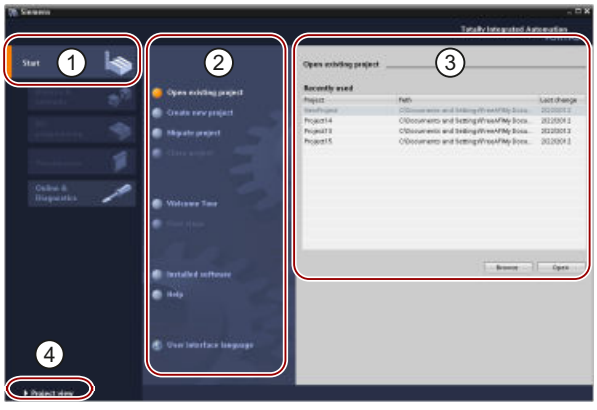
4.1 Different views to make the work easier

The TIA Portal provides two different views of the project that you use for your control application:

- Portal view: A task-oriented set of portals that are organized on the functionality of the tools
- Project view: A project-oriented view of the elements within the project

Choose which view helps you work most efficiently. With a single click, you can toggle between the Portal view and the Project view.

Portal view



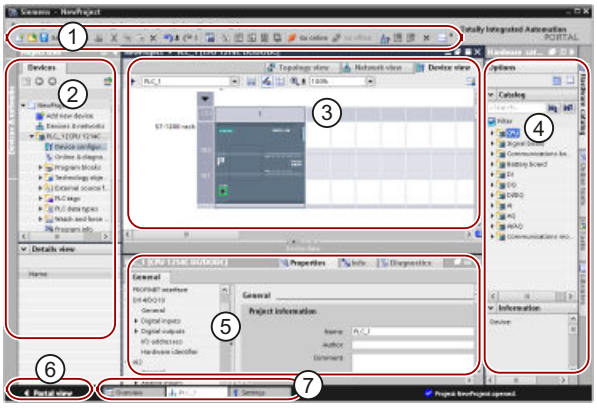
① Portals for the different tasks

② Tasks for the selected portal

③ Selection panel for the selected action

④ Changes to the Project view

Project view



① Menus and toolbar
② Project tree navigator
③ Work area
④ Task cards
⑤ Inspector window
⑥ Selector to change to the Portal view
⑦ Editor bar

With these components in one place, you have easy access to every aspect of your project. The work area consists of three tabbed views:

- Device view: Displays the device that you have added or selected and its associated modules
- Network view: Displays the CPUs and network connections in your network
- Topology view: Displays the PROFINET topology of the network including devices, passive components, ports, interconnections, and port diagnostics

Each view also enables you to perform configuration tasks. The inspector window shows the properties and information for the object that you have selected in the work area. As you select different objects, the inspector window displays the properties that you can configure. The inspector window includes tabs that allow you to see diagnostic information and other messages.

By showing all of the editors that are open, the editor bar helps you work more quickly and efficiently. To toggle between the open editors, simply click one of the open editors. You can also arrange two editors to appear together, arranged either vertically or horizontally. This feature allows you to drag and drop between editors.

4.2 Compatibility between STEP 7 and the S7-1200

STEP 7 supports configuration and programming of the S7-1200 CPU.

You can download projects for earlier versions of S7-1200 V4.x CPUs from STEP 7 to an S7-1200 V4.x CPU. Your configuration and program will be limited to the set of features and instructions that the previous version of the S7-1200 CPU and your version of STEP 7 supported.

This backwards compatibility makes it possible for you to run programs on S7-1200 V4.x CPU models that you previously designed and programmed for older versions.

You cannot download projects for S7-1200 CPU firmware versions V3.0 and earlier to an S7-1200 V4.x CPU without upgrading your project.

WARNING

Risks with editing and executing program logic from older versions of STEP 7

You cannot upgrade a project that is STEP 7 V13 or older to the current version by copying program logic.

You must upgrade your STEP 7 project as defined in Exchanging a V3.0 CPU for a V4.x CPU (Page 1285).

Executing STEP 7 program logic that you copied from an older version to a newer version can cause unpredictable program behavior and can result in death or severe personal injury.

NOTE

Projects with S7-1200 V1.x CPU versions

You cannot open a STEP 7 project that contains S7-1200 V1.x CPUs in STEP 7 V14.0 or later. To use your existing project, you must use STEP 7 V13 (with any update) to open your project and convert the S7-1200 V1.x CPUs to V2.0 or later. You can then use STEP 7 V14.0 or later to open the saved project with the converted CPUs.

Compatibility regarding secure communication

Refer to the following topics for information about STEP 7 and secure communication:

- Using the security wizard to set PLC security settings (Page 144)
- Enabling secure PG/PC and HMI communication and creating certificates (Page 155)

Installation 5

5.1 Guidelines for installing S7-1200 devices

The S7-1200 equipment is designed to be easy to install. You can install an S7-1200 either on a panel or on a standard rail, and you can orient the S7-1200 either horizontally or vertically. The small size of the S7-1200 allows you to make efficient use of space.

Electrical equipment standards classify the SIMATIC S7-1200 system as open Equipment. You must install the S7-1200 in a housing, cabinet, or electric control room. You should limit entry to the housing, cabinet, or electric control room to authorized personnel.

The installation should provide a dry environment for the S7-1200. SELV/PELV circuits are considered to provide protection against electric shock in dry locations.

The installation should provide the appropriate mechanical strength, flammability protection, and stability protection that is approved for open equipment in your particular location category according to applicable electrical and building codes.

Conductive contamination due to dust, moisture, and airborne pollution can cause operational and electrical faults in the PLC.

If you locate the PLC in an area where conductive contamination may be present, the PLC must be protected by an enclosure with appropriate protection rating. IP54 is one rating that is generally used for electronic equipment enclosures in dirty environments and may be appropriate for your application.

⚠ WARNING

Risks associated with improper installation

Improper installation of the S7-1200 can result in electrical faults or unexpected operation of machinery.

All instructions for installation and maintenance of a proper operating environment must be followed to ensure the equipment operates safely.

Electrical faults or unexpected machine operation can result in death, severe personal injury, and/or property damage.

Separating the S7-1200 devices from heat, high voltage, and electrical noise

When configuring the layout of the S7-1200 devices in a panel, always do the following:

- Separate the devices that generate high voltage and high electrical noise from the low-voltage, logic-type devices such as the S7-1200.
- Place electronic-type devices in the cooler areas of the cabinet away from heat-generating devices to reduce exposure to high-temperatures and extend the operating life of the devices.
- Avoid placing low-voltage signal wires and communications cables in the same tray with AC power wiring and high-energy, rapidly-switched DC wiring when routing wiring for the devices.

Providing adequate clearance for cooling and wiring

S7-1200 devices are designed for natural convection cooling. For proper cooling, you must provide a clearance of at least 25 mm above and below the devices. Also, allow at least 25 mm of depth between the front of the modules and the inside of the enclosure.

⚠ CAUTION

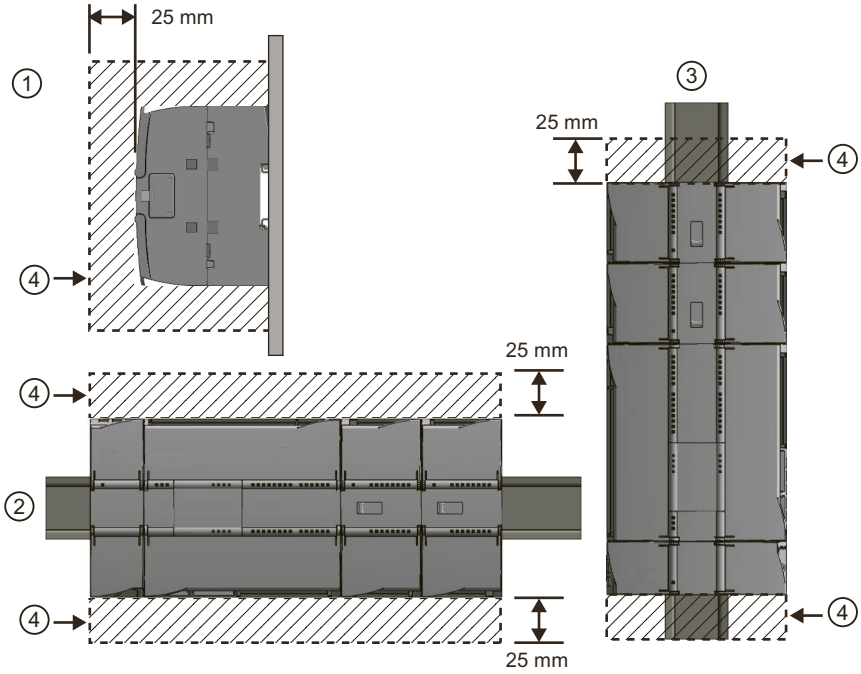
Effect of vertical mounting on allowable ambient temperature

Vertical mounting reduces the maximum allowable ambient temperature by 10 degrees C.

Orient a vertically mounted S7-1200 system as shown in the following figure. Ensure that the S7-1200 system is mounted correctly.

Improper installation of a vertically mounted system can result in personal injury.

When planning your layout for the S7-1200 system, allow enough clearance for the wiring and communications cable connections.



①	Side view	③	Vertical installation
②	Horizontal installation	④	Clearance area

5.2 Power budget

All S7-1200 CPUs have an internal power supply that provides power to the CPU, any expansion modules, and the 24 V DC Sensor power output.

Expansion modules include: signal modules, communication modules, signal boards, communication boards, and battery boards.

Refer to the technical specifications (Page 1090) for information about the 5 V DC logic budget supplied by your CPU and the 5 V DC power requirements of the various expansion modules. If you exceed the 5 V DC power budget, connecting the maximum number of

expansion modules to your CPU might not be possible. You must remove the expansion modules until the requirement is within the power budget.

NOTE

Exceeding the power budget can cause system failure.

Refer to "Calculating a power budget" (Page 1270) to determine how much power (or current) the CPU can provide for your configuration.

Each CPU has a 24 V DC sensor supply that can supply 24 V DC for local input points, for relay coils on the expansion modules, or for other requirements. If your 24 V DC power requirements exceed the budget of the sensor supply, you can add an external 24 V DC power supply to your system. You must manually connect the external 24 V DC supply to the input points or relay coils on the expansion modules. Refer to the technical specifications (Page 1090) for the 24 V DC sensor supply power budget for your particular CPU.

If you require an external 24 V DC power supply, ensure that the power supply is not connected in parallel with the sensor supply of the CPU. For improved electrical noise protection, it is recommended that the commons (M) of the different power supplies be connected.

WARNING

Risks with parallel connections

Connecting an external 24 V DC power supply in parallel with the 24 V DC sensor supply can result in a conflict between the two supplies as each seeks to establish its own preferred output voltage level. The result of this conflict can be shortened lifetime or immediate failure of one or both power supplies, with consequent unpredictable operation of the PLC system.

The DC sensor supply and any external power supply must provide power to different points.

Unpredictable operation can result in death, severe personal injury and/or property damage.

Some of the 24 V DC power input ports in the S7-1200 system are interconnected, with a common logic circuit connecting multiple M terminals. For example, the following circuits are interconnected when designated as "not isolated" in the data sheets: the 24 V DC power supply of the CPU, the power input for the relay coil of an SM, or the power supply for a non-isolated analog input. All non-isolated M terminals must connect to the same external reference potential.

WARNING

Risks with connecting non-isolated M terminals to different reference potentials

Connecting non-isolated M terminals to different reference potentials causes unpredictable current flows. Unpredictable current flows can cause PLC damage or abnormal PLC and equipment operation.

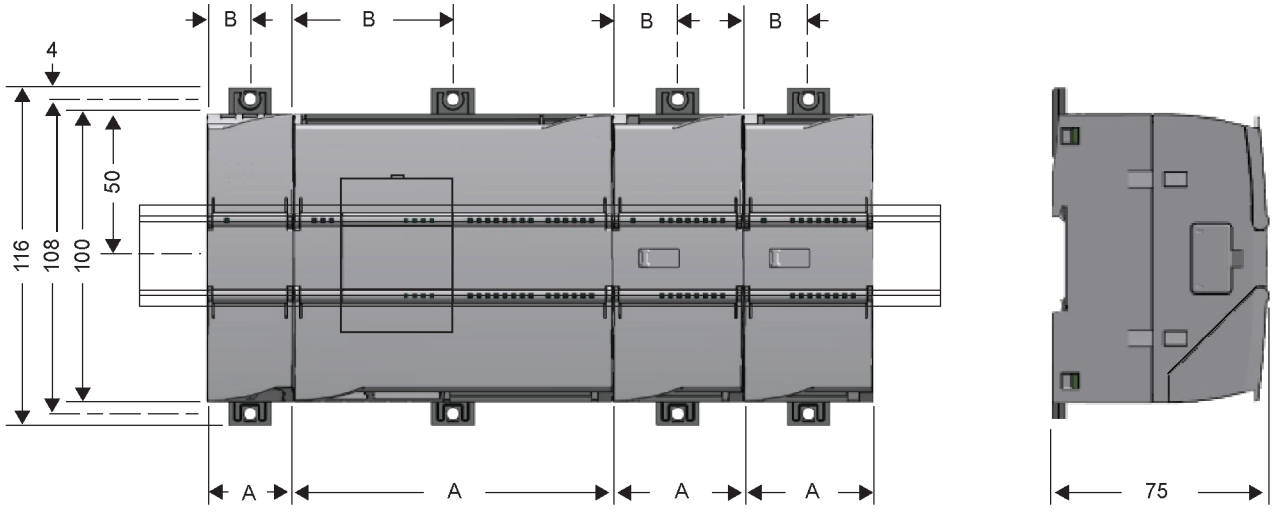
Always ensure that all non-isolated M terminals in an S7-1200 system are connected to the same reference potential.

PLC damage or abnormal PLC and equipment operation can result in death, severe personal injury, and/or property damage.

5.3 Installation and removal procedures

5.3.1 Mounting dimensions for the S7-1200 devices

CPU 1211C, CPU 1212C, CPU 1214C
(measurements in mm)



CPU 1215C, CPU 1217C
(measurements in mm)

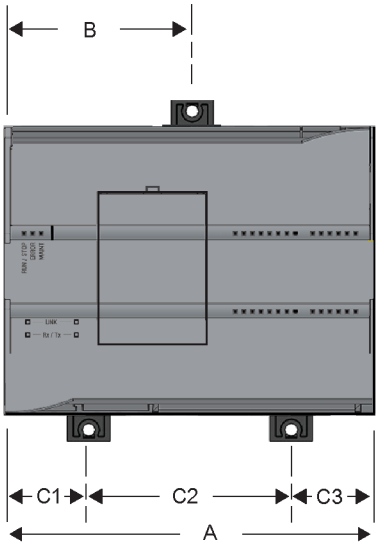


Table 5-1 Mounting dimensions (mm)

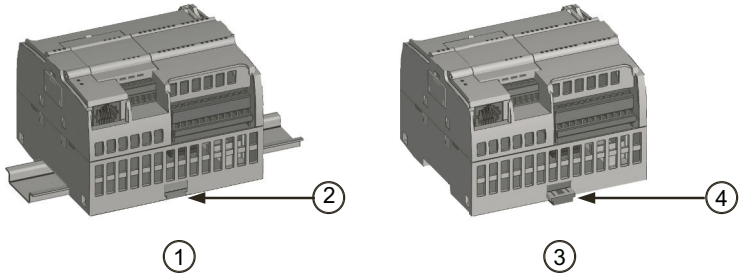
S7-1200 Devices		Width A (mm)	Width B (mm)	Width C (mm)
CPU	CPU 1211C and CPU 1212C	90	45	--
	CPU 1214C	110	55	--
	CPU 1215C	130	65 (top)	Bottom: C1: 32.5 C2: 65 C3: 32.5
	CPU 1217C	150	75	Bottom: C1: 37.5 C2: 75 C3: 37.5
Signal modules	Digital 8 and 16 point Analog 2, 4, and 8 point Thermocouple 4 and 8 point RTD 4 point SM 1278 IO Link-Master	45	22.5	--
	Digital DQ 8 x Relay (Changeover)	70	35	--
	Analog 16 point RTD 8 point	70	35	--
	SM 1238 Energy Meter module	45	22.5	--
Communication interfaces	CM 1241 RS232, and CM 1241 RS422/485 CM 1243-5 PROFIBUS master and CM 1242-5 PROFIBUS slave CM 1242-2 AS-i Master CP 1243-7 LTE-US CP 1243-7 LTE-EU CP 1243-1 CP 1243-8 IRC RF120C	30	15	--

Each CPU, SM, CM, and CP supports mounting on either a DIN rail or on a panel. Use the DIN rail clips on the module to secure the device on the rail. These clips also snap into an extended position to provide screw mounting positions to mount the unit directly on a panel. The interior dimension of the hole for the DIN clips on the device is 4.3 mm.

A 25 mm thermal zone must be provided above and below the unit for free air circulation.

Installing and removing the S7-1200 devices

The CPU can be easily installed on a standard DIN rail or on a panel. DIN rail clips are provided to secure the device on the DIN rail. The clips also snap into an extended position to provide a screw mounting position for panel-mounting the unit.



① DIN rail installation
② DIN rail clip in latched position
③ Panel installation
④ Clip in extended position for panel mounting

Before you install or remove any electrical device, ensure that the power to that equipment has been turned off. Also, ensure that the power to any related equipment has been turned off.

WARNING

Installation or removal of S7-1200 devices with power applied

Installation or removal of S7-1200 or related equipment with the power applied can cause electric shock or unexpected operation of equipment.

Always follow appropriate safety precautions and ensure that power to the S7-1200 is disabled before attempting to install or remove S7-1200 CPUs or related equipment.

Failure to disable all power to the S7-1200 and related equipment during installation or removal procedures can result in death, severe personal injury and/or property damage due to electric shock or unexpected equipment operation.

Always ensure that whenever you replace or install an S7-1200 device you use the correct module or equivalent device.

WARNING

Risks with incorrect installation of an S7-1200 module

Incorrect installation of an S7-1200 module can cause the program in the S7-1200 to function unpredictably.

Replace an S7-1200 device with the same model, and be sure to orient and position it correctly.

Failure to replace an S7-1200 device with the same model, orientation, or order can result in death, severe personal injury and/or property damage due to unexpected equipment operation.

WARNING

Risks when working in a flammable or combustible atmosphere

Disconnection of equipment when a flammable or combustible atmosphere is present can cause a fire or explosion.

Do not disconnect equipment when a flammable or combustible atmosphere is present. Always follow appropriate safety precautions when a flammable or combustible atmosphere is present.

A fire or explosion can result in death, serious injury and/or property damage.

NOTICE

Risks associated with electrostatic discharge

Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable.

To protect the memory card and receptacle from electrostatic discharge, do the following:

- Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card.
- Store the memory card in a conductive container.

Receptacle or memory card malfunction can result in property damage.

5.3.2 Installing and removing the CPU

You can install the CPU on a panel or on a DIN rail.

NOTE

Attach any communication modules to the CPU and install the assembly as a unit. Install signal modules separately after the CPU has been installed.

Consider the following when installing the units on the DIN rail or on a panel:

- For DIN rail mounting, make sure the upper DIN rail clip is in the latched (inner) position and that the lower DIN rail clip is in the extended position for the CPU and attached CMs.
- After installing the devices on the DIN rail, move the lower DIN rail clips to the latched position to lock the devices on the DIN rail.
- For panel mounting, make sure the DIN rail clips are pushed to the extended position.

To install the CPU on a panel, follow these steps:

1. Locate, drill, and tap the mounting holes (M4), using the dimensions shown in table, Mounting dimensions (mm) (Page 44).
2. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power.
3. Extend the mounting clips from the module. Make sure the DIN rail clips on the top and bottom of the CPU are in the extended position.

4. Secure the module to the panel, using a Pan Head M4 screw with spring and flat washer. Do not use a flat head screw.

NOTE

The type of screw will be determined by the material upon which it is mounted. You should apply appropriate torque until the spring washer becomes flat. Avoid applying excessive torque to the mounting screws. Do not use a flat head screw.

NOTE

Using DIN rail stops can be helpful if the CPU is in an environment with high vibration potential or if the CPU has been installed vertically. Use an end bracket (8WA1808 or 8WA1805) on the DIN rail to ensure that the modules remain connected.

Table 5-2 Installing the CPU on a DIN rail

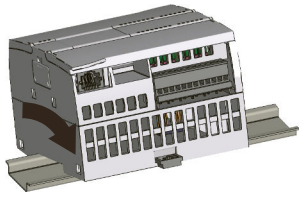
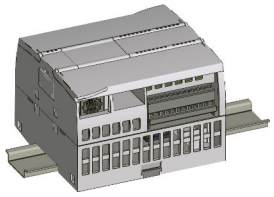
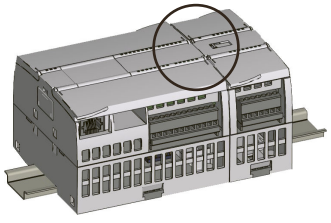
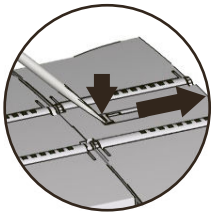
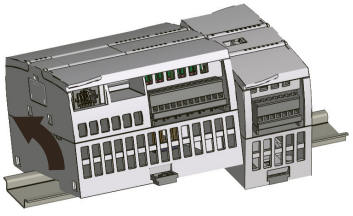
Task	Procedure
	1. Install the DIN rail. Secure the rail to the mounting panel every 75 mm. 2. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 3. Hook the CPU over the top of the DIN rail. 4. Pull out the DIN rail clip on the bottom of the CPU to allow the CPU to fit over the rail. 5. Rotate the CPU down into position on the rail. 6. Push in the clips to latch the CPU to the rail.
	

Table 5-3 Removing the CPU from a DIN rail

Task	Procedure
 	1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Disconnect the I/O connectors, wiring, and cables from the CPU (Page 52). 3. Remove the CPU and any attached communication modules as a unit. All signal modules should remain installed. 4. If an SM is connected to the CPU, retract the bus connector: – Place a screwdriver beside the tab on the top of the signal module. – Press down to disengage the connector from the CPU. – Slide the tab fully to the right. 5. Remove the CPU: – Pull out the DIN rail clip to release the CPU from the rail. – Rotate the CPU up and off the rail, and remove the CPU from the system.
	

5.3.3 Installing and removing an SB, CB, or BB

Table 5-4 Installing an SB, CB, or BB 1297

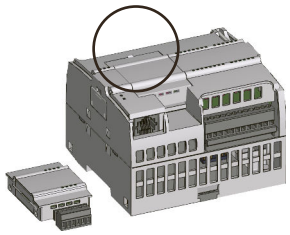
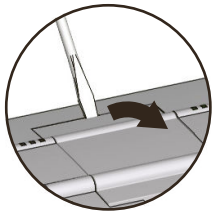
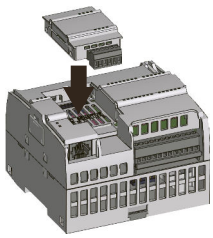
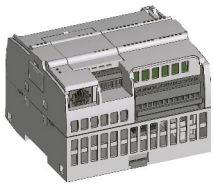
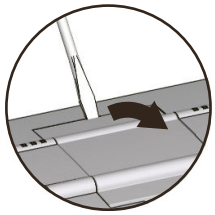
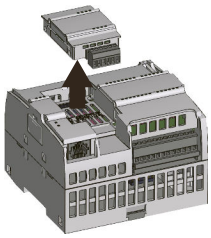
Task	Procedure
  	1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Remove the top and bottom terminal block covers from the CPU. 3. Place a screwdriver into the slot on top of the CPU at the rear of the cover. 4. Gently pry the cover straight up and remove it from the CPU. 5. Place the module straight down into its mounting position in the top of the CPU. 6. Firmly press the module into position until it snaps into place. 7. Replace the terminal block covers.

Table 5-5 Removing an SB, CB, or BB 1297

Task	Procedure
  	1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Remove the top and bottom terminal block covers from the CPU. 3. Remove the signal board connector (if installed) by gently disengaging with a screwdriver. 4. Place a screwdriver into the slot on top of the module. 5. Gently pry the module up to disengage it from the CPU. 6. Without using a screwdriver, remove the module straight up from its mounting position in the top of the CPU. 7. Replace the cover onto the CPU. 8. Replace the terminal block covers.

Installing or replacing the battery in the BB 1297 battery board

The BB 1297 requires battery type CR1025. The battery is not included with the BB 1297 and must be purchased. To install or replace the battery, follow these steps:

1. In the BB 1297, install a new battery with the positive side of the battery on top, and the negative side next to the printed wiring board.
2. The BB 1297 is ready to be installed in the CPU. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power and follow the installation directions above to install the BB 1297.

To replace the battery in the BB 1297:

1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. Remove the BB 1297 from the CPU following the removal directions above.
2. Carefully remove the old battery using a small screwdriver. Push the battery out from under the clip.
3. Install a new CR1025 replacement battery with the positive side of the battery on top and the negative side next to the printed wiring board.
4. Re-install the BB 1297 battery board following the installation directions above.

WARNING

Risks with installing or connecting unspecified batteries in the BB 1297

Installing an unspecified battery in the BB 1297, or otherwise connecting an unspecified battery to the circuit can result in fire or component damage and unpredictable operation of machinery.

Use only the specified CR1025 battery for backup of the Real-time clock.

Fire or unpredictable operation of machinery can result in death, severe personal injury, or property damage.

5.3.4 Installing and removing an SM

Table 5-6 Installing an SM

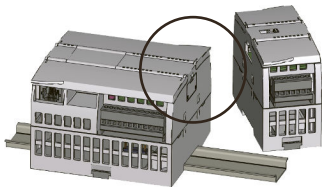
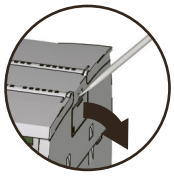
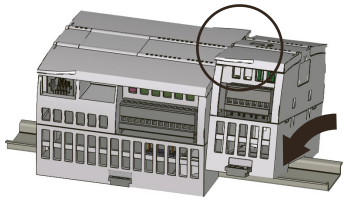
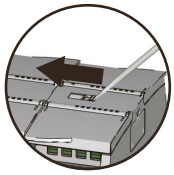
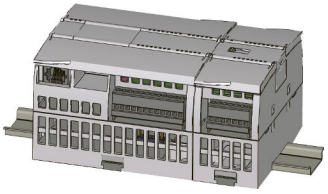
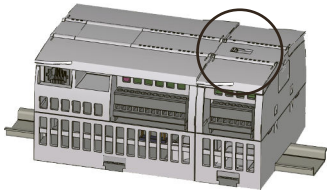
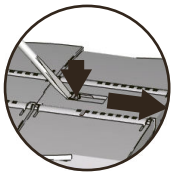
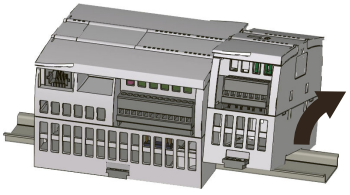
Task		Procedure
		Install your SM after installing the CPU. 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Remove the cover for the connector from the right side of the CPU: – Insert a screwdriver into the slot above the cover. – Gently pry the cover out at its top and remove the cover. 3. Retain the cover for reuse.
		Connect the SM to the CPU: 1. Position the SM beside the CPU. 2. Hook the SM over the top of the DIN rail. 3. Pull out the bottom DIN rail clip to allow the SM to fit over the rail. 4. Rotate the SM down into position beside the CPU and push the bottom clip in to latch the SM onto the rail.
		Extending the bus connector makes both mechanical and electrical connections for the SM. 1. Place a screwdriver beside the tab on the top of the SM. 2. Slide the tab fully to the left to extend the bus connector into the CPU. Follow the same procedure to install a signal module to a signal module.

Table 5-7 Removing an SM

Task	Procedure
	You can remove any SM without removing the CPU or other SMs in place. 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Remove the I/O connectors and wiring from the SM (Page 52). 3. Retract the bus connector. – Place a screwdriver beside the tab on the top of the SM. – Press down to disengage the connector from the CPU. – Slide the tab fully to the right. If there is another SM to the right, repeat this procedure for that SM.
	
	Remove the SM: 1. Pull out the bottom DIN rail clip to release the SM from the rail. 2. Rotate the SM up and off the rail. Remove the SM from the system. 3. If required, cover the bus connector on the CPU to avoid contamination. Follow the same procedure to remove a signal module from a signal module.

5.3.5 Installing and removing a CM or CP

Attach any communication modules to the CPU and install the assembly as a unit, as shown in Installing and removing the CPU (Page 47).

Table 5-8 Installing a CM or CP

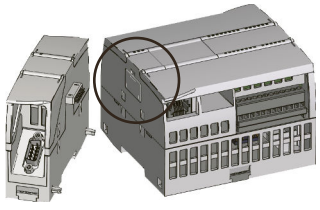
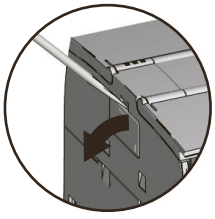
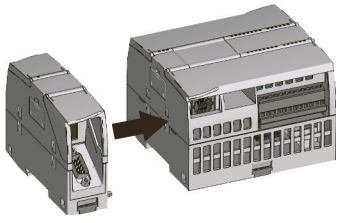
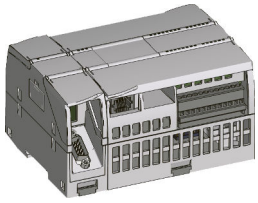
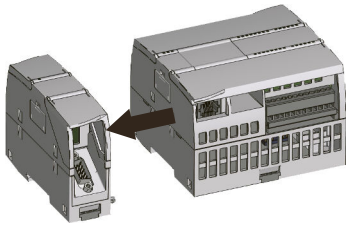
Task	Procedure
  	1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Attach the CM to the CPU before installing the assembly as a unit to the DIN rail or panel. 3. Remove the bus cover from the left side of the CPU: – Insert a screwdriver into the slot above the bus cover. – Gently pry out the cover at its top. 4. Remove the bus cover. Retain the cover for reuse. 5. Connect the CM or CP to the CPU: – Align the bus connector and the posts of the CM with the holes of the CPU – Firmly press the units together until the posts snap into place. 6. Install the CPU and CP on a DIN rail or panel.

Table 5-9 Removing a CM or CP

Task	Procedure
	Remove the CPU and CM as a unit from the DIN rail or panel. 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Remove the I/O connectors and all wiring and cables from the CPU and CMs. 3. For DIN rail mounting, move the lower DIN rail clips on the CPU and CMs to the extended position. 4. Remove the CPU and CMs from the DIN rail or panel. 5. Grasp the CPU and CMs firmly and pull apart.
	

NOTICE
Potential risks when separating modules Do not use a tool, like a screwdriver, to separate modules. Separating modules with a tool can damage the modules. Always follow the recommended procedure above when removing modules.

5.3.6 Removing and reinstalling the S7-1200 terminal block connector

The CPU, SB, and SM modules provide removable connectors to make connecting the wiring easy.

Table 5-10 Removing the connector

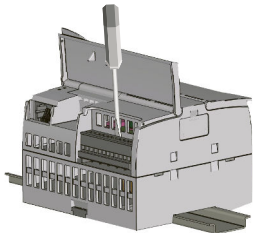
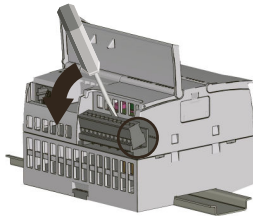
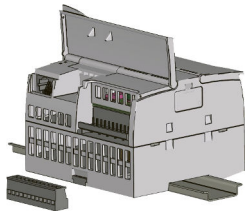
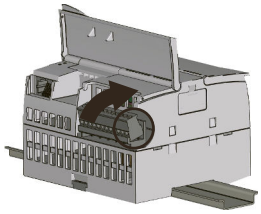
Task	Procedure
	Prepare the system for terminal block connector removal by removing the power from the CPU and opening the cover above the connector. 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Inspect the top of the connector and locate the slot for the tip of the screwdriver. 3. Insert a screwdriver into the slot. 4. Gently pry the top of the connector away from the CPU. The connector will release with a snap. 5. Grasp the connector and remove it from the CPU.
	

Table 5-11 Installing the connector

Task	Procedure
	Prepare the components for terminal block installation by removing power from the CPU and opening the cover for connector. 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Align the connector with the pins on the unit. 3. Align the wiring edge of the connector inside the rim of the connector base. 4. Press firmly down and rotate the connector until it snaps into place. Check carefully to ensure that the connector is properly aligned and fully engaged.
	

5.3.7 Installing and removing the expansion cable

The S7-1200 expansion cable provides additional flexibility in configuring the layout of your S7-1200 system. Only one expansion cable is allowed per CPU system. You install the expansion cable either between the CPU and the first SM, or between any two SMs.

Table 5-12 Installing and removing the male connector of the expansion cable

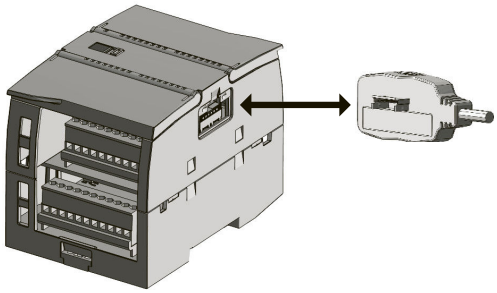
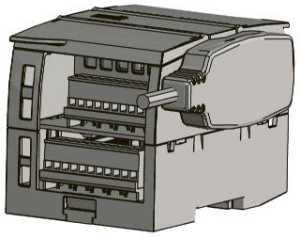
Task	Procedure
	To install the male connector: 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Push the connector into the bus connector on the right side of the signal module or CPU. To remove the male connector: 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Pull out the male connector to release it from the signal module or CPU.
	

Table 5-13 Installing the female connector of the expansion cable

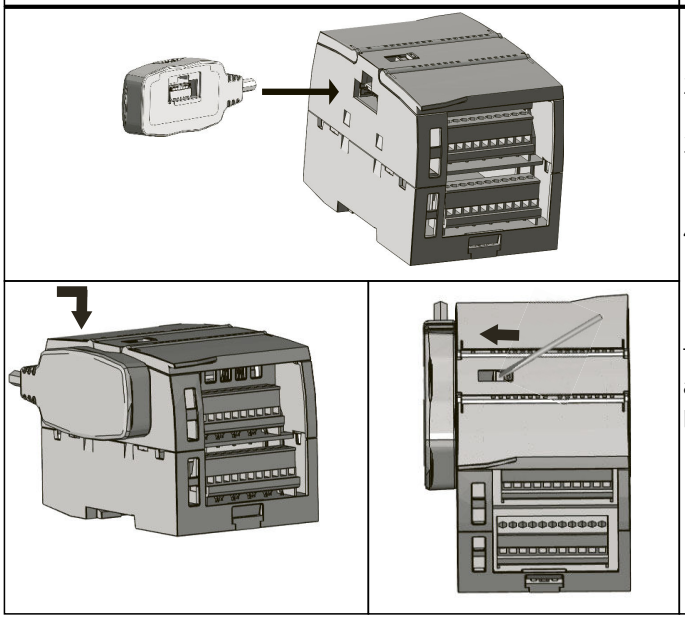
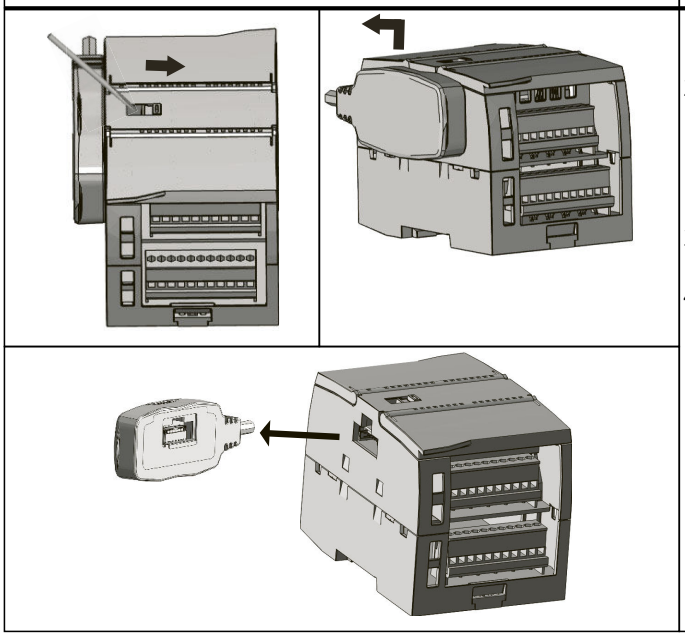
Task	Procedure
	1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Place the female connector to the bus connector on the left side of the signal module. 3. Slip the hook extension of the female connector into the housing at the bus connector and press down slightly to engage the hook. 4. Lock the connector into place: – Place a screwdriver beside the tab on the top of the signal module. – Slide the tab fully to the left. To engage the connector, you must slide the connector tab all the way to the left. The connector tab must be locked into place.

Table 5-14 Removing the female connector of the expansion cable

Task	Procedure
	1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Unlock the connector: – Place a screwdriver beside the tab on the top of the signal module. – Press down slightly and slide the tab fully to the right. 3. Lift the connector up slightly to disengage the hook extension. 4. Remove the female connector.

NOTE

Installing the expansion cable in a vibration environment

If the expansion cable is connected to modules that move, or are not firmly fixed, the cable male end snap-on connection can gradually become loose.

Use a cable tie to fix the male end cable on the DIN-rail (or other place) to provide extra strain relief.

Avoid using excessive force when you pull the cable during installation. Ensure the cable-module connection is in the correct position once installation is complete.

5.4 Wiring guidelines

Proper grounding and wiring of all electrical equipment is important to help ensure the optimum operation of your system and to provide additional electrical noise protection for your application and the S7-1200. Refer to the technical specifications (Page 1090) for the S7-1200 wiring diagrams.

Prerequisites

Before you ground or install wiring to any electrical device, ensure that the power to that equipment has been turned off. Also, ensure that the power to any related equipment has been turned off.

Ensure that you follow all applicable electrical codes when wiring the S7-1200 and related equipment. Install and operate all equipment according to all applicable national and local standards. Contact your local authorities to determine which codes and standards apply to your specific case.

⚠ WARNING

Risk of electrocution during installation and removal

Installing or wiring the S7-1200 or related equipment with power applied could cause electric shock or unexpected operation of equipment.

Always follow appropriate safety precautions and ensure that power is disabled to the S7-1200 or related equipment before attempting to install or remove any devices.

Failure to disable all power to the S7-1200 G2 and related equipment during installation or removal procedures could result in death, severe personal injury, and/or property damage due to electric shock or unexpected equipment operation.

Always take safety into consideration as you design the grounding and wiring of your S7-1200 system. Electronic control devices, such as the S7-1200, can fail and can cause unexpected operation of the equipment that is being controlled or monitored. For this reason, you should implement safeguards that are independent of the S7-1200 to protect against possible personal injury or equipment damage.

WARNING

Risk of unexpected equipment operation

Control devices can fail in unsafe conditions, resulting in unexpected equipment operation.

Use an emergency stop function, electromechanical overrides, or other redundant safeguards that are independent of the S7-1200.

Unexpected operation can result in death, severe personal injury and/or property damage.

Guidelines for isolation

S7-1200 AC power supply boundaries and I/O boundaries to AC circuits have been designed and approved to provide safe separation between AC line voltages and low voltage circuits. These boundaries include double or reinforced insulation, or basic plus supplementary insulation, according to various standards. Components which cross these boundaries such as optical couplers, capacitors, transformers, and relays have been approved as providing safe separation. Only circuits rated for AC line voltage include safety isolation to other circuits. Isolation boundaries between 24 V DC circuits are functional only, and you should not depend on these boundaries for safety.

The sensor supply output, communications circuits, and internal logic circuits of an S7-1200 with included AC power supply are sourced as SELV (safety extra-low voltage) according to EN 61131-2.

To ensure safe operation, you must power the external connections to the following items from approved sources that meet the requirements of SELV/PELV, Class 2, Limited Voltage, or Limited Power according to various standards:

- Communications ports
- Analog circuits
- 24 V DC nominal power supply
- Digital I/O circuits

WARNING

Risk of electrocution with use of non-isolated or single insulation supplies

Using non-isolated or single insulation supplies can cause circuits that are normally safe to the touch, like communications circuits and low voltage sensor wiring, to carry hazardous levels of voltage.

Do not use non-isolated or single insulation supplies to supply low voltage circuits from an AC line.

Only use high voltage to low voltage power converters that are approved as sources of touch safe, limited voltage circuits.

This can cause unexpected electric shock resulting in death, severe personal injury, and/or property damage.

The best way to ground your application is to ensure that all the common and ground connections of your S7-1200 and related equipment are grounded to a single point. This single point should be connected directly to the earth ground for your system. When using shielded cables, always connect the cable shields to the ground at both ends to reduce low and high frequency interference.

Use the shortest ground wire possible; use a large wire size, such as 2 mm^2 (14 AWG).

When locating grounds, consider safety-grounding requirements and the proper operation of protective interrupting devices.

Guidelines for wiring the S7-1200

When designing the wiring for your S7-1200, provide a single disconnect switch that simultaneously removes power from the S7-1200 CPU power supply, from all input circuits, and from all output circuits. Provide over-current protection, such as a fuse or circuit breaker, to limit fault currents on supply wiring. Consider providing additional protection by placing a fuse or other current limit in each output circuit.

Install appropriate surge suppression devices for any wiring that could be subject to lightning surges. For more information, see Surge immunity (Page 1090) in the General technical specifications section.

Avoid placing low-voltage signal wires and communications cables in the same wire tray with AC wires and high-energy, rapidly switched DC wires. Always route wires in pairs, with the neutral or common wire paired with the hot or signal-carrying wire.

Use the shortest wire possible and ensure that the wire is sized properly to carry the required current.

Wire and cable should have a temperature rating 30 °C higher than the ambient temperature around the S7-1200 (for example, a minimum of 85 °C-rated conductors for 55 °C ambient temperature). You should determine other wiring type and material requirements from the specific electrical circuit ratings and your installation environment.

Use shielded wires for optimum protection against electrical noise. Connect the shield to the ground at both ends of the cable. You should ground communication cable shields to S7-1200 communication connector shells using connectors that engage the cable shield, or by bonding the communication cable shields to a separate ground. You should ground other cable shields using clamps or copper tape around the shield to provide a high surface area connection to the grounding point.

When wiring input circuits that are powered by an external power supply, include an overcurrent protection device in that circuit. External protection is not necessary for circuits that are powered by the 24 V DC sensor supply from the S7-1200 because the sensor supply is already current-limited.

All S7-1200 modules have removable connectors for user wiring. To prevent loose connections, ensure that the connector is seated securely and that the wire is installed securely into the connector.

To help prevent unwanted current flows in your installation, the S7-1200 provides isolation boundaries at certain points. When you plan the wiring for your system, you should consider these isolation boundaries. Refer to the technical specifications (Page 1153) for the amount of isolation provided and the location of the isolation boundaries. Circuits rated for AC line voltage include safety isolation to other circuits. Isolation boundaries between 24 V DC circuits are functional only, and you should not depend on these boundaries for safety.

A summary of Wiring rules for the S7-1200 CPUs, SMs and SBs is shown below:

Table 5-15 Wiring rules for S7-1200 CPUs, SMs, and SBs

Wiring rules for...	**CPU and SM connector**		**SB connector**
Connection technology	**Push In**	**Screw**	**Screw**
Connectible conductor cross-sections for standard wires	2 mm^2 to 0.3 mm^2 (14 AWG to 22 AWG)		1.3 mm^2 to 0.3 mm^2 (16 AWG to 22 AWG)
Number of wires per connection	1 or combination of 2 wires in a double sleeve up to 2 mm^2 (total)		1 or combination of 2 wires up to 1.3 mm^2 (total)
Wire strip length	Using sleeves for secure electric connection	6.4 mm	6.3 to 7 mm
Tightening torque (maximum)	n/a	0.56 N-m (5 inch-pounds)	0.33 N-m (3 inch-pounds)
Tool	2.5 to 3.0 mm flathead screwdriver		

To avoid damaging the connector, do not overtighten the screws or you can use the Push in terminal block offered as an accessory.

NOTE

Ferrules or end sleeves on stranded conductors reduce the risk of stray strands causing short circuits. Ferrules longer than the recommended strip length should include an insulating collar to prevent shorts due to side movement of conductors. Cross-sectional area limits for bare conductors also apply to ferrules.

Guidelines for lamp loads

Lamp loads, including LED lamp loads, are damaging to relay contacts because of the high turn-on surge current. This surge current will nominally be 10 to 15 times the steady state current for a Tungsten lamp. A replaceable interposing relay or surge limiter is recommended for lamp loads that will be switched a large number of times during the lifetime of the application.

Guidelines for inductive loads

Use suppressor circuits with inductive loads to limit the voltage rise when a control output turns off. Suppressor circuits protect your outputs from premature failure caused by the high voltage transient that occurs when current flow through an inductive load is interrupted.

In addition, suppressor circuits limit the electrical noise generated when switching inductive loads. High frequency noise from poorly suppressed inductive loads can disrupt the operation of the PLC. Placing an external suppressor circuit so that it is electrically across the load and physically located near the load is the most effective way to reduce electrical noise.

S7-1200 DC outputs include internal suppressor circuits that are adequate for inductive loads in most applications. Since S7-1200 relay output contacts can be used to switch either a DC or an AC load, internal protection is not provided.

A good suppressor solution is to use contactors and other inductive loads for which the manufacturer provides suppressor circuits integrated in the load device, or as an optional accessory. However, some manufacturer provided suppressor circuits may be inadequate for your application. An additional suppressor circuit may be necessary for optimal noise reduction and contact life.

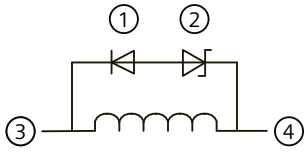
For AC loads, a metal oxide varistor (MOV) or other voltage clamping device may be used with a parallel RC circuit, but is not as effective when used alone. An MOV suppressor with no parallel RC circuit often results in significant high frequency noise up to the clamp voltage.

A well-controlled turn-off transient will have a ring frequency of no more than 10 kHz, with less than 1 kHz preferred. Peak voltage for AC lines should be within +/- 1200 V of ground. Negative peak voltage for DC loads using the PLC internal suppression will be ~40 V below the 24 V DC supply voltage. External suppression should limit the transient to within 36 V of the supply to unload the internal suppression.

NOTE

The effectiveness of a suppressor circuit depends on the application and must be verified for your particular usage. Ensure that all components are correctly rated and use an oscilloscope to observe the turn-off transient.

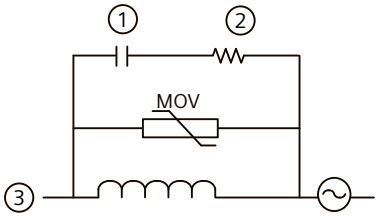
Typical suppressor circuit for DC or relay outputs that switch DC inductive loads



1. 1N4001 diode or equivalent
2. 8.2 V Zener (DC outputs), 36 V Zener (Relay outputs)
3. Output point
4. M, 24 V reference

In most applications, the addition of a diode (A) across a DC inductive load is suitable, but if your application requires faster turn-off times, then the addition of a Zener diode (B) is recommended. Be sure to size your Zener diode properly for the amount of current in your output circuit.

Typical suppressor circuit for relay outputs that switch AC inductive loads



1. See table for C value
2. See table for R value
3. Output point

Ensure that the working voltage of the metal oxide varistor (MOV) is at least 20% greater than the nominal line voltage.

Choose pulse-rated, non-inductive resistors, and capacitors recommended for pulse applications (typically metal film). Verify the components meet average power, peak power, and peak voltage requirements.

If you design your own suppressor circuit, the following table suggests resistor and capacitor values for a range of AC loads. These values are based on calculations with ideal component parameters. I rms in the table refers to the steady-state current of the load when fully ON.

Table 5-16 AC suppressor circuit resistor and capacitor values

Inductive load			Suppressor values		
I rms	230 V AC	120 V AC	Resistor		Capacitor
Amps	VA	VA	Ω	W (power rating)	nF
0.02	4.6	2.4	15000	0.1	15
0.05	11.5	6	5600	0.25	47
0.1	23	12	2700	0.5	100
0.2	46	24	1500	1	150
0.5	115	60	560	2.5	470
1	230	120	270	5	1000
2	460	240	150	10	1500

[2] **Conditions satisfied by the table values:**
Maximum turn-off transition step < 500 V
Resistor peak voltage < 500 V
Capacitor peak voltage < 1250 V
Suppressor current < 8% of load current (50 Hz)
Suppressor current < 11% of load current (60 Hz)
Capacitor dV/dt < 2 V/µs
Capacitor pulse dissipation : ∫(dv/dt) dt < 10000 V^2/µs
Resonant frequency < 300 Hz
Resistor power for 2 Hz max switching frequency
Power factor of 0.3 assumed for typical inductive load

Guidelines for differential inputs and outputs

Differential inputs and outputs behave differently than standard inputs and outputs. There are two pins per differential input and output. Determining whether a differential input or output is on or off requires that you measure the voltage difference between these two pins. See the detailed specifications for the CPU 1217C in Appendix A (Page 1153).

5.5 Maintenance and repair

The components of the S7-1200 automation system are maintenance-free.

NOTE

Only the manufacturer can carry out repairs to the components of the S7-1200 automation system.

PLC concepts

6

6.1 Execution of the user program

The CPU supports the following types of code blocks that allow you to create an efficient structure for your user program:

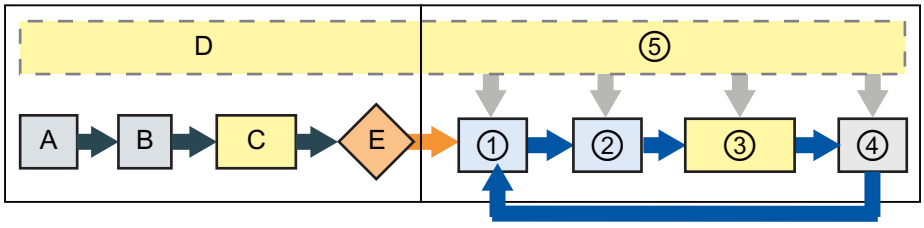
- Organization blocks (OBs) (Page 170) define the structure of the program. Some OBs run at startup. Some run continuously when the CPU is running your process. Some run under specific conditions.
- Functions (FCs) (Page 172) and function blocks (FBs) (Page 172) contain the program code that corresponds to specific tasks. FCs and FBs can be called from an OB or from another FC or FB. Each FC or FB provides a set of input and output parameters for sharing data with the calling block. An FB also uses an associated data block (called an instance DB) to maintain the data values for that instance of the FB call. You can call an FB multiple times, each time with a unique instance DB. Calls to the same FB with different instance DBs do not affect the data values in any of the other instance DBs.
- Data blocks (DBs) (Page 174) store data that can be used by the program blocks.

Execution of the user program begins with one or more optional startup OBs (Page 67) that execute once upon entering RUN mode, followed by one or more program cycle OBs (Page 67) that execute cyclically. You can also associate an OB with an interrupt event, which can be either a standard event or an error event. These OBs execute whenever the corresponding standard or error event occurs.

Operating modes

The CPU has three modes of operation: STOP mode, STARTUP mode, and RUN mode. Status LEDs on the front of the CPU indicate the current mode of operation.

- In STOP mode, the CPU handles any communication requests (as appropriate) and performs self-diagnostics. The CPU does not execute the user program. Automatic updates of the process image do not occur. You can download a project to the CPU.
- In STARTUP and RUN modes, the CPU performs the tasks shown in the following figure:



STARTUP		RUN	
A	Copies the state of the physical inputs to I memory	①	Writes Q memory to the physical outputs
B	Initializes the Q output (image) memory area with either zero, the last value, or the configured substitute value. Zeroes PB, PN, and AS-i outputs	②	Copies the state of the physical inputs to I memory
C	Initializes non-retentive M memory and data blocks to their initial value and enables configured cyclic interrupt and time of day events. Executes the startup OBs.	③	Executes the program cycle OBs and updates the output values in the process image output area
D	Stores any interrupt events into the queue to be processed after entering RUN mode	④	Performs self-test diagnostics
E	Enables the writing of Q memory to the physical outputs	⑤	Processes interrupts and communications during any part of the scan cycle

NOTE

Communication, including HMI communication, cannot interrupt OBs other than program cycle OBs.

You can download some parts of a project in RUN mode (Page 1072).

Process image update and process image partitions

The CPU updates local digital and analog I/O points synchronously with the scan cycle using an internal memory area called the process image. The process image contains a snapshot of the physical inputs and outputs (the physical I/O points on the CPU, signal board, and signal modules).

You can configure I/O points to be updated in the process image every scan cycle or when a specific event interrupt occurs. You can also configure an I/O point to be excluded from process image updates. For example, your process might only need certain data values when an event such as a hardware interrupt occurs. By configuring the process image update for these I/O points to be associated with a partition that you assign to a hardware interrupt OB,

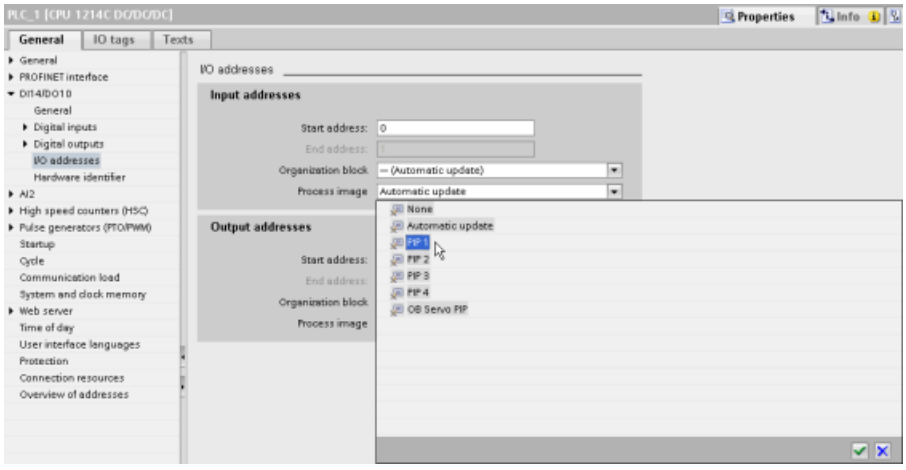
you avoid having the CPU update data values unnecessarily every scan cycle when your process does not need a continual update.

For controlling whether your process updates I/O points automatically on every scan cycle, or upon the triggering of events, the S7-1200 provides five process image partitions. The first process image partition, PIP0, is designated for I/O that is to be automatically updated every scan cycle, and is the default assignment. You can use the remaining four partitions, PIP1, PIP2, PIP3, and PIP4 for assigning I/O process image updates to various interrupt events. You assign I/O to process image partitions in Device Configuration and you assign process image partitions to interrupt events when you create interrupt OBs (Page 170) or edit OB properties (Page 170).

By default, when you insert a module in the device view, STEP 7 sets its I/O process image update to "Automatic update". For I/O configured for "Automatic update", the CPU handles the data exchange between the module and the process image area automatically during every scan cycle.

To assign digital or analog points to a process image partition, or to exclude I/O points from process image updates, follow these steps:

1. View the Properties tab for the appropriate device in Device configuration.
2. Expand the selections under "General" as necessary to locate the desired I/O points.
3. Select "I/O addresses".
4. Optionally select a specific OB from the "Organization block" drop-down list.
5. From the "Process image" drop-down list, change "Automatic update" to "PIP1", "PIP2", "PIP3", "PIP4" or "None". A selection of "None" means that you can only read from and write to this I/O using immediate instructions. To add the points back to the process image automatic update, change this selection back to "Automatic update".



You can immediately read physical input values and immediately write physical output values when an instruction executes. An immediate read accesses the current state of the physical input and does not update the process image input area, regardless of whether the point is configured to be stored in the process image. An immediate write to the physical output updates both the process image output area (if the point is configured to be stored in the process image) and the physical output point. Append the suffix ":P" to the I/O address if you want the program to immediately access I/O data directly from the physical point instead of using the process image.

NOTE

Use of process image partitions

If you assign I/O to one of the process image partitions PIP1 - PIP4, and do not assign an OB to that partition, then the CPU never updates that I/O to or from the process image. Assigning I/O to a PIP that does not have a corresponding OB assignment is the same as assigning the process image to "None". You can read the I/O directly from the physical I/O with an immediate read instruction, or write to the physical I/O with an immediate write instruction. The CPU does not update the process image.

The CPU supports distributed I/O for PROFINET (Page 530), PROFIBUS (Page 691), and AS-i (Page 696) networks.

6.1.1 Startup configuration and processing

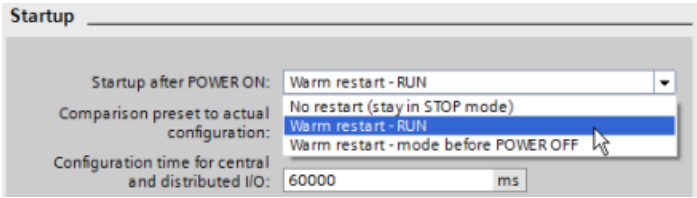
Startup configuration

The CPU supports a warm restart for entering the RUN mode. The CPU initializes all non-retentive system and user data at warm restart, and retains the values of all retentive user data.

Warm restart does not include a memory reset. A memory reset clears all work memory, clears retentive and non-retentive memory areas, copies load memory to work memory, and sets outputs to the configured "Reaction to CPU STOP". A memory reset does not clear the diagnostics buffer or the permanently saved values of the IP address.

You can configure the "startup after POWER ON" setting of the CPU. This configuration item appears under the "Device configuration" for the CPU under "Startup". Upon powering up, the CPU performs a sequence of power-up diagnostic checks and system initialization. During system initialization, the CPU deletes all non-retentive bit (M) memory and resets all non-retentive DB contents to the initial values from load memory. The CPU retains retentive bit (M) memory and retentive DB contents and then enters the appropriate operating mode. Certain detected errors prevent the CPU from entering the RUN mode. The CPU supports the following configuration choices:

- No restart (stay in STOP mode)
- Warm restart - RUN
- Warm restart - mode prior to POWER OFF



NOTICE
Risks associated with repairable faults The CPU can enter STOP mode due to repairable faults, such as the following: – Failure of a replaceable signal module – Temporary faults, such as power line disturbance or erratic power up event Such conditions can result in property damage. If you have configured the CPU to "Warm restart - mode prior to POWER OFF", the CPU goes to the operating mode that the CPU was in prior to the loss of power or fault. If the CPU was in STOP mode at the time of power loss or fault, the CPU goes to STOP mode on power up. The CPU stays in STOP mode until the CPU receives a command to go to RUN mode. If the CPU was in RUN mode at the time of power loss or fault, the CPU goes to RUN mode on the next power up. The CPU goes to RUN mode providing the CPU detects no errors that would inhibit a transition to RUN mode. Configure CPUs that you intend to operate independently of a STEP 7 connection to "Warm restart - RUN". This startup mode sets the CPU to return to RUN mode on the next power cycle.

Startup processing

See Downloading in RUN mode (Page 1072) for the processing sequence during startup.

Each startup OB includes startup information that helps you determine the validity of retentive data and the time-of-day clock. You can program instructions inside the startup OBs to examine these startup values and to take appropriate action.

The CPU also performs the following tasks during the startup processing:

- Interrupts are queued but not processed during the startup phase
- No cycle time monitoring is performed during the startup phase
- Configuration changes to HSC (high-speed counter), PTO (pulse train output), and PtP (point-to-point communication) modules can be made in startup
- Actual operation of HSC, PTO, and point-to-point communication modules only occurs in RUN

After the execution of the startup OBs finishes, the CPU goes to RUN mode and processes the control tasks in a continuous scan cycle.

Changing the operating mode

You can use the "STOP" or "RUN" commands (Page 1061) from the online tools of the TIA Portal to change the current operating mode. You can also include an STP instruction (Page 275) in your program to change the CPU to STOP mode. Other tools provide a means to change the operating mode as well.

6.1.2 Processing the scan cycle in RUN mode

For each scan cycle, the CPU performs processing as described in Execution of the user program (Page 61).

The CPU handles interrupt events that are enabled according to priority in the order in which they occur. For interrupt events, the CPU reads the inputs, executes the OB, and then writes the outputs, using the associated process image partition (PIP), if applicable.

The system guarantees that the scan cycle will be completed in a time period called the maximum cycle time; otherwise a time error event is generated.

- Each scan cycle begins by retrieving the current values of the digital and analog outputs from the process image and then writing them to the physical outputs of the CPU, SB, and SM modules configured for automatic I/O update (default configuration). When a physical output is accessed by an instruction, both the output process image and the physical output itself are updated.
- The scan cycle continues by reading the current values of the digital and analog inputs from the CPU, SB, and SMs configured for automatic I/O update (default configuration), and then writing these values to the process image. When a physical input is accessed by an instruction, the value of the physical input is accessed by the instruction, but the input process image is not updated.
- After reading the inputs, the user program is executed from the first instruction through the end instruction. This includes all the program cycle OBs plus all their associated FCs and FBs. The program cycle OBs are executed in order according to the OB number with the lowest OB number executing first.

Communications processing occurs periodically throughout the scan, possibly interrupting user program execution.

Self-diagnostic checks include periodic checks of the system and the I/O module status checks.

Interrupts can occur during any part of the scan cycle, and are event-driven. When an event occurs, the CPU interrupts the scan cycle and calls the OB that was configured to process that event. After the OB finishes processing the event, the CPU resumes execution of the user program at the point of interruption.

6.1.3 Organization blocks (OBs)

6.1.3.1 Organization blocks (OBs)

Organization blocks (OBs) control the execution of the user program.

The program cycle OB contains your main program. You can include more than one program cycle OB in your user program. During RUN mode, the program cycle OBs execute at the lowest priority level (Page 77) and can be interrupted by all other event types. The CPU executes the program cycle OBs in a continuous cycle known as the "program cycle" or "scan cycle". This cyclic processing is the normal type of processing used for programmable logic controllers. For many applications, the entire user program is located in a single program cycle OB.

Specific events in the CPU trigger the execution of other organization blocks. OBs cannot call each other. The startup OB runs when you start the CPU. It does not interrupt the program cycle OB. The CPU executes the startup OB before going to RUN mode.

Other OBs, called interrupt OBs, run when associated events or errors occur. These OBs interrupt the execution of the program cycle OBs.

An FC or FB cannot call an OB. Only an event such as a diagnostic interrupt or a time delay can start the execution of an OB. The CPU handles OBs according to their respective priority classes (Page 77), with higher priority OBs executing before lower priority OBs.

6.1.3.2 Program cycle OB

Program cycle OBs execute cyclically while the CPU is in RUN mode. The main block of the program is a program cycle OB. This is where you place the instructions that control your program and where you call additional user blocks. You can have multiple program cycle OBs, which the CPU executes in numerical order. Main (OB 1) is the default.

Program cycle events

The program cycle event happens once during each program cycle (or scan). During the program cycle, the CPU writes the outputs, reads the inputs and executes program cycle OBs. The program cycle event is required and is always enabled. You might have no program cycle OBs, or you might have multiple program cycle OBs. After the program cycle event occurs, the CPU executes the lowest numbered program cycle OB (usually "Main" OB 1). The CPU executes the other program cycle OBs sequentially (in numerical order) within the program cycle. Program execution is cyclical such that the program cycle event occurs at the following times:

- When the last startup OB finishes execution
- When the last program cycle OB finishes execution

You can delay the next program cycle after the program cycle OB finishes by configuring a minimum cycle time in the device configuration

Table 6-1 Start information for a program cycle OB

Input	Data type	Description
Initial_Call	Bool	True for initial call of the OB
Remanence	Bool	True if retentive data are available

6.1.3.3 Startup OB

Startup OBs execute one time when the operating mode of the CPU changes from STOP to RUN, including powering up in the RUN mode and in commanded STOP-to-RUN transitions. After completion, the main "Program cycle" begins executing. Refer to "Startup processing" in Startup configuration and processing (Page 64)
The Startup OBs support the following startup data bits:

Table 6-2 Startup locations supported by the startup OB

Input	Data Type	Description
LostRetentive	Bool	This bit is true if the retentive data storage areas have been lost
LostRTC	Bool	This bit is true if the time-of-day clock (Real time Clock) has been lost

6.1.3.4 Time delay interrupt OB

Time delay interrupt OBs execute after a time delay that you configure.

Time delay interrupt events

You configure time delay interrupt events to occur after a specified delay time has expired from the beginning of execution of the SRT_DINT instruction. You assign the delay time with the SRT_DINT instruction. The time delay events interrupt the program cycle to execute the corresponding time delay interrupt OB. You can attach only one time delay interrupt OB to a time delay event. The CPU supports four time delay events.

Table 6-3 Start information for a time delay interrupt OB

Input	Data type	Description
Sign	Word	Identifier passed to triggering call of SRT_DINT

6.1.3.5 Cyclic interrupt OB

Cyclic interrupt OBs execute at a specified interval. You can configure up to a total of four cyclic interrupt events, with one OB corresponding to each cyclic interrupt event.

Cyclic interrupt events

The cyclic interrupt events allow you to configure the execution of an interrupt OB at a configured cycle time. You configure the initial cycle time when you create the cyclic interrupt OB. A cyclic event interrupts the program cycle and executes the corresponding cyclic interrupt OB. Note that the cyclic interrupt event is at a higher priority class than the program cycle event.

You can attach only one cyclic interrupt OB to a cyclic event.

You can assign a phase shift to each cyclic interrupt so that the execution of cyclic interrupts can be offset from one another by the phase offset amount. For example, if you have a 5 ms cyclic event and a 10 ms cyclic event, every ten milliseconds both events occur at the same moment. If you phase shift the 5 ms event by 1 to 4 ms and the 10 ms event by 0 ms, then the two events do not occur at the same moment.

The default phase offset is 0. To change the initial phase shift, or to change the cyclic time for a cyclic event, follow these steps:

1. Right-click the cyclic interrupt OB in the project tree.
2. Select "Properties" from the context menu.
3. Click "Cyclic interrupt" from the "Cyclic interrupt [OB 30]" dialog, and enter the new initial values.

The maximum phase offset is 6000 ms (6 seconds) or the maximum Cyclic time, whichever is smaller.

You can also query and change the cycle time and the phase shift from your program using the Query cyclic interrupt (QRY_CINT) and Set cyclic interrupt (SET_CINT) instructions. Cycle time and phase shift values set by the SET_CINT instruction do not persist through a power cycle or a transition to STOP mode; cycle time and phase shift values return to the initial values following a power cycle or a transition to STOP. The CPU supports a total of four cyclic interrupt events.

6.1.3.6 Hardware interrupt OB

Hardware interrupt OBs execute when the relevant hardware event occurs. A hardware interrupt OB interrupts normal cyclic program execution in reaction to a signal from a hardware event.

Hardware interrupt events

Changes in the hardware, such as a rising or falling edge on an input point, or an HSC (High Speed Counter) event trigger hardware interrupt events. The S7-1200 supports one interrupt OB for each hardware interrupt event. You enable the hardware events in the device configuration, and assign an OB for an event in the device configuration or with an ATTACH instruction in the user program. The CPU supports several hardware interrupt events. The CPU model and the number of input points determine the exact events that are available.

Limits on hardware interrupt events are as follows:

Edges:

- Rising edge events: maximum of 16
- Falling edge events: maximum of 16

HSC events:

- CV=PV: maximum of 6
- Direction changed: maximum of 6
- External reset: maximum of 6

Table 6-4 Start information for a hardware interrupt OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier of the module that triggered the hardware interrupt
USI	WORD	User structure identifier (16#0001 to 16#FFFF), reserved for future use
IChannel	USINT	Number of the channel that triggered the interrupt
EventType	BYTE	Identifier for the module-specific event type associated with the event triggering the interrupt, for example falling edge or rising edge.

Table 6-5 Bits in EventType based on module and process event

Module / Submodule	Value	Process event
Onboard I/O from CPU or SB	16#0	Rising edge
	16#1	Falling edge
HSC	16#0	HSC CV=RV1
	16#1	HSC direction changed
	16#2	HSC reset

6.1.3.7 Time error interrupt OB

If configured, the time error interrupt OB (OB 80) executes when either the scan cycle exceeds the maximum cycle time or a time error event occurs. If triggered, it executes, interrupting normal cyclic program execution or any other event OB.

The occurrence of either of these events generates a diagnostics buffer entry describing the event. The diagnostics buffer entry is generated regardless of the existence of the time error interrupt OB.

Time error interrupt events

The occurrence of any of several different time error conditions results in a time error event:

- Scan cycle exceeds maximum cycle time
  The "maximum cycle time exceeded" condition results if the program cycle does not complete within the specified maximum scan cycle time. See the topic Monitoring and configuring the cycle time (Page 81) for more information.
- CPU cannot start requested OB because a second time interrupt (cyclic or time-delay) starts before the CPU finishes execution of the first interrupt OB
- Queue overflow occurred
  The "queue overflow occurred" condition results if the interrupts are occurring faster than the CPU can process them. The CPU limits the number of pending (queued) events by using a different queue for each event type. If an event occurs when the corresponding queue is full, the CPU generates a time error event.

All time error events trigger the execution of the time error interrupt OB if it exists. If the time error interrupt OB does not exist, then the following conditions determine the CPU behavior:

- If a time error interrupt OB has never been downloaded to the CPU, the CPU ignores the first scan timeout condition and remains in RUN mode. If a second scan timeout condition occurs in the same program scan (two times the maximum cycle time value), the CPU generates a diagnostic buffer entry and transitions to STOP mode.
- If the time error interrupt OB has previously been downloaded, but has since been deleted, the CPU transitions to STOP mode if a time error event occurs, because the CPU cannot find the time error OB.

The user program can extend the program cycle execution time up to ten times the configured maximum cycle time by executing the RE_TRIGR instruction (Page 274) to restart the cycle time monitor. However, if two "maximum cycle time exceeded" conditions occur within the same program cycle without resetting the cycle timer, then the CPU transitions to STOP, regardless of whether the time error interrupt OB exists. See the topic Monitoring and configuring the cycle time (Page 81).

Time error interrupt OB includes start information that helps you determine which event and OB generated the time error. You can program instructions inside the OB to examine these start values and to take appropriate action.

Table 6-6 Start information for the time error OB (OB 80)

Input	Data type	Description
Fault_ID	BYTE	16#01 - maximum cycle time exceeded 16#02 - requested OB cannot be started 16#07 and 16#09 - queue overflow occurred
Csg_OBnr	OB_ANY	Number of the OB which was being executed when the error occurred
Csg_Prio	UINT	Priority of the OB causing the error

See topic Organization blocks (OBs) (Page 66) for instructions on adding OBs to your project.

The priority for a V4.x CPU is 22. If you exchange a V3.0 CPU for a V4.0 CPU (Page 1285), the priority is 26, the priority that was in effect for V3.0. In either case, the priority field is editable and you can set the priority to any value in the range 22 to 26.

6.1.3.8 Diagnostic error interrupt OB

The diagnostic error interrupt OB executes when the CPU detects a diagnostic error, or if a diagnostics-capable module recognizes an error and you have enabled the diagnostic error interrupt for the module. The diagnostic error interrupt OB interrupts the normal cyclic program execution. You can include an STP instruction in the diagnostic error interrupt OB to put the CPU in STOP mode if you desire your CPU to enter STOP mode upon receiving this type of error.
If you do not include a diagnostic error interrupt OB in your program, the CPU ignores the error and stays in RUN mode.

Diagnostic error events

PROFINET, PROFIBUS, local analog, and some local digital devices are capable of detecting and reporting diagnostic errors. The occurrence or removal of any of several different diagnostic error conditions results in a diagnostic error event. Standard CPUs and modules can generate the following diagnostic errors:

- No user power
- High limit exceeded
- Low limit exceeded
- Wire break
- Short circuit

Fail-safe and Decentralized devices can generate additional diagnostic errors.
Diagnostic error events trigger the execution of the diagnostic error interrupt OB (OB 82) if it exists. If it does not exist, then the CPU ignores the error.
See topic Organization blocks (OBs) (Page 66) for instructions on adding an OB to your project.

NOTE
Diagnostic errors for multi-channel local analog devices (I/O, RTD, and Thermocouple)
The diagnostic error interrupt OB can process only one channel's diagnostic error at a time.
If two channels of a multi-channel device have an error, then the second error only triggers the diagnostic error interrupt OB under the following conditions: the first channel error clears, the execution of the diagnostic error interrupt OB that the first error triggered is complete, and the second error still exists.

The diagnostic error interrupt OB includes startup information that helps you determine whether the event is due to the occurrence or removal of an error, and the device and channel which reported the error. You can program instructions inside the diagnostic error interrupt OB to examine these startup values and to take appropriate action.

NOTE

If the outgoing event leaves the submodule with no pending diagnostics, the Diagnostic error OB start information references the submodule as a whole (16#8000), even if the source of the event was a specific channel.

Table 6-7 Startup information for the diagnostic error interrupt OB

Input	Data type	Description
IOstate	WORD	IO state of the device: • Bit 0 = 1 if the configuration is correct, and = 0 if the configuration is no longer correct. • Bit 4 = 1 if an error is present (such as a wire break). (Bit 4 = 0 if there is no error.) • Bit 5 = 1 if the configuration is **not** correct, and = 0 if the configuration is correct again. • Bit 7 = 1 if an I/O access error has occurred. Refer to LADDR for the hardware identifier of the I/O with the access error. (Bit 6 = 0 if there is no error.)
LADDR	HW_ANY	Hardware identifier of the device or functional unit that reported the error[1]
Channel	UINT	Channel number
MultiError	BOOL	TRUE if more than one error is present

[1] The LADDR input contains the hardware identifier of the device or functional unit which returned the error. The hardware identifier is assigned automatically when components are inserted in the device or network view and appears in the System constants tab of PLC tags. A name is also assigned automatically for the hardware identifier. These entries in the System constants tab of the PLC tags cannot be changed.

6.1.3.9 Pull or plug of modules OB

The "Pull or plug of modules" OB executes when a configured and non-disabled distributed I/O module or submodule (PROFIBUS, PROFINET, AS-i) generates an event related to inserting or removing a module.

Pull or plug of modules event

The following conditions generate a pull or plug of modules event:

- Someone removes or inserts a configured module
- A configured module is not physically present in an expansion rack
- An incompatible module is in an expansion rack that does not correspond to the configured module
- A compatible module for a configured module is in an expansion rack, but the configuration does not allow substitutes
- A module or submodule has parameterization errors

If you have not programmed this OB, the CPU remains in RUN mode when any of these conditions occur with a configured and non-disabled distributed I/O module.

Regardless of whether you have programmed this OB, the CPU changes to STOP mode when any of these conditions occur with a module in the central rack.

Table 6-8 Start information for pull or plug of modules OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier
Event_Class	Byte	16#38: module inserted 16#39: module removed
Fault_ID	Byte	Fault identifier

6.1.3.10 Rack or station failure OB

The "Rack or station failure" OB executes when the CPU detects the failure or communication loss of a distributed rack or station.

Rack or station failure event

The CPU generates a rack or station failure event when it detects one of the following:

- The failure of a DP master system or of a PROFINET IO system (in the case of either an incoming or an outgoing event).
- The failure of a DP slave or of an IO device (in the case of either an incoming or an outgoing event)
- Failure of some of the submodules of a PROFINET I-device

If you have not programmed this OB, the CPU remains in RUN mode when any of these conditions occur.

Table 6-9 Start information for rack or station failure OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier
Event_Class	Byte	16#38: outgoing event 16#39: incoming event
Fault_ID	Byte	Fault identifier

6.1.3.11 Time of day OB

Time of day OBs execute based on configured clock time conditions. The CPU supports two time of day OBs.

Time of day events

You can configure a time of day interrupt event to occur once on a specified date or time or cyclically with one of the following cycles:

- Every minute: The interrupt occurs every minute.
- Hourly: The interrupt occurs every hour.
- Daily: The interrupt occurs every day at a specified time (hour and minute).
- Weekly: The interrupt occurs every week at a specified time on a specified day of the week (for example, every Tuesday at 4:30 in the afternoon).

- Monthly: The interrupt occurs every month at a specified time on a specified day of the month. The day number must be between 1 and 28, inclusive.
- Every end of month: The interrupt occurs on the last day of every month at a specified time.
- Yearly: The interrupt occurs every year on the specified date (month and day). You cannot specify a date of February 29.

Table 6-10 Start information for a time of day event OB

Input	Data type	Description
CaughtUp	Bool	OB call is caught up because time was set forward
SecondTime	Bool	OB call is started a second time because time was set backward

6.1.3.12 Status OB

Status OBs execute if a DPV1 or PNIO slave triggers a status interrupt. This might be the case if a component (module or rack) of a DPV1 or PNIO slave changes its operating mode, for example from RUN to STOP.

Status events

For detailed information on events that trigger a status interrupt, refer to the manufacturer's documentation for the DPV1 or PNIO slave.

Table 6-11 Start information for status OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier
Slot	UInt	Slot number
Specifier	Word	Alarm specifier

6.1.3.13 Update OB

Update OBs execute if a DPV1 or PNIO slave triggers an update interrupt.

Update events

For detailed information on events that trigger an update interrupt, refer to the manufacturer's documentation for the DPV1 or PNIO slave.

Table 6-12 Start information for update OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier
Slot	UInt	Slot number
Specifier	Word	Alarm specifier

6.1.3.14 Profile OB

Profile OBs execute if a DPV1 or PNIO slave triggers a profile-specific interrupt.

Profile events

For detailed information on events that trigger a profile interrupt, refer to the manufacturer's documentation for the DPV1 or PNIO slave.

Table 6-13 Start information for profile OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier
Slot	UInt	Slot number
Specifier	Word	Alarm specifier

6.1.3.15 MC-Servo and MC-Interpolator OB

STEP 7 creates the read-only MC-Servo and MC-Interpolator OBs automatically when you create a motion technology object and set the drive interface to be "Analog drive connection" or "PROFIDrive". You do not need to edit any OB properties or create this OB directly. The CPU uses these OBs for closed loop control. Refer to the STEP 7 Information System for further details.
The MC Servo OB uses a system-defined PIP with the name "PIP OB Servo".

Table 6-14 Start information for MC-Servo OB

Input	Data type	Description
Initial_Call	BOOL	TRUE indicates first call of this OB on transition from STOP to RUN
PIP_Input	BOOL	TRUE indicates the associated process image input is up to date.
PIP_Output	BOOL	TRUE indicates that the CPU transferred the associated process image output to the outputs in good time after the last cycle.
IO_System	USINT	Number of the distributed I/O system triggering the interrupt
Event_Count	INT	n: number of lost cycles -1: unknown number of cycles lost (for example, because cycle has changed)
Synchronous	BOOL	TRUE: The MC-Servo [OB91] is called synchronously with a bus system

Table 6-15 Start information for MC-Interpolator OB

Input	Data type	Description
Initial_Call	BOOL	TRUE indicates first call of this OB on transition from STOP to RUN
PIP_Input	BOOL	TRUE indicates the associated process image input is up to date.
PIP_Output	BOOL	TRUE indicates that the CPU transferred the associated process image output to the outputs in good time after the last cycle.
IO_System	USINT	Number of the distributed I/O system triggering the interrupt
Event_Count	INT	n: number of lost cycles -1: unknown number of cycles lost (for example, because cycle has changed)
Reduction	UInt	Reduction ratio of MC-Interpolator [OB92] to MC-Servo [OB91]

6.1.3.16 MC-PreServo

You can program the MC-PreServo OB to contain program logic for the STEP 7 program to execute directly before the MC-Servo OB executes.

MC-PreServo events

The MC-PreServo OB allows you to read out the configured application cycle information in microseconds.

Table 6-16 Start information for MC-PreServo OB

Input	Data type	Description
Initial_Call	BOOL	TRUE indicates first call of this OB on transition from STOP to RUN
PIP_Input	BOOL	TRUE indicates the associated process image input is up to date.
PIP_Output	BOOL	TRUE indicates that the CPU transferred the associated process image output to the outputs in good time after the last cycle.
IO_System	USINT	Number of the distributed I/O system triggering the interrupt
Event_Count	INT	n: number of lost cycles -1: unknown number of cycles lost (for example, because cycle has changed)
Synchronous	BOOL	Reserved
CycleTime	UDINT	Display of the application cycle configured for the MC-Servo OB in microseconds

6.1.3.17 MC-PostServo

You can program the MC-PostServo OB to contain program logic for the STEP 7 program to execute directly after the MC-Servo OB executes.

MC-PostServo events

The MC-PostServo OB allows you to read out the configured application cycle information in microseconds.

Table 6-17 Start information for MC-PostServo OB

Input	Data type	Description
Initial_Call	BOOL	TRUE indicates first call of this OB on transition from STOP to RUN
PIP_Input	BOOL	TRUE indicates the associated process image input is up to date.
PIP_Output	BOOL	TRUE indicates that the CPU transferred the associated process image output to the outputs in good time after the last cycle.
IO_System	USINT	Number of the distributed I/O system triggering the interrupt
Event_Count	INT	n: number of lost cycles -1: unknown number of cycles lost (for example, because cycle has changed)
Synchronous	BOOL	Reserved
CycleTime	UDINT	Display of the application cycle configured for the MC-Servo OB in microseconds

6.1.3.18 Event execution priorities and queuing

Events control CPU processing. An event triggers an interrupt OB to be executed. You can specify the interrupt OB for an event during the creation of the block, during the device configuration, or with an ATTACH or DETACH instruction. Some events happen on a regular basis like the program cycle or cyclic events. Other events happen only a single time, like the startup event and time delay events. Some events happen when the hardware triggers an event, such as an edge event on an input point or a high speed counter event. Events like the diagnostic error and time error event only happen when an error occurs. The event priorities and queues are used to determine the processing order for the event interrupt OBs.

The CPU processes events in order of priority where 1 is the lowest priority and 26 is the highest priority. You can assign a priority class to an OB in the attributes of the OB properties.

Interruptible and non-interruptible execution modes

OBs (Page 66) execute in priority order of the events that trigger them. In the Startup properties of the device configuration of the CPU (Page 136), you can configure OB execution to be interruptible or non-interruptible. Non-interruptible is the default. Note that program cycle OBs are always interruptible, but you can configure all other OBs to be either interruptible or non-interruptible.

If you set interruptible mode, then if an OB is executing and a higher priority event occurs before the OB completes its execution, the running OB is interrupted to allow the higher-priority event OB to run. The higher-priority event runs, and at its completion, the OB that was interrupted continues. When multiple events occur while an interruptible OB is executing, the CPU processes those events in priority order.

If you do not set interruptible mode, then an OB runs to completion when triggered regardless of any other events that trigger during the time that it is running.

Consider the following two cases where interrupt events trigger a cyclic OB and a time delay OB. In both cases, the time delay OB (OB 201) has no process image partition assignment (Page 61) and executes at priority 4. The cyclic OB (OB 200) has a process image partition assignment of PIP1 and executes at priority 2. The following illustrations show the difference in execution between non-interruptible and interruptible execution modes:

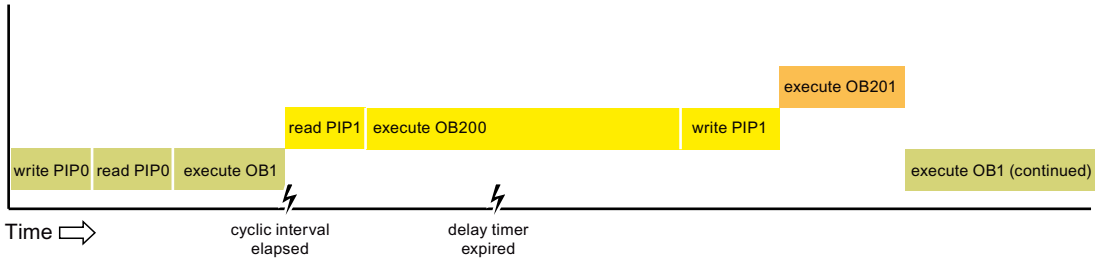


Figure 6-1 Case 1: Non-interruptible OB execution

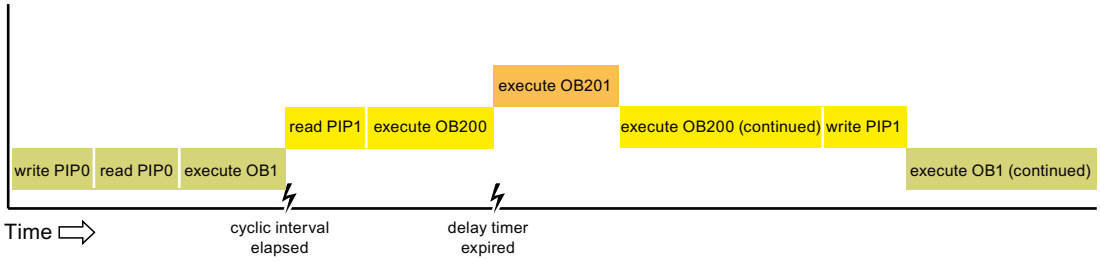


Figure 6-2 Case 2: Interruptible OB execution

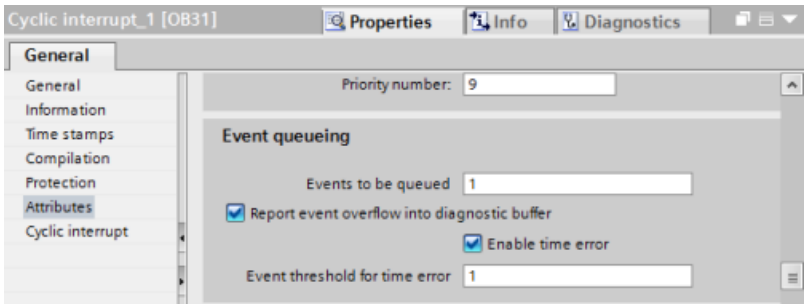
NOTE

If you configure the OB execution mode to be non-interruptible, then a time error OB cannot interrupt OBs other than program cycle OBs. Prior to V4.0 of the S7-1200 CPU, a time error OB could interrupt any executing OB. To make an OB interruptible by a time error OB or other higher-priority OB, you must configure OB execution to be interruptible.

Understanding event execution priorities and queuing

The CPU limits the number of pending (queued) events from a single source, using a different queue for each event type. Upon reaching the limit of pending events for a given event type, the next event is lost. You can use a time error interrupt OB (Page 70) to respond to queue overflows.

Note that STEP 7 allows you to configure some specific event queueing parameters for the Cyclic interrupt OB and the Time of day OB.



For further information on CPU overload behavior and event queueing, refer to the STEP 7 Information System.

Each CPU event has an associated priority. In general, the CPU services events in order of priority (highest priority first). The CPU services events of the same priority on a "first-come, first-served" basis.

Table 6-18 OB events

Event	Quantity allowed	Default OB priority
Program cycle	1 program cycle event[1] Multiple OBs allowed	1
Startup	1 startup event [1] Multiple OBs allowed	1
Time delay	Up to 4 time events 1 OB per event	OB 20: 3 OB 21: 4 OB 22: 5 OB 23: 6 OB 123 to OB 32767: 3
Cyclic interrupt	Up to 4 events 1 OB per event	OB 30: 8 OB 31: 9 OB 32: 10 OB 33: 11 OB 34: 12 OB 35: 13 OB 36: 14 OB 37: 16 OB 38: 17 OB 123 to OB 32767: 7

1 The startup event and the program cycle event never occur at the same time because the startup event runs to completion before the program cycle event starts.

2 You can have more than 50 hardware interrupt event OBs if you use the DETACH and ATTACH instructions.

3 You can configure the CPU to stay in RUN if the scan cycle exceeds the maximum scan cycle time or you can use the RE_TRIGR instruction to reset the cycle time. However, the CPU goes to STOP mode the second time that one scan cycle exceeds the maximum scan cycle time.

4 The priority is 22, but is editable to any value in the range 22 to 26.

Event	Quantity allowed	Default OB priority
Hardware interrupt	Up to 50 hardware interrupt events[2] 1 OB per event, but you can use the same OB for multiple events	18 18
Time error	1 event (only if configured)[3]	22 or 26[4]
Diagnostic error	1 event (only if configured)	5
Pull or plug of modules	1 event	6
Rack or station failure	1 event	6
Time of day	Up to 2 events	2
Status	1 event	4
Update	1 event	4
Profile	1 event	4
MC-Servo	1 event	25
MC-Interpolator	1 event	24

1 The startup event and the program cycle event never occur at the same time because the startup event runs to completion before the program cycle event starts.

2 You can have more than 50 hardware interrupt event OBs if you use the DETACH and ATTACH instructions.

3 You can configure the CPU to stay in RUN if the scan cycle exceeds the maximum scan cycle time or you can use the RE_TRIGR instruction to reset the cycle time. However, the CPU goes to STOP mode the second time that one scan cycle exceeds the maximum scan cycle time.

4 The priority is 22, but is editable to any value in the range 22 to 26.

Refer to the topic "Exchanging a V3.0 CPU for a V4.x CPU (Page 1285)" for more details.

In addition, the CPU recognizes other events that do not have associated OBs. The following table describes these events and the corresponding CPU actions:

Table 6-19 Additional events

Event	Description	CPU action
I/O access error	Direct I/O read/write error	The CPU logs the first occurrence in the diagnostics buffer and stays in RUN mode. You can access the error cause using the GET_ERROR_ID (Page 276) instruction.
Max cycle time error	CPU exceeds the configured cycle time twice	The CPU logs the error in the diagnostics buffer and transitions to STOP mode.
Peripheral access error	I/O error during process image update	The CPU logs the first occurrence in the diagnostics buffer and stays in RUN mode.
Programming error	program execution error	• If block-local error handling is enabled, the system enters an error cause in the error structure. You can access the error cause using the GET_ERROR_ID (Page 276) instruction. • If global error handling is enabled, the system enters an access error start event into the diagnostics buffer and stays in RUN mode.

Interrupt latency

The interrupt event latency (the time from notification of the CPU that an event has occurred until the CPU begins execution of the first instruction in the OB that services the event) is approximately 175 µsec, provided that a program cycle OB is the only event service routine active at the time of the interrupt event.

6.1.4 Monitoring and configuring the cycle time

The cycle time is the time that the CPU operating system requires to execute the cyclic phase of the RUN mode. The CPU provides two methods of monitoring the cycle time:

- Maximum scan cycle time
- Minimum scan cycle time

Scan cycle monitoring begins after the startup event is complete. Configuration for this feature appears under the "Device Configuration" for the CPU under "Cycle".

The CPU monitors the scan cycle. If the scan cycle time exceeds the configured maximum scan cycle time, the CPU generates an error and responds as follows:

- If the user program includes a time error interrupt OB (Page 70), then the CPU executes it.
- If the user program does not include a time error interrupt OB, then the time error event generates a diagnostic buffer entry. The CPU behavior is determined by the following:
  - If a time error interrupt OB has never been downloaded to the CPU, the CPU ignores the first scan timeout condition and remains in RUN mode. If a second scan timeout condition occurs in the same program scan (two times the maximum cycle time value), the CPU generates a diagnostic buffer entry and transitions to STOP mode.
  - If the time error interrupt OB has previously been downloaded, but has since been deleted, the CPU transitions to STOP mode if a time error event occurs, because the CPU cannot find the time error OB.

The RE_TRIGR instruction (Page 274) (re-trigger cycle time monitoring) allows you to reset the timer that measures the cycle time. If the elapsed time for the current program cycle execution is less than ten times the configured maximum scan cycle time, the RE_TRIGR instruction retriggers the cycle time monitoring and returns with ENO = TRUE. If not, the RE_TRIGR instruction does not retrigger the cycle time monitoring. It returns ENO = FALSE.

Typically, the scan cycle executes as fast as it can and the next scan cycle begins as soon as it completes. Depending upon the user program and communication tasks, the time period for a scan cycle can vary from scan to scan. To eliminate this variation, the CPU supports an optional minimum scan cycle time. If you enable this optional feature and provide a minimum scan cycle time in ms, then the CPU delays after the execution of the program cycle OBs until the minimum scan cycle time elapses before repeating the program cycle.

In the event that the CPU completes the normal scan cycle in less time than the specified minimum cycle time, the CPU spends the additional time of the scan cycle performing runtime diagnostics and/or processing communication requests.

In the event that the CPU does not complete the scan cycle in the specified minimum cycle time, the CPU completes the scan normally (including communication processing) and does not create any system reaction as a result of exceeding the minimum scan time. The following table defines the ranges and defaults for the cycle time monitoring functions:

Table 6-20 Range for the cycle time

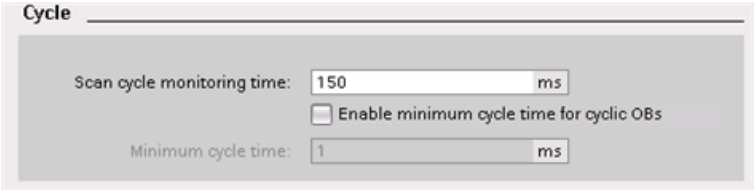
Cycle time	Range (ms)	Default
Maximum scan cycle time[1]	1 to 6000	150 ms
Minimum scan cycle time[2]	1 to maximum scan cycle time	Disabled

[1] The maximum scan cycle time is always enabled. Configure a cycle time between 1 ms to 6000 ms. The default is 150 ms.

[2] The minimum scan cycle time is optional, and is disabled by default. If required, configure a cycle time between 1 ms and the maximum scan cycle time.

You use the CPU properties in the Device configuration to configure the following parameters:

- Cycle: You can enter a maximum scan cycle monitoring time. You can also enable and enter a minimum scan cycle time.



- Communication load: You can configure a percentage of the time to be dedicated for communication tasks.

NOTE

Communication priority

Communication tasks have a priority of 1. Because 1 is the lowest priority, other CPU events can interrupt communication processing. Interruptions from other events can negatively affect communication processing during the scan cycle. You can adjust the "Cycle load due to communication" percentage to increase the portion of the scan cycle dedicated to communication processing.

For more information about the scan cycle, see Monitoring and configuring the cycle time (Page 81)

6.1.5 CPU memory

The CPU provides the following memory areas to store the user program, data, and configuration:

- Load memory is non-volatile storage for the user program, data and configuration. When you download a project to the CPU, the CPU first stores the program in the Load memory area. This area is located either in a SIMATIC memory card (if present) or in the CPU. The CPU maintains this non-volatile memory area through a power loss. The memory card supports a larger storage space than that built-in to the CPU.
- Work memory is volatile storage for some elements of the user project while executing the user program. The CPU copies some elements of the project from load memory into work memory. This volatile area is lost when power is removed and is restored by the CPU when power is restored.
- Retentive memory is non-volatile storage for a limited quantity of work memory values. The CPU uses the retentive memory area to store the values of selected user memory locations during power loss. When a power down or power loss occurs, the CPU restores these retentive values upon power up.

The size of the user program, data, and configuration is limited by the available load memory and work memory in the CPU.

To display the memory usage for a compiled program block, right-click the block in the "Program blocks" folder in the STEP 7 project tree and select "Properties" from the context menu. The Compilation properties display the load memory and work memory for the compiled block.

To display the memory usage for the online CPU, double-click "Online and diagnostics" in STEP 7, expand "Diagnostics", and select "Memory".

Retentive memory

You can avoid data loss after power failure by marking certain data as retentive. The CPU allows you to configure the following data as retentive:

- Bit memory (M): You can define the size of retentive memory for bit memory in the PLC tag table or in the assignment list. Retentive bit memory always starts at MB0 and runs consecutively up through a specified number of bytes. Specify this value from the PLC tag table or in the assignment list by clicking the "Retain" toolbar icon. Enter the number of M bytes to retain starting at MB0.

  Note: You can display an assignment list for bit memory (M) by selecting the CPU in the project tree and selecting the **Tools > Assignment list** menu command.
- Tags of a function block (FB): If an FB is of type "Optimized block access", then the interface editor for this FB includes a "Retain" column. In this column, you can select either "Retain", "Non-retain", or "Set in IDB" individually for each tag. When you place such an FB in the program, the instance DB that corresponds to the FB includes this "Retain" column as well. You can only change the retentive state of a tag from within the instance DB interface editor if you selected "Set in IDB" (Set in instance data block) in the Retain selection for the tag in the optimized FB.

  If an FB is **not** of type "Optimized block access", then the interface editor for this FB does not include a "Retain" column. When you place such an FB in the program, the instance DB that corresponds to the FB does, however, include a "Retain" column that is available for edit. In this case, selecting the "Retain" option for any tag results in the selection of **all** tags. Similarly, deselecting the option for any tag results in the deselection of **all** tags.

  To view or modify whether an FB is optimized, open the properties of the FB and select the attributes.

- Tags of a global data block: If you select "Optimized block access" for the attributes in the properties of the data block, you can set each tag to be retentive or not. If you do not select "Optimized block access", then all of the data block tags have the same state. The tags are either all retentive or all non-retentive.

The technical specifications for the CPUs state the retentive data allocation. The STEP 7 project version can alter the amount of retentive memory. From the PLC tag table in STEP 7 or the assignment list, click the "Retain" toolbar icon to see how much memory is available.

6.1.5.1 Notes about retentive memory

NOTE

Downloading a program does not clear or make any changes to existing values in retentive memory. If you want to clear retentive memory before a download, then reset your CPU to factory settings prior to downloading the program.

NOTE

When power failure occurs, the CPU switches off power to all signal modules. This ensures that the CPU has sufficient power to save retentive data to non-volatile memory.

6.1.5.2 System and clock memory

Use the CPU properties to enable bytes for "system memory" and "clock memory". Your program logic can reference the individual bits of these functions by their tag names.

The CPU initializes these bytes on the transition from STOP mode to STARTUP mode. The bits of the clock memory change synchronously to the CPU clock throughout the STARTUP and RUN modes.

WARNING

Risks with overwriting the system memory or clock memory bits

Overwriting the system memory or clock memory bits can corrupt the data in these functions and cause your user program to operate incorrectly. Because both the clock memory and system memory are unreserved in M memory, instructions or communications can write to these locations and corrupt the data.

Avoid writing data to these locations to ensure the proper operation of these functions, and always implement an emergency stop circuit for your process or machine.

Incorrect program operation can cause damage to equipment, severe injury, or death.

System memory

You can assign one byte in M memory for system memory. The byte of system memory provides the following four bits that can be referenced by your user program by the following tag names:

- First cycle: (Tag name "FirstScan") bit is set to1 for the duration of the first scan after the startup OB finishes. (After the execution of the first scan, the "first scan" bit is set to 0.)
- Diagnostics status changed: (Tag name: "DiagStatusUpdate") is set to 1 for one scan after the CPU logs a diagnostic event. Because the CPU does not set the "DiagStatusUpdate" bit until the end of the first execution of the program cycle OBs, your user program cannot detect if there has been a diagnostic change either during the execution of the startup OBs or the first execution of the program cycle OBs.
- Always 1 (high): (Tag name "AlwaysTRUE") bit is always set to 1.
- Always 0 (low): (Tag name "AlwaysFALSE") bit is always set to 0.

System memory bits have specific meanings, as shown in the table below:

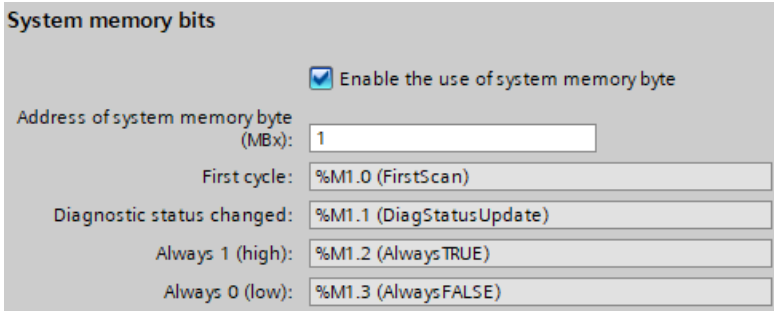


Table 6-21 System memory

7	6	5	4	3	2	1	0
Reserved Value 0				Always off Value 0	Always on Value 1	Diagnostic status indicator • 1: Change • 0: No change	First scan indicator • 1: First scan after startup • 0: Not first scan

Clock memory

You can assign one byte in M memory for clock memory. Each bit of the byte configured as clock memory generates a square wave pulse on the corresponding M memory bit. The byte of clock memory provides 8 different frequencies, from 0.5 Hz (slow) to 10 Hz (fast). You can use these bits as control bits, especially when combined with edge instructions, to trigger actions in the user program on a cyclic basis.

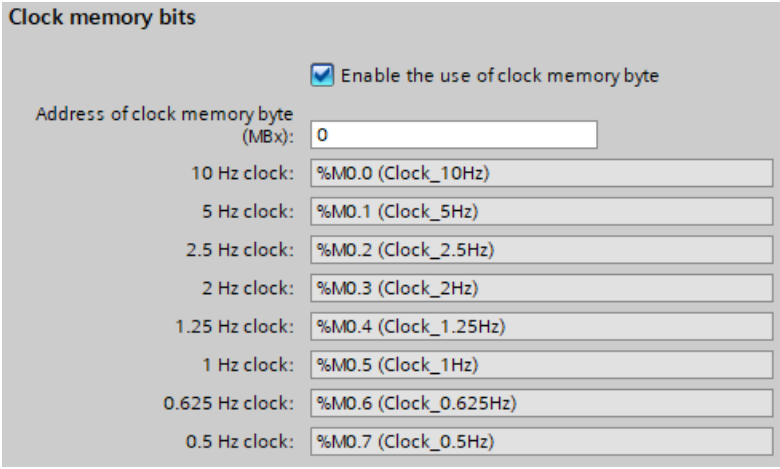


Table 6-22 Clock memory

Bit number	7	6	5	4	3	2	1	0
Period (s)	2.0	1.6	1.0	0.8	0.5	0.4	0.2	0.1
Frequency (Hz)	0.5	0.625	1	1.25	2	2.5	5	10

Because clock memory runs asynchronously to the CPU cycle, the status of the clock memory can change several times during a long cycle.

6.1.6 Diagnostics buffer

The CPU supports a diagnostics buffer that contains an entry for each diagnostic event. Each entry includes a date and time the event occurred, an event category, and an event description. The entries are displayed in chronological order, with the most recent event at the top. When the log is full, a new event replaces the oldest event in the log. If the CPU loses power, the diagnostics buffer retains the 50 most recent diagnostic events.

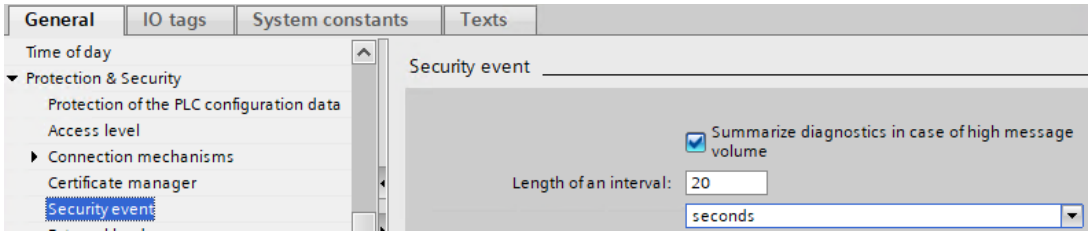
The following types of events are recorded in the diagnostics buffer:

- Each system diagnostic event; for example, CPU errors and module errors
- Each state change of the CPU (each power up, each transition to STOP, each transition to RUN)

To access the diagnostics buffer (Page 1062), you must be online. From the "Online & diagnostics" view, locate the diagnostics buffer under "Diagnostics > Diagnostics buffer".

Reducing the number of security diagnostic events

Some security events generate repeated entries in the diagnostics buffer. These messages can fill up the diagnostics buffer and potentially obscure other event messages. You can configure the PLC to limit the number of diagnostic messages from security events. You make selections in the device configuration of the CPU based on the time interval in which you want to suppress recurring messages:



If you choose to summarize security events within a time interval, you have the choice of setting a time interval in seconds, minutes, or hours, and a numerical value in the range 1 .. 255.

If you choose to restrict security events, you will be restricting these types of events:

- Going online with the correct or incorrect password
- Manipulated communications data detected
- Manipulated data detected on memory card
- Manipulated firmware update file detected
- Changed protection level (access protection) downloaded to the CPU
- Password legitimization restricted or enabled (by instruction or CPU display)
- Online access denied due to the possible number of simultaneous access attempts being exceeded
- Timeout when an existing online connection is inactive
- Logging in to the Web server with the correct or incorrect password
- Creating a backup of the CPU
- Restoring the CPU configuration

6.1.7 Time of day clock

The CPU supports a time-of-day clock. A super-capacitor supplies the energy required to keep the clock running during times when the CPU is powered down. The super-capacitor charges while the CPU has power. After the CPU has been powered up at least 24 hours, then the super-capacitor has sufficient charge to keep the clock running for typically 20 days.

STEP 7 sets the time-of-day clock to system time, which has a default value out of the box or following a factory reset. To utilize the time-of-day clock, you must set it. Timestamps such as those for diagnostics buffer entries, data log files, and data log entries, are based on the system time. You set the time of day from the "Set time of day" function (Page 1054) in the "Online & diagnostics" view of the online CPU. STEP 7 then calculates the system time from the time you set plus or minus the Windows operating system offset from UTC (Coordinated Universal Time). Setting the time of day to the current local time produces a system time of UTC if your Windows operating system settings for time zone and daylight savings time correspond to your locale.

WARNING

Risk of attacker accessing your networks through open interfaces

If an attacker can access your networks through open interfaces, such as software like STEP 7, the SIMATIC Automation Tool, or through an HMI, the attacker can possibly disrupt control of your process by shifting the CPU system time.

The CPU supports "time of day" interrupts and clock instructions that depend upon accurate CPU system time. You must restrict access to the CPU by enabling access control and disabling the "Anonymous" user. Failure to do so can cause a security breach that allows an unknown user to disrupt control of your process by shifting the CPU system time.

Disruptions to process control can possibly cause death, severe injury, or property damage.

For security information and recommendations, see the "Operational Guidelines" white paper on the Siemens Industrial Cybersecurity Website.

STEP 7 includes instructions (Page 295) to read and write the system time (RD_SYS_T and WR_SYS_T), to read the local time (RD_LOC_T), and to set the time zone (SET_TIMEZONE). The RD_LOC_T instruction calculates local time using the time zone and daylight saving time offsets that you set in the "Time of day" configuration in the general properties of the CPU (Page 136). These settings enable you to set your time zone for local time, optionally enable daylight saving time, and specify the start and end dates and times for daylight saving time. You can also use the SET_TIMEZONE instructions to configure these settings.

NOTE

Time zone differences

If you set the time of day clock and the time zone of your programming device is different from the time zone you configured in the device configuration for your CPU (Page 136), then you might see unexpected timestamps for items such as the following:

- Diagnostic buffer entries
- Data log files
- Entries in data logs

6.1.8 Configuring the outputs on a RUN-to-STOP transition

You can configure the behavior of the digital and analog outputs when the CPU is in STOP mode. For any output of a CPU, SB or SM, you can set the outputs to either freeze the value or use a substitute value:

- Substituting a specified output value (default): You enter a substitute value for each output (channel) of that CPU, SB, or SM device.
  The default substitute value for digital output channels is OFF, and the default substitute value for analog output channels is 0.
- Freezing the outputs to remain in last state: The outputs retain their current value at the time of the transition from RUN to STOP. After power up, the outputs are set to the default substitute value.

You configure the behavior of the outputs in Device Configuration. Select the individual devices and use the "Properties" tab to configure the outputs for each device.

NOTE

Some distributed I/O modules offer additional settings for the reaction to CPU stop mode. Select from the list of choices in Device Configuration for those modules.

When the CPU changes from RUN to STOP, the CPU retains the process image and writes the appropriate values for both the digital and analog outputs, based upon the configuration.

6.2 Data storage, memory areas, I/O, and addressing

6.2.1 Accessing the data of the CPU

STEP 7 facilitates symbolic programming. You can create symbolic names or "tags" for I/O and memory. To use these tags in your user program, enter the tag name for the instruction parameter.

The CPU provides several options for storing data:

- Global memory: The CPU provides a variety of specialized memory areas, including inputs (I), outputs (Q) and memory (M). This memory is accessible by all code blocks without restriction.
- PLC tag table: You can enter symbolic names in the STEP 7 PLC tag table for specific memory locations. These tags are global to the STEP 7 program and allow programming with names that are meaningful for your application.
- Data block (DB): You can include DBs in your user program to store data for the code blocks. The data stored persists when the execution of the associated code block comes to an end. A "global" DB stores data that can be used by all code blocks, while an instance DB stores data for a specific FB and is structured by the parameters for the FB.
- Temp memory: Whenever the program calls a code block, the CPU allocates temporary, or local, memory (L) to be used during the execution of the block. When the execution of the code block finishes, the CPU reallocates the local memory for the execution of other code blocks.

Each memory location has a unique address. Your user program uses these addresses to access the information in the memory location. References to the input (I) or output (Q) memory areas, such as I0.3 or Q1.7, access the process image. To immediately access the physical input or output, append the reference with ":P" (such as I0.3:P, Q1.7:P, or "Stop:P").

You can force values (Page 1070) for some memory areas. Some memory areas are retentive (Page 83) or optionally retentive.

Table 6-23 Memory areas

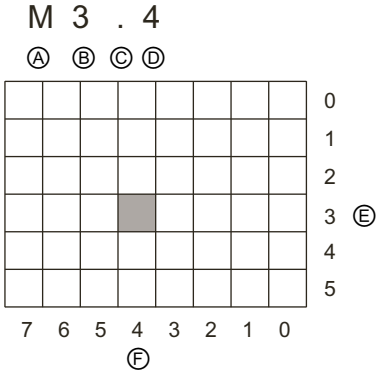
Memory area	Description	Force	Retentive
I Process image input I_:P [1] (Physical input)	Copied from physical inputs at the beginning of the scan cycle	No	No
	Immediate read of the physical input points on the CPU, SB, and SM	Yes	No
Q Process image output Q_:P [1] (Physical output)	Copied to physical outputs at the beginning of the scan cycle	No	No
	Immediate write to the physical output points on the CPU, SB, and SM	Yes	No
M Bit memory	Control and data memory	No	Yes (optional)
DB Data block	Data memory and also parameter memory for FBs	No	Yes (optional)
Temp memory	Temporary data for a block local to that block	No	No

[1] To immediately access (read or write) the physical inputs and physical outputs, append a ":P" to the address or tag (such as I0.3:P, Q1.7:P, or "Stop:P").

Each memory location has a unique address. Your user program uses these addresses to access the information in the memory location. The absolute address consists of the following elements:

- Memory area identifier (such as I, Q, or M)
- Size of the data to be accessed ("B' for Byte, "W" for Word, or "D" for DWord)
- Starting address of the data (such as byte 3 or word 3)

When accessing a bit in the address for a Boolean value, enter the memory area, the byte location, and the bit location for the data (such as I0.0, Q0.1, or M3.4).



A	Memory area identifier	E	Bytes of the memory area
B	Byte address: byte 3	F	Bits of the selected byte
C	Separator ("byte.bit")		
D	Bit location of the byte (bit 4 of 8)		

In the example, the memory area and byte address (M = bit memory area, and 3 = Byte 3) are followed by a period (".") to separate the bit address (bit 4).

When using symbolic names for data (Page 89), you typically create tags either in the PLC tag table, a data block, or in the interface of an OB, FC, or FB. These tags include a name, data type, offset, and comment. Additionally, in a data block, you can specify a start value. You can use these tags when programming by entering the tag name at the instruction parameter.

Optionally you can enter the absolute operand (memory area, size and offset) at the instruction parameter. The examples in the following sections show how to enter absolute operands. The % character is inserted automatically in front of the absolute operand by the program editor. You can toggle the view in the program editor to one of these: symbolic, symbolic and absolute, or absolute.

I (process image input): The CPU samples the peripheral (physical) input points just prior to the cyclic OB execution of each scan cycle (Page 61) and writes these values to the input process image. You can access the input process image as bits, bytes, words, or double words. Both read and write access is permitted, but typically, process image inputs are only read.

Table 6-24 Absolute addressing for I memory

Bit	I[byte address].[bit address]	I0.1
Byte, Word, or Double Word	I[size][starting byte address]	IB4, IW5, or ID12

By appending a ":P" to the address, you can immediately read the digital and analog inputs of the CPU, SB, SM or distributed module. The difference between an access using I_:P instead of I is that the data comes directly from the points being accessed rather than from the input process image. This I_:P access is referred to as an "immediate read" access because the data is retrieved immediately from the source instead of from a copy that was made the last time the input process image was updated.

Because the physical input points receive their values directly from the field devices connected to these points, you cannot write to these points. I_:P accesses are read-only, as opposed to I accesses which can be read or written to.

I_:P accesses are also restricted to the size of inputs supported by a single CPU, SB, or SM, rounded up to the nearest byte. For example, if the inputs of a 2 DI / 2 DQ SB are configured to start at I4.0, then the input points can be accessed as I4.0:P and I4.1:P or as IB4:P. Accesses to I4.2:P through I4.7:P are not rejected, but make no sense since these points are not used. Accesses to IW4:P and ID4:P are prohibited since they exceed the byte offset associated with the SB.

Accesses using I_:P do not affect the corresponding value stored in the input process image.

Table 6-25 Absolute addressing for I memory (immediate)

Bit	I[byte address].[bit address]:P	I0.1:P
Byte, Word, or Double word	I[size][starting byte address]:P	IB4:P, IW5:P, or ID12:P

Q (process image output): The CPU copies the values stored in the output process image to the physical output points just prior to the cyclic OB execution of each scan cycle. You can access the output process image in bits, bytes, words, or double words. Both read and write access is permitted for process image outputs.

Table 6-26 Absolute addressing for Q memory

Bit	Q[byte address].[bit address]	Q1.1
Byte, Word, or Double word	Q[size][starting byte address]	QB5, QW10, QD40

By appending a ":P" to the address, you can immediately write to the physical digital and analog outputs of the CPU, SB, SM or distributed module. The difference between an access

using Q_:P instead of Q is that the data goes directly to the points being accessed in addition to the output process image (writes to both places). This Q_:P access is sometimes referred to as an "immediate write" access because the data is sent immediately to the target point; the target point does not have to wait for the next update from the output process image.

Because the physical output points directly control field devices that are connected to these points, reading from these points is prohibited. That is, Q_:P accesses are write-only, as opposed to Q accesses which can be read or write.

Q_:P accesses are also restricted to the size of outputs supported by a single CPU, SB, or SM, rounded up to the nearest byte. For example, if the outputs of a 2 DI / 2 DQ SB are configured to start at Q4.0, then the output points can be accessed as Q4.0:P and Q4.1:P or as QB4:P. Accesses to Q4.2:P through Q4.7:P are not rejected, but make no sense since these points are not used. Accesses to QW4:P and QD4:P are prohibited since they exceed the byte offset associated with the SB.

Accesses using Q_:P affect both the physical output as well as the corresponding value stored in the output process image.

Table 6-27 Absolute addressing for Q memory (immediate)

Bit	Q[byte address].[bit address]:P	Q1.1:P
Byte, Word, or Double word	Q[size][starting byte address]:P	QB5:P, QW10:P or QD40:P

M (bit memory area): Use the bit memory area (M memory) for both control relays and data to store the intermediate status of an operation or other control information. You can access the bit memory area in bits, bytes, words, or double words. Both read and write access is permitted for M memory.

Table 6-28 Absolute addressing for M memory

Bit	M[byte address].[bit address]	M26.7
Byte, Word, or Double Word	M[size][starting byte address]	MB20, MW30, MD50

Temp (temporary memory): The CPU allocates the temp memory on an as-needed basis. The CPU allocates the temp memory for the code block and initializes the memory locations to 0 at the time when it starts the code block (for an OB) or calls the code block (for an FC or FB).

Temp memory is similar to M memory with one major exception: M memory has a "global" scope, and temp memory has a "local" scope:

- M memory: Any OB, FC, or FB can access the data in M memory, meaning that the data is available globally for all of the elements of the user program.
- Temp memory: The CPU restricts access to the data in temp memory to the OB, FC, or FB that created or declared the temp memory location. Temp memory locations remain local and different code blocks do not share temp memory, even when the code block calls another code block. For example: When an OB calls an FC, the FC cannot access the temp memory of the OB that called it.

The CPU provides temp (local) memory for each OB priority level:

- 16 Kbytes for startup and program cycle, including associated FBs and FCs
- 6 Kbytes for each additional interrupt event thread, including associated FBs and FCs

You access temp memory by symbolic addressing only.

You can find out the amount of temp (local) memory that the blocks in your program use through the call structure in STEP 7. From the project tree select Program info and then select the Call structure tab. You will see all of the OBs in your program and you can drill down to see the blocks that they call. For each block, you can see the local data allocation. You can also access the Call structure display from the STEP 7 **Tools > Call structure** menu command.

DB (data block): Use the DB memory for storing various types of data, including intermediate status of an operation or other control information parameters for FBs, and data structures required for many instructions such as timers and counters. You can access data block memory in bits, bytes, words, or double words. Both read and write access is permitted for read/write data blocks. Only read access is permitted for read-only data blocks.

Table 6-29 Absolute addressing for DB memory

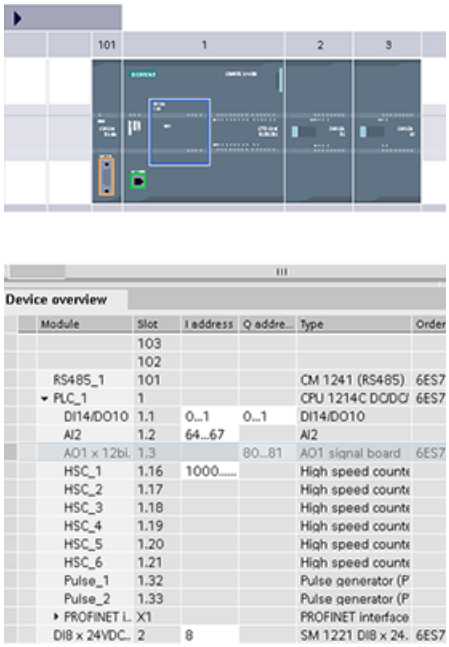
Bit	DB[data block number].DBX[byte address].[bit address]	DB1.DBX2.3
Byte, Word, or Double Word	DB[data block number].DB [size][starting byte address]	DB1.DBB4, DB10.DBW2, DB20.DBD8

NOTE

When you specify an absolute address in LAD or FBD, STEP 7 precedes this address with a "%" character to indicate that it is an absolute address. While programming, you can enter an absolute address either with or without the "%" character (for example %I0.0 or I.0). If omitted, STEP 7 supplies the "%" character.

In SCL, you must enter the "%" before the address to indicate that it is an absolute address. Without the "%", STEP 7 generates an undefined tag error at compile time

Configuring the I/O in the CPU and I/O modules



Figure

When you add a CPU and I/O modules to your device configuration, STEP 7 automatically assigns I and Q addresses. You can change the default addressing by selecting the address field in the device configuration and entering new numbers.

- STEP 7 assigns digital inputs and outputs in groups of 8 points (1 byte), whether the module uses all the points or not.
- STEP 7 allocates analog inputs and outputs in groups of 2, where each analog point occupies 2 bytes (16 bits).

The figure shows an example of a CPU 1214C with two SMs and one SB. In this example, you could change the address of the DI8 module to 2 instead of 8. The tool assists you by changing address ranges that are the wrong size or conflict with other addresses.

6.3 Processing of analog values

General purpose analog signal modules provide input signals or expect output values that represent either a voltage range or a current range. These ranges are ±10 V, ±5 V, ±2.5 V, or 0 - 20 mA. The values returned by the modules are integer values where 0 to 27648 represents the rated range for current, and -27648 to 27648 for voltage. Anything outside the range represents either an overflow or underflow. See the tables for analog input representation (Page 1195) and analog output representation (Page 1196) for details about the types of out-of-range values.

In your control program, you probably need to use these values in engineering units, for example to represent a volume, temperature, weight or other quantitative value. To do this for an analog input, you must first normalize the analog value to a real (floating point) value from 0.0 to 1.0. Then you must scale it to the minimum and maximum values of the engineering units that it represents. For values that are in engineering units that you need to convert to an analog output value, you first normalize the value in engineering units to a value between 0.0 and 1.0, and then scale it between 0 and 27648 or -27648 to 27648, depending on the range of the analog module. STEP 7 provides the NORM_X and SCALE_X instructions (Page 263) for this purpose. You can also use the CALCULATE instruction (Page 219) to scale the analog values.

Example: analog value processing

Consider, for example, an analog input that has a current range of 0 - 20 mA. The analog input module returns values in the range 0 to 27648 for measured values. For this example, consider that you are using this analog input value to measure a temperature range from 50 °C to 100 °C. A few sample values would have the following meanings:

Analog input value	Engineering units
0	50 °C
6192	62.5 °C
12384	75 °C
18576	87.5 °C
27648	100 °C

The calculation for determining engineering units from the analog input value in this example is as follows:

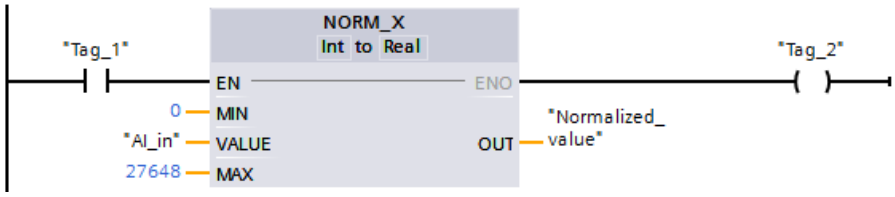
Engineering units value = 50 + (Analog input value) * (100 - 50) / (27648 - 0)

For the general case, the equation would be:

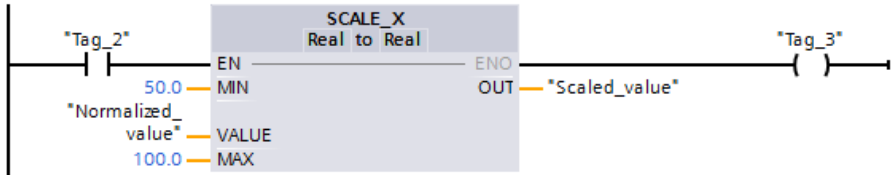
Engineering units value = (Low range of engineering units) +
(Analog input value) *
(High range of engineering units - Low range of engineering units) /
(Maximum analog input range - Minimum analog input range)

In PLC applications, the typical method is to normalize the analog input value to a floating point value between 0.0 and 1.0. Then, you would scale the resulting value to a floating point value in the range of your engineering units. For simplicity, the following LAD instructions use constant values for the ranges; you might actually choose to use tags:

Network 1



Network 2



6.4 Data types

Data types are used to specify both the size of a data element as well as how the data are to be interpreted. Each instruction parameter supports at least one data type, and some parameters support multiple data types. Hold the cursor over the parameter field of an instruction to see which data types are supported for a given parameter.

A formal parameter is the identifier on an instruction that marks the location of data to be used by that instruction (example: the IN1 input of an ADD instruction). An actual parameter is the memory location (preceded by a "%" character) or constant containing the data to be used by the instruction (example %MD400 "Number_of_Widgets"). The data type of the actual parameter specified by you must match one of the supported data types of the formal parameter specified by the instruction.

When specifying an actual parameter, you must specify either a tag (symbol) or an absolute (direct) memory address. Tags associate a symbolic name (tag name) with a data type, memory area, memory offset, and comment, and can be created either in the PLC tags editor or in the Interface editor for a block (OB, FC, FB and DB). If you enter an absolute address that has no associated tag, you must use an appropriate size that matches a supported data type, and a default tag will be created upon entry.

All data types except String, Struct, Array, and DTL are available in the PLC tags editor and the block Interface editors. String, Struct, Array, and DTL are available only in the block Interface editors. You can also enter a constant value for many of the input parameters.

- Bit and Bit sequences (Page 96): Bool (Boolean or bit value), Byte (8-bit byte value), Word (16-bit value), DWord (32-bit double word value)
- Integer (Page 97)
  - USInt (unsigned 8-bit integer), SInt (signed 8-bit integer),
  - UInt (unsigned 16-bit integer), Int (signed 16-bit integer)
  - UDInt (unsigned 32-bit integer), DInt (signed 32-bit integer)
- Floating-point Real (Page 97): Real (32-bit Real or floating-point value), LReal (64-bit Real or floating-point value)
- Time and Date (Page 98): Time (32-bit IEC time value), Date (16-bit date value), TOD (32-bit time-of-day value), DTL (12-byte date-and-time structure)
- Character and String (Page 99): Char (8-bit single character), String (variable-length string of up to 254 characters)
- Array (Page 101)

- Data structure (Page 102): Struct
- PLC data type (Page 102)
- Variant data type (Page 103)

Although not available as data types, the following BCD numeric format is supported by the conversion instructions:

Table 6-30 Size and range of the BCD format

Format	Size (bits)	Numeric Range	Constant Entry Examples
BCD16	16	-999 to 999	123, -123
BCD32	32	-9999999 to 9999999	1234567, -1234567

6.4.1 Bool, Byte, Word, and DWord data types

Table 6-31 Bit and bit sequence data types

Data type	Bit size	Number type	Number range	Constant examples	Address examples
Bool	1	Boolean	FALSE or TRUE	TRUE	I1.0 Q0.1 M50.7 DB1.DBX2.3 Tag_name
		Binary	2#0 or 2#1	2#0	
		Unsigned integer	0 or 1	1	
		Octal	8#0 or 8#1	8#1	
		Hexadecimal	16#0 or 16#1	16#1	
Byte	8	Binary	2#0 to 2#1111_1111	2#1000_1001	IB2 MB10 DB1.DBB4 Tag_name
		Unsigned integer	0 to 255	15	
		Signed integer	-128 to 127	-63	
		Octal	8#0 to 8#377	8#17	
		Hexadecimal	B#16#0 to B#16#FF, 16#0 to 16#FF	B#16#F, 16#F	
Word	16	Binary	2#0 to 2#1111_1111_1111_1111	2#1101_0010_1001_0110	MW10 DB1.DBW2 Tag_name
		Unsigned integer	0 to 65535	61680	
		Signed integer	-32768 to 32767	72	
		Octal	8#0 to 8#177_777	8#170_362	
		Hexadecimal	W#16#0 to W#16#FFFF, 16#0 to 16#FFFF	W#16#F1C0, 16#A67B	
DWord	32	Binary	2#0 to 2#1111_1111_1111_1111_1111-_1111_1111_1111	2#1101_0100_1111_111-0_1000_1100	MD10 DB1.DBD8 Tag_name
		Unsigned integer*	0 to 4_294_967_295	15_793_935	
		Signed integer*	-2_147_483_648 to 2_147_483_647	-400000	
		Octal	8#0 to 8#37_777_777_777	8#74_177_417	
		Hexadecimal	DW#16#0000_0000 to DW#16#FFFF_FFFF, 16#0000_0000 to 16#FFFF_FFFF	DW#16#20_F30A, 16#B_01F6	

* The underscore "_" is a thousands separator to enhance readability for numbers greater than eight digits.

6.4.2 Integer data types

Table 6-32 Integer data types (U = unsigned, S = short, D= double)

Data type	Bit size	Number Range	Constant examples	Address examples
USInt	8	0 to 255	78, 2#01001110	MB0, DB1.DBB4, Tag_name
SInt	8	-128 to 127	+50, 16#50	
UInt	16	0 to 65,535	65295, 0	MW2, DB1.DBW2, Tag_name
Int	16	-32,768 to 32,767	30000, +30000	
UDInt	32	0 to 4,294,967,295	4042322160	MD6, DB1.DBD8, Tag_name
DInt	32	-2,147,483,648 to 2,147,483,647	-2131754992	

6.4.3 Floating-point real data types

Real (or floating-point) numbers are represented as 32-bit single-precision numbers (Real), or 64-bit double-precision numbers (LReal) as described in the ANSI/IEEE 754-1985 standard. Single-precision floating-point numbers are accurate up to 6 significant digits and double-precision floating point numbers are accurate up to 15 significant digits. You can specify a maximum of 6 significant digits (Real) or 15 (LReal) when entering a floating-point constant to maintain precision.

Table 6-33 Floating-point real data types (L=Long)

Data type	Bit size	Number range	Constant Examples	Address examples
Real	32	-3.402823e+38 to -1.175 495e-38, ±0, +1.175 495e-38 to +3.402823e+38	123.456, -3.4, 1.0e-5	MD100, DB1.DBD8, Tag_name
LReal	64	-1.7976931348623158e+308 to -2.2250738585072014e-308, ±0, +2.2250738585072014e-308 to +1.7976931348623158e+308	12345.123456789e40, 1.2E+40	DB_name.var_name Rules: • No direct addressing support • Can be assigned in an OB, FB, or FC block interface table

NOTE

Considerations when using floating-point values

Calculations that involve a long series of values including very large and very small numbers can produce inaccurate results. This can occur if the numbers differ by 10 to the power of x, where x > 6 (), or 15 (). For example (): 100 000 000 + 1 = 100 000 000.

Avoid comparing floating-point numbers to exact values. Floating-point numbers are often estimations that are rounded to the nearest representable value. Numbers that are equal in practical terms might not be equal in binary representation in a computer. For this reason, use an acceptable range or tolerance for comparing floating-point values rather than comparing to an exact value.

6.4.4 Time and Date data types

Table 6-34 Time and date data types

Data type	Size	Range	Constant Entry Examples
Time	32 bits	T#-24d_20h_31m_23s_648ms to T#24d_20h_31m_23s_647ms Stored as: -2,147,483,648 ms to +2,147,483,647 ms	T#5m_30s T#1d_2h_15m_30s_45ms TIME#10d20h30m20s630ms 500h10000ms 10d20h30m20s630ms
Date	16 bits	D#1990-1-1 to D#2168-12-31	D#2009-12-31 DATE#2009-12-31 2009-12-31
Time_of_Day	32 bits	TOD#0:0:0.0 to TOD#23:59:59.999	TOD#10:20:30.400 TIME_OF_DAY#10:20:30.400 23:10:1
DTL (Date and Time Long)	12 bytes	Min.: DTL#1970-01-01-00:00:00.0 Max.: DTL#2262-04-11-23:47:16.854775807	DTL#2008-12-16-20:30:20.250

Time

TIME data is stored as a signed double integer interpreted as milliseconds. The editor format can use information for day (d), hours (h), minutes (m), seconds (s) and milliseconds (ms). It is not necessary to specify all units of time. For example T#5h10s and 500h are valid. The combined value of all specified unit values cannot exceed the upper or lower limits in milliseconds for the Time data type (-2,147,483,648 ms to +2,147,483,647 ms).

Date

DATE data is stored as an unsigned integer value which is interpreted as the number of days added to the base date 01/01/1990, to obtain the specified date. The editor format must specify a year, month and day.

TOD

TOD (TIME_OF_DAY) data is stored as an unsigned double integer which is interpreted as the number of milliseconds since midnight for the specified time of day (Midnight = 0 ms). The hour (24hr/day), minute, and second must be specified. The fractional second specification is optional.

DTL

DTL (Date and Time Long) data type uses a12 byte structure that saves information on date and time. You can define DTL data in either the Temp memory of a block or in a DB. A value for all components must be entered in the "Start value" column of the DB editor.

Table 6-35 Size and range for DTL

Length (bytes)	Format	Value range	Example of value input
12	Clock and calendar Year-Month-Day:Hour: Minute: Second.Nanoseconds	Min.: DTL#1970-01-01-00:00:00.0 Max.: DTL#2262-04-11-23:47:16.854775807[1]	DTL#2008-12-16-20: 30:20.250

[1] STEP 7 allows entry of values greater than #2262-04-11-23:47:16.854775807. This value is the recommended max value because values greater than this value can cause conversion or calculation errors.

Each component of the DTL contains a different data type and range of values. The data type of a specified value must match the data type of the corresponding components.

Table 6-36 Elements of the DTL structure

Byte	Component	Data type	Value range
0	Year	UINT	1970 to 2262
1			
2	Month	USINT	1 to 12
3	Day	USINT	1 to 31
4	Weekday [1]	USINT	1(Sunday) to 7(Saturday) [1]
5	Hour	USINT	0 to 23
6	Minute	USINT	0 to 59
7	Second	USINT	0 to 59
8	Nanoseconds	UDINT	0 to 999 999 999
9			
10			
11			

[1] The format Year-Month-Day:Hour:Minute: Second.Nanosecond does not include the weekday.

6.4.5 Character and String data types

Table 6-37 Character and String data types

Data type	Size	Range	Constant Entry Examples
Char	8 bits	16#00 to 16#FF	'A', 't', '@', 'ä', '∑'
WChar	16 bits	16#0000 to 16#FFFF	'A', 't', '@', 'ä', '∑', Asian characters, Cyrillic characters, and others
String	n+ 2 bytes	n = (0 to 254 bytes)	"ABC"
WString	n+ 2 words	n = (0 to 65534 words)	"ä123@XYZ.COM"

Char and WChar

A Char occupies one byte in memory and stores a single character coded in ASCII format, including the extended ASCII character codes. A WChar occupies one word in memory and can contain any double-byte character representation.

The editor syntax uses a single quote character before and after the character. You can use visible characters and control characters.

String and WString

The CPU supports the String data type for storing a sequence of single-byte characters. The String data type contains a total character count (number of characters in the string) and the current character count. The String type provides up to 256 bytes for storing the maximum total character count (1 byte), the current character count (1 byte), and up to 254 bytes in the string. Each byte in a String data type can be any value from 16#00 - 16#FF.

The WString data type provides for longer strings of one-word (double-byte) values. The first word contains the maximum total character count; the next word contains the total character count, and the following string can contain up to 65534 words. Each word in a WString data type can be any value from 16#0000 - 16#FFFF.

You can use literal strings (constants) for instruction parameters of type IN using single quotes. For example, ‘ABC’ is a three-character string that could be used as input for parameter IN of the S_CONV instruction. You can also create string variables by selecting data type "String" or "WString" in the block interface editors for OB, FC, FB, and DB. You cannot create a string in the PLC tags editor.

You can specify the maximum string size in bytes (String) or words (WString) by entering square brackets after the keyword "String" or "WString" after you select one of those data types from the data type drop-down list. For example, "MyString String[10]" would specify a 10-byte maximum size for MyString. If you do not include the square brackets with a maximum size, then 254 is assumed for a string and 65534 for a WString. "MyWString WString[1000]" would specify a 1000-word WString.

The following example defines a String with maximum character count of 10 and current character count of 3. This means the String currently contains 3 one-byte characters, but could be expanded to contain up to 10 one-byte characters.

Table 6-38 Example of a String data type

Total Character Count	Current Character Count	Character 1	Character 2	Character 3	...	Character 10
10	3	'C' (16#43)	'A' (16#41)	'T' (16#54)	...	-
Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	...	Byte 11

The following example defines a WString with maximum character count of 500 and current character count of 300. This means the String currently contains 300 one-word characters, but could be expanded to contain up to 500 one-word characters.

Table 6-39 Example of a WString data type

Total Character Count	Current Character Count	Character 1	Characters 2 to 299	Character 300	...	Character 500
500	300	'ä' (16#0084)	ASCII character words	'M' (16#004D)	...	-
Word 0	Word 1	Word 2	Words 3 to 300	Word 301	...	Word 501

ASCII control characters can be used in Char, Wchar, String and WString data. The following table shows examples of control character syntax.

Table 6-40 Valid ASCII control characters

Control characters	ASCII Hex value (Char)	ASCII Hex value (WChar)	Control function	Examples
$L or $l	16#0A	16#000A	Line feed	'$LText', '$0AText'
$N or $n	16#0A and 16#0D	16#000A and 16#000D	Line break The new line shows two characters in the string.	'$NText', '$0A$0DText'
$P or $p	16#0C	16#000C	Form feed	'$PText', '$0CText'
$R or $r	16#0D	16#000D	Carriage return (CR)	'$RText','$0DText'
$T or $t	16#09	16#0009	Tab	'$TText', '$09Text'
$$	16#24	16#0024	Dollar sign	'100$$', '100$24'
$'	16#27	16#0027	Single quote	'$'Text$","$27Text$27'

6.4.6 Array data type

Arrays

You can create an array that contains multiple elements of the same data type. Arrays can be created in the block interface editors for OB, FC, FB, and DB. You cannot create an array in the PLC tags editor.

To create an array from the block interface editor, name the array and choose data type "Array [lo .. hi] of type", then edit "lo", "hi", and "type" as follows:

- lo - the starting (lowest) index for your array
- hi - the ending (highest) index for your array
- type - one of the data types, such as BOOL, SINT, UDINT

Table 6-41 ARRAY data type rules

Data Type	Array syntax		
ARRAY	Name [index1_min..index1_max, index2_min..index2_max] of <data type> • All array elements must be the same data type. • The index can be negative, but the lower limit must be less than or equal to the upper limit. • Arrays can have one to six dimensions. • Multi-dimensional index min..max declarations are separated by comma characters. • Nested arrays, or arrays of arrays, are not allowed. • The memory size of an array = (size of one element * total number of elements in array)		
	Array index	**Valid index data types**	**Array index rules**
	Constant or variable	USInt, SInt, UInt, Int, UDInt, DInt	• Value limits: -32768 to +32767 • Valid: Mixed constants and variables • Valid: Constant expressions • Not valid: Variable expressions

Example: array declarations	ARRAY[1..20] of REAL	One dimension, 20 elements
	ARRAY[-5..5] of INT	One dimension, 11 elements
	ARRAY[1..2, 3..4] of CHAR	Two dimensions, 4 elements
Example: array addresses	ARRAY1[0]	ARRAY1 element 0
	ARRAY2[1,2]	ARRAY2 element [1,2]
	ARRAY3[i,j]	If i =3 and j=4, then ARRAY3 element [3, 4] is addressed

6.4.7 Data structure data type

You can use the data type "Struct" to define a structure of data consisting of other data types. You can use a Struct data type to handle a group of related process data as a single data unit. You can create Structs in the data block editor or a block interface editor.

You can assemble arrays and structures into larger structures. For example, you can create a structure of structures that contain arrays. A structure can be nested up to eight levels deep.

6.4.8 PLC data type

The PLC data type editor lets you define data structures that you can use multiple times in your program. You create a PLC data type by opening the "PLC data types" branch of the project tree and double-clicking the "Add new data type" item. On the newly created PLC data type item, use two single-clicks to rename the default name and double-click to open the PLC data type editor.

You create a custom PLC data type structure using the same editing methods that are used in the data block editor. Add new rows for any data types that are necessary to create the data structure that you want.

If you create a new PLC data type, then the new PLC type name appears in the data type selector drop-down lists in the DB editor and code block interface editor.

You can potentially use PLC data types in the following ways:

- As a data type in a code block interface or in data blocks
- As a template for the creation of multiple global data blocks that use the same data structure
- As a data type for PLC tag declarations the I and Q memory areas of the CPU

For example, a PLC data type could be a recipe for mixing colors. You can then assign this PLC data type to multiple data blocks. You can adjust the variables within each data block to create a specific color.

6.4.9 Variant pointer data type

The data type Variant can point to variables of different data types or parameters. The Variant pointer can point to structures and individual structural components. The Variant pointer does not occupy any space in memory.

Table 6-42 Properties of the Variant pointer

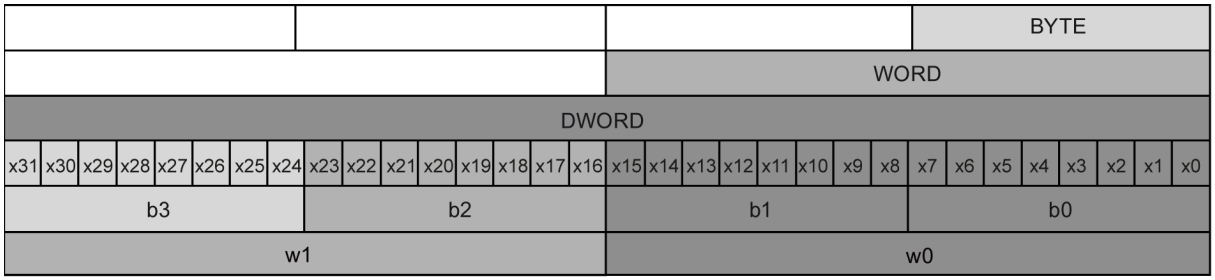
Length (Byte)	Representation	Format	Example entry
0	Symbolic	Operand	MyTag
		DB_name.Struct_name.element_name	MyDB.Struct1.pressure1
	Absolute	Operand	%MW10
		DB_number.Operand Type Length	P#DB10.DBX10.0 INT 12

6.4.10 Accessing a "slice" of a tagged data type

PLC tags and data block tags can be accessed at the bit, byte, or word level depending on their size. The syntax for accessing such a data slice is as follows:

- "<PLC tag name>".xn (bit access)
- "<PLC tag name>".bn (byte access)
- "<PLC tag name>".wn (word access)
- "<Data block name>".<tag name>.xn (bit access)
- "<Data block name>".<tag name>.bn (byte access)
- "<Data block name>".<tag name>.wn (word access)

A double word-sized tag can be accessed by bits 0 - 31, bytes 0 - 3, or word 0 - 1. A word-sized tag can be accessed by bits 0 - 15, bytes 0 - 1, or word 0. A byte-sized tag can be accessed by bits 0 - 7, or byte 0. Bit, byte, and word slices can be used anywhere that bits, bytes, or words are expected operands.

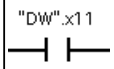
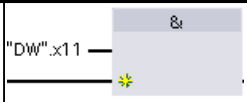
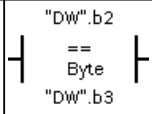
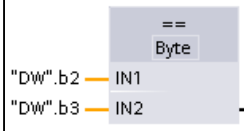
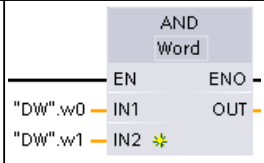
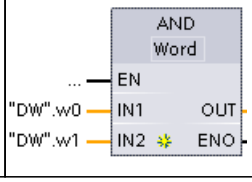


NOTE

Valid data types that can be accessed by slice are Byte, Char, Conn_Any, Date, DInt, DWord, Event_Any, Event_Att, Hw_Any, Hw_Device, HW_Interface, Hw_Io, Hw_Pwm, Hw_SubModule, Int, OB_Any, OB_Att, OB_Cyclic, OB_Delay, OB_WHINT, OB_PCYCLE, OB_STARTUP, OB_TIMEERROR, OB_Tod, Port, Rtm, SInt, Time, Time_Of_Day, UDInt, UInt, USInt, and Word. PLC Tags of type Real can be accessed by slice, but data block tags of type Real cannot.

Examples

In the PLC tag table, "DW" is a declared tag of type DWORD. The examples show bit, byte, and word slice access:

	LAD	FBD	SCL
Bit access			**IF "DW".x11 THEN** **...** **END_IF;**
Byte access			**IF "DW".b2 = "DW".b3 THEN** **...** **END_IF;**
Word access			**out:= "DW".w0 AND "DW".w1;**

6.4.11 Accessing a tag with an AT overlay

The AT tag overlay allows you to access an already-declared block tag with an overlaid declaration of a different data type. You can, for example, address the individual bits of a tag of a Byte, Word, or DWord data type with an Array of Bool. AT overlays are available for the following types of tags:

- Tags in a standard-access block
- Retentive tags in an optimized block

Declaration

To overlay a parameter, declare an additional parameter directly after the parameter that is to be overlaid and select the data type "AT". The editor creates the overlay, and you can then choose the data type, struct, or array that you wish to use for the overlay.

Example

This example shows the input parameters of a standard-access FB. An array of Booleans is an overlay for the byte tag B1:

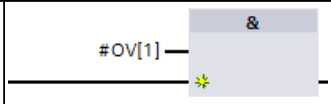
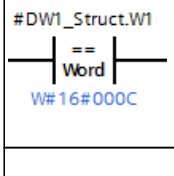
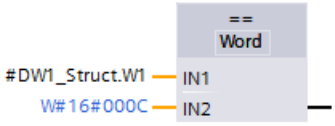
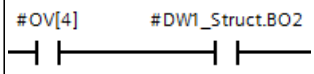
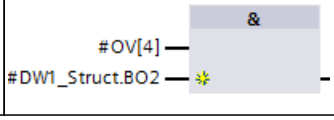
B1		Byte	0.0
OV	AT "B1"	Array[0..7] of Bool	0.0
OV[0]		Bool	0.0
OV[1]		Bool	0.1
OV[2]		Bool	0.2
OV[3]		Bool	0.3
OV[4]		Bool	0.4
OV[5]		Bool	0.5
OV[6]		Bool	0.6
OV[7]		Bool	0.7

Another example is a DWord tag overlaid with a Struct. The Struct includes a Word, Byte, and two Booleans:

DW1		DWord	2.0
DW1_Struct	AT "DW1"	Struct	2.0
W1		Word	0.0
B1		Byte	2.0
BO1		Bool	3.0
BO2		Bool	3.1

The Offset column of the block interface shows the location of the overlaid data types relative to the original tag.

You can address the overlay types directly in the program logic:

LAD	FBD	SCL
		**IF #OV[1] THEN** **...** **END_IF;**
		**IF #DW1_Struct.W1 = W#16#000C THEN** **...** **END_IF;**
		out1 := #DW1_Struct.B1;
		**IF #OV[4] AND #DW1_Struct.BO2 THEN** **...** **END_IF;**

Rules

- In FB and FC blocks with standard (not optimized) access, overlaying of tags is possible.
- In optimized FB and FC blocks, overlaying of tags is possible for any tags that are retentive.
- You can overlay parameters for all block types and all declaration sections.
- You can use an overlaid parameter like any other block parameter.

- You cannot overlay parameters of type VARIANT.
- The size of the overlaying parameter must be less than or equal to the size of the overlaid parameter.
- You must declare the overlaying variable immediately after the variable that it overlays and select the keyword "AT" as the initial data type selection.

6.5 Using a memory card

NOTE

The CPU supports only SIMATIC memory cards (Page 1263).

Before you copy any program to the memory card, delete any previously saved program from the memory card.

You can use a memory card in the following ways:

- As either a transfer card or as a program card
  Transfer cards and program cards contain the code blocks, data blocks, technology objects, and the device configuration. Transfer cards and program cards do **not** contain, for example, force tables, watch tables, or PLC tag tables.
  - Use a transfer card (Page 109) to copy a program to the internal load memory of the CPU without using STEP 7.
  - Use an empty transfer card to access a password-protected CPU when you have lost or forgotten the password (Page 119).
  - Use a program card (Page 112) as external load memory for the CPU.
- For downloading firmware updates (Page 117)
- To set or change the Protection of confidential PLC configuration data password (Page 115)

6.5.1 Inserting a memory card in the CPU

NOTICE

Risks associated with electrostatic discharge

Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable.

To protect the memory card and receptacle from electrostatic discharge, do the following:

- Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card.
- Store the memory card in a conductive container.

Receptacle or memory card malfunction can result in property damage.

Check that the memory card is not write-protected. Slide the protection switch away from the "Lock" position.

If you insert a write-protected memory card into the CPU, STEP 7 displays a diagnostic message on the next power up, alerting you to that fact. The CPU powers up without failure, but instructions involving recipes or data logs, for example, return errors if the card is write-protected.

WARNING

Risks when inserting a memory card

If you insert a memory card of any type into a running CPU, the CPU goes immediately to STOP mode, which can cause process disruption.

Before inserting or removing a memory card, always ensure that the CPU is not actively controlling a machine or process. Always install an emergency stop circuit for your application or process.

Process disruption can result in death or severe personal injury.

NOTE

Do not insert V3.0 program transfer cards into S7-1200 V4.x CPUs.

Version 3.0 program transfer cards are not compatible with version S7-1200 V4.x CPUs. Inserting a memory card that contains a V3.0 program causes a CPU error.

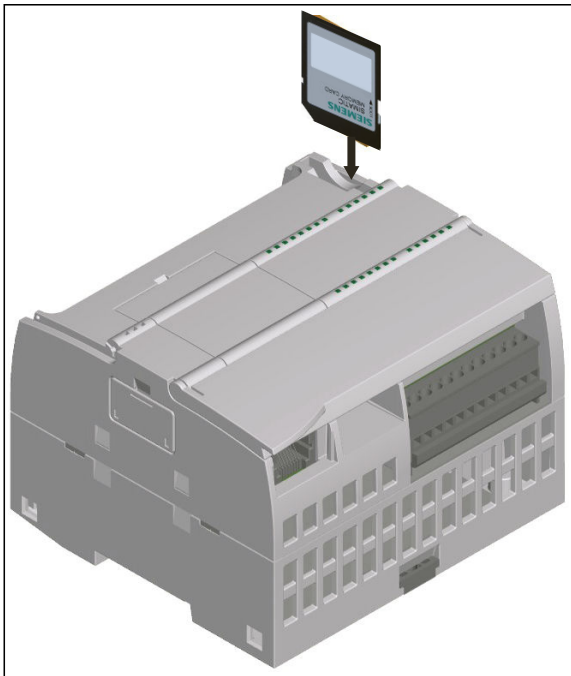
If you do insert an invalid version program transfer card (Page 109), remove the card and perform a STOP to RUN transition, a memory reset (MRES), or cycle power. After you recover the CPU from the error condition, you can download a valid V4.x CPU program.

To transfer a V3.0 program to a V4.x program, you must use the TIA Portal to Change Device in the Hardware Configuration.

NOTE

If you insert a memory card with the CPU in STOP mode, the diagnostics buffer displays a message that the memory card evaluation has been initiated. The CPU will evaluate the memory card the next time you change the CPU to RUN mode, reset the CPU memory with an MRES, or power-cycle the CPU.

Table 6-43 Inserting a memory card

	To insert a memory card, open the top CPU door and insert the memory card in the slot. A push-push type connector allows for easy insertion and removal. The memory card is keyed for proper installation.

CPU behavior when you insert a memory card

When you insert a memory card in the CPU, the CPU performs the following steps:

1. Transitions to STOP mode (if not already in STOP mode)
2. Prompts for one of the following choices:
   - Power cycle
   - Transition to RUN mode
   - Perform a memory reset
3. Evaluates the card

How the CPU evaluates the memory card

If you do not configure the CPU to "Disable copy from internal load memory to external load memory" in the Protection properties of the device configuration (Page 159), the CPU determines what type of memory card you inserted:

- **Empty memory card**: A blank memory card does not have a job file (S7_JOB.S7S). If you insert a blank memory card, the CPU adds a program job file. It then copies internal load memory to external load memory (the program file on the memory card) and erases internal load memory.
- **Blank program card**: A blank program card has a program job file that is empty. In this case, the CPU copies internal load memory to external load memory (the program file on the memory card) and erases internal load memory.

If you configured the CPU to "Disable copy from internal load memory to external load memory" in the Protection properties of the device configuration, the CPU behaves as follows:

- **Empty memory card**: A blank memory card does not have a job file (S7_JOB.S7S). If you insert a blank memory card, the CPU goes to STOP mode. It does not create a program job file and it does not copy internal load memory to external load memory (the program file on the memory card). It does not erase internal load memory.
- **Blank program card**: A blank program card has a program job file that is empty. In this case, the CPU goes to STOP mode. It does not copy internal load memory to external load memory (the program file on the memory card). It does not erase internal load memory.

If you insert a program card (Page 112), transfer card (Page 109), or card that contains a firmware update (Page 117) into the CPU, the configuration setting for "Disable copying from internal load memory to external load memory" has no effect on how the CPU evaluates the memory card.

6.5.2 Configuring the startup parameter of the CPU before copying the project to the memory card

When you copy a program to a transfer card or a program card, the program includes the startup parameter for the CPU (Page 64). Before copying the program to the memory card, always ensure that you have configured the operating mode for the CPU following a power-cycle. Select whether the CPU starts in STOP mode, RUN mode, or in the previous mode (prior to the power cycle).

6.5.3 Transfer card

NOTICE
Risks associated with electrostatic discharge Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable. To protect the memory card and receptacle from electrostatic discharge, do the following: • Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card. • Store the memory card in a conductive container. Receptacle or memory card malfunction can result in property damage.

Creating a transfer card

Remember to configure the startup parameter of the CPU (Page 109) before copying a program to the transfer card.

To create a transfer card, follow these steps:

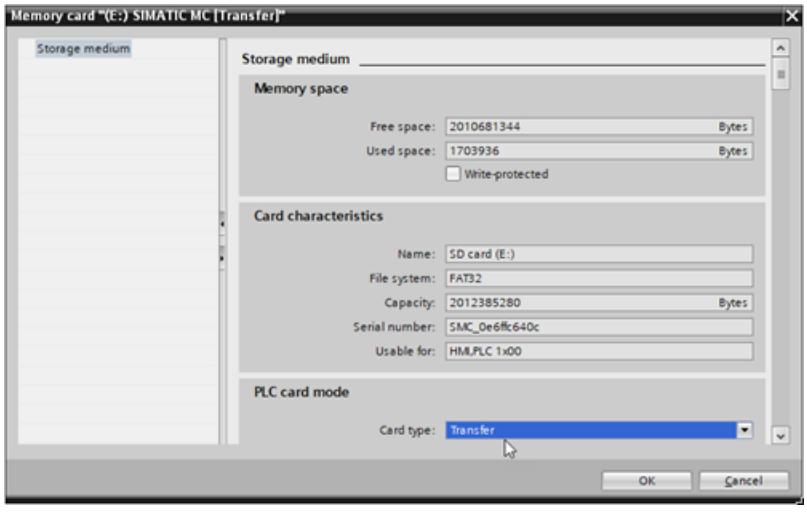
1. Insert a blank SIMATIC memory card that is not write-protected into an SD card reader/writer attached to your computer. (If the card is write-protected, slide the protection switch away from the "Lock" position.)

   If you are reusing a SIMATIC memory card that contains a user program, data logs, recipes, or a firmware update, you **must** delete the files before reusing the card. Use Windows File Explorer to display the contents of the memory card and delete the "S7_JOB.S7S" file and

also delete any existing folders (such as "SIMATIC.S7S","FWUPDATE.S7S", "DataLogs", and "Recipes").

NOTICE
Deleting hidden files The "__LOG__" and "crdinfo.bin" files are required for the memory card. Do NOT delete the hidden files "__LOG__" and "crdinfo.bin" from the memory card. If you delete these files, you cannot use the memory card with the CPU.

2. In the Project tree (Project view), expand the "Card Reader/USB memory" folder and select your card reader.
3. Right-click the drive letter corresponding to the memory card and select "Properties" from the shortcut menu.
4. In the "Memory card" dialog, select "Transfer" from the "Card type" drop-down menu.
   At this point, STEP 7 creates the empty transfer card. If you are creating an empty transfer card, such as to recover from a lost CPU password (Page 119), remove the transfer card from the card reader.



5. Add the program by selecting the CPU device (such as PLC_1 [CPU 1214C DC/DC/DC]) in the Project tree and dragging the CPU device to the memory card. Another method is to copy the CPU device and paste it to the memory card. Copying the CPU device to the memory card opens the "Load preview" dialog.
6. In the "Load preview" dialog, click the "Load" button to copy the CPU device to the memory card.
7. When the dialog displays a message that the CPU device (program) has been loaded without errors, click the "Finish" button.

Using a transfer card

WARNING

Risks when inserting a transfer card

Inserting a memory card will cause the CPU to go to STOP mode, which can affect the operation of an online process or machine.

Before inserting a transfer card, ensure that the CPU is in STOP mode and your process is in a safe state.

Unexpected operation of a process or machine can result in death or injury to personnel and/or property damage.

NOTE

Do not insert V3.0 program transfer cards into later model CPUs.

Version 3.0 program transfer cards are not compatible with later model S7-1200 CPUs. Inserting a memory card that contains a V3.0 program causes a CPU error.

If an invalid version program transfer card is inserted, remove the card. Perform a STOP to RUN transition, a memory reset (MRES), or cycle power to clear the error. After clearing the error, download a valid CPU program.

To transfer the program to a CPU, follow these steps:

1. Insert the transfer card into the CPU (Page 106). If the CPU is in RUN, the CPU will go to STOP mode. The maintenance (MAINT) LED flashes to indicate that the memory card needs to be evaluated. At this point, the existing program is still in the CPU.
2. Power-cycle the CPU to evaluate the memory card. Alternative methods for rebooting the CPU are to perform either a STOP-to-RUN transition or a memory reset (MRES) from STEP 7.
3. After the reboot, the CPU evaluates the memory card and copies the program to the internal load memory of the CPU.

   The RUN/STOP LED alternately flashes green and yellow to indicate that the program is being copied. When the RUN/STOP LED turns on (solid yellow) and the MAINT LED flashes (yellow), the copy process is finished and you can remove the memory card.
4. Reboot the CPU (either by restoring power or by the alternative methods for rebooting) to evaluate the new program that was transferred to internal load memory.

The CPU then goes to the start-up mode (RUN or STOP) that you configured for the project.

NOTE

Remove the transfer card before setting the CPU to RUN mode.

6.5.4 Program card

NOTICE
Risks associated with electrostatic discharge Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable. To protect the memory card and receptacle from electrostatic discharge, do the following: • Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card. • Store the memory card in a conductive container. Receptacle or memory card malfunction can result in property damage.

Check that the memory card is not write-protected. Slide the protection switch away from the "Lock" position.
Before you copy any program elements to the program card, delete any previously saved programs from the memory card.

Creating a program card

When used as a program card, the memory card is the external load memory of the CPU. If you remove the program card, the internal load memory of the CPU is empty.

NOTE

If you insert a blank memory card into the CPU, the CPU copies the program and force values from internal memory to the memory card if you do any one of the following:

- Power cycle the CPU
- Change the operating mode from STOP to RUN
- Perform a memory reset (MRES)

After the copy has been completed, the program in internal load memory is erased, and the CPU then goes to the configured startup mode.

Always remember to configure the startup parameter of the CPU (Page 109) before copying a project to the program card.

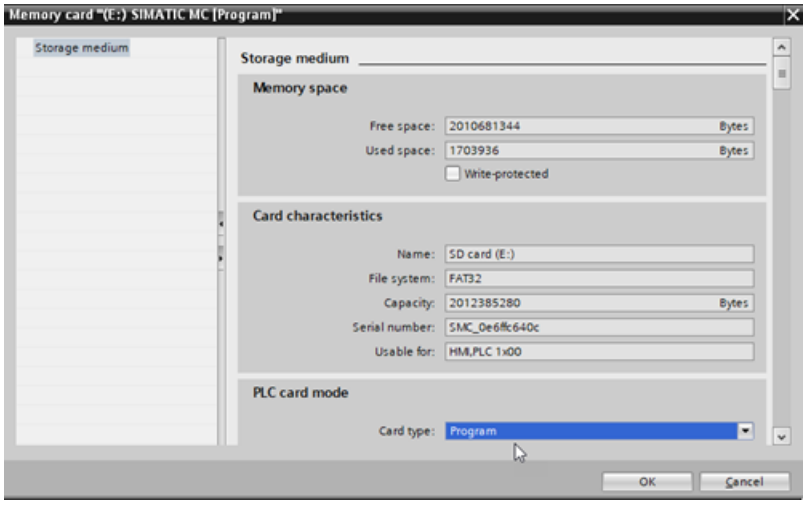
To create a program card, follow these steps:

1. Insert a blank SIMATIC memory card that is not write-protected into an SD card reader/writer attached to your computer. (If the card is write-protected, slide the protection switch away from the "Lock" position.)

   If you are reusing a SIMATIC memory card that contains a user program, data logs, recipes, or a firmware update, you **must** delete the files before reusing the card. Use Windows Explorer to display the contents of the memory card and delete the following files and folders if they exist:
   - S7_JOB.S7S
   - SIMATIC.S7S
   - FWUPDATE.S7S
   - DataLogs
   - Recipes
   - UserFiles

NOTICE
Deleting hidden files The "__LOG__" and "crdinfo.bin" files are required for the memory card. Do NOT delete the hidden files "__LOG__" and "crdinfo.bin" from the memory card. If you delete these files, you cannot use the memory card with the CPU.

2. In the Project tree (Project view), expand the "Card Reader/USB memory" folder and select the card reader.
3. Display the "Memory card" dialog by right-clicking the drive letter corresponding to the memory card in the card reader and selecting "Properties" from the context menu.
4. In the "Memory card" dialog, select "Program" from the shortcut menu.



5. Add the program by selecting the CPU device (such as PLC_1 [CPU 1214C DC/DC/DC]) in the Project tree and dragging the CPU device to the memory card. (Another method is to copy the CPU device and paste it to the memory card.) Copying the CPU device to the memory card opens the "Load preview" dialog.

6. In the "Load preview" dialog, click the "Load" button to copy the CPU device to the memory card.
7. When the dialog displays a message that the download completed without errors, click the "Finish" button.

Using a program card as the load memory for a CPU

WARNING

Risks associated with inserting a program card

Use caution when inserting a program card while the CPU is in RUN mode. If a program card is inserted while the CPU is in RUN mode, the CPU switches to STOP mode. Unexpected equipment operation can occur.

Ensure that the CPU is in STOP mode before inserting a program card.

Unexpected equipment operation can result in death, injury, and equipment damage.

To use a program card with a CPU, follow these steps:

1. Insert the program card into the CPU. If the CPU is in RUN mode, the CPU goes to STOP mode. The maintenance (MAINT) LED flashes to indicate that the memory card needs to be evaluated.
2. Power-cycle the CPU to evaluate the memory card. Alternative methods for rebooting the CPU are to perform either a STOP-to-RUN transition or a memory reset (MRES) from STEP 7.
3. After the CPU reboots and evaluates the program card, the CPU erases the internal load memory of the CPU.

The CPU then goes to the start-up mode (RUN or STOP) that you configured for the CPU.

The program card must remain in the CPU.

WARNING

Risks associated with removing a program card

If a program card is removed while the CPU is in RUN mode, the CPU switches to STOP mode and flashes the error LED.

Use caution when removing a program card while the CPU is in RUN mode. Removing the program card removes the program from the CPU.

Unexpected equipment operation can result in death, injury, and equipment damage.

Service life of a SIMATIC memory card

The service life of a SIMATIC memory card depends on factors such as the following:

- Number of delete and write operations per memory block
- Number of bytes written
- External influences, such as ambient temperature

NOTE

Effect of write and delete operations on SIMATIC memory card service life

Write or delete operations, particularly repeated (cyclic) write/delete operations, reduce the service life of the SIMATIC memory card.

Cyclic execution of the following actions reduces the service life of the memory card depending on the number of write operations and data:

- Data Log Handling (for example, DataLogWrite)
- Recipe Handling (for example, RecipeExport)
- System Function Calls (SFCs) that write/delete to the file system (for example, WRIT_DBL, CREATE_DB)
- System Function Blocks (SFBs) that write/delete to file system (for example, FileWriteC, FileDelete)
- Any other cyclic action that changes data on the persistent store (for example, Tracing, SET-TimeZone)

6.5.5 Using a memory card for protecting confidential PLC configuration data

You can use a SIMATIC memory card to set or change the password for Protection of confidential PLC configuration data.

NOTICE

Risks associated with electrostatic discharge

Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable.

To protect the memory card and receptacle from electrostatic discharge, do the following:

- Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card.
- Store the memory card in a conductive container.

Receptacle or memory card malfunction can result in property damage.

NOTICE

Reformatting memory cards

If a SIMATIC memory card is reformatted using the Windows formatter utility, the memory will no longer be usable by a S7-1200 CPU.

Do not use the Windows formatter utility or any other formatting utility to reformat memory cards.

Risks associated with the decommissioning process

S7-1200 CPUs do not support secure erasure of the memory card and internal flash. Therefore, during the decommissioning process, you must securely dispose of the CPU and memory card to prevent the loss of proprietary or confidential information.

How to create a memory card with the Protection of confidential PLC configuration data password

To create the memory card with this password, follow these steps:

1. Insert a blank SIMATIC memory card that is not write-protected into an SD card reader/writer attached to your computer. If the card is write-protected, slide the protection switch away from the "Lock" position.
   You can reuse a SIMATIC memory card that contains a user program or firmware update, but you must delete some of the files on the memory card. To reuse a memory card, you must delete the "S7_JOB.S7S" file before creating the Protection of confidential PLC configuration data file. Use Windows Explorer to display the contents of the memory card and to delete the "S7_JOB.S7S" file and folders.

NOTICE
Deleting hidden files The "__LOG__" and "crdinfo.bin" files are required for the memory card. Do NOT delete the hidden files "__LOG__" and "crdinfo.bin" from the memory card. If you delete these files, you cannot use the memory card with the CPU.

2. Create a file on the root of the memory card called "S7_JOB.S7S". Open the file with a text editor and type the following: SET_PWD.
3. Create a folder on the root of the memory card called: SET_PWD.S7S.
4. Under the "SET_PWD.S7S" folder, create a text file called "PWD.TXT". The file must be named "PWD.TXT". Enter your Protection of confidential PLC configuration data password as the text contents of the file. The file must contain a single line of text representing the Protection of confidential PLC configuration data password. Follow the STEP 7 rules for passwords when creating the password, using these characters:
   – 0123456789
   – A...Z a...z
   – !#$%&()*+,-./:;<=>?@ [\]_{|}~^
5. To clear the Protection of confidential PLC configuration data password on the PLC, the file must be empty.
6. Safely eject the card from the card reader/writer.

How to set the Protection of confidential PLC configuration data password

To set the Protect confidential PLC configuration data password, follow these steps:

1. Verify that the CPU is not actively running a process before setting the Protection of confidential PLC configuration data password.
2. If the CPU has an existing password for protection of PLC configuration data, reset the PLC as follows:
   – Select "Reset to factory settings" from the Functions menu.
   – Select "Delete password for protection of PLC configuration data".
   – Click "Reset PLC".
3. Insert the memory card into the CPU. If the CPU is in RUN mode, the CPU then goes to STOP mode. The maintenance (MAINT) LED flashes to indicate the memory card needs to be evaluated.

4. Power cycle the CPU to start the process. After the CPU reboots, the setting of the Protection of confidential PLC configuration data password occurs. When the RUN/STOP LED turns on solid yellow and the MAINT LED flashes, the process has finished. You must then remove the memory card.
5. After removing the memory card, reboot the CPU again to start using the new Protection of confidential PLC configuration data password.

If the existing user program requires a different Protection of confidential PLC configuration data password, it will not load after restarting. You must clear the existing program and download a program that uses the Protection of confidential PLC configuration data password that you set in the previous steps.

If the existing program requires the provided Protection of confidential PLC configuration data password, the PLC can go to RUN based on the project configuration.

6.5.6 Firmware update

You can use a SIMATIC memory card for performing a firmware update.

NOTICE

Risks associated with electrostatic discharge

Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable.

To protect the memory card and receptacle from electrostatic discharge, do the following:

- Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card.
- Store the memory card in a conductive container.

Receptacle or memory card malfunction can result in property damage.

You use a SIMATIC memory card when downloading firmware updates from Siemens Industry Online Support (http://support.industry.siemens.com). From this Web site, navigate to "Downloads". From there, search for the specific type of module that you need to update.

Alternatively, you can access the S7-1200 downloads Web page (https://support.industry.siemens.com/cs/ww/en/ps/13683/dl) directly.

NOTE

You cannot update an S7-1200 CPU V3.0 or earlier to S7-1200 V4.0 (or later) by firmware update.

You can also use one of these methods to perform a firmware update:

- Using the online and diagnostic tools of STEP 7 (Page 1055)
- Using the Web server "Module Information" standard Web page (Page 777)
- Using the SIMATIC Automation Tool (https://support.industry.siemens.com/cs/ww/en/view/98161300)

NOTICE

Reformatting memory cards

If a Siemens memory card is reformatted using the Microsoft Windows formatter utility, then the memory card will no longer be usable by a S7-1200 CPU.

Do not use the Windows formatter utility or any other formatting utility to reformat the memory card.

To download the firmware update to your memory card, follow these steps:

1. Insert a blank SIMATIC memory card that is not write-protected into an SD card reader/writer attached to your computer. If the card is write-protected, slide the protection switch away from the "Lock" position.

   You can reuse a SIMATIC memory card that contains a user program or another firmware update. To avoid any confusion, you should also delete files S7_JOB.SYS, SIMATIC.S7S, and FWUPDATE.S7S if they exist.

   NOTICE

   Deleting hidden files

   The "__LOG__" and "crdinfo.bin" files are required for the memory card.

   Do NOT delete the hidden files "__LOG__" and "crdinfo.bin" from the memory card.

   If you delete these files, you cannot use the memory card with the CPU.

2. Select the zip file for the firmware update that corresponds to your module, and download it to your computer. Double-click the file, set the file destination path to be the root directory of the SIMATIC memory card, and start the extraction process. After the extraction is complete, the root directory (folder) of the memory card will contain a "FWUPDATE.S7S" directory and the "S7_JOB.S7S" file.

   NOTE

   Do not put multiple firmware updates for the same article number (MLFB) on your memory card.

   Putting multiple firmware updates for the same article number on the memory card causes the firmware update to fail.

3. Safely eject the card from the card reader/writer.

To install the firmware update, follow these steps:

WARNING

Risks when installing firmware updates

Installing the firmware update will cause the CPU to go to STOP mode, which can affect the operation of an online process or machine.

Verify that the CPU is not actively running a process before installing the firmware update. Before inserting the memory card, always ensure that the CPU is offline and in a safe state.

Unexpected operation of a process or machine can result in death or injury to personnel and/or property damage.

1. Insert the memory card into the CPU. If the CPU is in RUN mode, the CPU then goes to STOP mode. The maintenance (MAINT) LED flashes to indicate that the memory card needs to be evaluated.
2. Power-cycle the CPU to start the firmware update. Alternative methods for rebooting the CPU are to perform either a STOP-to-RUN transition or a memory reset (MRES) from STEP 7.

   NOTE

   To complete the firmware upgrade for the module, you must ensure that the external 24 V DC power to the module remains on.

   After the CPU reboots, the firmware update starts. The RUN/STOP LED alternately flashes green and yellow to indicate that the update is being copied. When the RUN/STOP LED turns on (solid yellow) and the MAINT LED flashes, the copy process has finished. You must then remove the memory card.
3. After removing the memory card, reboot the CPU again (either by restoring power or by the alternative methods for rebooting) to load the new firmware.

The user program and hardware configuration are not affected by the firmware update. When the CPU is powered up, the CPU enters the configured start-up state. (If the startup mode for your CPU was configured to "Warm restart - mode before POWER OFF", the CPU is in STOP mode because the last state of the CPU was STOP.)

During update, the firmware update procedure ignores UPD files that do not correspond to any station hardware modules. This allows you to create a master firmware update memory card to update all S7-1200 CPU stations in your facility. No Diagnostics buffer entry is made to identify the ignored UPD files. This prevents the Diagnostics buffer from being clogged with extraneous, mostly meaningless entries that might hide the update operation entries of interest to you. For example, a Diagnostics buffer entry is made if firmware update attempts are made, whether successful or not. You can then easily scan the Diagnostics buffer for any unexpected anomalies without the noise of extraneous entries.

The Diagnostics buffer reports the results of all firmware update attempts. In the case of a failure, the Diagnostics buffer message provides an explanation for the failure.

NOTE

The firmware update process discards any additional data appended to the firmware update file. Appending data to a firmware update file has no effect on the firmware update or the S7-1200 CPU. You cannot append data, for example, to add components.

6.6 Recovery from a lost password

If you have lost the password for a password-protected CPU, use an empty transfer card (Page 109) to delete the password-protected program. The empty transfer card erases the internal load memory of the CPU. You can then download a new user program from STEP 7 to the CPU.

WARNING

Risks when inserting transfer cards

If you insert a transfer card in a running CPU, the CPU goes to STOP. Control devices can fail in an unsafe condition, resulting in unexpected operation of controlled equipment.

Verify that the CPU is not actively running a process before inserting the memory card. Before inserting a transfer card, always ensure that the CPU is in STOP mode and your process is in a safe state.

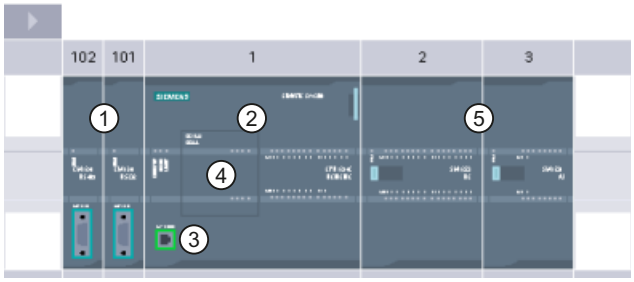
Such unexpected operations can result in death or serious injury to personnel, and/or damage to equipment

You must remove the transfer card before setting the CPU to RUN mode.

Device configuration

7

You create the device configuration for your PLC by adding a CPU and additional modules to your project.



① Communication module (CM) or communication processor (CP): Up to 3, inserted in slots 101, 102, and 103

② CPU: Slot 1

③ PROFINET port of CPU

④ Signal board (SB), communication board (CB) or battery board (BB): up to 1, inserted in the CPU

⑤ Signal module (SM) for digital or analog I/O: up to 8, inserted in slots 2 through 9
(This excludes CPUs 1212C, 1212FC, and 1211C. CPUs 1212C and 1212FC allow 2 signal modules. CPU 1211C does not allow any.)

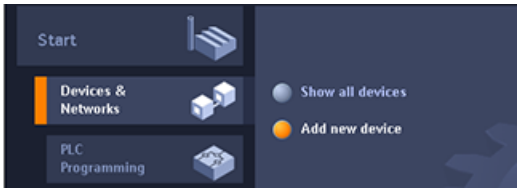
Configuration control

Device configuration for the S7-1200 also supports "configuration control (Page 127)" where you can configure a maximum configuration for a project including modules that you might not actually use. This feature, sometimes also called "option handling", allows you to configure a maximum configuration that you might use with variations in the installed modules in multiple applications.

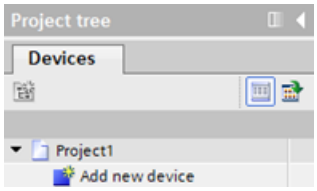
7.1 Inserting a CPU

You can insert a CPU into your project from either the Portal view or the Project view of STEP 7:

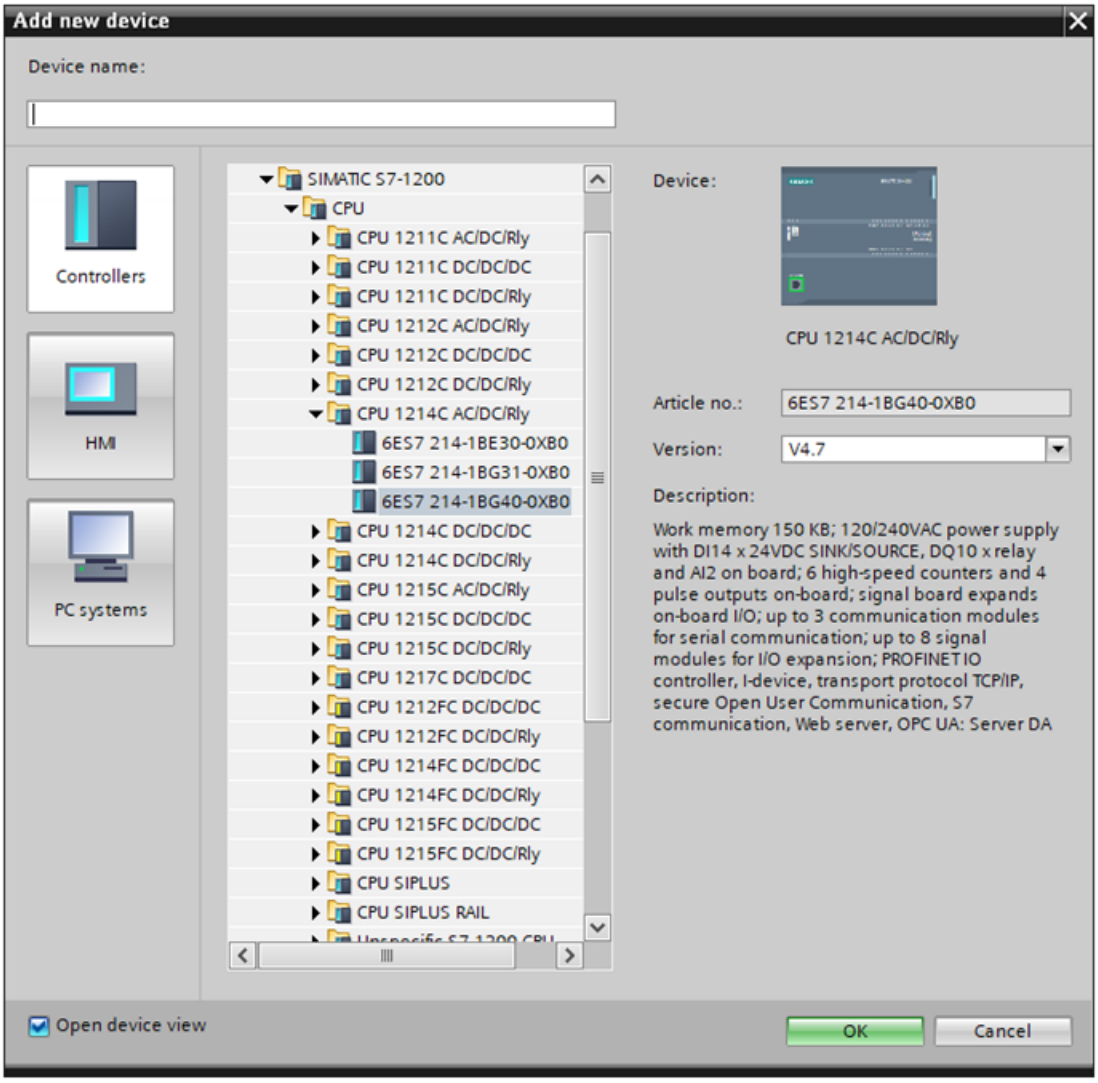
- In the Portal view, select "Devices & Networks" and click "Add new device".



- In the Project view, under the project name, double-click "Add new device".



From the "Add new device" dialog, select the correct model and firmware version from the list.

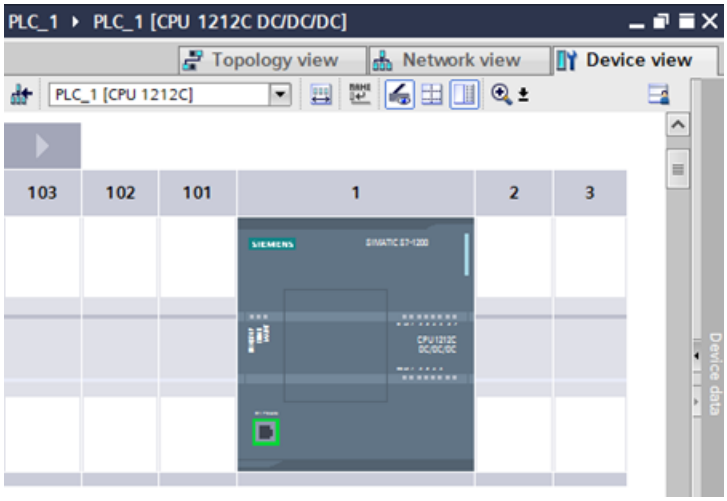


Configuring PLC security settings for your inserted CPU

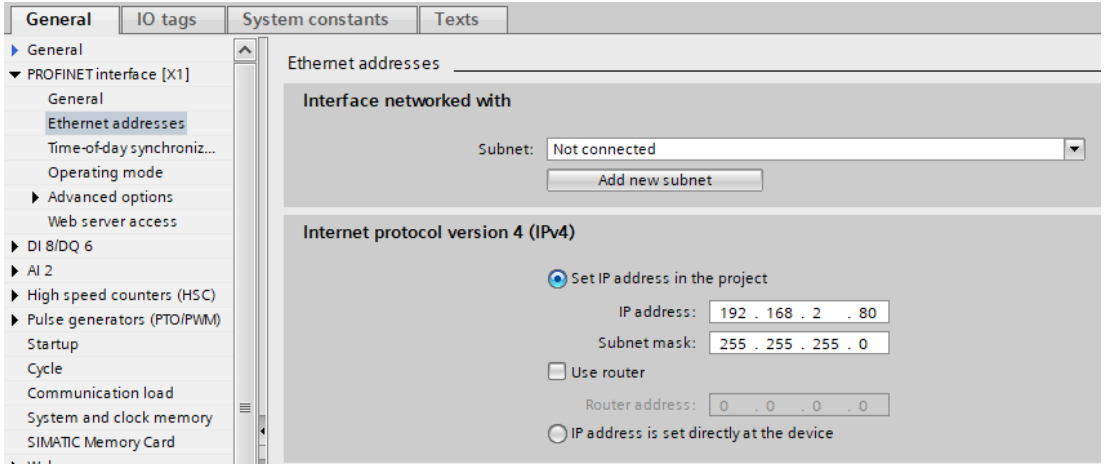
When you insert an S7-1200 CPU, STEP 7 launches the security wizard (Page 144) to help you set up your PLC security settings. Follow the steps in the wizard to set up your PLC security settings.

Device configuration for the inserted CPU

After you add a CPU, STEP 7 creates the rack and displays the CPU in the Device view:



Clicking the CPU in the Device view displays the CPU properties in the inspector window. You can assign an IP address for the CPU during the device configuration. If your CPU is connected to a router on the network, you also enter the IP address for a router.



7.2 Uploading the configuration of a connected CPU

STEP 7 provides two methods for uploading the hardware configuration of a connected CPU:

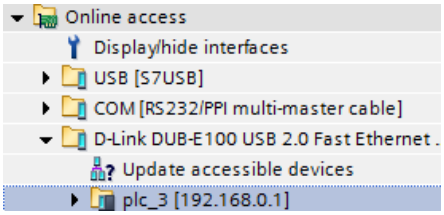
- Uploading the connected device as a new station
- Configuring an unspecified CPU and detecting the hardware configuration of the connected CPU

Note, however, that the first method uploads both the hardware configuration and the software of the connected CPU.

Uploading a device as a new station

To upload a connected device as a new station, follow these steps:

1. Expand your communications interface from the "Online access" node of the project tree.
2. Double-click "Update accessible devices".
3. Select the PLC from the detected devices.



4. From the Online menu of STEP 7, select the "Upload device as new station (hardware and software)" menu command.

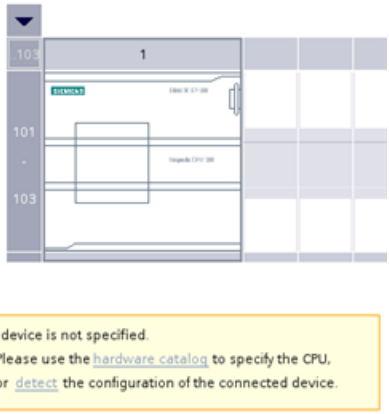
STEP 7 uploads both the hardware configuration and the program blocks.

Detecting the hardware configuration of an unspecified CPU

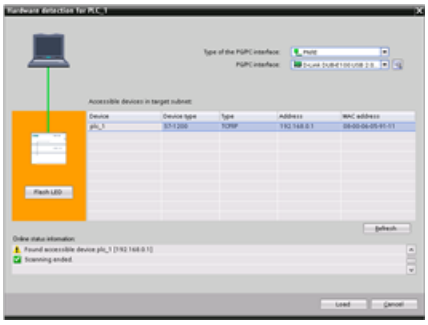
If you are connected to a CPU, you can upload the configuration of that CPU, including any modules, to your project. Simply create a new project and select the "unspecified CPU" instead of selecting a specific CPU.

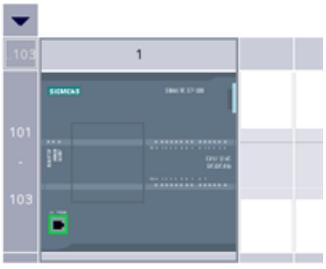
From the program editor, select the "Hardware detection" command from the "Online" menu.

From the device configuration editor, select the option to detect the configuration of the connected device.



After you select the CPU from the online dialog and click the Load button, STEP 7 uploads the hardware configuration from the CPU, including any modules (SM, SB, or CM). You can then configure the parameters for the CPU and the modules (Page 136).





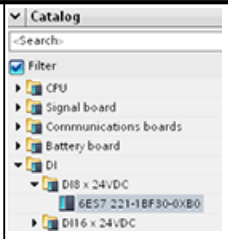
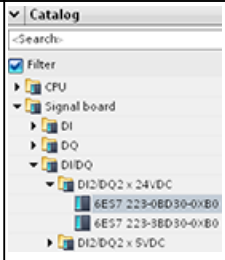
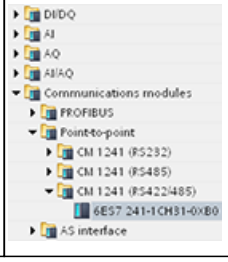
7.3 Adding modules to the configuration

Use the hardware catalog to add modules to the CPU:

- Signal modules (SM) provide additional digital or analog I/O points. These modules are connected to the right side of the CPU.
- Signal boards (SB) provide a few additional I/O points for the CPU. The SB is installed on the front of the CPU.
- Battery Board 1297 (BB) provides long-term backup of the realtime clock. The BB is installed on the front of the CPU.
- The communication board (CB) provides an additional communication port (such as RS485). The CB is installed on the front of the CPU.
- Communication modules (CM) and communication processors (CP) provide an additional communication port, such as for PROFIBUS or GPRS. These modules are connected to the left side of the CPU.

To insert a module into the device configuration, select the module in the hardware catalog and either double-click or drag the module to the highlighted slot. You must add the modules to the device configuration and download the hardware configuration to the CPU for the modules to be functional.

Table 7-1 Adding a module to the device configuration

Module	Select the module	Insert the module	Result
SM			
SB, BB or CB			
CM or CP			

With the "configuration control" feature (Page 127), you can add signal modules and signal boards to your device configuration that might not correspond to the actual hardware for a specific application, but that will be used in related applications that share a common user program, CPU model, and perhaps some of the configured modules.

7.4 Configuration control

7.4.1 Advantages and applications of configuration control

Configuration control can be a useful solution when you create an automation solution (machine) that you intend to use with variations in multiple installations.

You can load a STEP 7 device configuration and user program to different installed PLC configurations. You only need to make a few easy adaptations to make the STEP 7 project correspond to the actual installation.

7.4.2 Configuring the central installation and optional modules

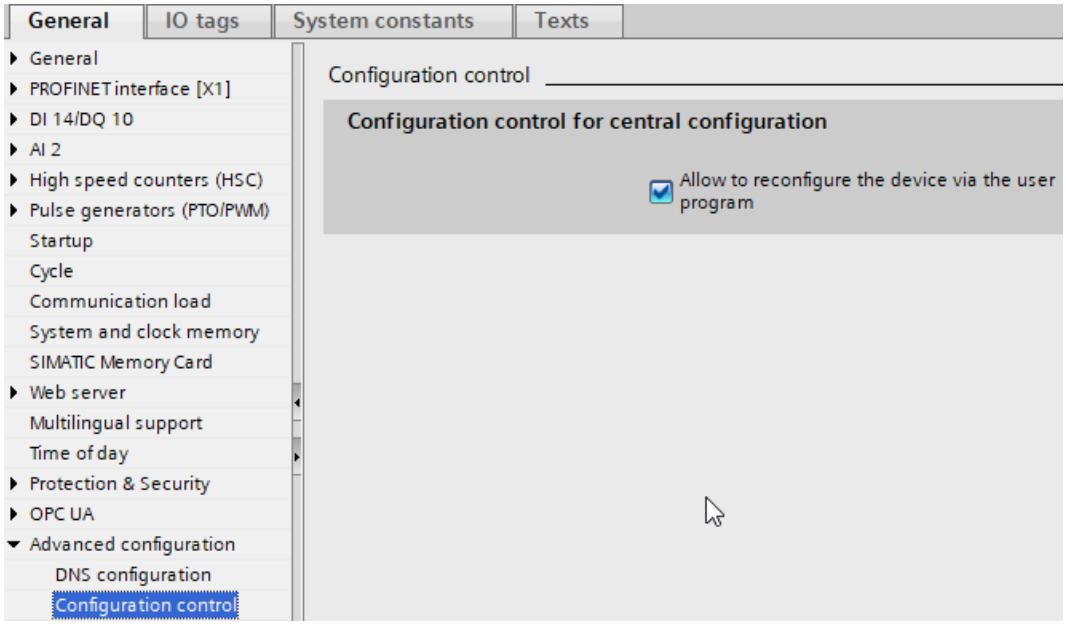
Configuration control with STEP 7 and the S7-1200 enables you to configure a maximum configuration for a standard machine and to operate versions (options) that use a subset of this configuration. The PROFINET with STEP 7 manual (http://support.automation.siemens.com/WW/view/en/49948856) refers to these types of projects as "standard machine projects".

A control data record that you program in the startup program block notifies the CPU as to which modules are missing in the real installation as compared to the configuration or which modules are located in different slots as compared to the configuration. Configuration control does not have an impact on the parameter assignment of the modules.

Configuration control gives you the flexibility to vary the installation as long as you can derive the real configuration from the maximum device configuration in STEP 7.

To activate configuration control and structure the required control data record, follow these steps:

1. Optionally, reset the CPU to factory settings to ensure that an incompatible control data record is not present in the CPU.
2. Select the CPU in device configuration in STEP 7.
3. From the Configuration control node in the CPU properties, select the "Allow to reconfigure the device via the user program" check box.

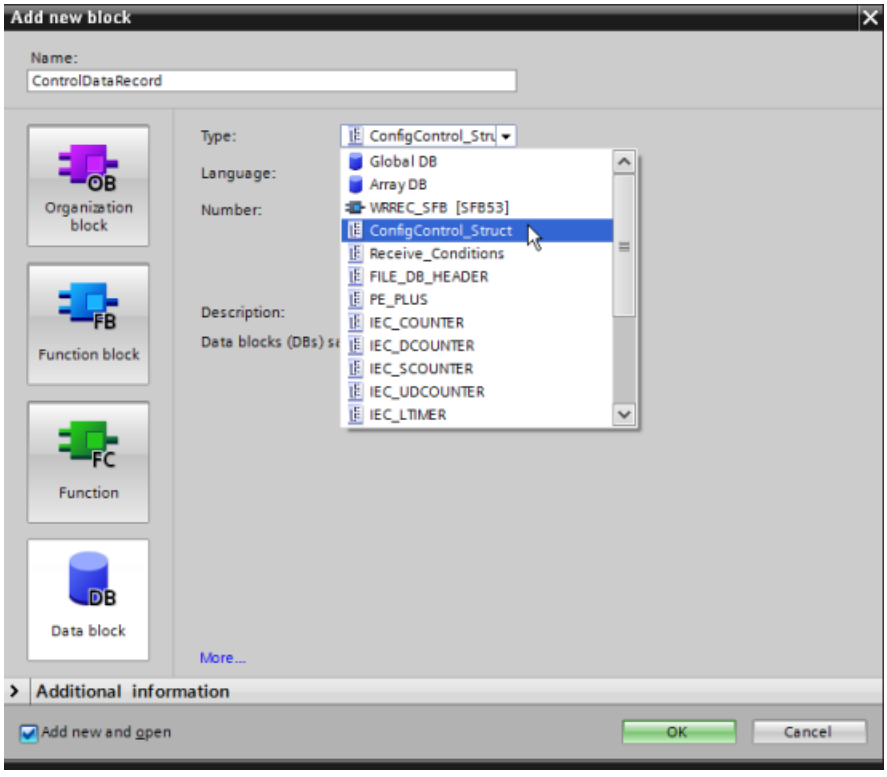


4. Create a PLC data type to contain the control data record. Configure it as a Struct that includes four USints for configuration control information and additional USints to correspond to the slots of a maximum S7-1200 device configuration, as follows:

ConfigControl_Struct

	Name	Data type	Default value	Comment
1	ConfigControl	Struct		
2	Block_length	USInt	16	Length of control data record, including header
3	Block_ID	USInt	196	Data record number
4	Version	USInt	5	
5	Subversion	USInt	0	
6	Slot_1	USInt	255	Assignment for CPU annex card/Actual annex card
7	Slot_2	USInt	255	Configured slot 2/ Assigned "real" slot
8	Slot_3	USInt	255	Configured slot 3 / Assigned "real" slot
9	Slot_4	USInt	255	Configured slot 4 / Assigned "real" slot
10	Slot_5	USInt	255	Configured slot 5 / Assigned "real" slot
11	Slot_6	USInt	255	Configured slot 6 / Assigned "real" slot
12	Slot_7	USInt	255	Configured slot 7 / Assigned "real" slot
13	Slot_8	USInt	255	Configured slot 8 / Assigned "real" slot
14	Slot_9	USInt	255	Configured slot 9 / Assigned "real" slot
15	Slot_101	USInt	255	Configured slot 101 / Assigned "real" slot
16	Slot_102	USInt	255	Configured slot 102 / Assigned "real" slot
17	Slot_103	USInt	255	Configured slot 103 / Assigned "real" slot

5. Create a data block of the PLC data type that you created.



6. In this data block, configure the Block_length, Block_ID, Version, and Subversion as shown below. Configure the values for the slots based on their presence or absence and position in your actual installation:
   - 0: Configured module is not present in the actual configuration. (The slot is empty.)
   - 1 to 9, 101 to 103: The actual slot position for the configured slot
   - 255: The STEP 7 device configuration does not include a module in this slot.

NOTE

Configuration control not available for HSCs and PTOs on the signal board

If you have a signal board in the CPU that you configure for HSCs or PTOs, you must not disable it with a "0" in Slot_1 of the configuration control data record. Configured HSC and PTO devices of the CPU are mandatory regarding configuration control.

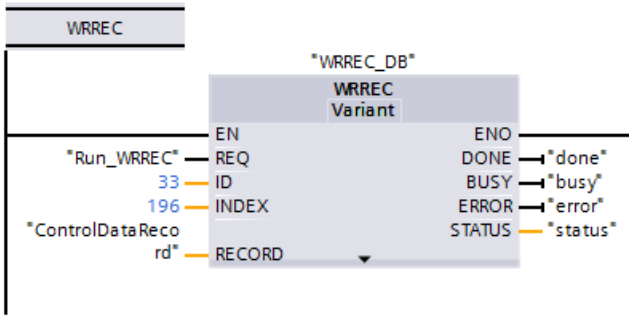
ControlDataRecord

	Name	Data type	Start value	Comment
1	Static			
2	ConfigControl	Struct		
3	Block_length	USInt	16	Length of control data record, including header
4	Block_ID	USInt	196	Data record number
5	Version	USInt	5	
6	Subversion	USInt	0	
7	Slot_1	USInt	255	Assignment for CPU annex card/Actual annex c...
8	Slot_2	USInt	255	Configured slot 2/ Assigned "real" slot
9	Slot_3	USInt	255	Configured slot 3 / Assigned "real" slot
10	Slot_4	USInt	255	Configured slot 4 / Assigned "real" slot
11	Slot_5	USInt	255	Configured slot 5 / Assigned "real" slot
12	Slot_6	USInt	255	Configured slot 6 / Assigned "real" slot
13	Slot_7	USInt	255	Configured slot 7 / Assigned "real" slot
14	Slot_8	USInt	255	Configured slot 8 / Assigned "real" slot
15	Slot_9	USInt	255	Configured slot 9 / Assigned "real" slot
16	Slot_101	USInt	255	Configured slot 101 / Assigned "real" slot
17	Slot_102	USInt	255	Configured slot 102 / Assigned "real" slot
18	Slot_103	USInt	255	Configured slot 103 / Assigned "real" slot

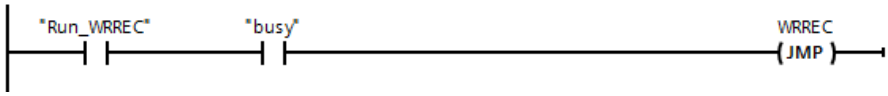
See Example of configuration control (Page 133) for an explanation of how to assign the slot values.

7. In the startup OB, call the extended WRREC (Write data record) instruction to transfer the control data record that you created to index 196 of hardware ID 33. Use a label and JMP (jump) instruction to wait for the WRREC instruction to complete.

   Network 1:



Network 2:



NOTE

Configuration control is not in effect until the WRREC instruction transfers the control data record in the startup OB. If you have enabled configuration control and the CPU does not have the control data record, it will go to STOP mode when it exits STARTUP mode. Be sure that you program the startup OB to transfer the control data record.

Module arrangement

The following table shows the slot number assignment:

Slot	Modules
1	Signal board or communication board (CPU annex card)
2 to 9	Signal modules
101 to 103	Communication modules

Control data record

A control data record 196 contains the slot assignment and represents the actual configuration, as shown below:

Byte	Element	Value	Explanation
0	Block length	16	Header
1	Block ID	196	
2	Version	5	
3	Subversion	0	
4	Assignment of CPU annex card	Actual annex card, 0, or 255*	Control element Describes in each element which real slot in the device is assigned to the configured slot.
5	Assignment of configured slot 2	Actual slot, 0, or 255*	
...	...	...	
12	Assignment of configured slot 9	Actual slot, 0, or 255*	
13	Assignment of configured slot 101	Actual slot or 255*	Unlike signal modules, the actual slot for physically-present communication modules must be the same as the configured slot.
14	Assignment of configured slot 102	Actual slot or 255*	
15	Assignment of configured slot 103	Actual slot or 255*	

***Slot values:**

0: Configured module is not present in the actual configuration. (The slot is empty.)

1 to 9, 101 to 103: The actual slot position for the configured slot

255: The STEP 7 device configuration does not include a module in this slot.

NOTE

Alternative to creating a PLC tag type

As an alternative to creating a custom PLC tag type, you can create a data block directly with all of the structure elements of a control data record. You could even configure multiple structs in this data block to serve as multiple control data record configurations. Either implementation is an effective way to transfer the control data record during startup.

Rules

Observe the following rules:

- Configuration control does not support position changes for communication modules. Also, you cannot use configuration control to deactivate communication modules. The control data record slot positions for slots 101 to 103 must correspond to the actual installation. If you have not configured a module for the slot in your device configuration, enter 255 for that slot position in the control data record. If you have configured a module for the slot, enter the configured slot as the actual slot for that slot position.
- F-I/O modules do not support configuration control. The control data record slot positions for an F-I/O module must equal the configured slot position for the F-I/O module. If you attempt to move or delete a configured F-I/O module using the control data record, then all actually-installed F-I/O modules will raise a "parameter assignment" error and disallow exchange.
- You cannot have embedded empty (unused) slots between filled (used) slots. For example, if the actual configuration has a module in slot 4, then the actual configuration must also have modules in slots 2 and 3. Correspondingly, if the actual configuration has a communication module in slot 102, then the actual configuration must also have a module in slot 101.
- If you have enabled configuration control, the CPU is not ready for operation without a control data record. The CPU returns from startup to STOP if a startup OB does not transfer a valid control data record. The CPU does not initialize the central I/O in this case and enters the cause for the STOP mode in the diagnostics buffer.
- The CPU saves a successfully-transferred control data record in retentive memory, which means that it is not necessary to write the control data record 196 again at a restart if you have not changed the configuration.
- Each real slot must be present only once in the control data record.
- You can only assign a real slot to one configured slot.

NOTE

Modifying a configuration

The writing of a control data record with a modified configuration triggers the following automatic reaction by the CPU: Memory reset with subsequent startup with this modified configuration.

As a result of this reaction, the CPU deletes the original control data record and saves the new control data record retentively.

Behavior during operation

For the online display and for the display in the diagnostics buffer (module OK or module faulty), STEP 7 uses the device configuration and not the differing real configuration.

Example: A module outputs diagnostics data. This module is configured in slot 4, but is actually inserted in slot 3. The online view indicates that configured slot 4 is faulty. In the real configuration, the module at slot 3 indicates an error by its LED display.

If you have configured modules as missing in the control data record (0 entry), the automation system behaves as follows:

- Modules designated as not present in the control data record do not supply diagnostics and their status is always OK. The value status is OK.
- Direct writing access to the outputs or writing access to the process image of outputs that are not present proceeds with no effect; the CPU reports no access error.
- Direct read access to the inputs or read access to the process image of inputs that are not present results in a value "0" for each input; the CPU reports no access error.
- Writing a data record to a module that is not present proceeds with no effect; the CPU reports no error.
- Attempting to read a data record from module that is not present results in an error because the CPU cannot return a valid data record.

Error messages

The CPU returns the following error messages if an error occurs during writing of the control data record:

Error code	Meaning
16#80B1	Invalid length; the length information in the control data record is not correct.
16#80B5	Configuration control parameters not assigned
16#80E2	Data record was transferred in the wrong OB context. The data record must be transferred in the start-up OB.
16#80B0	Block type (byte 2) of control data record is not equal to 196.
16#80B8	Parameter error; module signals invalid parameters, for example: • The control data record attempts to modify the configuration of a communication module or a communication annex card. The real configuration for communication modules and a communication annex card must equal the STEP 7 configuration. • The assigned value for an unconfigured slot in the STEP 7 project is not equal to 255. • The assigned value for a configured slot is out of range. • The assigned configuration has an "internal" empty slot, for example, slot n is assigned and slot n-1 is not assigned.

7.4.3 Example of configuration control

This example describes a configuration consisting of a CPU and three I/O modules. The module at slot 3 is not present in the first actual installation, so you use configuration control to "hide" it.

In the second installation, the application includes the module that was initially hidden but now includes it in the last slot. A modified control data record provides the information about the slot assignments of the modules.

Example: Actual installation with configured but unused module

The device configuration contains all modules that can be present in an actual installation (maximum configuration). In this case, the module that is in slot 3 in the device configuration is not present in the real installation.

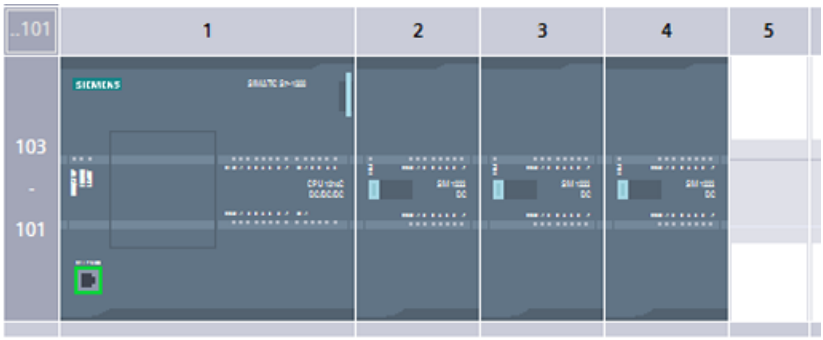


Figure 7-1 Device configuration of maximum installation with three signal modules

Figure 7-2 Actual installation with module configured in slot 3 absent, and module configured for slot 4 in actual slot 3

To indicate the absence of the missing module, you must configure slot 3 in the control data record with 0.

ControlDataRecord

		Name	Data type	Start value	Comment
1		Static			
2		ConfigControl	Struct		
3		Block_length	USInt	16	Length of control data record, including header
4		Block_ID	USInt	196	Data record number
5		Version	USInt	5	
6		Subversion	USInt	0	
7		Slot_1	USInt	255	Assignment for CPU annex card/Actual annex ca...
8		Slot_2	USInt	2	Configured slot 2 / Assigned "real" slot
9		Slot_3	USInt	0	Configured slot 3 / Assigned "real" slot
10		Slot_4	USInt	3	Configured slot 4 / Assigned "real" slot
11		Slot_5	USInt	255	Configured slot 5 / Assigned "real" slot
12		Slot_6	USInt	255	Configured slot 6 / Assigned "real" slot
13		Slot_7	USInt	255	Configured slot 7 / Assigned "real" slot
14		Slot_8	USInt	255	Configured slot 8 / Assigned "real" slot
15		Slot_9	USInt	255	Configured slot 9 / Assigned "real" slot
16		Slot_101	USInt	255	Configured slot 101 / Assigned "real" slot
17		Slot_102	USInt	255	Configured slot 102 / Assigned "real" slot
18		Slot_103	USInt	255	Configured slot 103 / Assigned "real" slot

Example: Actual installation with module subsequently added to a different slot

In the second example, the module in slot 3 of the device configuration is present in the actual installation but is in slot 4.

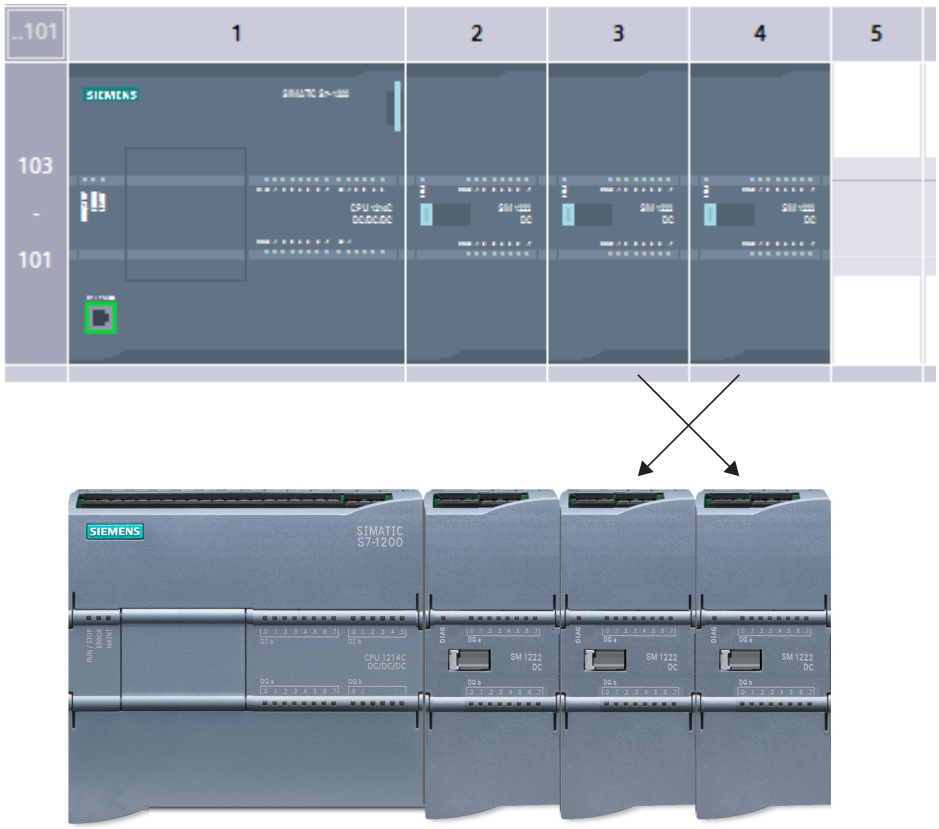


Figure 7-3 Device configuration compared to actual installation with modules in slots 3 and 4 swapped

To correlate the device configuration to the actual installation, edit the control data record to assign the modules to the correct slot positions.

ControlDataRecord

	Name	Data type	Start value	Comment
1	Static			
2	ConfigControl	Struct		
3	Block_length	USInt	16	Length of control data record, including header
4	Block_ID	USInt	196	Data record number
5	Version	USInt	5	
6	Subversion	USInt	0	
7	Slot_1	USInt	255	Assignment for CPU annex card/Actual annex card
8	Slot_2	USInt	2	Configured slot 2/ Assigned "real" slot
9	Slot_3	USInt	4	Configured slot 3 / Assigned "real" slot
10	Slot_4	USInt	3	Configured slot 4 / Assigned "real" slot
11	Slot_5	USInt	255	Configured slot 5 / Assigned "real" slot
12	Slot_6	USInt	255	Configured slot 6 / Assigned "real" slot
13	Slot_7	USInt	255	Configured slot 7 / Assigned "real" slot
14	Slot_8	USInt	255	Configured slot 8 / Assigned "real" slot
15	Slot_9	USInt	255	Configured slot 9 / Assigned "real" slot
16	Slot_101	USInt	255	Configured slot 101 / Assigned "real" slot
17	Slot_102	USInt	255	Configured slot 102 / Assigned "real" slot
18	Slot_103	USInt	255	Configured slot 103 / Assigned "real" slot

7.5 Changing a device

You can change the device type of a configured CPU or module. From Device configuration, right-click the device and select "Change device" from the context menu. From the dialog, navigate to and select the CPU or module that you want to replace. The Change device dialog shows you compatibility information between the two devices.

For considerations on changing devices between different CPU versions, refer to Exchanging a V3.0 CPU for a V4.x CPU (Page 1285).

7.6 Configuring the operation of the CPU

7.6.1 CPU properties

To configure the operational parameters for the CPU, select the CPU in the Device view and use the "Properties" tab of the inspector window.

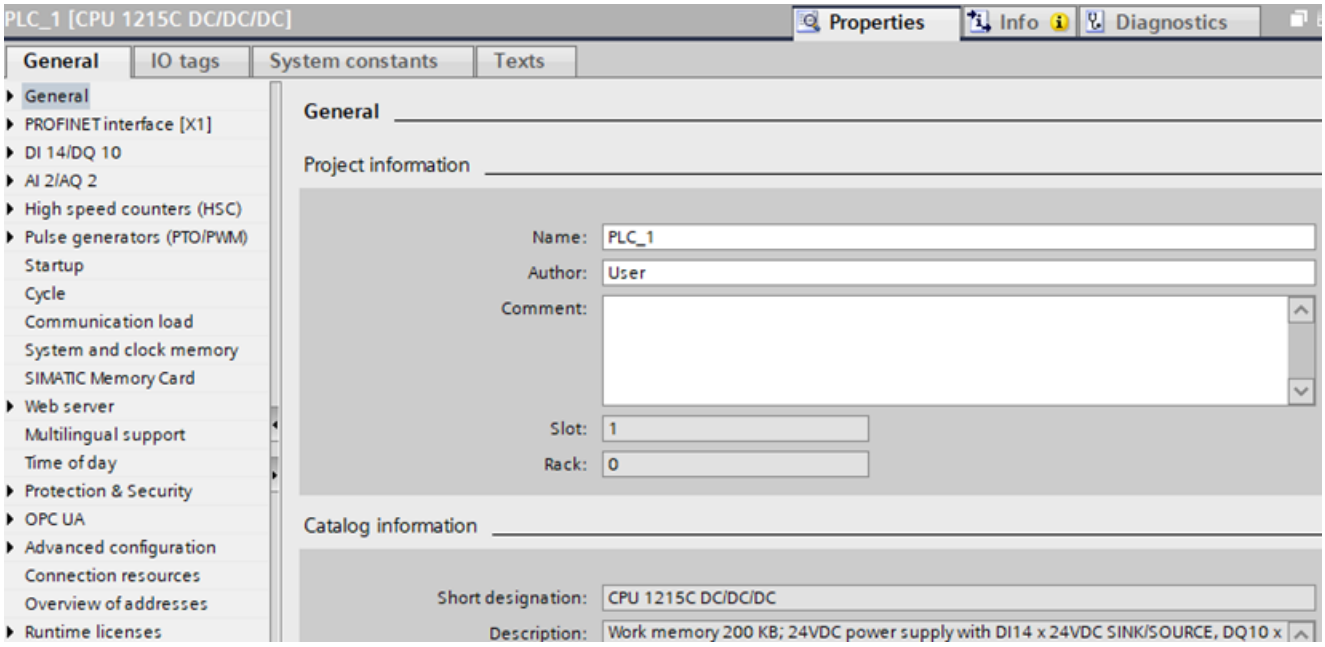


Table 7-2 CPU properties

Property	Description
General	Contains Project information, Catalog information, Identification & Maintenance, and Checksums.
PROFINET interface	Sets the IP address for the CPU and time synchronization.
DI, DO, and AI	Configures the behavior of the local (onboard) digital and analog I/O (Page 138) (for example, digital input filter times (Page 139) and digital output reaction (Page 1047) to a CPU stop).
High-speed counters (Page 480) and pulse generators (Page 419)	Enables and configures the high-speed counters (HSC) and the pulse generators used for pulse train operations (PTO) and pulse-width modulation (PWM). When you configure the outputs of the CPU or signal board as pulse generators (for use with the PWM, PTO, or motion control instructions), the corresponding output addresses are removed from the Q memory and cannot be used for other purposes in your user program. If your user program writes a value to an output used as a pulse generator, the CPU does not write that value to the physical output.

Property	Description
Startup (Page 64)	**Startup after POWER ON:** Selects the behavior of the CPU following an off-to-on transition, such as to start in STOP mode or to go to RUN mode after a warm restart.
	Comparison preset to actual configuration: Specifies the startup characteristics of the CPU for situations in which the actual configuration of the S7-1200 station does not correspond to the preset configuration: • Startup of the CPU only if compatible • Startup of the CPU even if mismatch A module in the configured slot must be compatible with the configured module. Compatible means that the module that is present matches the number of inputs and outputs and must match with respect to its electrical and functional properties. It may be more capable, but not less capable.
	Configuration time: Specifies a maximum amount of time (default: 60000 ms) in which the central I/O and distributed I/O must start up. (The CMs and CPs receive power and communication parameters from the CPU during startup. This assignment time allows time for the I/O connected to the CM or CP to be brought online.) The CPU goes to RUN as soon as the central I/O and distributed I/O and have started and are ready for operation, regardless of the assignment time. If the central I/O and distributed I/O have not been brought online within this time, the CPU still goes to RUN--without the central I/O and distributed I/O.
	OBs should be interruptible: Configures whether OB execution (for all OBs) in the CPU is interruptible or non-interruptible. (Page 77)
Cycle (Page 81)	Defines a maximum cycle time or a fixed minimum cycle time.
Communication load	Allocates a percentage of the CPU time to be dedicated to communication tasks.
System and clock memory (Page 84)	Enables a byte for "system memory" functions and enables a byte for "clock memory" functions (where each bit toggles on and off at a predefined frequency).
SIMATIC Memory Card	Allows you to configure the CPU to determine when the SD card has aged to a configured percentage value. You select "Aging of the SIMATIC Memory card" checkbox to configure the threshold value percentage. You can use the GetSMCInfo (Page 412) instruction to check the SIMATIC memory card against this configured value.
Web server (Page 753)	Enables and configures the Web server feature.
Multilingual support (Page 142)	Assigns a project language for the Web server to use for displaying diagnostics buffer entry texts for each of the possible Web server user interface display languages.
Time of day	Selects the time zone and configures daylight saving time.
Protection & Security (Page 151)	Sets the read/write protection and passwords for accessing the CPU. You have the following options for security settings: • Protection of PLC configuration data • Access protection • Connection mechanism • Certificate manager • Security events • System logging • External load memory

Property	Description
OPC UA (Page 720)	Shows the name of the OPC UA application. Allows for enabling and configuring of the OPC UA server and security settings You have the following options for the security settings: • Secure channel • Certificates Provides Diagnostics on status change, Diagnostics of additional events, and Summarize diagnostics incase of high message volume.
Advanced configuration	Contains: • DNS configuration (Page 558) - Configure the DNS server address. • Configuration control (Page 127) - Enables a configuration change in the user program within certain limits. • SNMP (Page 686) - activate SNMP (Simple Network Management Protocol.
Connection resources (Page 526)	Provides a summary of the communication connection resources that are available for the CPU and the number of connection resources that have been configured.
Overview of addresses	Provides a summary of the I/O addresses that have been configured for the CPU.
Runtime licenses	Select Type of required license and Type of purchased license (OPC-UA).

7.6.2 Configuring the onboard I/O

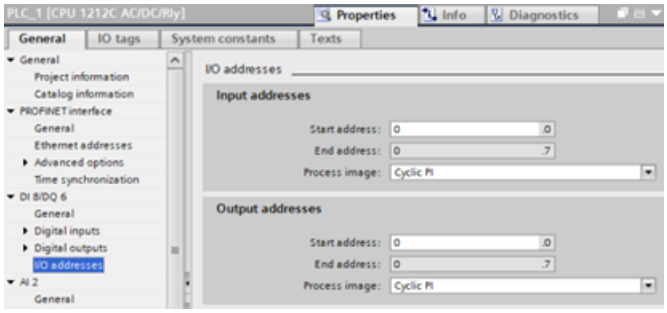
To configure the operational parameters for the modules, select the module in the Device view and use the "Properties" tab of the inspector window to configure the parameters for the module.

Configurable parameters

The device configuration for onboard I/O provides the means to configure the following:

- Digital I/O: You can configure inputs for rising-edge detection (Page 69), falling-edge detection (Page 69), or pulse catch (Page 140). Outputs can use freeze or substitute values (Page 88).
- Analog I/O: For individual inputs, configure parameters, such as measurement type (voltage or current), range and smoothing, and to enable underflow or overflow diagnostics. Analog outputs provide parameters such as output type (voltage or current) and for diagnostics, such as short circuit (for voltage outputs) or upper/lower limit diagnostics. You do not configure ranges of analog inputs and outputs in engineering units on the Properties dialog. You must handle this in your program logic as described in the topic "Processing of analog values (Page 94)".

- I/O addresses: You configure the start address for the I/O here. You can also assign the inputs and outputs to a process image partition (PIP0, PIP1, PIP2, PIP3, PIP4) or to automatically update, or to use no process image partition. See "Execution of the user program (Page 61)" for an explanation of the process image and process image partitions.



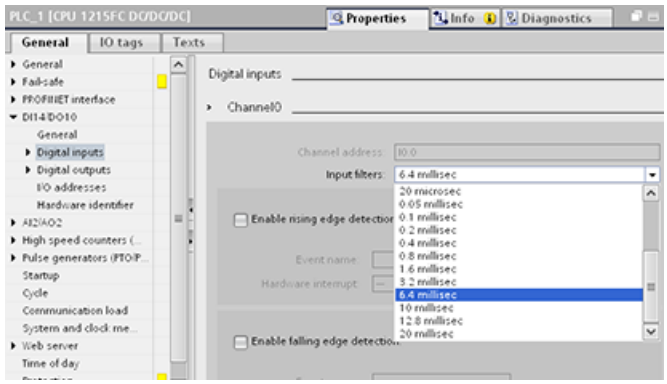
7.6.3 Configuring digital input filter times

The digital input filters protect your program from responding to unwanted fast changes in the input signals, as may result from switch contact bounce or electrical noise. The default filter time of 6.4 ms blocks unwanted transitions from typical mechanical contacts. Different points in your application can require shorter filter times to detect and respond to inputs from fast sensors, or longer filter times to block slow contact bounce or longer impulse noise.

An input filter time of 6.4 ms means that a single signal change, from ‘0’ to ‘1’ or from ‘1’ to ‘0’, must continue for approximately 6.4 ms to be detected, and a single high or low pulse shorter than approximately 6.4 ms is not detected. If an input signal switches between ‘0’ and ‘1’ more rapidly than the filter time, the input point value can change in the user program when the accumulated duration of new value pulses over old value pulses exceeds the filter time.

The digital input filter works as follows:

- When a "1" is input, it counts up, stopping at the filter time. The image register point changes from "0" to "1" when the count reaches the filter time.
- When a "0" is input, it counts down, stopping at "0". The image register point changes from "1" to "0" when the count reaches "0".
- If the input is changing back and forth, the counter will count up some and count down some. The image register will change when the net accumulation of counts reaches either the filter time or "0".
- A rapidly-changing signal with more "0’s" than "1’s" will eventually go to "0", and if there are more "1’s" than "0’s", the image register will eventually change to "1".



Each input point has a single filter configuration that applies to all uses: process inputs, interrupts, pulse catch (Page 140), and HSC inputs. To configure input filter times, select "Digital Inputs".
The default filter time for the digital inputs is 6.4 ms. You can select a filter time from the Input filters drop-down list. Valid filter times range from 0.1 us to 20.0 ms.

WARNING

Risks with changes to filter time for digital input channel

When changing the filter time for a digital input channel, a new input level transition value might need to stay constant for up to 20 ms before the filter becomes fully responsive. Because short input level transitions (less than 20.0 ms) might not be detected, unexpected machine or process operation can occur.

To ensure that the new filter time goes into effect immediately, power cycle the CPU.

Unexpected machine or process operation can cause death, injury, and equipment damage.

Configuring filter times for digital inputs used as HSCs

For inputs that you use as high-speed counters (HSCs), change the input filter time to an appropriate value to avoid missing counts.
Siemens recommends the following settings:

Type of HSC	Recommended input filter time
1 MHz	0.1 microseconds
100 kHz	0.8 microseconds
30 kHz	3.2 microseconds

7.6.4 Pulse catch

The S7-1200 CPU provides a pulse catch feature for digital input points. The pulse catch feature allows you to capture high-going pulses or low-going pulses that are of such a short duration that they would not always be seen when the CPU reads the digital inputs at the beginning of the scan cycle.

Enabling pulse catch

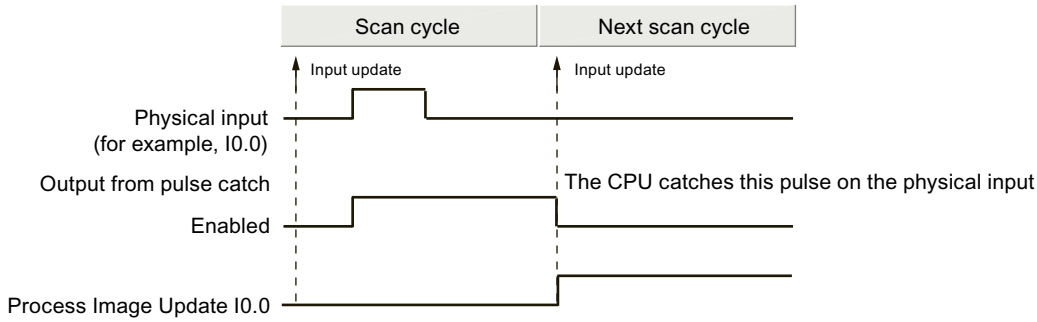
To enable pulse catch for a digital input, follow these steps:

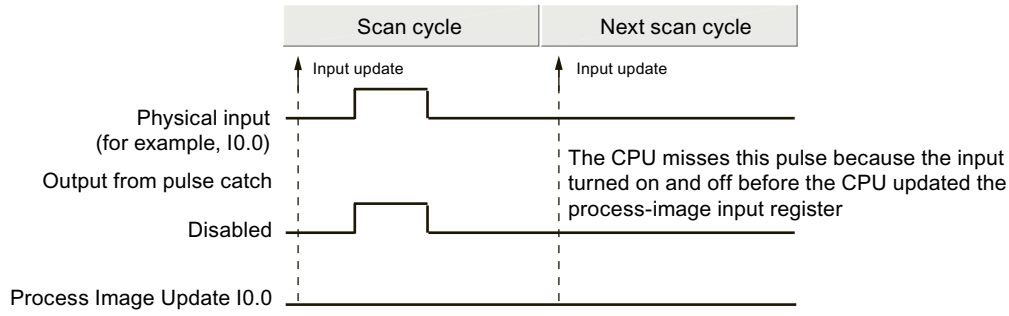
1. Select "Digital inputs" in the Inspector window.
2. Select the desired channel.
3. Select "Enable pulse catch."

Basic operation of pulse catch

When you enable pulse catch for an input, a change in state of the input is latched and held until the next input cycle update. This ensures that a pulse that lasts for a short period of time will be caught and held until the CPU reads the inputs.

The figures below show the basic operation of the S7-1200 CPU with and without pulse catch enabled:

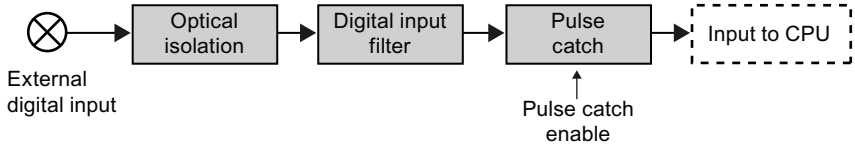




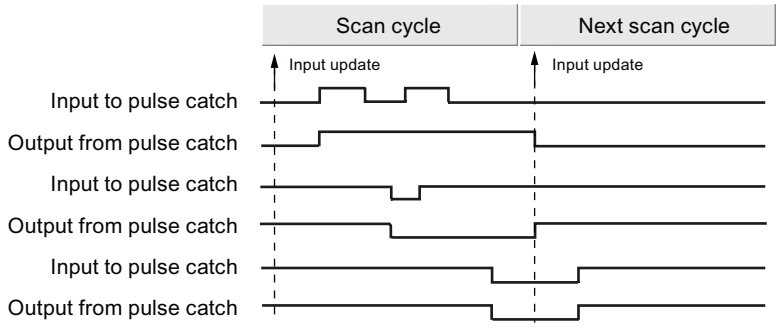
NOTE

Because the pulse catch function operates on the input after it passes through the input filter, you must adjust the input filter time so that the filter does not remove the pulse.

The figure below shows a block diagram of the digital input circuit:



The figure below shows the response of an enabled pulse catch function to various input conditions. If you have more than one pulse in a given scan, only the first pulse is read. If you have multiple pulses in a given scan, you should use the rising/falling edge interrupt events:



7.7 Configuring multilingual support

The Multilingual support settings allow you to assign one of two project languages for each user interface language for the S7-1200 Web server (Page 753). You can also configure no project language for a user interface language.

What is a project language?

The project language is the language that the TIA Portal uses to display user-defined project texts as network comments and block comments.

You select project languages in the TIA Portal from the **Tools > Project languages** menu command for the selected project in the project tree.

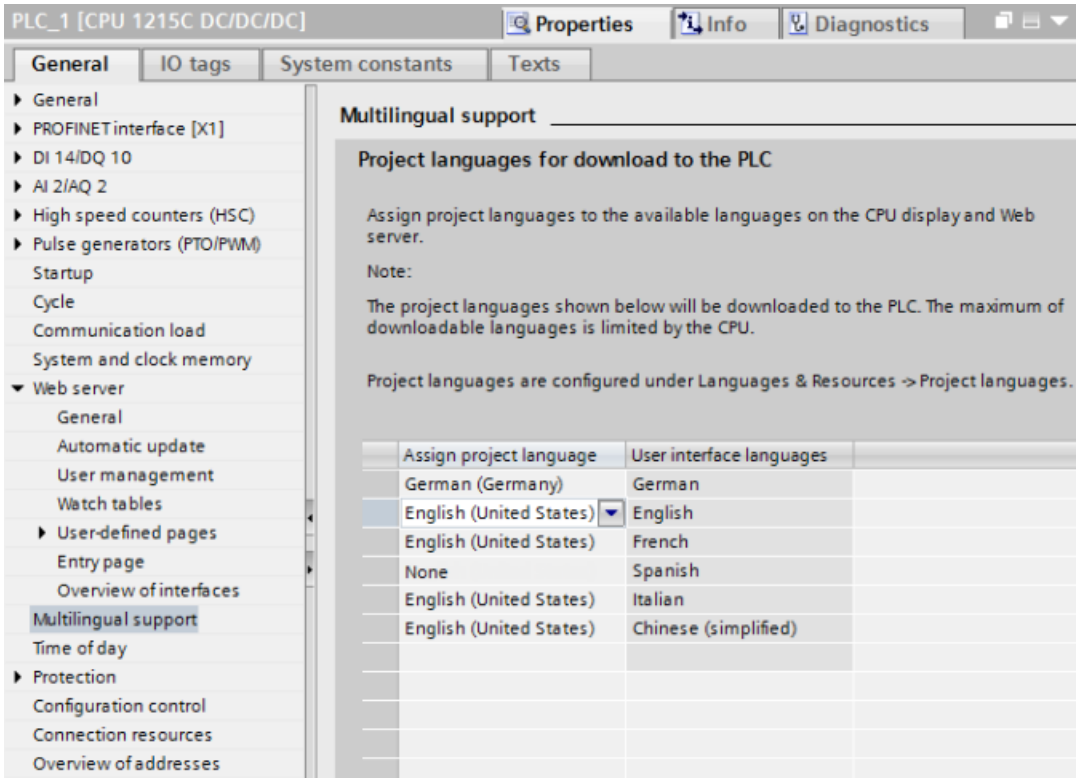
You can then configure user texts such as network comments and block comments in each project language from the **Tools > Project texts** menu command. Then when you change the TIA Portal user interface language, the network comments, block comments, and other multilingual project texts display in the corresponding project language. You set the TIA Portal user interface language from the **Options > Settings** project language menu command.

Project languages and project texts are also configurable from the **Languages & resources** node of the project tree.

The Web server can use one or two of the STEP 7 project languages for the display of diagnostics buffer messages.

Project language correspondence to user interface language in the Web server

The Web server supports the same user interface languages as the TIA Portal; however, it only supports up to two project languages. You can configure the Web server to use one of two project languages for diagnostics buffer text entries depending on the user interface language of the Web server. You configure these settings in the "Multilingual support" properties in the device configuration of the CPU. (Network comments and block comments and other multilingual texts are not visible from the Web server.)



In the Multilingual support properties, the user interface languages on the right are not editable. They are the pre-defined languages that are available for both the TIA Portal and for the Web server user interfaces. The "Assign project language" setting is configurable and can be one of two of your configured project languages, or it can be "None". Because the S7-1200 CPU only supports two project languages, you cannot configure the project language to be the same as the user interface language for all of the supported user interface languages.

In the configuration below, the Web server displays diagnostics buffer entries (Page 776) in German when the Web server user interface is German, displays no texts for diagnostics buffer events when the Web server user interface is Spanish, and displays diagnostics buffer entries in English for all other languages.

7.8 Protection & security

7.8.1 Using the security wizard to set PLC security settings

The security wizard in the TIA Portal provides a central place for you to configure PLC security settings. When you insert a CPU (Page 122) into your project, the TIA Portal launches the security wizard.

The security wizard consists of the following parts:

- Protection of confidential PLC data
- Mode for PG/PC and HMI communication
- PLC access protection
- Access control
- Overview

STEP 7 stores the settings that you make in the wizard to the project when you click "Finish" from the wizard. If you click "Cancel", STEP 7 does not keep your changes. The changes you make from the wizard affect only the STEP 7 project.

Protection of confidential PLC data

The "Protection of confidential PLC configuration data (Page 145)" feature allows you to protect each CPU in your project individually. Use the security wizard to enable this protection and to set a password for the protection of confidential PLC configuration data.

You can also configure protection of confidential PLC configuration data from the device configuration of the CPU (Page 145).

Mode for PG/PC and HMI communication

The mode for PG/PC and HMI communication allows you to use a PLC communication certificate (Page 521) to protect communication between your CPU and other devices such as the following:

- Programming devices (PGs) such as TIA Portal and the SIMATIC Automation Tool
- HMIs

From the wizard, select "Only allow secure PG/PC and HMI communication" to enable only secure communication.

If you need to communicate with devices that do not support secure communication, deselect "Only allow secure PG/PC and HMI communication". This selection enables your PLC to communicate using either secure communication or legacy communication (Page 521).

You can also configure the mode for PG/PC and HMI communication (Page 155) in the connection mechanisms in the device configuration of the CPU.

PLC access protection

PLC access protection allows you to restrict access to the PLC.

From the "PLC access protection" area under "Access control configuration", you can select from the following options:

- Disable access control
- Enable access control
- Enable access control and Use access control via access levels

The STEP 7 project enables access control by default. When enabled, only users with access rights can access the PLC after authenticating.

If you enable "Use access control via access levels", you can set access level passwords for the CPU from the "Access control" dialog of the security wizard.

Access control via access levels

After enabling "Use access control via access levels" from the "PLC access protection" area of the security wizard or from the device configuration of the CPU, you can set access level passwords (Page 151).

Overview

The overview selection of the security wizard displays your settings for the following areas:

- Protection of confidential PLC data (Page 145)
- Mode for PG/PC and HMI communication (Page 155)
- PLC access protection (Page 147)
- Access control (Page 151)

Review your settings and use the Back button if necessary to make changes. When you are satisfied with your settings, click "Finish". STEP 7 stores your settings in the project. You must download the project to the CPU for the security settings to take effect.

Launching the security wizard from the device configuration of the CPU

Alternatively, you can launch the security wizard manually from the "Device configuration" of the CPU in the "Protection & Security" section.

See also

OPC UA Server (Page 720)

Web server (Page 753)

7.8.2 Protection of confidential PLC configuration data

The "Protection of confidential PLC configuration data" feature allows you to protect the configuration of each CPU in your project. From the Protection & Security section of the device configuration, you can enable this protection and set a password for the protection of confidential PLC configuration data.

If you configure protection of confidential PLC configuration data note the following:

- If the device does not have this password, the TIA Portal prompts you to enter the password for protection of confidential PLC configuration data on the first download.
- If the device already has this protection password, the password in the STEP 7 project and in the device must match. If the passwords do not match, you cannot download the project to the CPU. You must delete the password for protection of confidential PLC configuration data or set it to the password in the device. You can set or delete the password in the device from Online & Diagnostics (Page 1056).

Security wizard

You can also use the security wizard (Page 144) to enable this feature and set the password. The security wizard launches when you first insert a CPU. You can also launch the security wizard from the Protection & Security section of the device configuration.

Benefit of protecting confidential PLC configuration data

The CPUs together with TIA Portal provide protection for each individual CPU. Protection of confidential PLC configuration data provides increased project storage security for each PLC.

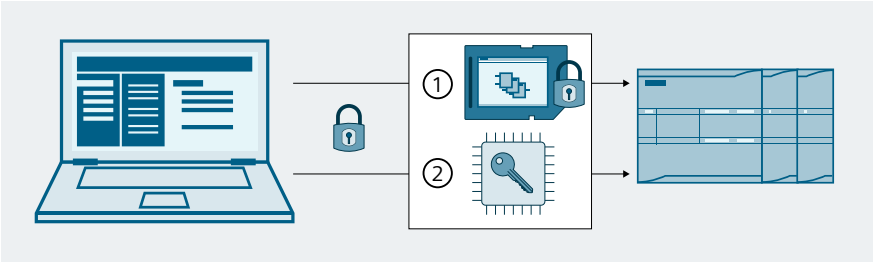
How the protection works

The protection functions much like a lock and key. You enable the protection of confidential PLC configuration data in the TIA Portal and set a password for this protection. Downloading the project sets the "protection of confidential PLC configuration data" password in the CPU. The CPU must have the password from either a project download or from a memory card (Page 115) to read project files. The project files contain your confidential configuration data.

Encryption:
You enable the "Protection of confidential PLC configuration data" in the TIA Portal and set a password. This password is the means to protect the confidential PLC configuration data.

Decryption:
You download the project to the CPU or alternatively load the project from a memory card (Page 115).
The CPU can now read (unlock) project files.

The password encryption in the project and the subsequent decryption in the CPU thus provide a high degree of protection for your confidential PLC configuration data.



① Project with password-protected confidential data on the memory card of the CPU

② Key information, generated from the password, in the memory area of the CPU that enables access to the protected confidential configuration data.

NOTE

Responsibility for CPUs

If you have configured and downloaded protection for confidential PLC configuration data to a CPU, securely dispose of the CPU when you decommission it.

If you have configured and downloaded protection for confidential PLC configuration data to a CPU and you later download a project to the CPU where the firmware version of the CPU in the STEP 7 project is earlier than V4.5, the CPU still contains the encrypted protection. If you decommission this CPU, securely dispose of it.

Securely disposing of decommissioned CPUs protects against third parties gaining access to the protected confidential configuration data.

Online tools

When the CPU is online, you can also set, delete, or change the password for "protection of confidential PLC configuration data" from the online and diagnostics tools (Page 1056).

Additional information

For additional information on the functionality and implementation, refer to the "Secure Communication" chapter in the TIA Portal Information System.

7.8.3 User Management & Access Control (UMAC)

UMAC allows you to grant specific users or user groups access to a PLC and can significantly reduce security risks.

You can perform local management of users, roles, and CPU function rights in the STEP 7 project.

UMAC provides the following features:

- Central management of local user administration in the STEP 7 project
- Ability to define roles and function rights for each CPU
- Ability to load UMAC configuration changes while the CPU is in STOP or RUN mode
- Ability to disable or enable the local user from the "Security settings > Users & roles" area of the Project tree
- Addition of Access protection for PG/HMI with authentication
- Ability to set password requirements and expiration for added security
- Improvement to algorithm for protection from brute force attacks
- Ability to add a configured CPU into an existing STEP 7 project and edit its UMAC configuration
- Ability to change passwords during runtime after you enter the original password

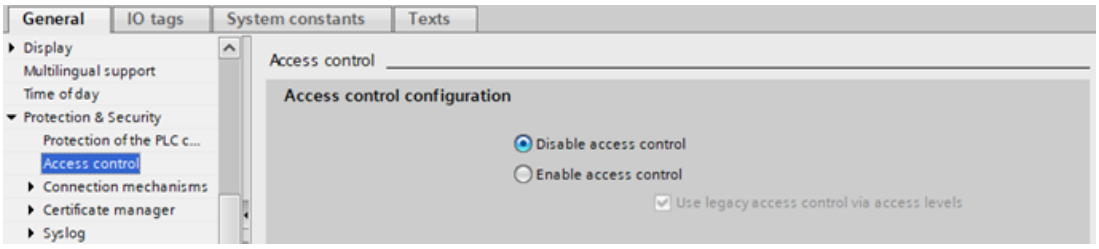
NOTE

UMAC does not support global user management for CPU-specific function rights. Use the User Management Component (UMC) to manage CPU-specific function rights for global users. UMC allows you to manage global users on connected servers. For example, with UMC you can manage global users through the connection of an MS Active Directory. UMC manages user authentication.

For more infomation on UMC, see "Managing global users and user groups" in the TIA Portal Help System.

Enabling and using UMAC

When you create a STEP 7 project, UMAC is enabled by default. You can disable UMAC from the security wizard when you add a CPU to the STEP 7 project. You can also disable UMAC from the device configuration of the CPU in the STEP 7 project. From the "Protection & Security > Access control" area, select "Disable access control". If you disable access control, every user has full access to the CPU without a password. You are essentially granting users "Full access (no protection)" (if using a standard CPU) or "Full access incl. fail-safe (no protection)" (if using an F-CPU). Users can access most CPU functions. Because of this, Siemens recommends disabling access control only during commissioning and that only authorized persons have access to the CPU during this phase.



NOTE

You do not need to enable access control via access levels (Page 151) when using UMAC.

When you create a STEP 7 project, you have the role of project administrator. Only the project administrator can create new user roles and assign function rights. Function rights determine what level of access each user has to the STEP 7 project and PLC process data. Each user role has unique function rights, giving the project administrator a more flexible and customizable security solution. As project administrator, you can update or change the function rights of a user role or delete a user role. You can also view the assigned function rights of a user from the secure STEP 7 project.

Project administrators can perform the following actions:

- Add or remove users
- Manage global users with UMC or TIA Portal Openness
- Create or delete user roles
- Set the STEP 7 project password for single sign-on access
- Assign or unassign function rights to all types of user roles
- Activate or deactivate the "Anonymous" user

After adding users and making role assignments, you must load the configuration to the CPU(s) to activate UMAC. After you load the configuration, each CPU in the configuration "knows" who can and cannot access certain services and execute certain functions.

WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server or OPC UA users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

- Enable Access control under "Protection & Security > Access control".
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Enable the setting "Only allow secure PG/PC and HMI communication" under "Protection & Security > Connection mechanisms".
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC from a location outside your protected network.
- Enable access to the Web server only with the HTTPS protocol.
- Perform error-checking and range-checking on your variables in your program logic because Web server or OPC UA users can change PLC variables to invalid values.
- For the OPC UA server: In your STEP 7 Device configuration, navigate to "Properties > OPC UA > Server > Security" and deselect "No security" in "Security policies available on the server for the secure channel".

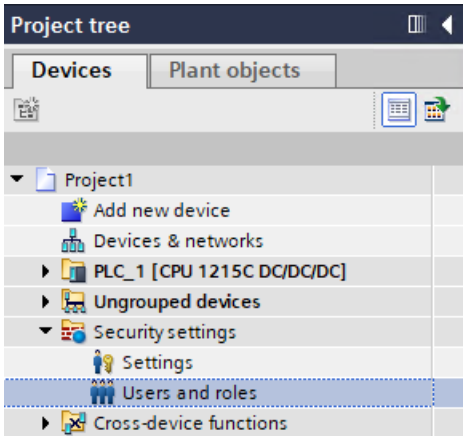
Disruption of process operations can result in death, severe personal injury, and/or property damage.

Creating and managing users, roles, and access rights

The CPU imposes the following limits in configuring users and roles:

- Maximum of 42 users
- Maximum of 14 user groups
- Maximum of 20 roles

You can create and manage all local project users, their roles, and their access rights from the "Security settings > Users and roles" area of the Project tree.



From this location, you manage access protection for engineering/HMI access, OPC UA, and Web server.

NOTE

If you see an information banner at the top of the User and roles section, close it to access the "Users", "User groups", and "Roles" tabs.

Defining roles and function rights for CPUs

The STEP 7 project includes defined function rights and assigned roles for each CPU.

NOTE

System-defined roles such as "HMI Administrator" do not have predefined function rights; you cannot add function rights to system-defined roles. You must create new roles and assign function rights to them.

To view a list of the CPU's function rights in the STEP 7 project, do the following:

1. From the Project tree, navigate to "Security settings > Users and roles".
2. Select the "Roles" tab, and then the "Runtime rights" tab.

From the "Roles" tab, you can "Add new roles" and select "Runtime rights" for each new role.

From "Users and roles" under the "Users" tab, you can select a user from the list and assign roles to it from the "Assigned roles" tab. Select the "Assigned rights" tab to see a comprehensive list of the "Runtime rights" assigned to any selected user.

The CPU function rights are valid during runtime. These rights are located in the "Runtime rights" tab in the editor for users and roles.

For more information on defining roles and function rights, refer to "Managing users and roles" in the TIA Portal Information System.

Activating or deactivating the "Anonymous" user

The STEP 7 project creates the "Anonymous" user by default; it is disabled for security reasons. You must enable it before use. Once enabled, the "Anonymous" user can log into the STEP 7 project without a password and the project administrator can assign roles or function rights to it. Any authorized user can enable or disable the "Anonymous" user.

You can set the default authentication procedure so that the "Anonymous" user account is always used when opening the project. For information on how to set the default authentication procedure, refer to the "Overview of user management settings" topic in the TIA Portal Information System.

NOTE

You can enable or disable the "Anonymous" user, but you cannot delete it. You cannot edit the "Anonymous" user's data:

- User name
- Password
- Runtime timeout
- UM domain ID
- Comment

WARNING

Security risks when activating the "Anonymous" user

Activating the "Anonymous" user makes a STEP 7 project more vulnerable, especially if you grant extensive rights to the "Anonymous" user.

For a more secure STEP 7 project, do not activate the "Anonymous" user.

Unauthorized access to the CPU or changing PLC variables to invalid values could disrupt process operation and could result in death, severe personal injury and/or property damage.

To enable or disable the "Anonymous" user, follow these steps:

1. From the "Project tree", select "Security settings > Users and roles".
2. Select the "Users" tab.
3. Select or deselect the check box for the "Anonymous" user.

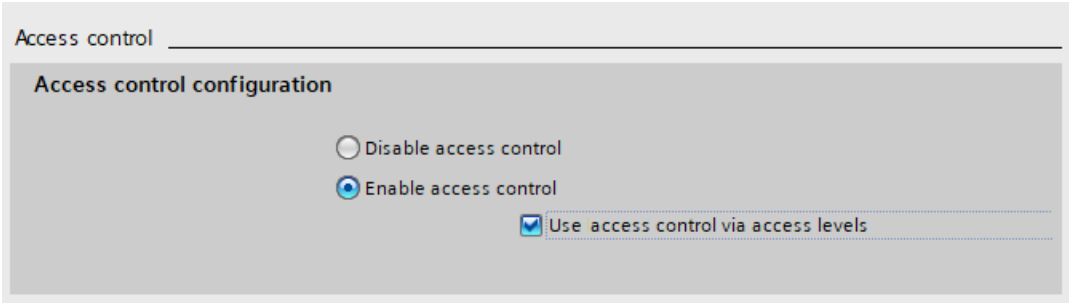
NOTE

After activating the anonymous user in the STEP 7 project, a window containing a security note opens to warn you of the potential security risks associated with activating the anonymous user. Click "Ok" if you wish to proceed.

For more information on UMAC or the actions a project administrator can perform refer to "Managing users and roles" in the TIA Portal Information System.

7.8.4 Access control for the S7-1200 CPU

When you enable Access control in the CPU's device configuration, the CPU provides levels of security for restricting access to specific functions. You can configure the access levels and passwords for the access levels.



If you select "Use access control via access levels", you can set access level passwords from the table, but you cannot configure the levels. You set access levels for CPU users from "Security settings > Users and roles > Roles > Runtime rights" (UMAC (Page 147)).

For security reasons, the STEP 7 project disables the "Anonymous" user by default. When it is disabled, the access level for users with no password is "No access (complete protection)". When it is enabled, the function right(s) assigned to the "Anonymous" user determines the CPU access level given to a user who logs in as the "Anonymous" user.

NOTE

You do not need to enable the "Anonymous" user to use access control. However, if you wish to change the access levels for the "Anonymous" user, you must enable it and set the desired function rights.

WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server or OPC UA users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

- Enable Access control (Page 147) under "Protection & Security > Access control".
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Enable the setting "Only allow secure PG/PC and HMI communication" under "Protection & Security > Connection mechanisms".
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC from a location outside your protected network.
- Enable access to the Web server only with the HTTPS protocol.
- Perform error-checking and range-checking on your variables in your program logic because Web server or OPC UA users can change PLC variables to invalid values.
- For the OPC UA server: In your STEP 7 Device configuration, navigate to "Properties > OPC UA > Server > Security" and deselect "No security" in "Security policies available on the server for the secure channel".

Disruption of process operations can result in death, severe personal injury, and/or property damage.

Each access level allows certain functions to be accessed without a password. The default setting for the CPU is "No access (complete protection)". To use any protection access level, you must provide a password for that level.

Access level	Access			Access permission
	HMI	Read	Write	Password
Full access (no protection)	✓	✓	✓	
Read access	✓	✓		
HMI access	✓			
No access (complete protection)				

Passwords are case-sensitive. The "Update password encryption" button upgrades the storage format of existing access level passwords.

Entering the password over a network does not compromise the password protection for the CPU. Password protection does not apply to the execution of user program instructions, including communication functions. Entering the correct password provides access to all of the functions at that level.

PLC-to-PLC communications (using communication instructions in the code blocks) are not restricted by the access level of the CPU.

Table 7-3 Access levels for the CPU

Access level	Access restrictions
Full access incl. fail-safe (no protection)[1]	Allows full access to an F-CPU without password protection.
Full access (no protection)	Allows full access to a standard CPU without password protection.
Read access	Allows read-only access to the hardware configuration and the blocks without entering a password. You can upload hardware configuration and blocks to the programming device. In addition, you have HMI access and access to diagnostics data. You can display offline/online comparison results, change the operating mode (RUN/STOP), and set the time of day. You cannot download blocks or a hardware configuration into the CPU. Firmware updates are not possible.
HMI access	Allows only HMI access In addition to providing access for HMI panels, HMI access allows use of most online functions. See the TIA Portal Information System for details.
No access (complete protection)	Allows no access without password. You can only see identification data, for example, "Accessible devices".

[1] The Full access incl. fail-safe (no protection) option is visible in the STEP 7 project only when using a Fail-safe CPU.

When using Access control, you can set an emergency (temporary) IP address (Page 719) for the CPU at any access level.

To activate Access control via access levels, follow these steps:

1. In the CPU properties, go to "Protection & Security > Access control".
2. Select "Enable access control" and "Use access control via access levels".
3. Enter passwords for the desired access levels.

NOTE

You can also set access level passwords from the security wizard (Page 144).

You can grant the "Anonymous" user access by assigning access level Function rights. The access level of the "Anonymous" user corresponds to the access level displayed in the access level table.

The following example shows how to set the access level to "Read access" for a CPU named "PLC_1":

1. Go to "Security Settings > Users and roles" in the CPU device configuration in the STEP 7 project.
2. Activate the "Anonymous" user.
3. Navigate to the "Roles" tab.
4. Add a new role and assign it a meaningful name, e.g. "PLC_1-Read-Access-Role". If you assign this role to a user, this user has read access to PLC_1 during operation.
5. Select the "Runtime rights" tab.

6. From the "Function rights categories" table, select the desired CPU, "PLC_1".
7. From the "Function rights" table, select the function rights to assign to the CPU for the role "PLC_1-Read-Access-Role". For this example, select "Read access".
8. Switch to the "User" tab and assign the "PLC_1-Read-Access-Role" role to the activated "Anonymous" user.

After activating access control and setting the access level, as described in the procedures above, the "Anonymous" user has read access to "PLC_1", and the access level for access control is preset to "Read access". Users who go online as the "Anonymous" user have only have read access.

For full access, or full access including fail-safe, you must configure a password for the "Full access" level in the table found on the CPU's Properties tab under Protection & Security > Access control. Local users who need full access to the CPU during runtime must log in with the configured CPU access level password. Local users can also log in with the user name and password of an existing user who already has full access to the CPU.

After configuring access levels and passwords in the STEP 7 project, you must download the project to the CPU to enable them.

For more information on how to set roles and function rights, see User Management & Access Control (UMAC) (Page 147).

Disabling access control

If you disable access control, every user has full access to the CPU without a password. You are essentially granting users "Full access (no protection)" (if using a standard CPU) or "Full access incl. fail-safe (no protection)" (if using an F-CPU). Users can access most CPU functions. Because of this, Siemens recommends disabling access control only during commissioning and that only authorized persons have access to the CPU during this phase.

See also

Assigning Web server user privileges for V4.7 configured CPUs (Page 757)

7.8.5 Configuring connection mechanisms

7.8.5.1 Setting access mechanism for remote partners

To access remote connection partners with PUT/GET instructions, the user must also have permission.

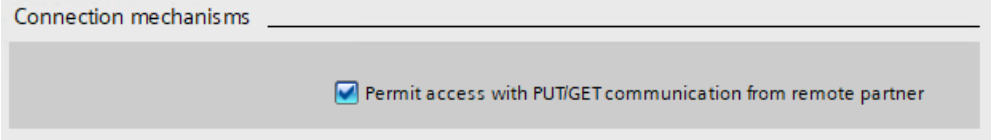
By default, the "Permit access with PUT/GET communication" option is not enabled. In this case, read and write access to CPU data is only possible for communication connections that require configuration or programming both for the local CPU and for the communication partner. Access through BSEND/BRCV instructions is possible, for example.

Connections for which the local CPU is only a server (meaning that no configuration/programming of the communication with the communication partner exists at the local CPU), are therefore not possible during operation of the CPU, for example:

- PUT/GET, FETCH/WRITE or FTP access through communication modules
- PUT/GET access from other S7 CPUs
- HMI access through PUT/GET communication

If you want to allow access to CPU data from the client side, follow these steps:

1. Enable the "Anonymous" user under "Security Settings" > "Users and roles".
2. Assign the "Anonymous" user any CPU access level.
3. In the CPU's "Device configuration" inspector window, select the "Properties" tab > "Protection & Security" and click the check box for "Permit access with PUT/GET communication from remote partner".



When you download this configuration to the CPU, the CPU permits PUT/GET communication from remote partners.

WARNING

Avoiding security risks from physical network attacks

If an attacker can physically access your networks, the attacker can possibly read and write data.

For example, I/O exchange through PROFIBUS, PROFINET, AS-i, or other I/O bus, GET/PUT, T-Block, and communication modules (CMs) have no security features. You must protect these forms of communication by limiting physical access. If an attacker can physically access your networks using these forms of communication, the attacker can possibly read and write data.

If you fail to protect these forms of communication, death or severe personal injury can result.

For security information and recommendations, see the "Operational Guidelines" white paper on the Siemens Industrial Cybersecurity Web site (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

7.8.5.2 Enabling secure PG/PC and HMI communication and creating certificates

Use the "Connection mechanisms" in the device configuration of your CPU to configure whether the CPU accepts only secure communication or accepts both secure and legacy communication. Secure communication uses X.509 certificates over TLS (Transport Layer Security) 1.3. The CPU uses these certificates to provide secure communication between the CPU and clients. Clients include:

- TIA Portal
- SIMATIC Automation Tool
- HMIs

Select "Permit only secure PG/PC and HMI communication" to disable legacy PG/PC and HMI communication.

You can also create your own certificates (Page 529). Click "..." next to "PLC communication certificate" to add a new certificate for the CPU or to select an existing certificate. Refer to the topic "Create / renew certificates" in the TIA Portal Information System for details about certificate configuration parameters.

The configuration sections within "Protection & Security" of the device configuration provide on-screen guidance about your security choices. These sections also provide links to topics in

the TIA Portal Information System for each configuration task and the related security concepts.

Legacy communication

If you need to communicate with a device that does not support secure communication, deselect "Permit only secure PG/PC and HMI communication". This selection enables your PLC to communicate using either secure communication or legacy communication (Page 521).

TIA Portal defaults to the highest level of secure communications; however, for commissioning reasons you can force the TIA Portal to use legacy PG/PC communications by selecting "Use only legacy PG/PC communication" from the Online menu.

Security wizard

You can also use the security wizard (Page 144) to configure PG/PC and HMI communication for V4.x CPUs.

WARNING

Potential safety risks during commissioning

During commissioning, the CPU provides a self-signed certificate that you must trust to establish a connection. In an unprotected environment, attackers can manipulate these certificates and access communication between the programming device/HMI and the CPU, for example, through man-in-the-middle attacks.

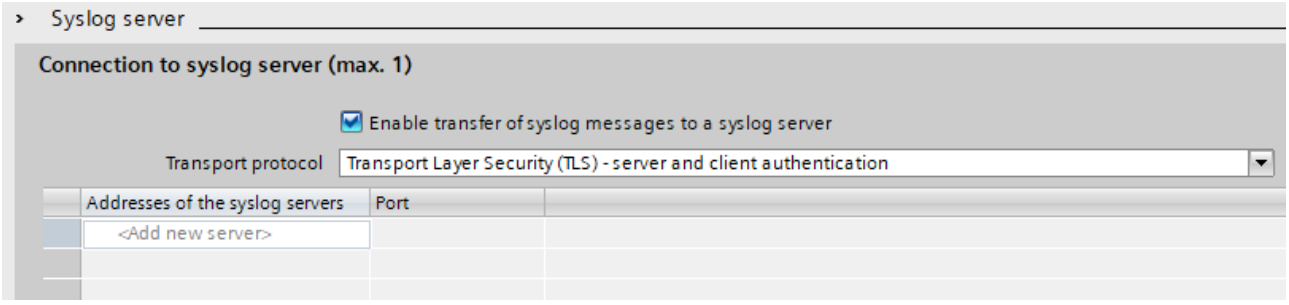
Only trust the self-signed certificate if the programming device and the CPU are on a protected network and directly connected to each other.

Attacks due to an unprotected communication environment can disrupt process operation and lead to death, severe personal injury, or property damage.

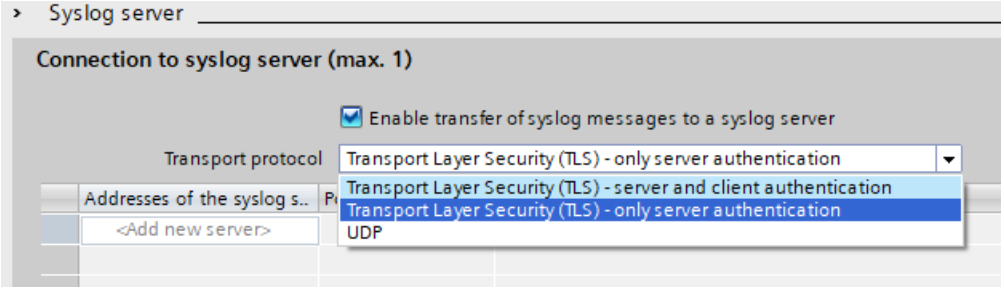
7.8.6 Syslog server

To configure the CPU to transfer syslog messages to a syslog server, follow these steps:

1. Select the required CPU in the device or network view of STEP 7.
2. In the Inspector window, navigate to "Properties > Protection & Security > Syslog > Syslog server".
3. In the "Connection to syslog server" area, check the option "Enable transfer of syslog messages to syslog servers". The selection options below become editable.



4. Select one of the following options from the "Transport protocol" drop-down list:
   - Transport Layer Security (TLS) - server and client authentication: Encrypted data transfer; syslog server and client (CPU) must authenticate themselves.
   - Transport Layer Security (TLS) - only server authentication: Encrypted data transfer; only the syslog server needs to authenticate itself.
   - UDP: Unencrypted data transfer, syslog server and client (CPU) do not need to authenticate themselves.

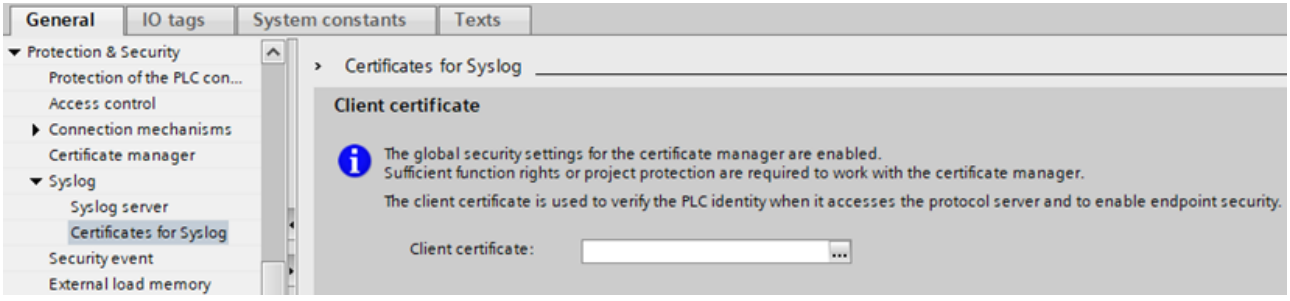


5. In the "Addresses of the syslog servers" column, enter a valid server address.
6. In the "Port" column, enter one of the following port numbers depending on the transport protocol used:
   - Standard TCP port for TLS: 6514
   - Standard UDP port: 514

Selecting the client certificate

STEP 7 provides the required client certificate for a CPU for the TLS transport protocol. If the certificate is managed within the CPU, you can either choose an existing certificate or create a new certificate. To do so, follow these steps:

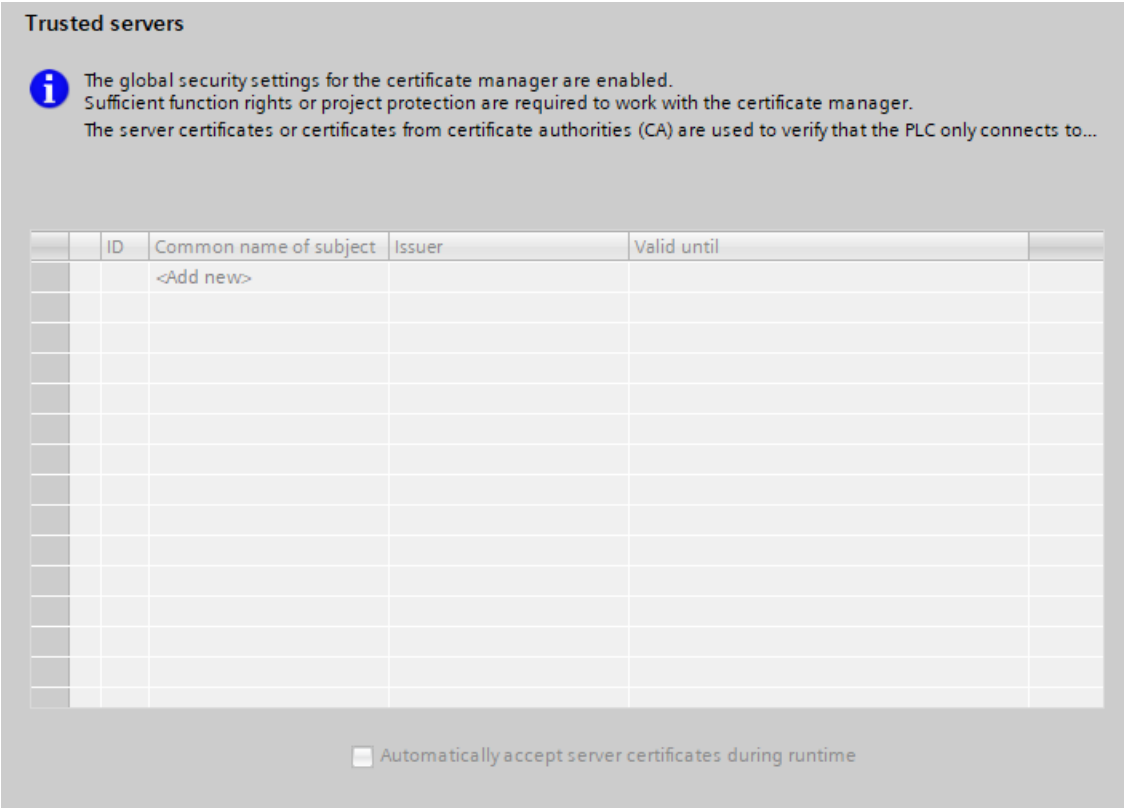
1. Select the required CPU in the device or network view of STEP 7.
2. In the Inspector window, navigate to "Properties > Protection & Security > Syslog > Certificates for Syslog".
   The certificate generated by STEP 7 is displayed next to "Client certificate".



Selecting the server authentication

After selecting the TLS transport protocol, the configured syslog server must authenticate itself. This ensures that the CPU only connects to a trusted server. If you want to waive server authentication, activate the automatic acceptance of server certificates during runtime. To configure these settings, do the following:

1. Select the required CPU in the device or network view of STEP 7.
2. In the Inspector window, navigate to "Properties > Protection & Security > Syslog > Certificates for Syslog".
3. In the "Trusted servers" area, specify whether the connected syslog server should be authenticated.



– Add trusted server: Add a valid server certificate in the "Common name of subject" column.
– Automatically accept certificates during runtime: If you want to waive server authentication, activate the "Automatically accept server certificates during runtime" option. Editing in the table is then not possible.

NOTE

No authentication with automatically accepted server certificates

If you enable the "Automatically accept server certificates during runtime" option, a server does not need to authenticate itself. This means that the CPU can also connect to unknown servers, which might create a security risk.

Only select this option during commissioning or in a protected environment.

7.8.7 External load memory

You can also prevent copies of internal load memory to external load memory (SIMATIC memory card). To prevent the copying of internal load memory to external load memory follow these steps:

1. From the device configuration of the CPU in STEP 7, select "Protection & Security" from the General properties.
2. In the "External Load Memory" section, select "Disable copy from internal load memory to external load memory".

See also the topic Inserting a memory card in the CPU (Page 106) for a description of how this property affects the insertion of a memory card into the CPU.

7.8.8 Know-how protection

Know-how protection allows you to prevent one or more code blocks (OB, FB, FC, or DB) in your program from unauthorized access. You create a password to limit access to the code block. The password-protection prevents unauthorized reading or modification of the code block. Without the password, you can read only the following information about the code block:

- Block title, block comment, and block properties
- Transfer parameters (IN, OUT, IN_OUT, Return)
- Call structure of the program
- Global tags in the cross references (without information on the point of use), but local tags are hidden

When you configure a block for "know-how" protection, the code within the block cannot be accessed unless you enter the password.

Use the "Properties" task card of the code block to configure the know-how protection for that block. After opening the code block, select "Protection" from Properties.

1. Click the "Protection" button to display the "Know-how protection" dialog.

Figure

2. Click the "Define" button to enter the password.
3. Enter a new password and confirm it.
4. Click "OK" to finish.

7.8.9 Write protection

Write protection for blocks prevents them from being changed unintentionally. Blocks with write protection can only be opened as "read only"; the block properties can however still be edited.

To set Write protection for a code block, follow these steps:

1. Open the "Properties" task card of the code block.
2. After opening the properties of the code block, select "Protection".
3. In the area "Write protection" select "Define password".
4. From the "Define protection" dialog, enter the password in the fields "New password" and "Confirm password".
5. Confirm your entries with "OK".
6. Select the "Write protection" check box.
7. From the "Access protection" dialog, enter the correct password.

After these steps, Write protection is enabled and will be active the next time the block is opened

7.8.10 Copy protection

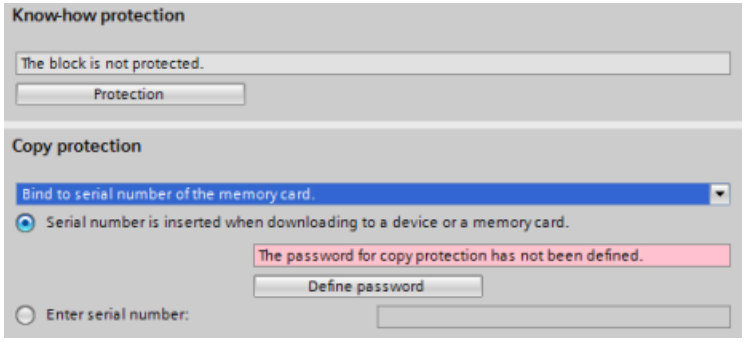
An additional security feature allows you to bind program blocks for use with a specific memory card or CPU. This feature is especially useful for protecting your intellectual property. When you bind a program block to a specific device, you restrict the program or code block for use only with a specific memory card or CPU. This feature allows you to distribute a program or code block electronically or by sending a SIMATIC memory card. Copy protection is available for OBs (Page 170), FBs (Page 172), and FCs (Page 172). The S7-1200 CPU supports three types of block protection:

- Binding to the serial number of a CPU
- Binding to the serial number of a memory card
- Dynamic binding with mandatory password

Use the "Properties" task card of the code block to bind the block to a specific CPU or memory card.

1. After opening the code block, select "Protection".

2. From the drop-down list under "Copy protection" task, select the type of copy protection that you want to use.



3. For binding to the serial number of a CPU or memory card, select either to insert the serial number when downloading, or enter the serial number for the memory card or CPU.

NOTE

The serial number is case-sensitive.

For dynamic binding with mandatory password, define the password that you must use to download or copy the block.

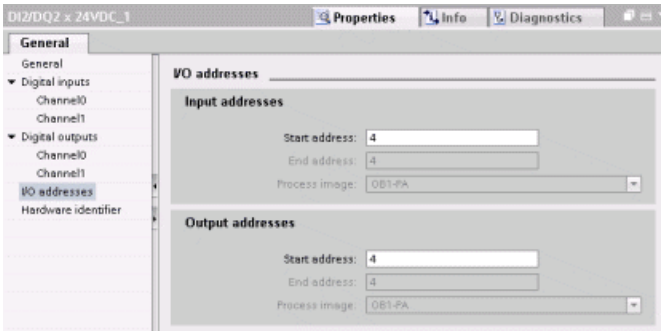
When you subsequently download (Page 189) a block with dynamic binding, you must enter the password to be able to download the block. Note that the copy protection password and the know-how protection (Page 159) password are two separate passwords.

7.9 Configuring the parameters of the modules

To configure the operational parameters for the modules, select the module in the Device view and use the "Properties" tab of the inspector window to configure the parameters for the module.

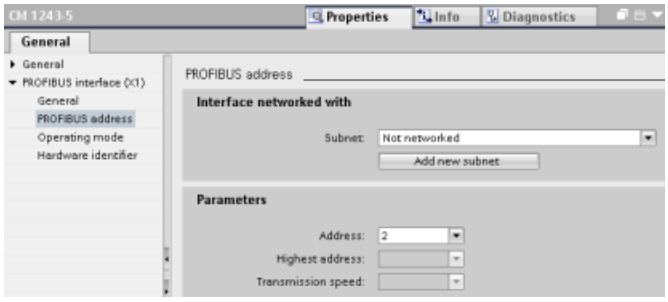
Configuring a signal module (SM) or a signal board (SB)

Use the same steps for configuring the onboard I/O (Page 138) of a CPU to configure the I/O of an SM or SB. You cannot configure signal module inputs for rising-edge detection (Page 69), falling-edge detection (Page 69), or pulse catch (Page 140).



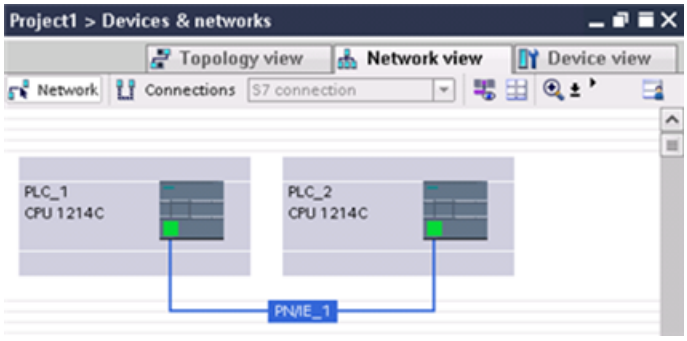
Configuring a communication interface (CM, CP or CB)

Depending on the type of communication interface, configure the parameters for the network.



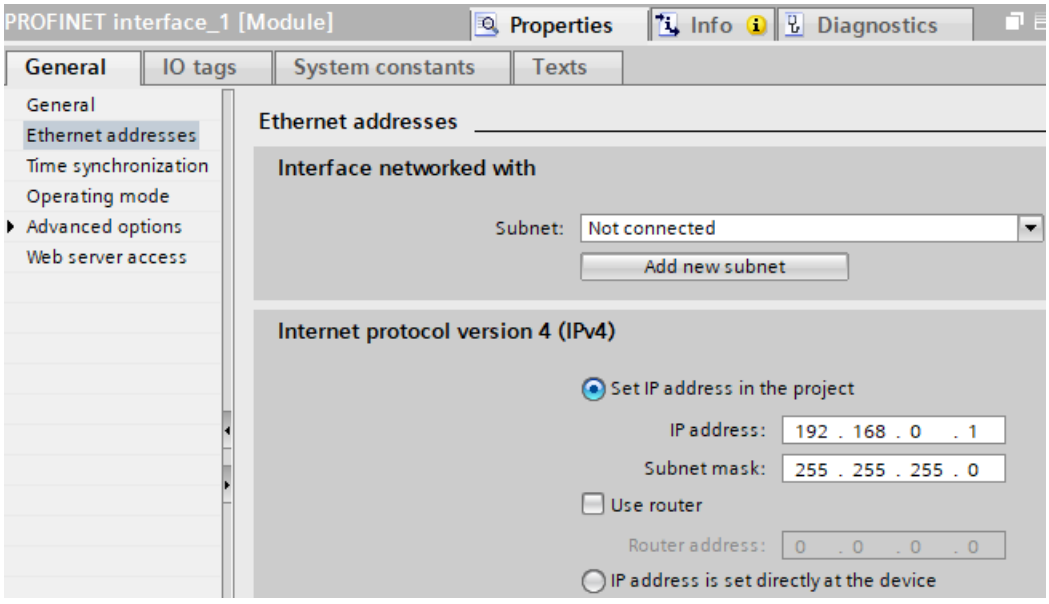
7.10 Configuring the CPU for communication

The S7-1200 is designed to solve your communications and networking needs by supporting not only the simplest of networks but also supporting more complex networks. The S7-1200 also provides tools that allow you to communicate with other devices, such as printers and weigh scales which use their own communications protocols.



Use the "Network view" of Device configuration to create the network connections between the devices in your project. After creating the network connection, use the "Properties" tab of the inspector window to configure the parameters of the network.

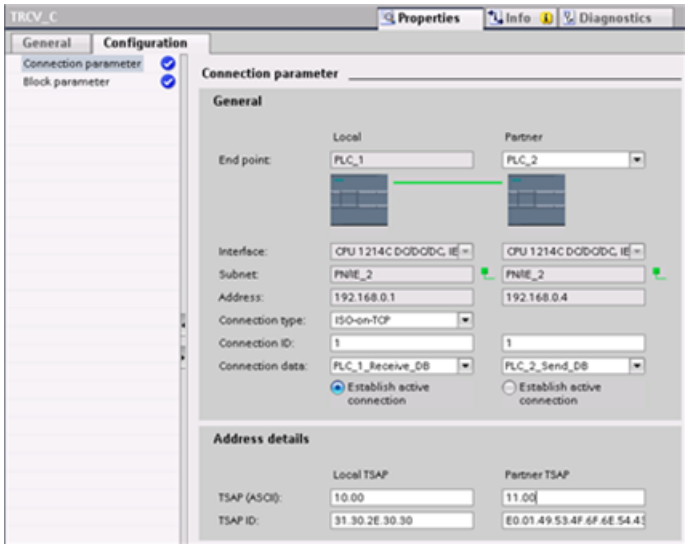
Refer to "Creating a network connection" (Page 531) for further information.



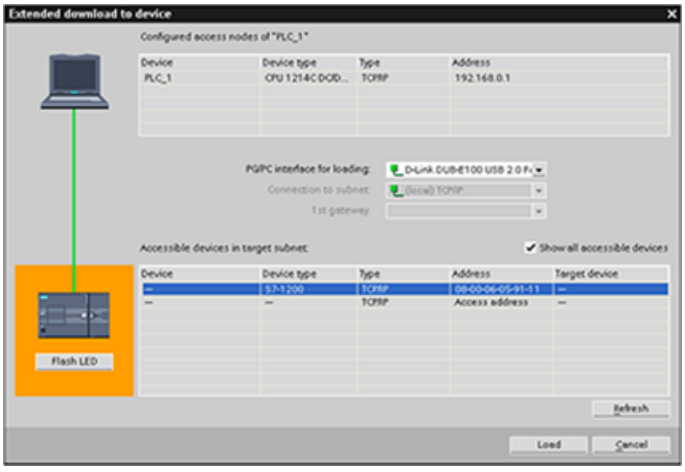
In the Properties window, select the "Ethernet addresses" configuration entry. STEP 7 displays the Ethernet address configuration dialog, which associates the software project with the IP address of the CPU that will receive that project.

Note: The S7-1200 CPU does not have a pre-configured IP address. You must manually assign an IP address for the CPU.

Refer to "Assigning Internet Protocol (IP) addresses" (Page 535) for further information.



For the TCP, ISO-on-TCP, and UDP Ethernet protocols, use the "Properties" of the instruction (TSEND_C, TRCV_C, or TCON) to configure the "Local/Partner" connections.
The figure shows the "Connection properties" of the "Configuration tab" for an ISO-on-TCP connection.
Refer to "Configuring the Local/Partner connection path" (Page 532) for further information.



After completing the configuration, download the project to the CPU. All IP addresses are configured when you download the project.
Refer to "Testing the PROFINET network" (Page 542) for further information.

NOTE

To make a connection to your CPU, your network interface card (NIC) and the CPU must be on the same class of network and on the same subnet. You can either set up your network interface card to match the default IP address of the CPU, or you can change the IP address of the CPU to match the network class and subnet of your network interface card.

Refer to "Assigning Internet Protocol (IP) addresses" (Page 535) for information about how to accomplish this.

7.11 Time synchronization

The objective of time synchronization of the time-of-day clocks is to have one master clock that synchronizes all other local clocks. The master clock synchronizes the local clocks initially and also periodically re-synchronizes the clocks to avoid the effects of drift over time.

In the case of the S7-1200 and its local base components, only the CPU and some of the CP modules have time-of-day clocks that might need to be synchronized. You can configure the CPU's time-of-day clock to be synchronized to an external master clock. The external master clock might supply the time of day using an NTP server or through a CP in the local rack of the S7-1200 that is connected to a SCADA system that includes a master clock.

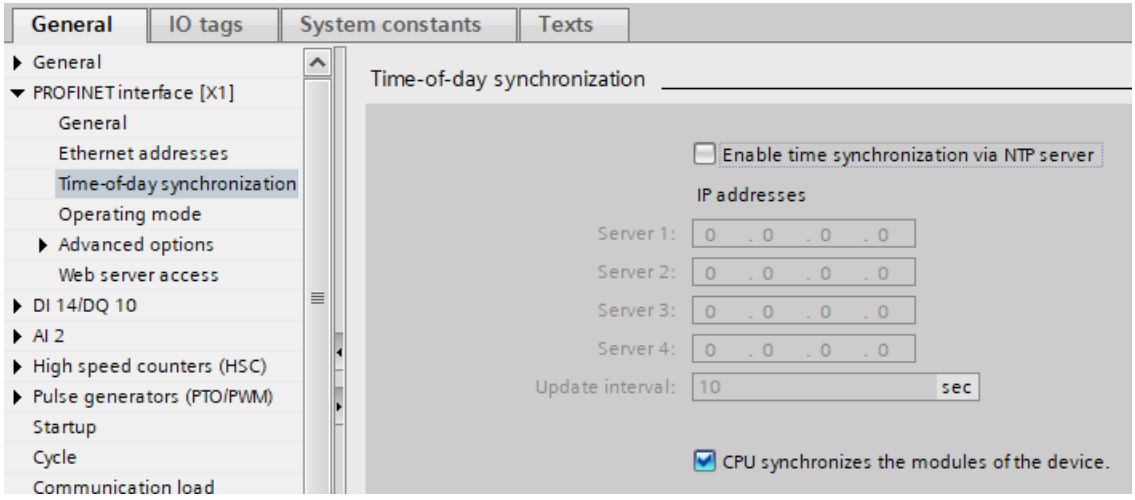
Refer to S7-1200 CPs (https://support.industry.siemens.com/cs/us/en/ps) at Siemens Industry Online Support for further information on all S7-1200 CPs that support the Time synchronization function.

Setting the time-of-day clock

There are five ways to set the time-of-day clock in the S7-1200 CPU:

- Using the NTP server (Page 544)
- Using STEP 7
- From the user program
- Using an HMI panel
- From the SIMATIC Automation Tool

You configure time synchronization of the CP modules to the CPU's clock by selecting the "CPU synchronizes the modules of the device." check box as shown:



By default, neither time synchronization using the NTP server nor time synchronization of the CP clocks to the CPU's clock is enabled.

You configure time synchronization of the CPU's clock and time synchronization of the CP clocks independently. Consequently, you can enable time synchronization of the CP clocks by the CPU when the CPU's clock is set by any of the above-mentioned methods.

You can select the update interval using the NTP server. The update interval of the NTP server is set to 10 seconds by default.

When you activate time synchronization in a module, STEP 7 prompts you to select the "CPU synchronizes the modules of the device." if you have not already selected the check box in the CPU's "Time synchronization" dialog. STEP 7 also warns you if you configured more than one master clock source for time synchronization.

WARNING

Risk of attacker accessing your networks through open interfaces

If an attacker can access your networks through open interfaces, such as software like STEP 7 or SAT, or through an HMI, the attacker can possibly disrupt control of your process by shifting the CPU system time.

The S7-1200 CPU supports "time of day" interrupts and clock instructions that depend upon accurate CPU system time. You must restrict access to the CPU by enabling access control and disabling the "Anonymous" user. Failure to do so can cause a security breach that allows an unknown user to disrupt control of your process by shifting the CPU system time.

Disruptions to process control can possibly cause death, severe injury, or property damage.

For security information and recommendations, see the "Operational Guidelines" white paper on the Siemens Industrial Cybersecurity Website.

NOTE

Only configure one time source for the CPU

Receiving time synchronizations for the CPU from more than one source (NTP server or CP module, for example) could cause conflicting time updates. Time synchronizations from multiple sources could adversely affect instructions and events based on time of day.

Programming concepts 8

8.1 Guidelines for designing a PLC system

When designing a PLC system, you can choose from a variety of methods and criteria. The following general guidelines can apply to many design projects. Of course, you must follow the directives of your own company's procedures and the accepted practices of your own training and location.

Table 8-1 Guidelines for designing a PLC system

Recommended steps	Tasks
Partition your process or machine	Divide your process or machine into sections that have a level of independence from each other. These partitions determine the boundaries between controllers and influence the functional description specifications and the assignment of resources.
Create the functional specifications	Write the descriptions of operation for each section of the process or machine, such as the I/O points, the functional description of the operation, the states that must be achieved before allowing action for each actuator (such as a solenoid, a motor, or a drive), a description of the operator interface, and any interfaces with other sections of the process or machine.
Design the safety circuits	Identify any equipment that might require hard-wired logic for safety. Remember that control devices can fail in an unsafe manner, which can produce unexpected startup or change in the operation of machinery. Where unexpected or incorrect operation of the machinery could result in physical injury to people or significant property damage, consider the implementation of electromechanical overrides (which operate independently of the PLC) to prevent unsafe operations. The following tasks should be included in the design of safety circuits: • Identify any improper or unexpected operation of actuators that could be hazardous. • Identify the conditions that would assure the operation is not hazardous, and determine how to detect these conditions independently of the PLC. • Identify how the PLC affects the process when power is applied and removed, and also identify how and when errors are detected. Use this information only for designing the normal and expected abnormal operation. You should not rely on this "best case" scenario for safety purposes. • Design the manual or electromechanical safety overrides that block the hazardous operation independent of the PLC. • Provide the appropriate status information from the independent circuits to the PLC so that the program and any operator interfaces have necessary information. • Identify any other safety-related requirements for safe operation of the process.
Plan system security	Determine what level of protection (Page 144) you require for access to your process. You can password-protect CPUs and program blocks from unauthorized access.
Specify the operator stations	Based on the requirements of the functional specifications, create the following drawings of the operator stations: • Overview drawing that shows the location of each operator station in relation to the process or machine. • Mechanical layout drawing of the devices for the operator station, such as display, switches, and lights. • Electrical drawings with the associated I/O of the PLC and signal modules.

Recommended steps	Tasks
Create the configuration drawings	Based on the requirements of the functional specification, create configuration drawings of the control equipment: • Overview drawing that shows the location of each PLC in relation to the process or machine. • Mechanical layout drawing of each PLC and any I/O modules, including any cabinets and other equipment. • Electrical drawings for each PLC and any I/O modules, including the device model numbers, communications addresses, and I/O addresses.
Create a list of symbolic names	Create a list of symbolic names for the absolute addresses. Include not only the physical I/O signals, but also the other elements (such as tag names) to be used in your program.

8.2 Structuring your user program

When you create a user program for the automation tasks, you insert the instructions for the program into code blocks:

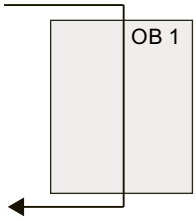
- An organization block (OB) responds to a specific event in the CPU and can interrupt the execution of the user program. The default for the cyclic execution of the user program (OB 1) provides the base structure for your user program. If you include other OBs in your program, these OBs interrupt the execution of OB 1. The other OBs perform specific functions, such as for startup tasks, for handling interrupts and errors, or for executing specific program code at specific time intervals.
- A function block (FB) is a subroutine that is executed when called from another code block (OB, FB, or FC). The calling block passes parameters to the FB and also identifies a specific data block (DB) that stores the data for the specific call or instance of that FB. Changing the instance DB allows a generic FB to control the operation of a set of devices. For example, one FB can control several pumps or valves, with different instance DBs containing the specific operational parameters for each pump or valve.
- A function (FC) is a subroutine that is executed when called from another code block (OB, FB, or FC). The FC does not have an associated instance DB. The calling block passes parameters to the FC. The output values from the FC must be written to a memory address or to a global DB.

Choosing the type of structure for your user program

Based on the requirements of your application, you can choose either a linear structure or a modular structure for creating your user program:

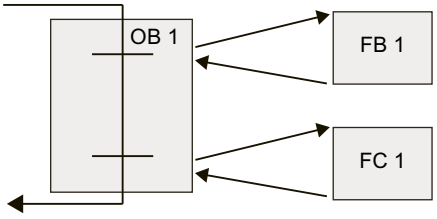
- A linear program executes all of the instructions for your automation tasks in sequence, one after the other. Typically, the linear program puts all of the program instructions into the OB for the cyclic execution of the program (OB 1).
- A modular program calls specific code blocks that perform specific tasks. To create a modular structure, you divide the complex automation task into smaller subordinate tasks that correspond to the technological functions of the process. Each code block provides the program segment for each subordinate task. You structure your program by calling one of the code blocks from another block.

Linear structure:



Figure

Modular structure:



Figure

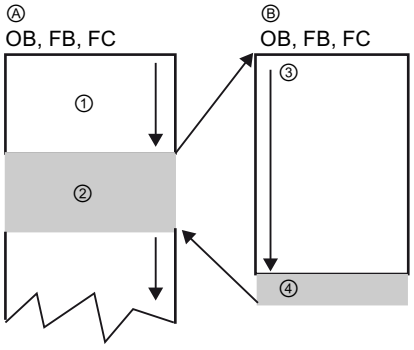
By creating generic code blocks that can be reused within the user program, you can simplify the design and implementation of the user program. Using generic code blocks has a number of benefits:

- You can create reusable blocks of code for standard tasks, such as for controlling a pump or a motor. You can also store these generic code blocks in a library that can be used by different applications or solutions.
- When you structure the user program into modular components that relate to functional tasks, the design of your program can be easier to understand and to manage. The modular components not only help to standardize the program design, but can also help to make updating or modifying the program code quicker and easier.
- Creating modular components simplifies the debugging of your program. By structuring the complete program as a set of modular program segments, you can test the functionality of each code block as it is developed.
- Creating modular components that relate to specific technological functions can help to simplify and reduce the time involved with commissioning the completed application.

8.3 Using blocks to structure your program

By designing FBs and FCs to perform generic tasks, you create modular code blocks. You then structure your program by having other code blocks call these reusable modules. The calling block passes device-specific parameters to the called block.

When a code block calls another code block, the CPU executes the program code in the called block. After execution of the called block is complete, the CPU resumes the execution of the calling block. Processing continues with execution of the instruction that follows after the block call.



A Calling block

B Called (or interrupting) block

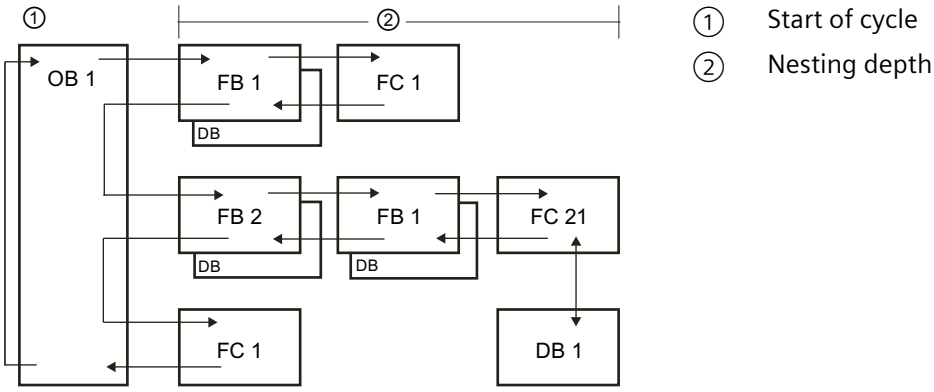
① Program execution

② Instruction or event that initiates the execution of another block

③ Program execution

④ Block end (returns to calling block)

You can nest the block calls for a more modular structure. In the following example, the nesting depth is 3: the program cycle OB plus 3 layers of calls to code blocks.



The maximum nesting depth is 16 from a cycle or startup OB. From an interrupt OB, the nesting depth is 6.

Safety programs have a nesting depth of 4 for safety blocks.

8.3.1 Organization block (OB)

Organization blocks provide structure for your program. They serve as the interface between the operating system and the user program. OBs are event driven. An event, such as a diagnostic interrupt or a time interval, causes the CPU to execute an OB. Some OBs have predefined start events and behavior.

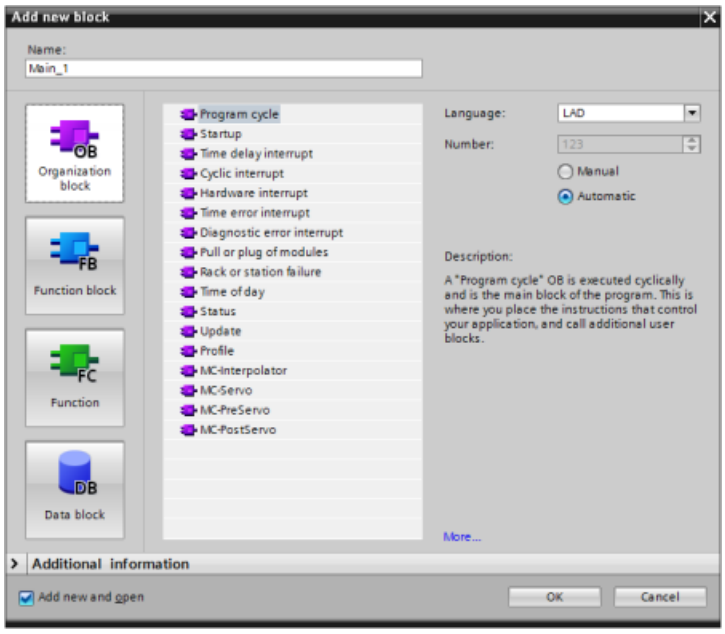
The program cycle OB contains your main program. You can include more than one program cycle OB in your user program. During RUN mode, the program cycle OBs execute at the lowest priority level and can be interrupted by all other event types. The startup OB does not interrupt the program cycle OB because the CPU executes the startup OB before going to RUN mode.

After finishing the processing of the program cycle OBs, the CPU immediately executes the program cycle OBs again. This cyclic processing is the "normal" type of processing used for programmable logic controllers. For many applications, the entire user program is located in a single program cycle OB.

You can create other OBs to perform specific functions, such as for handling interrupts and errors, or for executing specific program code at specific time intervals. These OBs interrupt the execution of the program cycle OBs.

Creating an OB

Use the "Add new block" dialog to create new OBs in your user program.



Interrupt handling is always event-driven. When such an event occurs, the CPU interrupts the execution of the user program and calls the OB that was configured to handle that event. After finishing the execution of the interrupting OB, the CPU resumes the execution of the user program at the point of interruption.

The CPU determines the order for handling interrupt events by priority. You can assign multiple interrupt events to the same priority class. For more information, refer to the topics on organization blocks (Page 66) and execution of the user program (Page 61).

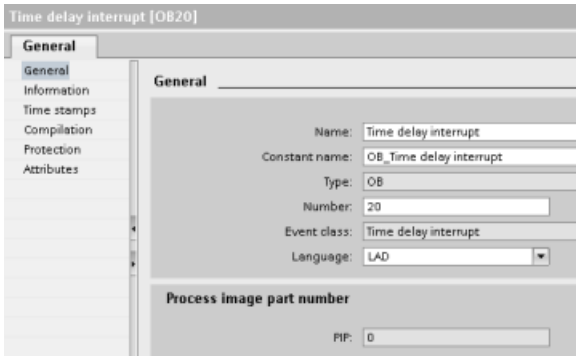
Creating additional OBs

You can create multiple OBs for your user program, even for the program cycle and startup OB events. Use the "Add new block" dialog to create an OB and enter a name for your OB.

If you create multiple program cycle OBs for your user program, the CPU executes each program cycle OB in numerical sequence, starting with the program cycle OB with the lowest number (such as OB 1). For example: after the first program cycle OB (such as OB 1) finishes, the CPU executes the program cycle OB with the next higher number.

Configuring the properties of an OB

You can modify the properties of an OB. For example, you can configure the OB number or programming language.



NOTE

Note that you can assign a process image part number to an OB that corresponds to PIP0, PIP1, PIP2, PIP3, or PIP4. If you enter a number for the process image part number, the CPU creates that process image partition. See the topic "Execution of the user program (Page 61)" for an explanation of the process image partitions.

8.3.2 Function (FC)

A function (FC) is a code block that typically performs a specific operation on a set of input values. The FC stores the results of this operation in memory locations. For example, use FCs to perform standard and reusable operations (such as for mathematical calculations) or technological functions (such as for individual controls using bit logic operations). An FC can also be called several times at different points in a program. This reuse simplifies the programming of frequently recurring tasks.

An FC does not have an associated instance data block (DB). The FC uses the local data stack for the temporary data used to calculate the operation. The temporary data is not saved. To store data permanently, assign the output value to a global memory location, such as M memory or to a global DB.

8.3.3 Function block (FB)

A function block (FB) is a code block that uses an instance data block for its parameters and static data. FBs have variable memory that is located in a data block (DB), or "instance" DB. The instance DB provides a block of memory that is associated with that instance (or call) of the FB and stores data after the FB finishes. You can associate different instance DBs with different calls of the FB. The instance DBs allow you to use one generic FB to control multiple devices. You structure your program by having one code block make a call to an FB and an instance DB. The CPU then executes the program code in that FB, and stores the block parameters and the static local data in the instance DB. When the execution of the FB finishes, the CPU returns to the code block that called the FB. The instance DB retains the values for that instance of the FB. These values are available to subsequent calls to the function block either in the same scan cycle or other scan cycles.

Reusable code blocks with associated memory

You typically use an FB to control the operation for tasks or devices that do not finish their operation within one scan cycle. To store the operating parameters so that they can be quickly accessed from one scan to the next, each FB in your user program has one or more instance DBs. When you call an FB, you also specify an instance DB that contains the block parameters and the static local data for that call or "instance" of the FB. The instance DB maintains these values after the FB finishes execution.

By designing the FB for generic control tasks, you can reuse the FB for multiple devices by selecting different instance DBs for different calls of the FB.

An FB stores the Input, Output, and InOut, and Static parameters in an instance DB.

You can also modify and download the function block interface in RUN mode (Page 1077).

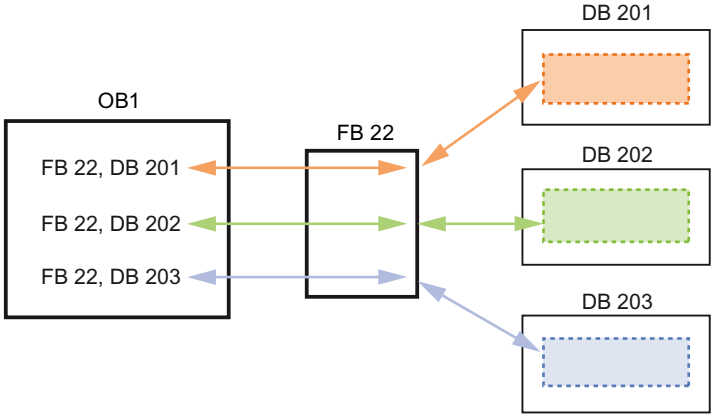
Assigning the start value in the instance DB

The instance DB stores both a default value and a start value for each parameter. The start value provides the value to be used when the FB is executed. The start value can then be modified during the execution of your user program.

The FB interface also provides a "Default value" column that allows you to assign a new start value for the parameter as you are writing the program code. This default value in the FB is then transferred to the start value in the associated instance DB. If you do not assign a new start value for a parameter in the FB interface, the default value from instance DB is copied to start value.

Using a single FB with DBs

The following figure shows an OB that calls one FB three times, using a different data block for each call. This structure allows one generic FB to control several similar devices, such as motors, by assigning a different instance data block for each call for the different devices. Each instance DB stores the data (such as speed, ramp-up time, and total operating time) for an individual device.



In this example, FB 22 controls three separate devices, with DB 201 storing the operational data for the first device, DB 202 storing the operational data for the second device, and DB 203 storing the operational data for the third device.

8.3.4 Data block (DB)

You create data blocks (DB) in your user program to store data for the code blocks. All of the program blocks in the user program can access the data in a global DB, but an instance DB stores data for a specific function block (FB).

The data stored in a DB is not deleted when the execution of the associated code block comes to an end. There are two types of DBs:

- A global DB stores data for the code blocks in your program. Any OB, FB, or FC can access the data in a global DB.
- An instance DB stores the data for a specific FB. The structure of the data in an instance DB reflects the parameters (Input, Output, and InOut) and the static data for the FB. (The Temp memory for the FB is not stored in the instance DB.)

NOTE

Although the instance DB reflects the data for a specific FB, any code block can access the data in an instance DB.

You can also modify and download data blocks in RUN mode (Page 1077).

Read-only data blocks

You can configure a DB as being read-only:

1. Right-click the DB in the project navigator and select "Properties" from the context menu.
2. In the "Properties" dialog, select "Attributes".
3. Select the "Data block write-protected in the device" option and click "OK".

Optimized and standard data blocks

You can also configure data block access to be optimized. If the block is not optimized, it is considered a standard data block. A standard DB is compatible with STEP 7 Classic programming tools and the classic S7-300 and S7-400 CPUs. Data blocks with optimized access have no fixed defined structure. The data elements contain only a symbolic name in the declaration and no fixed address within the block. The CPU stores the elements automatically in the available memory area of the block so that there are no gaps in the memory. This makes for optimal use of the memory capacity.

To set optimized access for a data block, follow these steps:

1. Expand the program blocks folder in the STEP 7 project tree.
2. Right-click the data block and select "Properties" from the context menu.
3. For the attributes, select "Optimized block access".

Note that optimized block access is the default for new data blocks. If you deselect "Optimized block access", the block uses standard access.

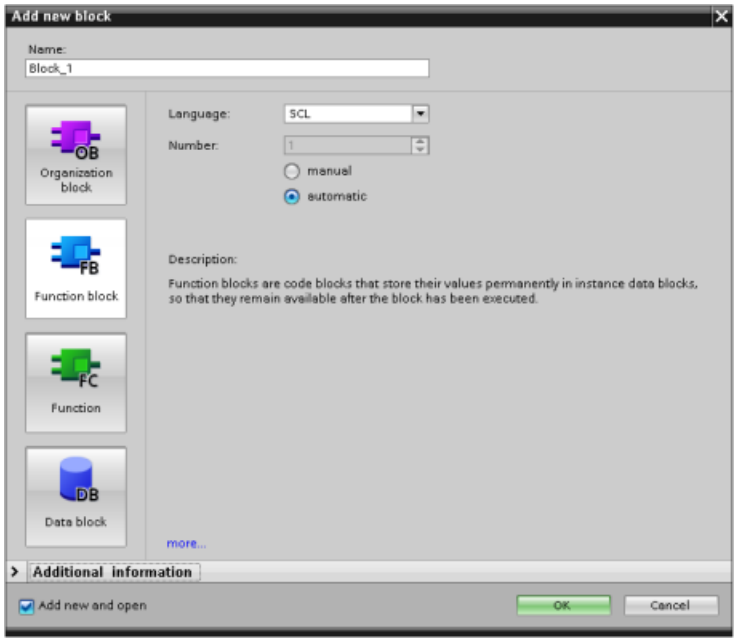
NOTE

Block access type for an FB and its instance DB

Be sure that if your FB setting is "Optimized block access" then the setting of the instance DB for that FB is also "Optimized block access". Similarly if you have not selected "Optimized block access" for the FB such that the FB is of type standard access, then be sure that the instance DB is also standard, or not optimized block access.

If you do not have compatible block access types, then changes to the IN/OUT parameter values of the FB from an HMI during execution of the FB could be lost.

8.3.5 Creating reusable code blocks



Use the "Add new block" dialog under "Program blocks" in the Project navigator to create OBs, FBs, FCs, and global DBs.

When you create a code block, you select the programming language for the block. You do not select a language for a DB because it only stores data.

Selecting the "Add new and open" check box (default) opens the code block in the Project view.

You can store objects you want to reuse in libraries. For each project, there is a project library that is connected to the project. In addition to the project library, you can create any number of global libraries that can be used over several projects. Since the libraries are compatible with each other, library elements can be copied and moved from one library to another.

Libraries are used, for example, to create templates for blocks that you first paste into the project library and then further develop there. Finally, you copy the blocks from the project library to a global library. You make the global library available to other colleagues working on your project. They use the blocks and further adapt them to their individual requirements, where necessary.

For details about library operations, refer to the TIA Portal Information system.

8.3.6 Passing parameters to blocks

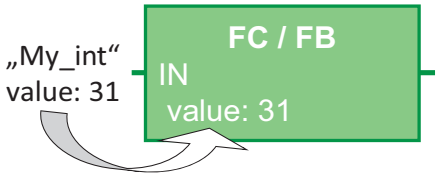
Function Blocks (FB) and Functions (FC) have three different interface types:

- IN
- IN/OUT
- OUT

FBs and FCs receive parameters through the IN and IN/OUT interface types. The blocks process the parameters and return values to the caller through the IN/OUT and OUT interface types.
The user program transfers parameters using one of two methods.

Call-by-value

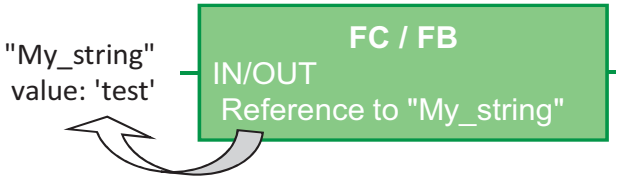
When the user program passes a parameter to a function as "call-by-value", the user program copies the actual parameter value into the input parameter of the block for the IN interface type. This operation requires additional memory for the copied value.



When the user program calls the block, it copies the values.

Call-by-reference

When the user program passes a parameter to a function as "call-by-reference", the user program references the address of the actual parameter for the IN/OUT interface type and does not copy the value. This operation does not require additional memory.



When the user program calls the block, it references the address of the actual parameters.

NOTE

Generally, use the IN/OUT interface type for structured tags (for example, ARRAY, STRUCT, and STRING) in order to avoid increasing the required data memory unnecessarily.

Block optimization and passing parameters

The user program passes FC parameters as "call-by-value" for simple data types (for example, INT, DINT, and REAL). It passes complex data types (for example, STRUCT, ARRAY, and STRING) as "call-by-reference".

The user program normally passes FB parameters in the instance Data block (DB) associated with the FB:

- The user program passes simple data types (for example, INT, DINT, and REAL) as "call-by-value" by copying the parameters to/from the instance DB.
- The user program copies complex data types (for example, STRUCT, ARRAY, and STRING) to and from the instance DB for IN and OUT parameter types.
- The user program passes complex data types as "call-by-reference" for the IN/OUT interface type.

DBs can be created as either "Optimized" or "Standard" (non-optimized). The optimized data blocks are more compact than the non-optimized data blocks. Also, the ordering of the data elements within the DB is different for optimized versus non-optimized DBs. Refer to the "Optimized blocks" section of the S7-Programming Guideline for S7-1200/1500, STEP 7 (TIA Portal), 12/2018 (http://support.automation.siemens.com/WW/view/en/81318674) for a discussion of optimized blocks.

You create FBs and FCs to process either optimized or non-optimized data. You can select the "Optimized block access" check box as one of the attributes for the block. The user program optimizes program blocks by default, and the program blocks expect data passed to the block to be in the optimized format.

When the user program passes a complex parameter (for example, a STRUCT) to a function, the system checks the optimization setting of the data block containing the structure and the optimization setting of the program block. If you optimize both the data block and the function, then the user program passes the STRUCT as a "call-by-reference". The same is true if you select non-optimized for both the data block and the function.

However, if you make the function and data block optimization different (meaning that you optimized one block and not the other block), the STRUCT must be converted to the format expected by the function. For example, if you select non-optimized for the data block and optimized for the function, then a STRUCT in the data block must be converted to an optimized format before the function can process the STRUCT. The system does this conversion by making a "copy" of the STRUCT and converting it to the optimized format that the function expects.

In summary, when the user program passes a complex data type (for example, a STRUCT) to a function as an IN/OUT parameter, the function expects the user program to pass the STRUCT as a "call-by-reference":

- If you select optimized or non-optimized for both the data block containing the STRUCT and the function, the user program passes the data as "call-by-reference".
- If you do not configure the data block and the function with the same optimization settings (one is optimized and the other is non-optimized), the system must make a copy of the STRUCT before passing it to the function. Because the system has to make this copy of the structure, this converts the "call-by-reference", effectively, into a "call-by-value".

Effect of optimization settings on user programs

The copying of the parameter can cause an issue in a user program if an HMI or interrupt OB modifies elements of the structure. For example, there is an IN/OUT parameter of a function (normally passed as "call-by-reference"), but the optimization settings of the data block and function are different:

1. When the user program is ready to call the function, the system must make a "copy" of the structure to change the format of the data to match the function.
2. The user program calls the function with a reference to the "copy" of the structure.
3. An interrupt OB occurs while the function is executing, and the interrupt OB changes a value in the original structure.
4. The function completes and, since the structure is an IN/OUT parameter, the system copies the values back to the original structure in the original format.

The effect of making the copy of the structure to change the format is that the data written by the interrupt OB is lost. The same can happen when writing a value with an HMI. The HMI can interrupt the user program and write a value in the same manner as an interrupt OB.

There are multiple ways to correct this issue:

- The best solution for this this issue is to match the optimization settings of the program block and the data block when using complex data types (for example, a STRUCT). This ensures that the user program always passes the parameters as "call-by-reference".
- Another solution is that an interrupt OB or HMI does not directly modify an element in the structure. The OB or HMI can modify another variable, and then you can copy this variable into the structure at a specific point in the user program.

8.4 Understanding data consistency

The CPU maintains the data consistency for all of the elementary data types (such as Words or DWords) and all of the system-defined structures (for example, IEC_TIMERS or DTL). The reading or writing of the value cannot be interrupted. (For example, the CPU protects the access to a DWord value until the four bytes of the DWord have been read or written.) To ensure that the program cycle OBs and the interrupt OBs cannot write to the same memory location at the same time, the CPU does not execute an interrupt OB until the read or write operation in the program cycle OB has been completed.

If your user program shares multiple values in memory between a program cycle OB and an interrupt OB, your user program must also ensure that these values are modified or read consistently. You can use the DIS_AIRT (disable alarm interrupt) and EN_AIRT (enable alarm interrupt) instructions in your program cycle OB to protect any access to the shared values.

- Insert a DIS_AIRT instruction in the code block to ensure that an interrupt OB cannot be executed during the read or write operation.
- Insert the instructions that read or write the values that could be altered by an interrupt OB.
- Insert an EN_AIRT instruction at the end of the sequence to cancel the DIS_AIRT and allow the execution of the interrupt OB.

A communication request from an HMI device or another CPU can also interrupt execution of the program cycle OB. The communication requests can also cause problems with data consistency. The CPU ensures that the elementary data types are always read and written consistently by the user program instructions. Because the user program is interrupted periodically by communications, it is not possible to guarantee that multiple values in the CPU will all be updated at the same time by the HMI. For example, the values displayed on a given HMI screen could be from different scan cycles of the CPU.

The following instruction groups transfer buffers of data that could be interrupted:

- PtP (Point-to-Point) instructions (Page 839)
- PROFINET instructions (such as TSEND_C and TRCV_C) (Page 644)
- PROFINET Distributed I/O instructions (Page 330)
- PROFIBUS Distributed I/O Instructions (Page 355)

Ensure the data consistency for the buffers of data by avoiding any read or write operation to the buffers in both the program cycle OB and an interrupt OB. If it is necessary to modify the buffer values for these instructions in an interrupt OB, use a DIS_AIRT instruction to delay any interruption (an interrupt OB or a communication interrupt from an HMI or another CPU) until an EN_AIRT instruction is executed.

NOTE

The use of the DIS_AIRT instruction delays the processing of interrupt OBs until the EN_AIRT instruction is executed, affecting the interrupt latency (time from an event to the time when the interrupt OB is executed) of your user program.

See also

Distributed I/O instructions (Page 705)

8.5 Programming language

STEP 7 provides the following standard programming languages for S7-1200:

- LAD (ladder logic) (Page 179) is a graphical programming language. The representation is based on circuit diagrams.
- FBD (Function Block Diagram) (Page 180) is a programming language that is based on the graphical logic symbols used in Boolean algebra.
- SCL (structured control language) (Page 181) is a text-based, high-level programming language.

When you create a code block, you select the programming language to be used by that block. You can also use CEM (Cause-Effect-Matrix) for programming Function Blocks (FBs) (Page 172). See the STEP 7 Information System for information on CEM programming for Function Blocks.

The user program can utilize code blocks created in any or all of the programming languages.

8.5.1 Ladder logic (LAD)

The elements of a circuit diagram, such as normally closed and normally open contacts, and coils are linked to form networks.

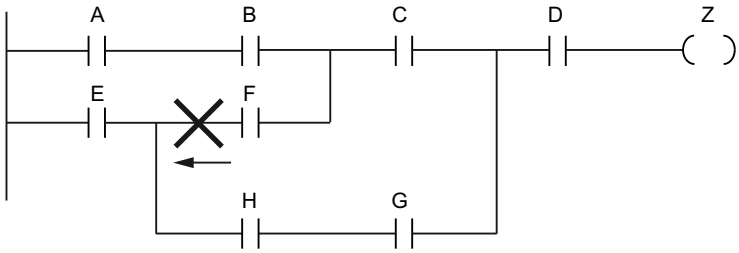
To create the logic for complex operations, you can insert branches to create the logic for parallel circuits. Parallel branches are opened downwards or are connected directly to the power rail. You terminate the branches upwards.
LAD provides "box" instructions for a variety of functions, such as math, timer, counter, and move.
STEP 7 does not limit the number of instructions (rows and columns) in a LAD network.

NOTE

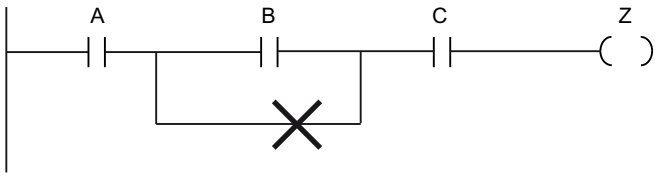
Every LAD network must terminate with a coil or a box instruction.

Consider the following rules when creating a LAD network:

- You cannot create a branch that could result in a power flow in the reverse direction.

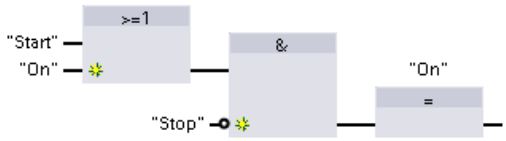


- You cannot create a branch that would cause a short circuit.



8.5.2 Function Block Diagram (FBD)

Like LAD, FBD is also a graphical programming language. The representation of the logic is based on the graphical logic symbols used in Boolean algebra.



To create the logic for complex operations, insert parallel branches between the boxes.

Mathematical functions and other complex functions can be represented directly in conjunction with the logic boxes.
STEP 7 does not limit the number of instructions (rows and columns) in an FBD network.

8.5.3 SCL

Structured Control Language (SCL) is a high-level, PASCAL-based programming language for the SIMATIC S7 CPUs. SCL supports the block structure of STEP 7 (Page 169). Your project can include program blocks in any of the three programming languages: SCL, LAD, and FBD.

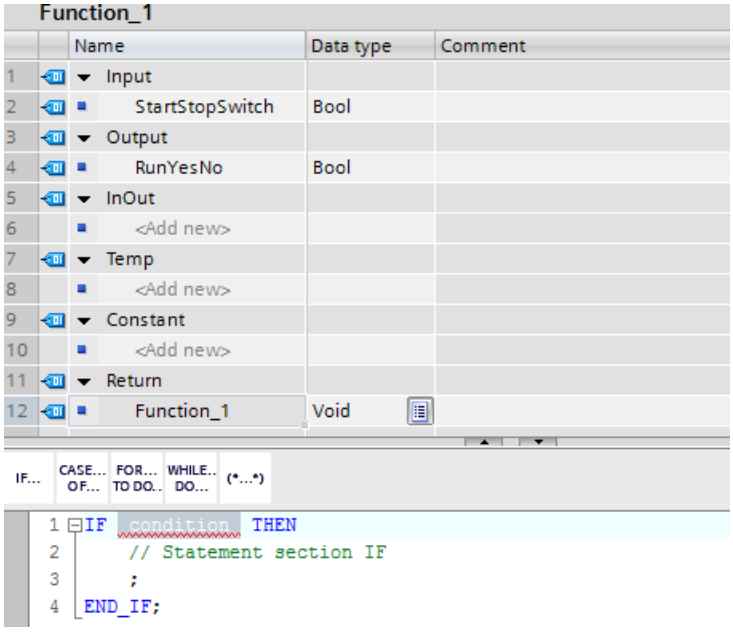
SCL instructions use standard programming operators, such as for assignment (:=), mathematical functions (+ for addition, - for subtraction, * for multiplication, and / for division). SCL also uses standard PASCAL program control operations, such as IF-THEN-ELSE, CASE, REPEAT-UNTIL, GOTO and RETURN. You can use any PASCAL reference for syntactical elements of the SCL programming language. Many of the other instructions for SCL, such as timers and counters, match the LAD and FBD instructions. For more information about specific instructions, refer to the specific instructions in the chapters for Basic instructions (Page 197) and Extended instructions (Page 293).

8.5.3.1 SCL program editor

You can designate any type of block (OB, FB, or FC) to use the SCL programming language at the time you create the block. STEP 7 provides an SCL program editor that includes the following elements:

- Interface section for defining the parameters of the code block
- Code section for the program code
- Instruction tree that contains the SCL instructions supported by the CPU

You enter the SCL code for your instruction directly in the code section. The editor includes buttons for common code constructs and comments. For more complex instructions, simply drag the SCL instructions from the instruction tree and drop them into your program. You can also use any text editor to create an SCL program and then import that file into STEP 7.



In the Interface section of the SCL code block you can declare the following types of parameters:

- Input, Output, InOut, and Ret_Val: These parameters define the input tags, output tags, and return value for the code block. The tag name that you enter here is used locally during the execution of the code block. You typically would not use the global tag name in the tag table.
- Static (FBs only; the illustration above is for an FC): The code block uses static tags for storage of static intermediate results in the instance data block. The block retains static data until overwritten, which can be after several cycles. The names of the blocks, which this block calls as multi-instance, are also stored in the static local data.
- Temp: These parameters are the temporary tags that are used during the execution of the code block.
- Constant: These are named constant values for your code block.

If you call the SCL code block from another code block, the parameters of the SCL code block appear as inputs or outputs.

In this example, the tags for "Start" and "On" (from the project tag table) correspond to "StartStopSwitch" and "RunYesNo" in the declaration table of the SCL program.

8.5.3.2 SCL expressions and operations

Constructing an SCL expression

An SCL expression is a formula for calculating a value. The expression consists of operands and operators (such as *, /, + or -). The operands can be tags, constants, or expressions.

The evaluation of the expression occurs in a certain order, which is defined by the following factors:

- Every operator has a pre-defined priority; the highest-priority operation is performed first.
- For operators with equal priority, the operators are processed in a left-to-right sequence.
- Parentheses designate a series of operators to be evaluated together.

The result of an expression can be used either for assigning a value to a tag used by your program, as a condition to be used by a control statement, or as parameters for another SCL instruction or for calling a code block.

Table 8-2 Operators in SCL

Type	Operation	Operator	Priority
Parentheses	(*Expression*)	(,)	1
Math	Power	**	2
	Sign (unary plus)	+	3
	Sign (unary minus)	-	3
	Multiplication	*	4
	Division	/	4
	Modulo	MOD	4

Type	Operation	Operator	Priority
Math	Addition	+	5
	Subtraction	-	5
Comparison	Less than	<	6
	Less than or equal to	<=	6
	Greater than	>	6
	Greater than or equal to	>=	6
	Equal to	=	7
	Not equal to	<>	7
Bit logic	Negation (unary)	NOT	3
	AND logic operation	AND or &	8
	Exclusive OR logic operation	XOR	9
	OR logic operation	OR	10
Assignment	Assignment	:=	11

As a high-level programming language, SCL uses standard statements for basic tasks:

- Assignment statement: :=
- Mathematical functions: +, -, *, and /
- Addressing of global variables (tags): "<tag name>" (Tag name or data block name enclosed in double quotes)
- Addressing of local variables: #<variable name> (Variable name preceded by "#" symbol)

The following examples show different expressions for different uses:

`"C" := #A+#B;`	Assigns the sum of two local variables to a tag
`"Data_block_1".Tag := #A;`	Assignment to a data block tag
`IF #A > #B THEN "C" := #A;`	Condition for the IF-THEN statement
`"C" := SQRT (SQR (#A) + SQR (#B));`	Parameters for the SQRT instruction

Arithmetic operators can process various numeric data types. The data type of the result is determined by the data type of the most-significant operands. For example, a multiplication operation that uses an INT operand and a REAL operand yields a REAL value for the result.

Control statements

A control statement is a specialized type of SCL expression that performs the following tasks:

- Program branching
- Repeating sections of the SCL program code
- Jumping to other parts of the SCL program
- Conditional execution

The SCL control statements include IF-THEN, CASE-OF, FOR-TO-DO, WHILE-DO, REPEAT-UNTIL, CONTINUE, GOTO, and RETURN.

A single statement typically occupies one line of code. You can enter multiple statements on one line, or you can break a statement into several lines of code to make the code easier to read. Separators (such as tabs, line breaks and extra spaces) are ignored during the syntax check. An END statement terminates the control statement.

The following examples show a FOR-TO-DO control statement. (Both forms of coding are syntactically valid.)

```
FOR x := 0 TO max DO sum := sum + value(x); END_FOR;
FOR x := 0 TO max DO
    sum := sum + value(x);
END_FOR;
```

A control statement can also be provided with a label. A label is set off by a colon at the beginning of the statement:

```
Label: <Statement>;
```

The TIA Portal Information system provides a complete SCL programming language reference.

Conditions

A condition is a comparison expression or a logical expression whose result is of type BOOL (with the value of either TRUE or FALSE). The following example shows conditions of various types:

`#Temperature > 50`	Relational expression
`#Counter <= 100`	
`#CHAR1 < 'S'`	
`(#Alpha <> 12) AND NOT #Beta`	Comparison and logical expression
`5 + #Alpha`	Arithmetic expression

A condition can use arithmetic expressions:

- The condition of the expression is TRUE if the result is any value other than zero.
- The condition of the expression is FALSE if the result equals zero.

Calling other code blocks from your SCL program

To call another code block in your user program, simply enter the name (or absolute address) of the FB or FC with the parameters. For an FB, you must provide the instance DB to be called with the FB.

`<DB name> (Parameter list)`	Call as a single instance
`<#Instance name> (Parameter list)`	Call as multi-instance

```
"MyDB"(MyInput:=10, MyInOut:="Tag1");
```

`<FC name> (Parameter list)`	Standard call
`<Operand>:=<FC name> (Parameter list)`	Call in an expression

```
"MyFC"(MyInput:=10, MyInOut:="Tag1");
```

You can also drag blocks from the navigation tree to the SCL program editor, and complete the parameter assignment.

Adding block comments to SCL code

To include a block comment in the SCL code, place text between (* and *). There is no limit to the number of lines allowed per comment. Use the block comment button in the SCL editor to enter block comments quickly:

Addressing

As with LAD and FBD, SCL allows you to use either tags (symbolic addressing) or absolute addresses in your user program. SCL also allows you to use a variable as an array index.

Absolute addressing

%I0.0 **%MB100**	Precede absolute addresses with the "%" symbol. Without the "%", STEP 7 generates an undefined tag error at compile time.

Symbolic addressing

"PLC_Tag_1"	Tag in PLC tag table
"Data_block_1".Tag_1	Tag in a data block
"Data_block_1".MyArray[#i]	Array element in a data block array

8.5.3.3 Indexed addressing with PEEK and POKE instructions

SCL provides PEEK and POKE instructions that allow you to read from or write to data blocks, I/O, or memory. You provide parameters for specific byte offsets or bit offsets for the operation.

NOTE

To use the PEEK and POKE instructions with data blocks, you must use standard (not optimized) data blocks. Also note that the PEEK and POKE instructions merely transfer data. They have no knowledge of data types at the addresses.

PEEK(area:=_in_, dbNumber:=_in_, byteOffset:=_in_);	Reads the byte referenced by byteOffset of the referenced data block, I/O or memory area. Example referencing data block: **%MB100 := PEEK(area:=16#84, dbNumber:=1, byteOffset:=#i);** Example referencing IB3 input: **%MB100 := PEEK(area:=16#81, dbNumber:=0, byteOffset:=#i); // when #i = 3**

`PEEK_WORD(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_);`
	Reads the word referenced by byteOffset of the referenced data block, I/O or memory area.
	Example:
	`%MW200 := PEEK_WORD(area:=16#84, dbNumber:=1, byteOffset:=#i);`

`PEEK_DWORD(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_);`
	Reads the double word referenced by byteOffset of the referenced data block, I/O or memory area.
	Example:
	`%MD300 := PEEK_DWORD(area:=16#84, dbNumber:=1, byteOffset:=#i);`

`PEEK_BOOL(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_,`
`bitOffset:=_in_);`
	Reads a Boolean referenced by the bitOffset and byteOffset of the referenced data block, I/O or memory area
	Example:
	`%MB100.0 := PEEK_BOOL(area:=16#84, dbNumber:=1, byteOffset:=#ii, bitOffset:=#j);`

`POKE(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_,`
`value:=_in_);`
	Writes the value (Byte, Word, or DWord) to the referenced byteOffset of the referenced data block, I/O or memory area
	Example referencing data block:
	`POKE(area:=16#84, dbNumber:=2, byteOffset:=3, value:="Tag_1");`
	Example referencing QB3 output:
	`POKE(area:=16#82, dbNumber:=0, byteOffset:=3, value:="Tag_1");`

`POKE_BOOL(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_,`
`bitOffset:=_in_,`
`value:=_in_);`
	Writes the Boolean value to the referenced bitOffset and byteOffset of the referenced data block, I/O or memory area
	Example:
	`POKE_BOOL(area:=16#84, dbNumber:=2, byteOffset:=3, bitOffset:=5, value:=0);`

`POKE_BLK(area_src:=_in_,`
`dbNumber_src:=_in_,`
`byteOffset_src:=_in_,`
`area_dest:=_in_,`
`dbNumber_dest:=_in_,`
`byteOffset_dest:=_in_,`
`count:=_in_);`
	Writes "count" number of bytes starting at the referenced byte Offset of the referenced source data block, I/O or memory area to the referenced byteOffset of the referenced destination data block, I/O or memory area
	Example:
	`POKE_BLK(area_src:=16#84, dbNumber_src:=#src_db, byteOffset_src:=#src_byte, area_dest:=16#84, dbNumber_dest:=#src_db, byteOffset_dest:=#src_byte, count:=10);`

For PEEK and POKE instructions, the following values for the "area", "area_src" and "area_dest" parameters are applicable. For areas other than data blocks, the dbNumber parameter must be 0.

16#81	I
16#82	Q
16#83	M
16#84	DB

8.5.4 EN and ENO for LAD, FBD and SCL

Determining "power flow" (EN and ENO) for an instruction

Certain instructions (such as the Math and the Move instructions) provide parameters for EN and ENO. These parameters relate to power flow in LAD or FBD and determine whether the instruction is executed during that scan. SCL also allows you to set the ENO parameter for a code block.

- EN (Enable In) is a Boolean input. Power flow (EN = 1) must be present at this input for the box instruction to be executed. If the EN input of a LAD box is connected directly to the left power rail, the instruction will always be executed.
- ENO (Enable Out) is a Boolean output. If the box has power flow at the EN input and the box executes its function without error, then the ENO output passes power flow (ENO = 1) to the next element. If an error is detected in the execution of the box instruction, then power flow is terminated (ENO = 0) at the box instruction that generated the error.

Table 8-3 Operands for EN and ENO

Program editor	Inputs/outputs	Operands	Data type
LAD	EN, ENO	Power flow	Bool
FBD	EN	I, I:P, Q, M, DB, Temp, Power Flow	Bool
	ENO	Power Flow	Bool
SCL	EN[1]	TRUE, FALSE	Bool
	ENO[2]	TRUE, FALSE	Bool

[1] The use of EN is only available for FBs.

[2] The use of ENO with the SCL code block is optional. You must configure the SCL compiler to set ENO when the code block finishes.

Configuring SCL to set ENO

To configure the SCL compiler for setting ENO, follow these steps:

1. Select the "Settings" command from the "Options" menu.
2. Expand the "PLC programming" properties and select "SCL (Structured Control Language)".
3. Select the "Set ENO automatically" option.

Using ENO in program code

You can also use ENO in your program code, for example by assigning ENO to a PLC tag, or by evaluating ENO in a local block.

Examples:

```
"MyFunction"
  ( IN1 := … ,
    IN2 := … ,
    OUT1 => #myOut,
    ENO => #statusFlag ); // PLC tag statusFlag holds the value of
ENO

"MyFunction"
  ( IN1 := …
    IN2 := … ,
    OUT1 => #myOut,
    ENO => ENO );  // block status flag of "MyFunction"
                   // is stored in the local block

IF ENO = TRUE THEN
    // execute code only if MyFunction returns true ENO
```

Effect of Ret_Val or Status parameters on ENO

Some instructions, such as the communication instructions or the string conversion instructions, provide an output parameter that contains information about the processing of the instruction. For example, some instructions provide a Ret_Val (return value) parameter, which is typically an Int data type that contains status information in a range from -32768 to +32767. Other instructions provide a Status parameter, which is typically a Word data type that stores status information in a range of hexadecimal values from 16#0000 to 16#FFFF. The numerical value stored in a Ret_Val or a Status parameter determines the state of ENO for that instruction.

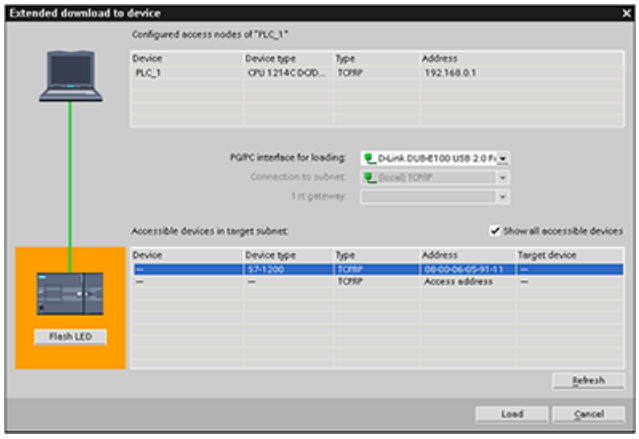
- Ret_Val: A value from 0 to 32767 typically sets ENO = 1 (or TRUE). A value from -32768 to -1 typically sets ENO = 0 (or FALSE). To evaluate Ret_Val, change the representation to hexadecimal.
- Status: A value from 16#0000 16#7FFF typically sets ENO = 1 (or TRUE). A value from 16#8000 to 16#FFFF typically sets ENO = 0 (or FALSE).

Instructions that take more than one scan to execute often provide a Busy parameter (Bool) to signal that the instruction is active but has not completed execution. These instructions often also provide a Done parameter (Bool) and an Error parameter (Bool). Done signals that the instruction was completed without error, and Error signals that the instruction was completed with an error condition.

- When Busy = 1 (or TRUE), ENO = 1 (or TRUE).
- When Done = 1 (or TRUE), ENO = 1 (or TRUE).
- When Error = 1 (or TRUE), ENO = 0 (or FALSE).

8.6 Downloading the elements of your program

You can download the elements of your project from the programming device to the CPU. When you download a project, the CPU stores the user program (OBs, FCs, FBs and DBs) in internal load memory or, if a SIMATIC memory card is present, in external load memory (the card).



You can download your project from the programming device to your CPU from any of the following locations:

- Project tree: Right-click the program element, and then click the context-sensitive "Download" selection.
- Online menu: Click the "Download to device" selection.
- Toolbar: Click the "Download to device" icon.
- Device configuration: Right-click the CPU and select the elements to download.

Note that if you have applied dynamic binding with mandatory password (Page 160) to any of the program blocks, you must enter the password for the protected blocks in order to download them. If you have configured this type of copy protection for multiple blocks, you must enter the password for each of the protected blocks in order to download them.

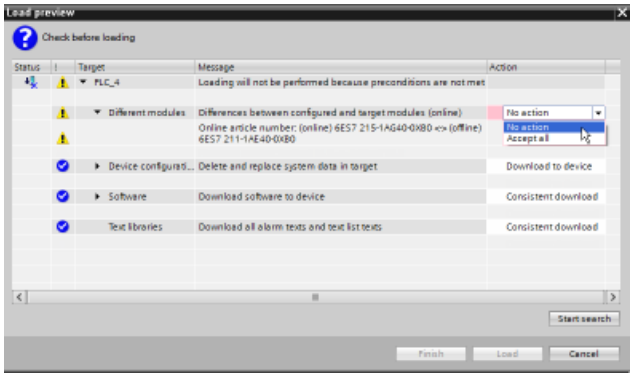
NOTE

Downloading a program does not clear or make any changes to existing values in retentive memory. To clear retentive memory before a download, reset the CPU to factory settings.

You can also download a panel project for the Basic HMI panels (Page 36) from the TIA Portal to a memory card in the S7-1200 CPU.

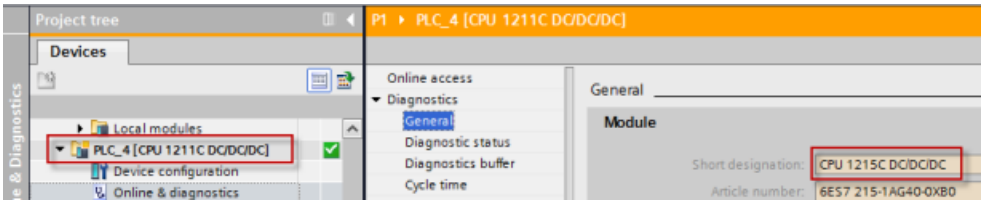
Downloading when the configured CPU is different from the connected CPU

STEP 7 and the S7-1200 permit a download if the connected CPU has the capacity to store a download from the configured CPU, based on the memory requirements of the project and the compatibility of the I/O. You can download the configuration and program from a CPU to a larger CPU, for example, from a CPU 1211C DC/DC/DC to a CPU 1215C DC/DC/DC because the I/O is compatible and the memory is sufficient. In this case, the download operation displays a warning, "Differences between configured and target modules (online)" along with the article numbers and firmware versions in the "Load preview" dialog. You must choose either "No action" if you do not want the download to proceed or "Accept all" if you do want the download to proceed:



NOTE

When you go online (Page 1051) after downloading the configured CPU to a different connected CPU, you see the project for the configured CPU with online status indicators in the project tree. In the online and diagnostics view, however, you see the actual connected CPU module type.

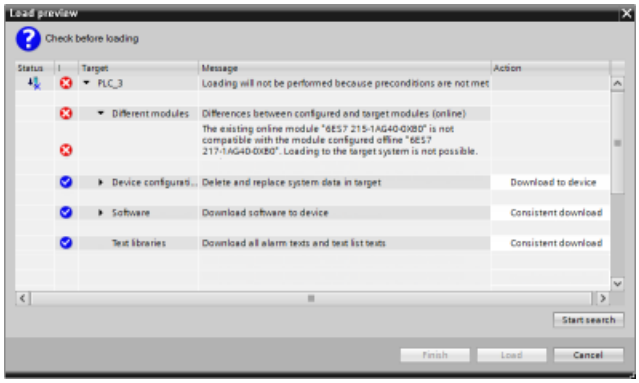


You can change your device (Page 136) in the device configuration so that the configured CPU is the same module type as the connected CPU. The "Change device" dialog provides complete compatibility details when you try to change a device.

STEP 7 and the S7-1200 prohibit a download if the connected CPU does not have the capacity to store a download from the configured CPU; for example, you cannot download the hardware configuration and program for the following cases:

- CPU 1215C DC/DC/DC to a CPU 1212C DC/DC/DC due to insufficient work memory
- CPU 1211C DC/DC/Relay to a CPU 1211C DC/DC/DC due to I/O differences
- CPU 1217C DC/DC/DC to any CPU 1211C, CPU 1212C, CPU 1214C, or CPU 1215C due to the 1.5 V DC outputs in the CPU 1217C
- CPU 1214C V4.6 to CPU 1214C V4.5.x or earlier, due to downward firmware version incompatibility

The "Load preview" dialog displays an error in such cases:



CPUs with protection of confidential PLC configuration data

If you have configured Protection of confidential PLC configuration data (Page 145) note the following:

- If the device does not have the password for protection of confidential PLC configuration data, the TIA Portal prompts you to enter the password for protection of confidential PLC configuration data on the first download.
- If the device already has the password for protection of confidential PLC configuration data, the password in the STEP 7 project and in the device must match. If the passwords do not match, you cannot download the project to the CPU. You must delete the password for protection of confidential PLC configuration data or set it to the password in the device. You can also set or delete the password for protection of confidential PLC configuration data from Online & Diagnostics (Page 1056).

Recovering from a failed download

If the download fails, the Info tab of the Inspector Window displays the reason. The diagnostics buffer also provides information. After a failed download, follow these steps to be able to download successfully:

1. Correct the problem as described in the error message.
2. Reattempt the download.

In rare cases, the download succeeds but a subsequent power cycle of the CPU fails. In this case you may see an error in the diagnostics buffer such as:

- 16# 02:4175 -- CPU error: Memory card evaluation error: Unknown or incompatible version of CPU configuration description current card type: No memory card Function finished/aborted, new startup inhibit set: ..- Memory card missing, wrong type, wrong content or protected

If this occurs and additional attempts to download fail, you must clear the internal load memory or external load memory:

1. If using internal load memory, reset the CPU to factory settings.
2. If using a SIMATIC memory card, remove it and delete the contents of the memory card (Page 112) before reinserting.
3. Download the hardware configuration and software.

8.7 Synchronizing the online CPU and offline project

When you download project blocks to the CPU, the CPU can detect whether blocks or tags have changed in the online CPU since the last download. In such cases, the CPU offers you the choice to synchronize the changes. This means that you can upload the online CPU changes to the project before downloading the project to the CPU. Changes in the online CPU can be due to a variety of factors:

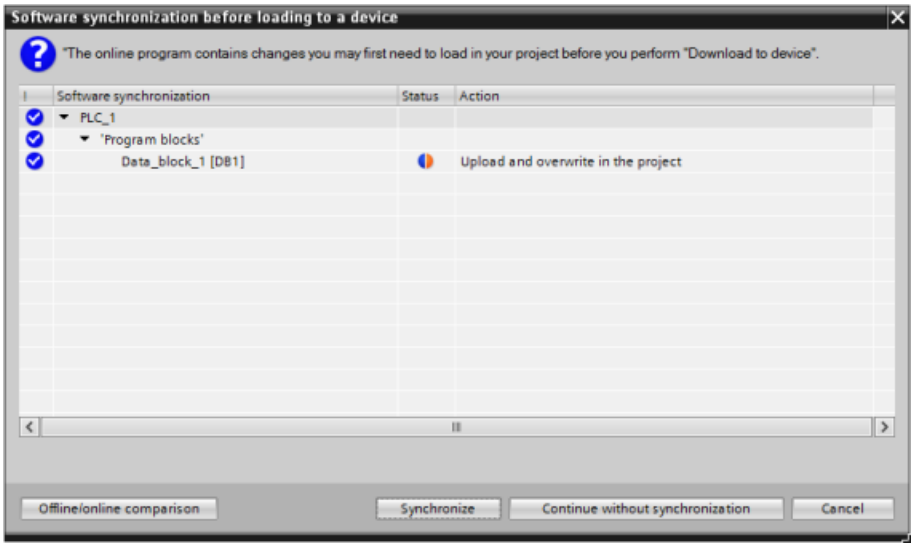
- Changes to the start values of data block tags during runtime, for example by the WRIT_DBL instruction (Page 462) or by loading a recipe
- A download from a "secondary" project (a project other than the one that originated the last download) where one or more of the following conditions exist:
  - The online CPU includes program blocks that do not exist in the project.
  - Data block tags or block attributes differ between the offline project and online CPU.
  - PLC tags exist in the online CPU that do not exist in the offline project.

NOTE

If you edit blocks or tags in the project that you used for the last download, you do not have to make any choices about synchronization. STEP 7 and the CPU detect that the offline project changes are newer than the online CPU and proceeds with a normal download operation.

Synchronization choices

When you download a project to the CPU, you see the synchronization dialog if STEP 7 detects that data blocks or tags in the online CPU are newer than the project values. For example, if the STEP 7 program has executed WRIT_DBL and changed a start value for a tag in Data_block_1, STEP 7 displays the following synchronization dialog when you initiate a download:



This dialog lists the program blocks where differences exist. From this dialog, you have the following choices:

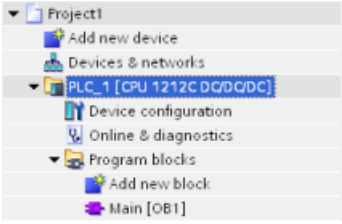
- Online/offline comparison: If you click this button, STEP 7 displays the program blocks, system blocks, technology objects, PLC tags, and PLC data types for the project as compared to the online CPU (Page 1063). For each object, you can click to see a detailed analysis of the differences including time stamps. You can use this information to decide what to do about the differences between the online CPU and the project.
- Synchronize: If you click this button, STEP 7 uploads the data blocks, tags, and other objects from the online CPU to the project. You can then continue with the program download, unless program execution has again caused the project to be out of sync with the CPU.
- Continue without synchronization: If you click this button, STEP 7 downloads the project to the CPU.
- Cancel: If you click this button, you cancel the download operation.

8.8 Uploading from the online CPU

You can also copy the program blocks from an online CPU or a memory card attached to your programming device.

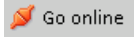
Prepare the offline project for the copied program blocks:

1. Add a CPU device that matches the online CPU.
2. Expand the CPU node once so that the "Program blocks" folder is visible.

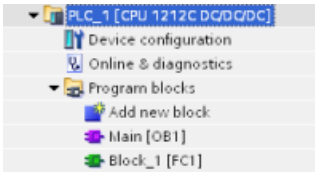


To upload the program blocks from the online CPU to the offline project, follow these steps:

1. Click the "Program blocks" folder in the offline project.
2. Click the "Go online" button.
3. Click the "Upload" button.
4. Confirm your decision from the Upload dialog (Page 1051).



When the upload is complete, STEP 7 displays all of the uploaded program blocks in the project.



8.8.1 Comparing the online CPU to the offline CPU

You can use the "Compare" editor (Page 1063) in STEP 7 to find differences between the online and offline projects. You might find this useful prior to uploading from the CPU.

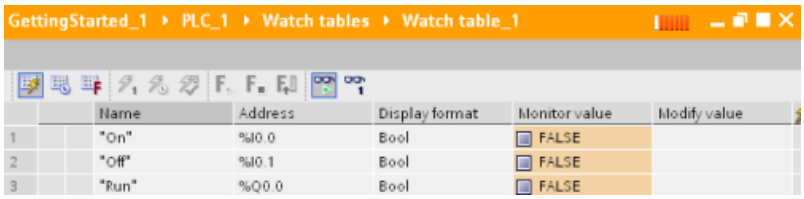
8.9 Debugging and testing the program

8.9.1 Monitor and modify data in the CPU

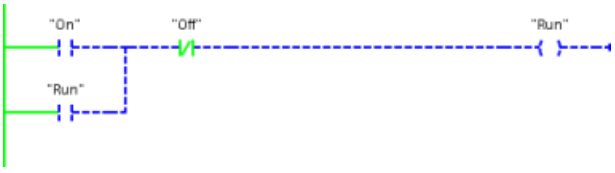
As shown in the following table, you can monitor and modify values in the online CPU.

Table 8-4 Monitoring and modifying data with STEP 7

Editor	Monitor	Modify	Force
Watch table	Yes	Yes	No
Force table	Yes	No	Yes
Program editor	Yes	Yes	No
Tag table	Yes	No	No
DB editor	Yes	Yes	No



Monitoring with a watch table



Monitoring with the LAD editor

Refer to the "Online and diagnostics" chapter for more information about monitoring and modifying data in the CPU (Page 1065).

8.9.2 Watch tables and force tables

You use "watch tables" for monitoring and modifying the values of a user program being executed by the online CPU. You can create and save different watch tables in your project to support a variety of test environments. This allows you to reproduce tests during commissioning or for service and maintenance purposes.

With a watch table, you can monitor and interact with the CPU as it executes the user program. You can display or change values not only for the tags of the code blocks and data blocks, but also for the memory areas of the CPU, including the inputs and outputs (I and Q), peripheral inputs (I:P), bit memory (M), and data blocks (DB).

With the watch table, you can enable the physical outputs (Q:P) of a CPU in STOP mode. For example, you can assign specific values to the outputs when testing the wiring for the CPU.

STEP 7 also provides a force table for "forcing" a tag to a specific value. For more information about forcing, see the section on forcing values in the CPU (Page 1071) in the "Online and Diagnostics" chapter.

NOTE

The force values are stored in the CPU and not in the watch table.

You cannot force an input (or "I" address). However, you can force a peripheral input. To force a peripheral input, append a ":P" to the address (for example: "On":P).

STEP 7 also provides the capability of tracing and recording program variables based on trigger conditions (Page 1081).

8.9.3 Cross reference to show usage

The Inspector window displays cross-reference information about how a selected object is used throughout the complete project, such as the user program, the CPU and any HMI devices. The "Cross-reference" tab displays the instances where a selected object is being used and the other objects using it. The Inspector window also includes blocks which are only available online in the cross-references. To display the cross-references, select the "Show cross-references" command. (In the Project view, find the cross references in the "Tools" menu.)

NOTE

You do not have to close the editor to see the cross-reference information.

You can sort the entries in the cross-reference. The cross-reference list provides an overview of the use of memory addresses and tags within the user program.

- When creating and changing a program, you retain an overview of the operands, tags and block calls you have used.
- From the cross-references, you can jump directly to the point of use of operands and tags.
- During a program test or when troubleshooting, you are notified about which memory location is being processed by which command in which block, which tag is being used in which screen, and which block is called by which other block.

Table 8-5 Elements of the cross reference

Column	Description
Object	Name of the object that uses the lower-level objects or that is being used by the lower-level objects
Number	Number of uses
Point of use	Each location of use, for example, network
Property	Special properties of referenced objects, for example, the tag names in multi-instance declarations
as	Shows additional information about the object, such as whether an instance DB is used as template or as a multiple instance
Access	Type of access, whether access to the operand is read access (R) and/or write access (W)

Column	Description
Address	Address of the operand
Type	Information on the type and language used to create the object
Path	Path of object in project tree

Depending on the installed products, the cross-reference table displays additional or different columns.

8.9.4 Call structure to examine the calling hierarchy

The call structure describes the call hierarchy of the block within your user program. It provides an overview of the blocks used, calls to other blocks, the relationships between blocks, the data requirements for each block, and the status of the blocks. You can open the program editor and edit blocks from the call structure.

Displaying the call structure provides you with a list of the blocks used in the user program. STEP 7 highlights the first level of the call structure and displays any blocks that are not called by any other block in the program. The first level of the call structure displays the OBs and any FCs, FBs, and DBs that are not called by an OB. If a code block calls another block, the called block is shown as an indentation under the calling block. The call structure only displays those blocks that are called by a code block.

You can selectively display only the blocks causing conflicts within the call structure. The following conditions cause conflicts:

- Blocks that execute any calls with older or newer code time stamps
- Blocks that call a block with modified interface
- Blocks that use a tag with modified address and/or data type
- Blocks that are called neither directly nor indirectly by an OB
- Blocks that call a non-existent or missing block

You can group several block calls and data blocks as a group. You use a drop-down list to see the links to the various call locations.

You can also perform a consistency check to show time stamp conflicts. Changing the time stamp of a block during or after the program is generated can lead to time stamp conflicts, which in turn cause inconsistencies among the blocks that are calling and being called.

- Most time stamp and interface conflicts can be corrected by recompiling the code blocks.
- If compilation fails to clear up inconsistencies, use the link in the "Details" column to go to the source of the problem in the program editor. You can then manually eliminate any inconsistencies.
- Any blocks marked in red must be recompiled.

Basic instructions

9

9.1 Bit logic operations

9.1.1 Bit logic instructions

LAD and FBD are very effective for handling Boolean logic. While SCL is especially effective for complex mathematical computation and for project control structures, you can use SCL for Boolean logic.

LAD contacts

Table 9-1 Normally open and normally closed contacts

LAD	SCL	Description

"IN"	**IF in THEN**
	Statement;
	ELSE
	Statement;
	END_IF;
		Normally open and normally closed contacts: You can connect contacts to other contacts and create your own combination logic. If the input bit you specify uses memory identifier I (input) or Q (output), then the bit value is read from the process-image register. The physical contact signals in your control process are wired to I terminals on the PLC. The CPU scans the wired input signals and continuously updates the corresponding state values in the process-image input register.
		You can perform an immediate read of a physical input using ":P" following the I offset (example: "%I3.4:P"). For an immediate read, the bit data values are read directly from the physical input instead of the process image. An immediate read does not update the process image.

"IN"	**IF NOT (in)** **THEN** **Statement;** **ELSE** **Statement;** **END_IF;**	

Table 9-2 Data types for the parameters

Parameter	Data type	Description
IN	Bool	Assigned bit

- The Normally Open contact is closed (ON) when the assigned bit value is equal to 1.
- The Normally Closed contact is closed (ON) when the assigned bit value is equal to 0.
- Contacts connected in series create AND logic networks.
- Contacts connected in parallel create OR logic networks.

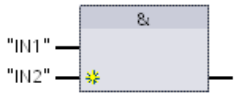
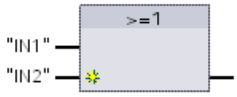
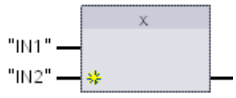
FBD AND, OR, and XOR boxes

In FBD programming, LAD contact networks are transformed into AND (&), OR (>=1), and EXCLUSIVE OR (x) box networks where you can specify bit values for the box inputs and outputs. You may also connect to other logic boxes and create your own logic combinations. After the box is placed in your network, you can drag the "Insert input" tool from the "Favorites" toolbar or instruction tree and then drop it onto the input side of the box to add more inputs. You can also right-click on the box input connector and select "Insert input".

Box inputs and outputs can be connected to another logic box, or you can enter a bit address or bit symbol name for an unconnected input. When the box instruction is executed, the

current input states are applied to the binary box logic and, if true, the box output will be true.

Table 9-3 AND, OR, and XOR boxes

FBD	SCL[1]	Description
	**out := in1 AND in2;**	All inputs of an AND box must be TRUE for the output to be TRUE.
	**out := in1 OR in2;**	Any input of an OR box must be TRUE for the output to be TRUE.
	**out := in1 XOR in2;**	An odd number of the inputs of an XOR box must be TRUE for the output to be TRUE.

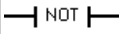
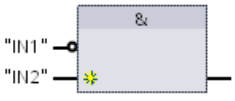
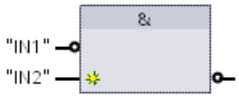
[1] For SCL: You must assign the result of the operation to a variable to be used for another statement.

Table 9-4 Data types for the parameters

Parameter	Data type	Description
IN1, IN2	Bool	Input bit

NOT logic inverter

Table 9-5 Invert RLO (Result of Logic Operation)

LAD	FBD	SCL	Description
	 	**NOT**	For FBD programming, you can drag the "Invert RLO" tool from the "Favorites" toolbar or instruction tree and then drop it on an input or output to create a logic inverter on that box connector. The LAD NOT contact inverts the logical state of power flow input. • If there is no power flow into the NOT contact, then there is power flow out. • If there is power flow into the NOT contact, then there is no power flow out.

Output coil and assignment box

The coil output instruction writes a value for an output bit. If the output bit you specify uses memory identifier Q, then the CPU turns the output bit in the process-image register on or off, setting the specified bit equal to power flow status. The output signals for your control actuators are wired to the Q terminals of the CPU. In RUN mode, the CPU system continuously scans your input signals, processes the input states according to your program logic, and then reacts by setting new output state values in the process-image output register. The CPU system transfers the new output state reaction that is stored in the process-image register, to the wired output terminals.

Table 9-6 Assignment and negate assignment

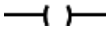
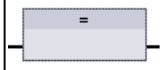
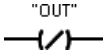
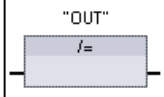
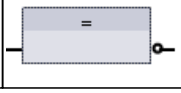
LAD	FBD	SCL	Description
"OUT" 	"OUT" 	**out := <Boolean expression>;**	In FBD programming, LAD coils are transformed into assignment (= and /=) boxes where you specify a bit address for the box output. Box inputs and outputs can be connected to other box logic or you can enter a bit address. You can specify an immediate write of a physical output using ":P" following the Q offset (example: "%Q3.4:P"). For an immediate write, the bit data values are written to the process image output and directly to physical output.
"OUT" 	"OUT" 	**out := NOT <Boolean expression>;**	
	"OUT" 		

Table 9-7 Data types for the parameters

Parameter	Data type	Description
OUT	Bool	Assigned bit

- If there is power flow through an output coil or an FBD "=" box is enabled, then the output bit is set to 1.
- If there is no power flow through an output coil or an FBD "=" assignment box is not enabled, then the output bit is set to 0.
- If there is power flow through an inverted output coil or an FBD "/=" box is enabled, then the output bit is set to 0.
- If there is no power flow through an inverted output coil or an FBD "/=" box is not enabled, then the output bit is set to 1.

9.1.2 Set and reset instructions

Set and Reset 1 bit

Table 9-8 S and R instructions

LAD	FBD	SCL	Description
"OUT" —(S)—	"OUT" S "IN"	Not available	Set output: When S (Set) is activated, then the data value at the OUT address is set to 1. When S is not activated, OUT is not changed.
"OUT" —(R)—	"OUT" R "IN"	Not available	Reset output: When R (Reset) is activated, then the data value at the OUT address is set to 0. When R is not activated, OUT is not changed.

1 For LAD and FBD: These instructions can be placed anywhere in the network.

2 For SCL: You must write code to replicate this function within your application.

Table 9-9 Data types for the parameters

Parameter	Data type	Description
IN (or connect to contact/gate logic)	Bool	Bit tag of location to be monitored
OUT	Bool	Bit tag of location to be set or reset

Set and Reset Bit Field

Table 9-10 SET_BF and RESET_BF instructions

LAD[1]	FBD	SCL	Description
"OUT" —(SET_BF)— "n"	"OUT" SET_BF EN N	Not available	Set bit field: When SET_BF is activated, a data value of 1 is assigned to "n" bits starting at address tag OUT. When SET_BF is not activated, OUT is not changed.
"OUT" —(RESET_BF)— "n"	"OUT" RESET_BF EN N	Not available	Reset bit field: RESET_BF writes a data value of 0 to "n" bits starting at address tag OUT. When RESET_BF is not activated, OUT is not changed.

1 For LAD and FBD: These instructions must be the right-most instruction in a branch.

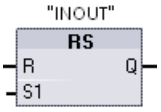
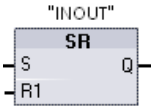
2 For SCL: You must write code to replicate this function within your application.

Table 9-11 Data types for the parameters

Parameter	Data type	Description
OUT	Bool	Starting element of a bit field to be set or reset (Example: #MyArray[3])
n	Constant (UInt)	Number of bits to write

Set-dominant and Reset-dominant flip-flops

Table 9-12 RS and SR instructions

LAD / FBD	SCL	Description
	Not available	Reset/set flip-flop: RS is a set dominant latch where the set dominates. If the set (S1) and reset (R) signals are both true, the value at address INOUT will be 1.
	Not available	Set/reset flip-flop: SR is a reset dominant latch where the reset dominates. If the set (S) and reset (R1) signals are both true, the value at address INOUT will be 0.

[1] For LAD and FBD: These instructions must be the right-most instruction in a branch.

[2] For SCL: You must write code to replicate this function within your application.

Table 9-13 Data types for the parameters

Parameter	Data type	Description
S, S1	Bool	Set input; 1 indicates dominance
R, R1	Bool	Reset input; 1 indicates dominance
INOUT	Bool	Assigned bit tag "INOUT"
Q	Bool	Follows state of "INOUT" bit

The "INOUT" tag assigns the bit address that is set or reset. The optional output Q follows the signal state of the "INOUT" address.

Instruction	S1	R	"INOUT" bit
RS	0	0	Previous state
	0	1	0
	1	0	1
	1	1	1
	S	**R1**	
SR	0	0	Previous state
	0	1	0
	1	0	1
	1	1	0

9.1.3 Positive and negative edge instructions

Table 9-14 Positive and negative transition detection

LAD	FBD	SCL	Description
"IN" P "M_BIT"	"IN" P "M_BIT"	Not available [1]	Scan operand for positive signal edge. LAD: The state of this contact is TRUE when a positive transition (OFF-to-ON) is detected on the assigned "IN" bit. The contact logic state is then combined with the power flow in state to set the power flow out state. The P contact can be located anywhere in the network except the end of a branch. FBD: The output logic state is TRUE when a positive transition (OFF-to-ON) is detected on the assigned input bit. The P box can only be located at the beginning of a branch.
"IN" N "M_BIT"	"IN" N "M_BIT"	Not available [1]	Scan operand for negative signal edge. LAD: The state of this contact is TRUE when a negative transition (ON-to-OFF) is detected on the assigned input bit. The contact logic state is then combined with the power flow in state to set the power flow out state. The N contact can be located anywhere in the network except the end of a branch. FBD: The output logic state is TRUE when a negative transition (ON-to-OFF) is detected on the assigned input bit. The N box can only be located at the beginning of a branch.
"OUT" (P) "M_BIT"	"OUT" P= "M_BIT"	Not available [1]	Set operand on positive signal edge. LAD: The assigned bit "OUT" is TRUE when a positive transition (OFF-to-ON) is detected on the power flow entering the coil. The power flow in state always passes through the coil as the power flow out state. The P coil can be located anywhere in the network. FBD: The assigned bit "OUT" is TRUE when a positive transition (OFF-to-ON) is detected on the logic state at the box input connection or on the input bit assignment if the box is located at the start of a branch. The input logic state always passes through the box as the output logic state. The P= box can be located anywhere in the branch.
"OUT" (N) "M_BIT"	"OUT" N= "M_BIT"	Not available [1]	Set operand on negative signal edge. LAD: The assigned bit "OUT" is TRUE when a negative transition (ON-to-OFF) is detected on the power flow entering the coil. The power flow in state always passes through the coil as the power flow out state. The N coil can be located anywhere in the network. FBD: The assigned bit "OUT" is TRUE when a negative transition (ON-to-OFF) is detected on the logic state at the box input connection or on the input bit assignment if the box is located at the start of a branch. The input logic state always passes through the box as the output logic state. The N= box can be located anywhere in the branch.

[1] For SCL: You must write code to replicate this function within your application.

Table 9-15 P_TRIG and N_TRIG

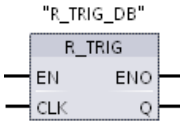
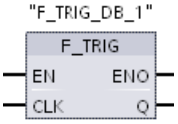
LAD / FBD	SCL	Description
P_TRIG CLK Q "M_BIT"	Not available [1]	Scan RLO (result of logic operation) for positive signal edge. The Q output power flow or logic state is TRUE when a positive transition (OFF-to-ON) is detected on the CLK input state (FBD) or CLK power flow in (LAD). In LAD, the P_TRIG instruction cannot be located at the beginning or end of a network. In FBD, the P_TRIG instruction can be located anywhere except the end of a branch.

[1] For SCL: You must write code to replicate this function within your application.

LAD / FBD	SCL	Description
	Not available [1]	Scan RLO for negative signal edge. The Q output power flow or logic state is TRUE when a negative transition (ON-to-OFF) is detected on the CLK input state (FBD) or CLK power flow in (LAD). In LAD, the N_TRIG instruction cannot be located at the beginning or end of a network. In FBD, the N_TRIG instruction can be located anywhere except the end of a branch.

[1] For SCL: You must write code to replicate this function within your application.

Table 9-16 R_TRIG and F_TRIG instructions

LAD / FBD	SCL	Description
	**"R_TRIG_DB"(CLK:=_in_, Q=> _bool_out_);**	Set tag on positive signal edge. The assigned instance DB is used to store the previous state of the CLK input. The Q output power flow or logic state is TRUE when a positive transition (OFF-to-ON) is detected on the CLK input state (FBD) or CLK power flow in (LAD). In LAD, the R_TRIG instruction cannot be located at the beginning or end of a network. In FBD, the R_TRIG instruction can be located anywhere except the end of a branch.
	"F_TRIG_DB"(CLK:=_in_, Q=> _bool_out_);	Set tag on negative signal edge. The assigned instance DB is used to store the previous state of the CLK input. The Q output power flow or logic state is TRUE when a negative transition (ON-to-OFF) is detected on the CLK input state (FBD) or CLK power flow in (LAD). In LAD, the F_TRIG instruction cannot be located at the beginning or end of a network. In FBD, the F_TRIG instruction can be located anywhere except the end of a branch.

For R_TRIG and F_TRIG, when you insert the instruction in the program, the "Call options" dialog opens automatically. In this dialog you can assign
whether the edge memory bit is stored in its own data block (single instance) or as a local tag (multiple instance) in the
block interface. If you create a separate data block, you will find it in the project tree in the "Program resources" folder
under "Program blocks > System blocks".

Table 9-17 Data types for the parameters (P and N contacts/coils, P=, N=, P_TRIG and N_TRIG)

Parameter	Data type	Description
M_BIT	Bool	Memory bit in which the previous state of the input is saved
IN	Bool	Input bit whose transition edge is detected
OUT	Bool	Output bit which indicates a transition edge was detected
CLK	Bool	Power flow or input bit whose transition edge is detected
Q	Bool	Output which indicates an edge was detected

All edge instructions use a memory bit (M_BIT: P/N contacts/coils, P_TRIG/N_TRIG) or (instance DB bit: R_TRIG, F_TRIG) to store the previous state of the monitored input signal. An edge is detected by comparing the state of the input with the previous state. If the states indicate a change of the input in the direction of interest, then an edge is reported by writing the output TRUE. Otherwise, the output is written to FALSE.

NOTE

Edge instructions evaluate the input and memory-bit values each time they are executed, including the first execution. You must account for the initial states of the input and memory bit in your program design either to allow or to avoid edge detection on the first scan.

Because the memory bit must be maintained from one execution to the next, you should use a unique bit for each edge instruction, and you should not use this bit any other place in your program. You should also avoid temporary memory and memory that can be affected by other system functions, such as an I/O update. Use only M, global DB, or Static memory (in an instance DB) for M_BIT memory assignments.

9.2 Timer operations

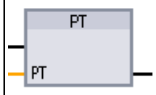
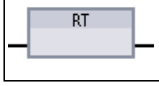
You use the timer instructions to create programmed time delays. The number of timers that you can use in your user program is limited only by the amount of memory in the CPU. Each timer uses a 16 byte IEC_Timer data type DB structure to store timer data that is specified at the top of the box or coil instruction. STEP 7 automatically creates the DB when you insert the instruction.

Table 9-18 Timer instructions

LAD / FBD boxes	LAD coils	SCL	Description
IEC_Timer_0 TP Time IN Q PT ET	TP_DB TP "PRESET_Tag"	**"IEC_Timer_0_DB".TP(IN:=_bool_in_, PT:=_time_in_, Q=>_bool_out_, ET=>_time_out_);**	The TP timer generates a pulse with a preset width time.
IEC_Timer_1 TON Time IN Q PT ET	TON_DB TON "PRESET_Tag"	**"IEC_Timer_0_DB".TON (IN:=_bool_in_, PT:=_time_in_, Q=>_bool_out_, ET=>_time_out_);**	The TON timer sets output Q to ON after a preset time delay.
IEC_Timer_2 TOF Time IN Q PT ET	TOF_DB TOF "PRESET_Tag"	**"IEC_Timer_0_DB".TOF (IN:=_bool_in_, PT:=_time_in_, Q=>_bool_out_, ET=>_time_out_);**	The TOF timer resets output Q to OFF after a preset time delay.
IEC_Timer_3 TONR Time IN Q R ET PT	TONR_DB TONR "PRESET_Tag"	**"IEC_Timer_0_DB".TONR (IN:=_bool_in_, R:=_bool_in_, PT:=_time_in_, Q=>_bool_out_, ET=>_time_out_);**	The TONR timer sets output Q to ON after a preset time delay. Elapsed time is accumulated over multiple timing periods until the R input is used to reset the elapsed time.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL examples, "IEC_Timer_0_DB" is the name of the instance DB.

LAD / FBD boxes	LAD coils	SCL	Description
FBD only: 	TON_DB —(PT)— "PRESET_Tag"	**PRESET_TIMER(PT:=_time_in_, TIMER:=_iec_timer_in_);**	The PT (Preset timer) coil loads a new PRESET time value in the specified IEC_Timer.
FBD only: 	TON_DB —(RT)—	**RESET_TIMER(_iec_timer_in_);**	The RT (Reset timer) coil resets the specified IEC_Timer.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL examples, "IEC_Timer_0_DB" is the name of the instance DB.

Table 9-19 Data types for the parameters

Parameter	Data type	Description
Box: IN Coil: Power flow	Bool	TP, TON, and TONR: Box: 0=Disable timer, 1=Enable timer Coil: No power flow=Disable timer, Power flow=Enable timer TOF: Box: 0=Enable timer, 1=Disable timer Coil: No power flow=Enable timer, Power flow=Disable timer
R	Bool	TONR box only: 0=No reset 1= Reset elapsed time and Q bit to 0
Box: PT Coil: "PRESET_Tag"	Time	Timer box or coil: Preset time input
Box: Q Coil: DBdata.Q	Bool	Timer box: Q box output or Q bit in the timer DB data Timer coil: you can only address the Q bit in the timer DB data
Box: ET Coil: DBdata.ET	Time	Timer box: ET (elapsed time) box output or ET time value in the timer DB data Timer coil: you can only address the ET time value in the timer DB data.

Table 9-20 Effect of value changes in the PT and IN parameters

Timer	Changes in the PT and IN box parameters and the corresponding coil parameters
TP	• Changing PT has no effect while the timer runs. • Changing IN has no effect while the timer runs.
TON	• Changing PT has no effect while the timer runs. • Changing IN to FALSE, while the timer runs, resets and stops the timer.
TOF	• Changing PT has no effect while the timer runs. • Changing IN to TRUE, while the timer runs, resets and stops the timer.
TONR	• Changing PT has no effect while the timer runs, but has an effect when the timer resumes. • Changing IN to FALSE, while the timer runs, stops the timer but does not reset the timer. Changing IN back to TRUE will cause the timer to start timing from the accumulated time value.

PT (preset time) and ET (elapsed time) values are stored in the specified IEC_TIMER DB data as signed double integers that represent milliseconds of time. TIME data uses the T# identifier and can be entered as a simple time unit (T#200ms or 200) and as compound time units like T#2s_200ms.

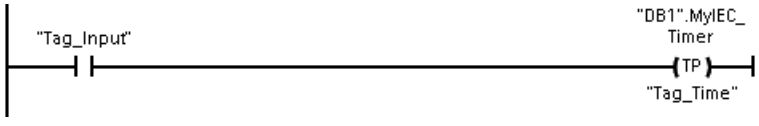
Table 9-21 Size and range of the TIME data type

Data type	Size	Valid number ranges[1]
TIME	32 bits, stored as DInt data	T#-24d_20h_31m_23s_648ms to T#24d_20h_31m_23s_647ms Stored as -2,147,483,648 ms to +2,147,483,647 ms

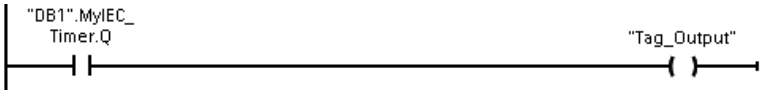
[1] The negative range of the TIME data type shown above cannot be used with the timer instructions. Negative PT (preset time) values are set to zero when the timer instruction is executed. ET (elapsed time) is always a positive value.

Timer coil example

The -(TP)-, -(TON)-, -(TOF)-, and -(TONR)- timer coils must be the last instruction in a LAD network. As shown in the timer example, a contact instruction in a subsequent network evaluates the Q bit in a timer coil's IEC_Timer DB data. Likewise, you must address the ELAPSED element in the IEC_timer DB data if you want to use the elapsed time value in your program.



The pulse timer is started on a 0 to 1 transition of the Tag_Input bit value. The timer runs for the time specified by Tag_Time time value.



As long as the timer runs, the state of DB1.MyIEC_Timer.Q=1 and the Tag_Output value=1. When the Tag_Time value has elapsed, then DB1.MyIEC_Timer.Q=0 and the Tag_Output value=0.

Reset timer -(RT)- and Preset timer -(PT)- coils

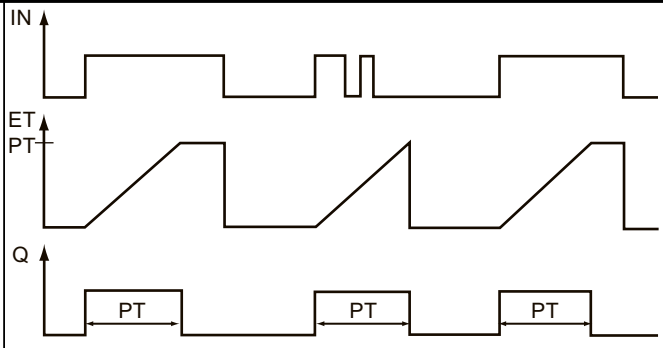
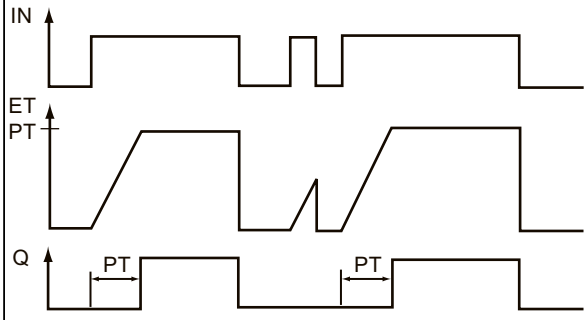
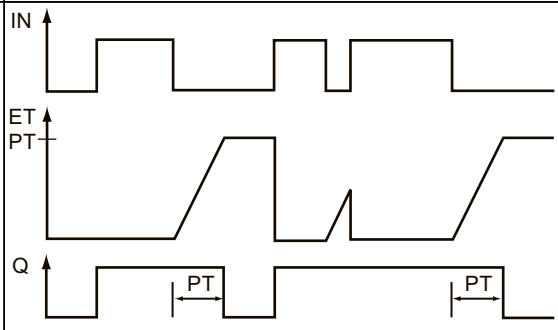
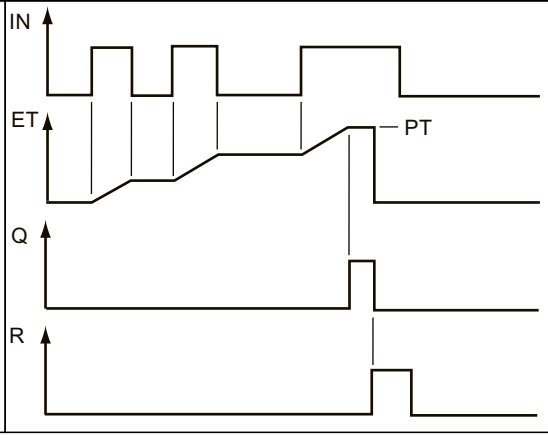
These coil instructions can be used with box or coil timers and can be placed in a mid-line position. The coil output power flow status is always the same as the coil input status. When the -(RT)- coil is activated, the ELAPSED time element of the specified IEC_Timer DB data is reset to 0. When the -(PT)- coil is activated, the PRESET time element of the specified IEC_Timer DB data is loaded with the assigned time-duration value..

NOTE

When you place timer instructions in an FB, you can select the "Multi-instance data block" option. The timer structure names can be different with separate data structures, but the timer data is contained in a single data block and does not require a separate data block for each timer. This reduces the processing time and data storage necessary for handling the timers. There is no interaction between the timer data structures in the shared multi-instance DB.

Operation of the timers

Table 9-22 Types of IEC timers

Timer	Timing diagram
TP: Generate pulse The TP timer generates a pulse with a preset width time.	
TON: Generate ON-delay The TON timer sets output Q to ON after a preset time delay.	
TOF: Generate OFF-delay The TOF timer resets output Q to OFF after a preset time delay.	
TONR: Time accumulator The TONR timer sets output Q to ON after a preset time delay. Elapsed time is accumulated over multiple timing periods until the R input is used to reset the elapsed time.	

NOTE

In the CPU, no dedicated resource is allocated to any specific timer instruction. Instead, each timer utilizes its own timer structure in DB memory and a continuously-running internal CPU timer to perform timing.

When a timer is started due to an edge change on the input of a TP, TON, TOF, or TONR instruction, the value of the continuously-running internal CPU timer is copied into the START member of the DB structure allocated for this timer instruction. This start value remains unchanged while the timer continues to run, and is used later each time the timer is updated. Each time the timer is started, a new start value is loaded into the timer structure from the internal CPU timer.

When a timer is updated, the start value described above is subtracted from the current value of the internal CPU timer to determine the elapsed time. The elapsed time is then compared with the preset to determine the state of the timer Q bit. The ELAPSED and Q members are then updated in the DB structure allocated for this timer. Note that the elapsed time is clamped at the preset value (the timer does not continue to accumulate elapsed time after the preset is reached).

A timer update is performed when and only when:

- A timer instruction (TP, TON, TOF, or TONR) is executed
- The "ELAPSED" member of the timer structure in DB is referenced directly by an instruction
- The "Q" member of the timer structure in DB is referenced directly by an instruction

Timer programming

The following consequences of timer operation should be considered when planning and creating your user program:

- You can have multiple updates of a timer in the same scan. The timer is updated each time the timer instruction (TP, TON, TOF, TONR) is executed and each time the ELAPSED or Q member of the timer structure is used as a parameter of another executed instruction. This is an advantage if you want the latest time data (essentially an immediate read of the timer). However, if you desire to have consistent values throughout a program scan, then place your timer instruction prior to all other instructions that need these values, and use tags from the Q and ET outputs of the timer instruction instead of the ELAPSED and Q members of the timer DB structure.
- You can have scans during which no update of a timer occurs. It is possible to start your timer in a function, and then cease to call that function again for one or more scans. If no other instructions are executed which reference the ELAPSED or Q members of the timer structure, then the timer will not be updated. A new update will not occur until either the timer instruction is executed again or some other instruction is executed using ELAPSED or Q from the timer structure as a parameter.
- Although not typical, you can assign the same DB timer structure to multiple timer instructions. In general, to avoid unexpected interaction, you should only use one timer instruction (TP, TON, TOF, TONR) per DB timer structure.
- Self-resetting timers are useful to trigger actions that need to occur periodically. Typically, self-resetting timers are created by placing a normally-closed contact which references the timer bit in front of the timer instruction. This timer network is typically located above one or more dependent networks that use the timer bit to trigger actions. When the timer expires (elapsed time reaches preset value), the timer bit is ON for one scan, allowing the dependent network logic controlled by the timer bit to execute. Upon the next execution

of the timer network, the normally closed contact is OFF, thus resetting the timer and clearing the timer bit. The next scan, the normally closed contact is ON, thus restarting the timer. When creating self-resetting timers such as this, do not use the "Q" member of the timer DB structure as the parameter for the normally-closed contact in front of the timer instruction. Instead, use the tag connected to the "Q" output of the timer instruction for this purpose. The reason to avoid accessing the Q member of the timer DB structure is because this causes an update to the timer and if the timer is updated due to the normally closed contact, then the contact will reset the timer instruction immediately. The Q output of the timer instruction will not be ON for the one scan and the dependent networks will not execute.

Time data retention after a RUN-STOP-RUN transition or a CPU power cycle

If a run mode session is ended with stop mode or a CPU power cycle and a new run mode session is started, then the timer data stored in the previous run mode session is lost, unless the timer data structure is specified as retentive (TP, TON, TOF, and TONR timers).

When you accept the defaults in the call options dialog after you place a timer instruction in the program editor, you are automatically assigned an instance DB which **cannot be made retentive**. To make your timer data retentive, you must either use a global DB or a Multi-instance DB.

Assign a global DB to store timer data as retentive data

This option works regardless of where the timer is placed (OB, FC, or FB).

1. Create a global DB:
   - Double-click "Add new block" from the Project tree
   - Click the data block (DB) icon
   - For the Type, choose global DB
   - If you want to be able to select individual data elements in this DB as retentive, be sure the DB type "Optimized" box is checked. The other DB type option "Standard - compatible with S7-300/400" only allows setting all DB data elements retentive or none retentive.
   - Click OK
2. Add timer structure(s) to the DB:
   - In the new global DB, add a new static tag using data type IEC_Timer.
   - In the "Retain" column, check the box so that this structure will be retentive.
   - Repeat this process to create structures for all the timers that you want to store in this DB. You can either place each timer structure in a unique global DB, or you can place multiple timer structures into the same global DB. You can also place other static tags besides timers in this global DB. Placing multiple timer structures into the same global DB allows you to reduce your overall number of blocks.
   - Rename the timer structures if desired.
3. Open the program block for editing where you want to place a retentive timer (OB, FC, or FB).
4. Place the timer instruction at the desired location.

5. When the call options dialog appears, click the cancel button.
6. On the top of the new timer instruction, type the name (do not use the helper to browse) of the global DB and timer structure that you created above (example: "Data_block_3.Static_1").

Assign a multi-instance DB to store timer data as retentive data

This option only works if you place the timer in an FB.

This option depends upon whether the FB properties specify "Optimized block access" (allows symbolic access only). To verify how the access attribute is configured for an existing FB, right-click on the FB in the Project tree, choose properties, and then choose Attributes.

If the FB specifies "Optimized block access" (allows symbolic access only):

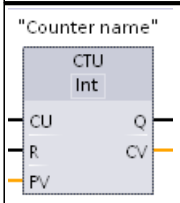
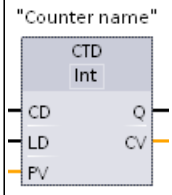
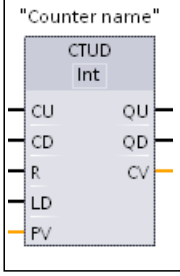
1. Open the FB for edit.
2. Place the timer instruction at the desired location in the FB.
3. When the Call options dialog appears, click the Multi instance icon. The Multi Instance option is only available if the instruction is being placed into an FB.
4. In the Call options dialog, rename the timer if desired.
5. Click OK. The timer instruction appears in the editor, and the IEC_TIMER structure appears in the FB Interface under Static.
6. If necessary, open the FB interface editor (may have to click on the small arrow to expand the view).
7. Under Static, locate the timer structure that was just created for you.
8. In the Retain column for this timer structure, change the selection to "Retain". Whenever this FB is called later from another program block, an instance DB will be created with this interface definition which contains the timer structure marked as retentive.

If the FB does not specify "Optimized block access", then the block access type is standard, which is compatible with S7-300/400 classic configurations and allows symbolic and direct access. To assign a multi-instance to a standard block access FB, follow these steps:

1. Open the FB for edit.
2. Place the timer instruction at the desired location in the FB.
3. When the Call options dialog appears, click on the multi instance icon. The multi instance option is only available if the instruction is being placed into an FB.
4. In the Call options dialog, rename the timer if desired.
5. Click OK. The timer instruction appears in the editor, and the IEC_TIMER structure appears in the FB Interface under Static.
6. Open the block that will use this FB.
7. Place this FB at the desired location. Doing so results in the creation of an instance data block for this FB.
8. Open the instance data block created when you placed the FB in the editor.
9. Under Static, locate the timer structure of interest. In the Retain column for this timer structure, check the box to make this structure retentive.

9.3 Counter operations

Table 9-23 Counter instructions

LAD / FBD	SCL	Description
	**"IEC_Counter_0_DB".CTU(CU:=_bool_in, R:=_bool_in, PV:=_in, Q=>_bool_out, CV=>_out);**	Use the counter instructions to count internal program events and external process events. Each counter uses a structure stored in a data block to maintain counter data. You assign the data block when the counter instruction is placed in the editor. • CTU is a count-up counter • CTD is a count-down counter • CTUD is a count-up-and-down counter
	**"IEC_Counter_0_DB".CTD(CD:=_bool_in, LD:=_bool_in, PV:=_in, Q=>_bool_out, CV=>_out);**	
	**"IEC_Counter_0_DB".CTUD(CU:=_bool_in, CD:=_bool_in, R:=_bool_in, LD:=_bool_in, PV:=_in_, QU=>_bool_out, QD=>_bool_out, CV=>_out_);**	

[1] For LAD and FBD: Select the count value data type from the drop-down list below the instruction name.

[2] STEP 7 automatically creates the DB when you insert the instruction.

[3] In the SCL examples, "IEC_Counter_0_DB" is the name of the instance DB.

Table 9-24 Data types for the parameters

Parameter	Data type[1]	Description
CU, CD	Bool	Count up or count down, by one count
R (CTU, CTUD)	Bool	Reset count value to zero
LD (CTD, CTUD)	Bool	Load control for preset value
PV	SInt, Int, DInt, USInt, UInt, UDInt	Preset count value
Q, QU	Bool	True if CV >= PV
QD	Bool	True if CV <= 0
CV	SInt, Int, DInt, USInt, UInt, UDInt	Current count value

[1] The numerical range of count values depends on the data type you select. If the count value is an unsigned integer type, you can count down to zero or count up to the range limit. If the count value is a signed integer, you can count down to the negative integer limit and count up to the positive integer limit.

The amount of memory in the CPU limits the number of counters allowed in the user program. Counters use the following amount of memory:

- For SInt or USInt data types, the counter instruction uses 3 bytes.
- For Int or UInt data types, the counter instruction uses 6 bytes.
- For DInt or UDInt data types, the counter instruction uses 12 bytes.

These instructions use software counters whose maximum counting rate is limited by the execution rate of the OB in which they are placed. The OB that the instructions are placed in must be executed often enough to detect all transitions of the CU or CD inputs. For faster counting operations, see the CTRL_HSC instruction (Page 480).

NOTE

When you place counter instructions in an FB, you can select the multi-instance DB option, the counter structure names can be different with separate data structures, but the counter data is contained in a single DB and does not require a separate DB for each counter. This reduces the processing time and data storage necessary for the counters. There is no interaction between the counter data structures in the shared multi-instance DB.

Operation of the counters

Table 9-25 Operation of CTU (count up)

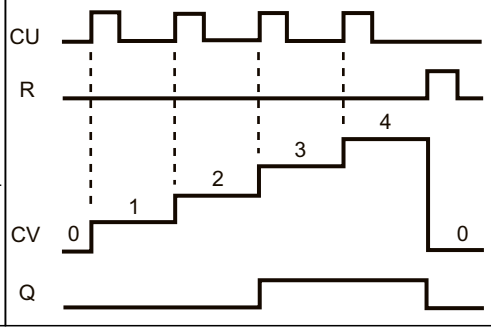
Counter	Operation
The CTU counter counts up by 1 when the value of parameter CU changes from 0 to 1. The CTU timing diagram shows the operation for an unsigned integer count value (where PV = 3). • If the value of parameter CV (current count value) is greater than or equal to the value of parameter PV (preset count value), then the counter output parameter Q = 1. • If the value of the reset parameter R changes from 0 to 1, then the current count value is reset to 0.	

Table 9-26 Operation of CTD (count down)

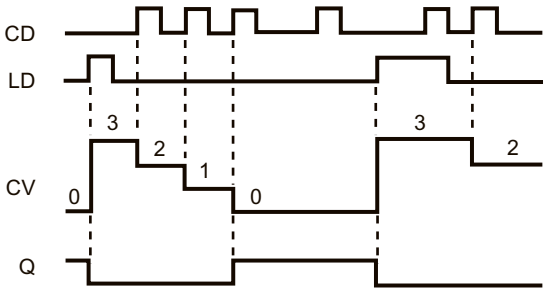
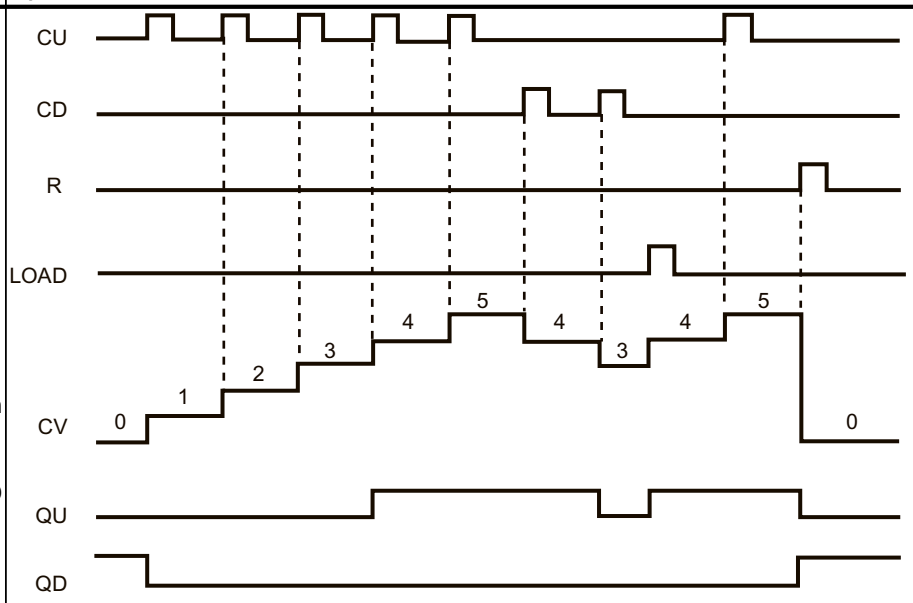
Counter	Operation
The CTD counter counts down by 1 when the value of parameter CD changes from 0 to 1. The CTD timing diagram shows the operation for an unsigned integer count value (where PV = 3). • If the value of parameter CV (current count value) is equal to or less than 0, the counter output parameter Q = 1. • If the value of parameter LOAD changes from 0 to 1, the value at parameter PV (preset value) is loaded to the counter as the new CV (current count value).	

Table 9-27 Operation of CTUD (count up and down)

Counter	Operation
The CTUD counter counts up or down by 1 on the 0 to 1 transition of the count up (CU) or count down (CD) inputs. The CTUD timing diagram shows the operation for an unsigned integer count value (where PV = 4). • If the value of parameter CV is equal to or greater than the value of parameter PV, then the counter output parameter QU = 1. • If the value of parameter CV is less than or equal to zero, then the counter output parameter QD = 1. • If the value of parameter LOAD changes from 0 to 1, then the value at parameter PV is loaded to the counter as the new CV. • If the value of the reset parameter R is changes from 0 to 1, the current count value is reset to 0.	

Counter data retention after a RUN-STOP-RUN transition or a CPU power cycle

If a run mode session is ended with stop mode or a CPU power cycle and a new run mode session is started, then the counter data stored in the previous run mode session is lost, unless the counter data structure is specified as retentive (CTU, CTD, and CTUD counters).

When you accept the defaults in the call options dialog after you place a counter instruction in the program editor, you are automatically assigned an instance DB which **cannot be made retentive**. To make your counter data retentive, you must either use a global DB or a Multi-instance DB.

Assign a global DB to store counter data as retentive data

This option works regardless of where the counter is placed (OB, FC, or FB).

1. Create a global DB:
   - Double-click "Add new block" from the Project tree
   - Click the data block (DB) icon
   - For the Type, choose global DB
   - If you want to be able to select individual items in this DB as retentive, be sure the symbolic-access-only box is checked.
   - Click OK

2. Add counter structure(s) to the DB:
   - In the new global DB, add a new static tag using one of the counter data types. Be sure to consider the Type you want to use for your Preset and Count values.
   - In the "Retain" column, check the box so that this structure will be retentive.
   - Repeat this process to create structures for all the counters that you want to store in this DB. You can either place each counter structure in a unique global DB, or you can place multiple counter structures into the same global DB. You can also place other static tags besides counters in this global DB. Placing multiple counter structures into the same global DB allows you to reduce your overall number of blocks.
   - Rename the counter structures if desired.
3. Open the program block for editing where you want to place a retentive counter (OB, FC, or FB).
4. Place the counter instruction at the desired location.
5. When the call options dialog appears, click the cancel button. You should now see a new counter instruction which has "???" both just above and just below the instruction name.
6. On the top of the new counter instruction, type the name (do not use the helper to browse) of the global DB and counter structure that you created above (example: "Data_block_3.Static_1"). This causes the corresponding preset and count value type to be filled in (example: UInt for an IEC_UCounter structure).

Counter Data Type	Corresponding Type for the Preset and Count Values
IEC_Counter	INT
IEC_SCounter	SINT
IEC_DCounter	DINT
IEC_UCounter	UINT
IEC_USCounter	USINT
IEC_UDCounter	UDINT

Assign a multi-instance DB to store counter data as retentive data

This option only works if you place the counter in an FB.

This option depends upon whether the FB properties specify "Optimized block access" (allows symbolic access only). To verify how the access attribute is configured for an existing FB, right-click on the FB in the Project tree, choose properties, and then choose Attributes.

If the FB specifies "Optimized block access" (allows symbolic access only):

1. Open the FB for edit.
2. Place the counter instruction at the desired location in the FB.
3. When the Call options dialog appears, click on the Multi instance icon. The Multi Instance option is only available if the instruction is being placed into an FB.
4. In the Call options dialog, rename the counter if desired.
5. Click OK. The counter instruction appears in the editor with type INT for the preset and count values, and the IEC_COUNTER structure appears in the FB Interface under Static.
6. If desired, change the type in the counter instruction from INT to one of the other types. The counter structure will change correspondingly.
7. If necessary, open the FB interface editor (may have to click on the small arrow to expand the view).

8. Under Static, locate the counter structure that was just created for you.
9. In the Retain column for this counter structure, change the selection to "Retain". Whenever this FB is called later from another program block, an instance DB will be created with this interface definition which contains the counter structure marked as retentive.

If the FB does not specify "Optimized block access", then the block access type is standard, which is compatible with S7-300/400 classic configurations and allows symbolic and direct access. To assign a multi-instance to a standard block access FB, follow these steps:

1. Open the FB for edit.
2. Place the counter instruction at the desired location in the FB.
3. When the Call options dialog appears, click on the multi instance icon. The multi instance option is only available if the instruction is being placed into an FB.
4. In the Call options dialog, rename the counter if desired.
5. Click OK. The counter instruction appears in the editor with type INT for the preset and count value, and the IEC_COUNTER structure appears in the FB Interface under Static.
6. If desired, change the type in the counter instruction from INT to one of the other types. The counter structure will change correspondingly.
7. Open the block that will use this FB.
8. Place this FB at the desired location. Doing so results in the creation of an instance data block for this FB.
9. Open the instance data block created when you placed the FB in the editor.
10. Under Static, locate the counter structure of interest. In the Retain column for this counter structure, check the box to make this structure retentive.

Type shown in counter instruction (for preset and count values)	Corresponding structure Type shown in FB interface
INT	IEC_Counter
SINT	IEC_SCounter
DINT	IEC_DCounter
UINT	IEC_UCounter
USINT	IEC_USCounter
UDINT	IEC_UDCounter

9.4 Comparator operations

9.4.1 Compare values instructions

Table 9-28 Compare instructions

LAD	FBD	SCL	Description
"IN1" == Byte "IN2"	== Byte "IN1" IN1 "IN2" IN2	**out := in1 = in2;** or **IF in1 = in2 THEN out := 1; ELSE out := 0; END_IF;**	Compares two values of the same data type. When the LAD contact comparison is TRUE, then the contact is activated. When the FBD box comparison is TRUE, then the box output is TRUE.

[1] For LAD and FBD: Click the instruction name (such as "==") to change the comparison type from the drop-down list. Click the "???" and select data type from the drop-down list.

Table 9-29 Data types for the parameters

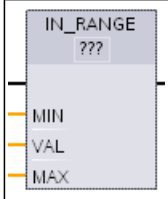
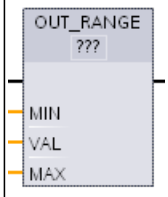
Parameter	Data type	Description
IN1, IN2	Byte, Word, DWord, SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, String, WString, Char, Char, Time, Date, TOD, DTL, Constant	Values to compare

Table 9-30 Comparison descriptions

Relation type	The comparison is true if ...
=	IN1 is equal to IN2
<>	IN1 is not equal to IN2
>=	IN1 is greater than or equal to IN2
<=	IN1 is less than or equal to IN2
>	IN1 is greater than IN2
<	IN1 is less than IN2

9.4.2 IN_Range (Value within range) and OUT_Range (Value outside range)

Table 9-31 Value within Range and value outside range instructions

LAD / FBD	SCL	Description
	**out := IN_RANGE(min, val, max);**	Tests whether an input value is in or out of a specified value range. If the comparison is TRUE, then the box output is TRUE.
	**out := OUT_RANGE(min, val, max);**	

[1] For LAD and FBD: Click the "???" and select the data type from the drop-down list.

Table 9-32 Data types for the parameters

Parameter	Data type[1]	Description
MIN, VAL, MAX	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Constant	Comparator inputs

[1] The input parameters MIN, VAL, and MAX must be the same data type.

- The IN_RANGE comparison is true if: MIN <= VAL <= MAX
- The OUT_RANGE comparison is true if: VAL < MIN or VAL > MAX

9.4.3 OK (Check validity) and NOT_OK (Check invalidity)

Table 9-33 OK (check validity) and Not OK (check invalidity) instructions

LAD	FBD	SCL	Description
"IN" OK	"IN" OK	Not available	Tests whether an input data reference is a valid real number according to IEEE specification 754.
"IN" NOT_OK	"IN" NOT_OK	Not available	

[1] For LAD and FBD: When the LAD contact is TRUE, the contact is activated and passes power flow. When the FBD box is TRUE, then the box output is TRUE.

Table 9-34 Data types for the parameter

Parameter	Data type	Description
IN	Real, LReal	Input data

Table 9-35 Operation

Instruction	The Real number test is TRUE if:
OK	The input value is a valid real number [1]
NOT_OK	The input value is not a valid real number [1]

[1] A Real or LReal value is invalid if it is +/- INF (infinity), NaN (Not a Number), or if it is a denormalized value. A denormalized value is a number very close to zero. The CPU substitutes a zero for a denormalized value in calculations.

9.4.4 Variant and array comparison instructions

9.4.4.1 Equality and non-equality comparison instructions

The S7-1200 CPU provides instructions for querying the data type of a tag to which a Variant operand points for either equality or non-equality to the data type of the other operand.

In addition, the S7-1200 CPU provides instructions for querying the data type of an array element for either equality or non-equality to the data type of the other operand.

In these instructions, you are comparing <Operand1> to <Operand2>. <Operand1> must have the Variant data type. <Operand2> can be an elementary data type of a PLC data type. In LAD and FBD, <Operand1> is the operand above the instruction. In LAD, <Operand2> is the operand below the instruction.

For all instructions, the result of logic operation (RLO) is 1 (true) if the equality or non-equality test passes, and is 0 (false) if not.

The equality and non-equality type comparison instructions are as follows:

- EQ_Type (Compare data type for EQUAL with the data type of a tag)
- NE_Type (Compare data type for UNEQUAL with the data type of a tag)
- EQ_ElemType (Compare data type of an ARRAY element for EQUAL with the data type of a tag)
- NE_ElemType (Compare data type of an ARRAY element for UNEQUAL with the data type of a tag)

Table 9-36 EQ and NE instructions

LAD	FBD	SCL	Description
#Operand1 EQ_Type "Operand2"	#Operand1 EQ_Type "Operand2" IN2 OUT	Not available	Tests whether the tag pointed to by the Variant at Operand1 is of the same data type as the tag at Operand2.
#Operand1 NE_Type "Operand2"	#Operand1 NE_Type "Operand2" IN2 OUT	Not available	Tests whether the tag pointed to by the Variant at Operand1 is of a different data type as the tag at Operand2.
#Operand1 EQ_ElemType "Operand2"	#Operand1 EQ_ElemType "Operand2" IN2 OUT	Not available	Tests whether the array element pointed to by the Variant at Operand1 is of the same data type as the tag at Operand2.
#Operand1 NE_ElemType "Operand2"	#Operand1 NE_ElemType "Operand2" IN2 OUT	Not available	Tests whether the array element pointed to by the Variant at Operand1 is of a different data type as the tag at Operand2.

Table 9-37 Data types for the parameters

Parameter	Data type	Description
Operand1	Variant	First operand
Operand2	Bit strings, integers, floating-point numbers, timers, date and time, character strings, ARRAY, PLC data types	Second operand

9.4.4.2 Null comparision instructions

You can use the instructions IS_NULL and NOT_NULL to determine whether or not the input actually points to an object or not.

For both instructions, <Operand> must have the Variant data type.

Table 9-38 IS_NULL (Query for EQUALS ZERO pointer) and NOT_NULL (Query for EQUALS ZERO pointer) instructions

LAD	FBD	SCL	Description
#Operand IS_NULL	#Operand IS_NULL OUT	Not available	Tests whether the tag pointed to by the Variant at Operand is null and therefore not an object.
#Operand NOT_NULL	#Operand NOT_NULL OUT	Not available	Tests whether the tag pointed to by the Variant at Operand is not null and therefore does point to an object.

Table 9-39 Data types for the parameters

Parameter	Data type	Description
Operand	Variant	Operand to evaluate for null or not null.

9.4.4.3 IS_ARRAY (Check for ARRAY)

You can use the "Check for ARRAY" instruction to query whether the Variant points to a tag of the Array data type.
The <Operand> must have the Variant data type.
The instructions returns 1 (true) if the operand is an array.

Table 9-40 IS_ARRAY (Check for ARRAY)

LAD	FBD	SCL	Description
#Operand IS_ARRAY	#Operand IS_ARRAY OUT	IS_ARRAY(_variant_in_)	Tests whether the tag pointed to by the Variant at Operand is an array.

Table 9-41 Data types for the parameters

Parameter	Data type	Description
Operand	Variant	Operand to evaluate for whether it is an array.

9.5 Math functions

9.5.1 CALCULATE (Calculate)

Table 9-42 CALCULATE instruction

LAD / FBD	SCL	Description
CALCULATE ??? EN ENO OUT := <???> IN1 OUT IN2	Use the standard SCL math expressions to create the equation.	The CALCULATE instruction lets you create a math function that operates on inputs (IN1, IN2, .. INn) and produces the result at OUT, according to the equation that you define. • Select a data type first. All inputs and the output must be the same data type. • To add another input, click the icon at the last input.

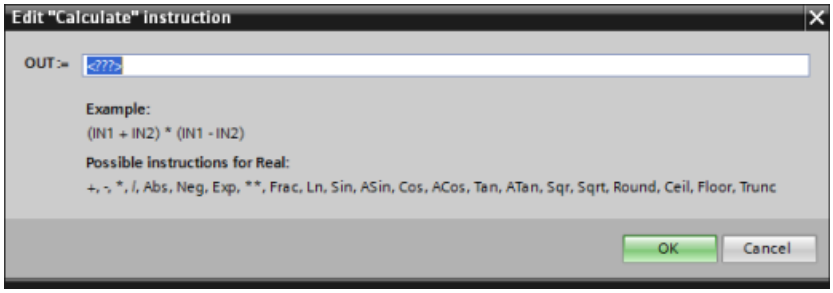
Table 9-43 Data types for the parameters

Parameter	Data type[1]
IN1, IN2, ..INn	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord

[1] The IN and OUT parameters must be the same data type (with implicit conversions of the input parameters). For example: A SINT value for an input would be converted to an INT or a REAL value if OUT is an INT or REAL

Click the calculator icon to open the dialog and define your math function. You enter your equation as inputs (such as IN1 and IN2) and operations. When you click "OK" to save the function, the dialog automatically creates the inputs for the CALCULATE instruction.

The dialog shows an example and a list of possible instructions that you can include based on the data type of the OUT parameter:



NOTE

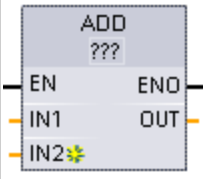
You also must create an input for any constants in your function. The constant value would then be entered in the associated input for the CALCULATE instruction.

By entering constants as inputs, you can copy the CALCULATE instruction to other locations in your user program without having to change the function. You then can change the values or tags of the inputs for the instruction without modifying the function.

When CALCULATE is executed and all the individual operations in the calculation complete successfully, then the ENO = 1. Otherwise, ENO = 0.

9.5.2 Add, subtract, multiply and divide instructions

Table 9-44 Add, subtract, multiply and divide instructions

LAD / FBD	SCL	Description
	**out := in1 + in2;** **out := in1 - in2;** **out := in1 * in2;** **out := in1 / in2;**	• ADD: Addition (IN1 + IN2 = OUT) • SUB: Subtraction (IN1 - IN2 = OUT) • MUL: Multiplication (IN1 * IN2 = OUT) • DIV: Division (IN1 / IN2 = OUT) An Integer division operation truncates the fractional part of the quotient to produce an integer output.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-45 Data types for the parameters (LAD and FBD)

Parameter	Data type[1]	Description
IN1, IN2	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Constant	Math operation inputs
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal	Math operation output

[1] Parameters IN1, IN2, and OUT must be the same data type.

To add an ADD or MUL input, click the "Create" icon or right-click on an input stub for one of the existing IN parameters and select the "Insert input" command.

To remove an input, right-click on an input stub for one of the existing IN parameters (when there are more than the original two inputs) and select the "Delete" command.

When enabled (EN = 1), the math instruction performs the specified operation on the input values (IN1 and IN2) and stores the result in the memory address specified by the output

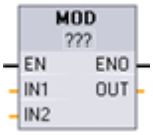
parameter (OUT). After the successful completion of the operation, the instruction sets ENO = 1.

Table 9-46 ENO status

ENO	Description
1	No error
0	The Math operation result value would be outside the valid number range of the data type selected. The least significant part of the result that fits in the destination size is returned.
0	Division by 0 (IN2 = 0): The result is undefined and zero is returned.
0	Real/LReal: If one of the input values is NaN (not a number) then NaN is returned.
0	ADD Real/LReal: If both IN values are INF with different signs, this is an illegal operation and NaN is returned.
0	SUB Real/LReal: If both IN values are INF with the same sign, this is an illegal operation and NaN is returned.
0	MUL Real/LReal: If one IN value is zero and the other is INF, this is an illegal operation and NaN is returned.
0	DIV Real/LReal: If both IN values are zero or INF, this is an illegal operation and NaN is returned.

9.5.3 MOD (return remainder of division)

Table 9-47 Modulo (return remainder of division) instruction

LAD / FBD	SCL	Description
	**out := in1 MOD in2;**	You can use the MOD instruction to return the remainder of an integer division operation. The value at the IN1 input is divided by the value at the IN2 input and the remainder is returned at the OUT output.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-48 Data types for parameters

Parameter	Data type[1]	Description
IN1 and IN2	SInt, Int, DInt, USInt, UInt, UDInt, Constant	Modulo inputs
OUT	SInt, Int, DInt, USInt, UInt, UDInt	Modulo output

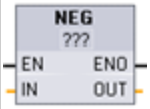
[1] The IN1, IN2, and OUT parameters must be the same data type.

Table 9-49 ENO values

ENO	Description
1	No error
0	Value IN2 = 0, OUT is assigned the value zero

9.5.4 NEG (Create twos complement)

Table 9-50 NEG (create twos complement) instruction

LAD / FBD	SCL	Description
	**-(in);**	The NEG instruction inverts the arithmetic sign of the value at parameter IN and stores the result in parameter OUT.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-51 Data types for parameters

Parameter	Data type[1]	Description
IN	SInt, Int, DInt, Real, LReal, Constant	Math operation input
OUT	SInt, Int, DInt, Real, LReal	Math operation output

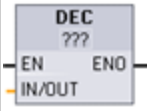
[1] The IN and OUT parameters must be the same data type.

Table 9-52 ENO status

ENO	Description
1	No error
0	The resulting value is outside the valid number range of the selected data type. Example for SInt: NEG (-128) results in +128 which exceeds the data type maximum.

9.5.5 INC (Increment) and DEC (Decrement)

Table 9-53 INC and DEC instructions

LAD / FBD	SCL	Description
	in_out := in_out + 1;	Increments a signed or unsigned integer number value: IN_OUT value +1 = IN_OUT value
	**in_out := in_out - 1;**	Decrements a signed or unsigned integer number value: IN_OUT value - 1 = IN_OUT value

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-54 Data types for parameters

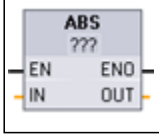
Parameter	Data type	Description
IN/OUT	SInt, Int, DInt, USInt, UInt, UDInt	Math operation input and output

Table 9-55 ENO status

ENO	Description
1	No error
0	The resulting value is outside the valid number range of the selected data type. Example for SInt: INC (+127) results in +128, which exceeds the data type maximum.

9.5.6 ABS (Form absolute value)

Table 9-56 ABS (absolute value) instruction

LAD / FBD	SCL	Description
	**out := ABS(in);**	Calculates the absolute value of a signed integer or real number at parameter IN and stores the result in parameter OUT.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-57 Data types for parameters

Parameter	Data type[1]	Description
IN	SInt, Int, DInt, Real, LReal	Math operation input
OUT	SInt, Int, DInt, Real, LReal	Math operation output

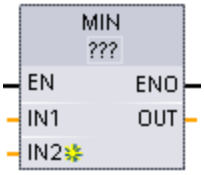
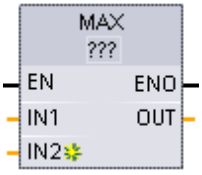
[1] The IN and OUT parameters must be the same data type.

Table 9-58 ENO status

ENO	Description
1	No error
0	The math operation result value is outside the valid number range of the selected data type. Example for SInt: ABS (-128) results in +128 which exceeds the data type maximum.

9.5.7 MIN (Get minimum) and MAX (Get maximum)

Table 9-59 MIN (get minimum) and MAX (get maximum) instructions

LAD / FBD	SCL	Description
	**out:= MIN(in1:=_variant_in_, in2:=_variant_in_ [,...in32]);**	The MIN instruction compares the value of two parameters IN1 and IN2 and assigns the minimum (lesser) value to parameter OUT.
	**out:= MAX(in1:=_variant_in_, in2:=_variant_in_ [,...in32]);**	The MAX instruction compares the value of two parameters IN1 and IN2 and assigns the maximum (greater) value to parameter OUT.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-60 Data types for the parameters

Parameter	Data type[1]	Description
IN1, IN2 [...IN32]	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Time, Date, TOD, Constant	Math operation inputs (up to 32 inputs)
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Time, Date, TOD	Math operation output

[1] The IN1, IN2, and OUT parameters must be the same data type.

To add an input, click the "Create" icon or right-click on an input stub for one of the existing IN parameters and select the "Insert input" command.

To remove an input, right-click on an input stub for one of the existing IN parameters (when there are more than the original two inputs) and select the "Delete" command.

Table 9-61 ENO status

ENO	Description
1	No error
0	For Real data type only: • At least one input is not a real number (NaN). • The resulting OUT is +/- INF (infinity).

9.5.8 LIMIT (Set limit value)

Table 9-62 LIMIT (set limit value) instruction

LAD / FBD	SCL	Description
	LIMIT(MN:=_variant_in_, IN:=_variant_in_, MX:=_variant_in_, OUT:=_variant_out_);	The Limit instruction tests if the value of parameter IN is inside the value range specified by parameters MIN and MAX and if not, clamps the value at MIN or MAX.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-63 Data types for the parameters

Parameter	Data type[1]	Description
MN, IN, and MX	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Time, Date, TOD· Constant	Math operation inputs
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Time, Date, TOD	Math operation output

[1] The MN, IN, MX, and OUT parameters must be the same data type.

If the value of parameter IN is within the specified range, then the value of IN is stored in parameter OUT. If the value of parameter IN is outside of the specified range, then the OUT value is the value of parameter MIN (if the IN value is less than the MIN value) or the value of parameter MAX (if the IN value is greater than the MAX value).

Table 9-64 ENO status

ENO	Description
1	No error
0	Real: If one or more of the values for MIN, IN and MAX is NaN (Not a Number), then NaN is returned.
0	If MIN is greater than MAX, the value IN is assigned to OUT.

SCL examples:

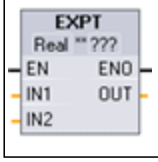
- MyVal := LIMIT(MN:=10,IN:=53, MX:=40); //Result: MyVal = 40
- MyVal := LIMIT(MN:=10,IN:=37, MX:=40); //Result: MyVal = 37
- MyVal := LIMIT(MN:=10,IN:=8, MX:=40); //Result: MyVal = 10

9.5.9 Exponent, logarithm, and trigonometry instructions

You use the floating point instructions to program mathematical operations using a Real or LReal data type:

- SQR: Form square ($IN^2 = OUT$)
- SQRT: Form square root ($\sqrt{IN} = OUT$)
- LN: Form natural logarithm (LN(IN) = OUT)
- EXP: Form exponential value ($e^{IN} = OUT$), where base e = 2.71828182845904523536
- EXPT: exponentiate ($IN1^{IN2} = OUT$)
  EXPT parameters IN1 and OUT are always the same data type, for which you must select Real or LReal. You can select the data type for the exponent parameter IN2 from among many data types.
- FRAC: Return fraction (fractional part of floating point number IN = OUT)
- SIN: Form sine value (sin(IN radians) = OUT)
- ASIN: Form arcsine value (arcsine(IN) = OUT radians), where the sin(OUT radians) = IN
- COS: Form cosine (cos(IN radians) = OUT)
- ACOS: Form arccosine value (arccos(IN) = OUT radians), where the cos(OUT radians) = IN
- TAN: Form tangent value (tan(IN radians) = OUT)
- ATAN: Form arctangent value (arctan(IN) = OUT radians), where the tan(OUT radians) = IN

Table 9-65 Examples of floating-point math instructions

LAD / FBD	SCL	Description
	out := SQR(in); or **out := in * in;**	Square: $IN^2 = OUT$ For example: If IN = 9, then OUT = 81.
	**out := in1 ** in2;**	General exponential: $IN1^{IN2} = OUT$ For example: If IN1 = 3 and IN2 = 2, then OUT = 9.

[1] For LAD and FBD: Click the "???" (by the instruction name) and select a data type from the drop-down menu.

[2] For SCL: You can also use the basic SCL math operators to create the mathematical expressions.

Table 9-66 Data types for parameters

Parameter	Data type	Description
IN, IN1	Real, LReal, Constant	Inputs
IN2	SInt, Int, DInt, USInt, UInt,UDInt, Real, LReal, Constant	EXPT exponent input
OUT	Real, LReal	Outputs

Table 9-67 ENO status

ENO	Instruction	Condition	Result (OUT)
1	All	No error	Valid result
0	SQR	Result exceeds valid Real/LReal range	+INF
		IN is +/- NaN (not a number)	+NaN
	SQRT	IN is negative	-NaN
		IN is +/- INF (infinity) or +/- NaN	+/- INF or +/- NaN
	LN	IN is 0.0, negative, -INF, or -NaN	-NaN
		IN is +INF or +NaN	+INF or +NaN
	EXP	Result exceeds valid Real/LReal range	+INF
		IN is +/- NaN	+/- NaN
	SIN, COS, TAN	IN is +/- INF or +/- NaN	+/- INF or +/- NaN
	ASIN, ACOS	IN is outside valid range of -1.0 to +1.0	+NaN
		IN is +/- NaN	+/- NaN
	ATAN	IN is +/- NaN	+/- NaN
	FRAC	IN is +/- INF or +/- NaN	+NaN
	EXPT	IN1 is +INF and IN2 is not -INF	+INF
		IN1 is negative or -INF	+NaN if IN2 is Real/LReal, -INF otherwise
		IN1 or IN2 is +/- NaN	+NaN
		IN1 is 0.0 and IN2 is Real/LReal (only)	+NaN

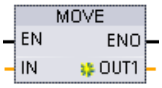
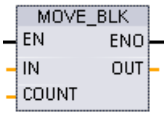
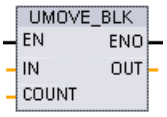
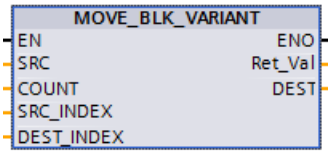
9.6 Move operations

9.6.1 MOVE (Move value), MOVE_BLK (Move block), UMOVE_BLK (Move block uninterruptible), and MOVE_BLK_VARIANT (Move block)

Use the Move instructions to copy data elements to a new memory address and convert from one data type to another. The source data is not changed by the move process.

- The MOVE instruction copies a single data element from the source address specified by the IN parameter to the destination addresses specified by the OUT parameter.
- The MOVE_BLK and UMOVE_BLK instructions have an additional COUNT parameter. The COUNT specifies how many data elements are copied. The number of bytes per element copied depends on the data type assigned to the IN and OUT parameter tag names in the PLC tag table.

Table 9-68 MOVE, MOVE_BLK, UMOVE_BLK, and MOVE_BLK_VARIANT instructions

LAD / FBD	SCL	Description
	**out1 := in;**	Copies a data element stored at a specified address to a new address or multiple addresses.[1]
	**MOVE_BLK(in:=_variant_in, count:=_uint_in, out=>_variant_out);**	Interruptible move that copies a block of data elements to a new address.
	**UMOVE_BLK(in:=_variant_in, count:=_uint_in, out=>_variant_out);**	Uninterruptible move that copies a block of data elements to a new address.
	**MOVE_BLK_VARIANT(SRC:=_variant_in, COUNT:=_udint_in, SRC_INDEX:=_dint_in, DESTINDEX:=_dint_in, DEST=>_variant_out);**	Moves the contents of a source memory area to a destination memory area. You can copy a complete array or elements of an array to another array of the same data type. The size (number of elements) of source and destination array may be different. You can copy multiple or single elements within an array. You use Variant data types to point to both the source and destination arrays.

[1] MOVE instruction: To add another output in LAD or FBD, click the "Create" icon by the output parameter. For SCL, use multiple assignment statements. You might also use one of the loop constructions.

Table 9-69 Data types for the MOVE instruction

Parameter	Data type	Description
IN	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Char, WChar, Array, Struct, DTL, Time, Date, TOD, IEC data types, PLC data types	Source address
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Char, WChar, Array, Struct, DTL, Time, Date, TOD, IEC data types, PLC data types	Destination address

To add MOVE outputs, click the "Create" icon or right-click on an output stub for one of the existing OUT parameters and select the "Insert output" command.

To remove an output, right-click on an output stub for one of the existing OUT parameters (when there are more than the original two outputs) and select the "Delete" command.

Table 9-70 Data types for the MOVE_BLK and UMOVE_BLK instructions

Parameter	Data type	Description
IN	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal Byte, Word, DWord, Time, Date, TOD, WChar	Source start address
COUNT	UInt	Number of data elements to copy
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, WChar	Destination start address

Table 9-71 Data types for the MOVE_BLK_VARIANT instruction

Parameter	Data type	Description
SRC	Variant (which points to an array or individual array element)	Source block from which to copy
COUNT	UDInt	Number of data elements to copy
SRC_INDEX	DInt	Zero-based index into the SRC array
DEST_INDEX	DInt	Zero-based index into the DEST array
RET_VAL	Int	Error information
DEST	Variant (which points to an array or individual array element)	Destination area into which to copy the contents of the source block

NOTE

Rules for data copy operations

- To copy the Bool data type, use SET_BF, RESET_BF, R, S, or output coil (LAD) (Page 200)
- To copy a single elementary data type, use MOVE
- To copy an array of an elementary data type, use MOVE_BLK or UMOVE_BLK
- To copy a structure, use MOVE
- To copy a string, use S_MOVE (Page 301)
- To copy a single character in a string, use MOVE
- The MOVE_BLK and UMOVE_BLK instructions cannot be used to copy arrays or structures to the I, Q, or M memory areas.

MOVE_BLK and UMOVE_BLK instructions differ in how interrupts are handled:

- Interrupt events are **queued and processed** during MOVE_BLK execution. Use the MOVE_BLK instruction when the data at the move destination address is not used within an interrupt OB subprogram or, if used, the destination data does not have to be consistent. If a MOVE_BLK operation is interrupted, then the last data element moved is complete and consistent at the destination address. The MOVE_BLK operation is resumed after the interrupt OB execution is complete.
- Interrupt events are **queued but not processed** until UMOVE_BLK execution is complete. Use the UMOVE_BLK instruction when the move operation must be completed and the destination data consistent, before the execution of an interrupt OB subprogram. For more information, see the section on data consistency (Page 178).

ENO is always true following execution of the MOVE instruction.

Table 9-72 ENO status

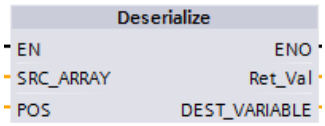
ENO	Condition	Result
1	No error	All COUNT elements were successfully copied.
0	Either the source (IN) range or the destination (OUT) range exceeds the available memory area.	Elements that fit are copied. No partial elements are copied.

Table 9-73 Condition codes for the MOVE_BLK_VARIANT instruction

RET_VAL (W#16#...)	Description
0000	No error
80B4	Data types do not correspond.
8151	Access to the SRC parameter is not possible.
8152	The operand at the SRC parameter is an invalid type.
8153	Code generation error at the SRC parameter
8154	The operand at the SRC parameter has the data type Bool.
8281	The COUNT parameter has an invalid value.
8382	The value at the SRC_INDEX parameter is outside the limits of the Variant.
8383	The value at parameter SRC_INDEX is outside the high limit of the array.
8482	The value at the DEST_INDEX parameter is outside the limits of the Variant.
8483	The value at parameter DEST_INDEX is outside the high limit of the array.
8534	The DEST parameter is write-protected.
8551	Access to the DEST parameter is not possible.
8552	The operand at the DEST parameter is an invalid type.
8553	Code generation error at the DEST parameter
8554	The operand at the DEST parameter has the data type Bool.
*You can display error codes in the program editor as integer or hexadecimal values.	

9.6.2 Deserialize

Table 9-74 DESERIALIZE instruction

LAD / FBD	SCL	Description
	**ret_val := Deserialize(SRC_ARRAY:=_variant_in_, DEST_VARIABLE=>_variant_out_, POS:=_dint_inout_);**	You can use the "Deserialize" instruction to convert the sequential representation of a PLC data type (UDT) back to a PLC data type and to fill its entire contents. If the comparison is TRUE, then the box output is TRUE.

The memory area which holds the sequential representation of a PLC data type must have the Array of Byte data type and you must declare the data block to have standard (not optimized) access. Make sure that there is enough memory space prior to the conversion.

The instruction enables you to convert multiple sequential representations of converted PLC data types back to their original data types.

NOTE

If you only want to convert back a single sequential representation of a PLC data type (UDT), you can also use the instruction "TRCV: Receive data via communication connection".

Table 9-75 Parameters for the DESERIALIZE instruction

Parameter	Type	Data type	Description
SRC_ARRAY	IN	Variant	Global data block that contains the data stream
DEST_VARIABLE	INOUT	Variant	Tag in which to store the converted PLC data type (UDT)
POS	INOUT	DInt	Number of bytes that the converted PLC data type uses
RET_VAL	OUT	Int	Error information

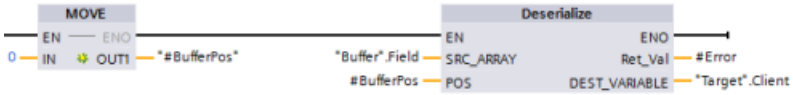
Table 9-76 RET_VAL parameter

RET_VAL* (W#16#...)	Description
0000	No error
80B0	The memory areas for the SRC_ARRAY and DEST_VARIABLE parameters overlap.
8136	The data block at the DEST_VARIABLE parameter is not a block with standard access.
8150	The Variant data type at the SRC_ARRAY parameter contains no value.
8151	Code generation error at the SRC_ARRAY parameter.
8153	There is not enough free memory available at the SRC_ARRAY parameter.
8250	The Variant data type at the DEST_VARIABLE parameter contains no value.
8251	Code generation error at the DEST_VARIABLE parameter.
8254	Invalid data type at the DEST_VARIABLE parameter.
8382	The value at parameter POS is outside the limits of the array.
*You can view the error codes as either integer or hexadecimal in the program editor.	

Example: Deserialize instruction

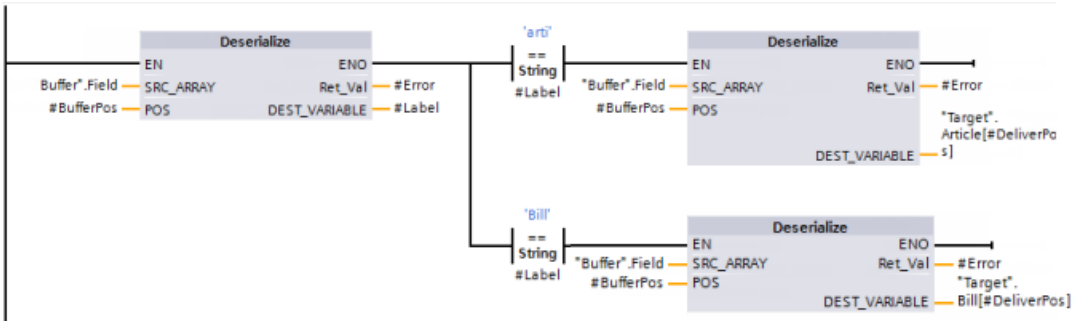
The following example shows how the instruction works:

Network 1:



The "MOVE" instruction moves the value "0" to the "#BufferPos" data block tag. The Deserialize instruction then deserializes the sequential representation of the customer data from the "Buffer" data block and writes it to the "Target" data block. The Deserialize instruction calculates the number of bytes that the converted data uses and stores it in the "#BufferPos" data block tag.

Network 2:



The "Deserialize" instruction deserializes the sequential representation of the data stream pointed to by "Buffer" and writes the characters to the "#Label" operand. The logic compares the characters using the comparison instructions "arti" and "Bill". If the comparison for "arti" = TRUE, the data is article data that is to be deserialized and written to the "Article" data structure of the "Target" data block. If the comparison for "Bill" = TRUE, the data is billing data that is to be deserialized and written to the "Bill" data structure of the "Target" data block.

Function block (or Function) interface:

Name	Data type
Input	
DeliverPos	Int
Output	
InOut	
Static	
Temp	
BufferPos	DInt
Error	Int
Label	String[4]

Custom PLC data types:

The structure of the two PLC data types (UDTs) for this example are as follows:

Article

	Name	Data type
1	Number	DInt
2	Declaration	String
3	Colli	Int

Client

	Name	Data type
1	Title	Int
2	Firstname	String[10]
3	Surname	String[10]

Data blocks:

The two data blocks for this example are as follows:

Target

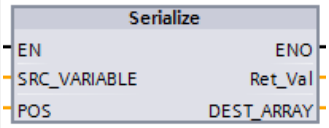
	Name	Data type
1	Static	
2	Client	"Client"
3	Article	Array[0..10] of "Article"
4	Bill	Array[0..10] of Int

Buffer

	Name	Data type
1	Static	
2	Field	Array[0..294] of Byte

9.6.3 Serialize

Table 9-77 SERIALIZE instruction

LAD / FBD	SCL	Description
	**ret_val := Serialize(SRC_VARIABLE=>_variant_in_, DEST_ARRAY:=_variant_out_, POS:=_dint_inout_);**	Use the "Serialize" instruction to convert several PLC data types (UDTs) to a sequential representation without any loss of structure.

You can use the instruction to temporarily save multiple structured data items from your program to a buffer, for example to a global data block, and send them to another CPU. The memory area in which the converted PLC data types are stored must have the ARRAY of BYTE data type and be declared with standard access. Make sure that there is enough memory space prior to the conversion.

The POS parameter contains information about the number of bytes that the converted PLC data types use.

NOTE

If you only want to send a single PLC data type (UDT), you can use the instruction "TSEND: Send data via communication connection".

Table 9-78 Parameters for the SERIALIZE instruction

Parameter	Type	Data type	Description
SRC_VARIABLE	IN	Variant	PLC data type (UDT) that is to be converted to a serial representation
DEST_ARRAY	INOUT	Variant	Data block in which the generated data stream is to be stored
POS	INOUT	DInt	Number of bytes that the converted PLC data types use. The calculated POS parameter is zero-based.
RET_VAL	OUT	Int	Error information

Table 9-79 RET_VAL parameter

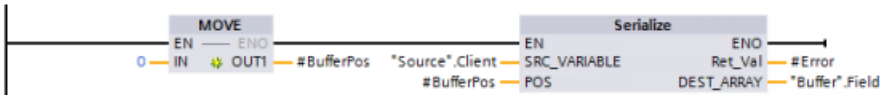
RET_VAL* (W#16#...)	Description
0000	No error
80B0	The memory areas for the SRC_VARIABLE and DEST_ARRAY parameters overlap.
8150	The Variant data type at the SRC_VARIABLE parameter contains no value.
8152	Code generation error at the SRC_VARIABLE parameter.
8236	The data block at the DEST_ARRAY parameter is not a block with standard access.
8250	The Variant data type at the DEST_ARRAY parameter contains no value.
8252	Code generation error at the DEST_ARRAY parameter.
8253	There is not enough free memory available at the DEST_ARRAY parameter.

RET_VAL* (W#16#...)	Description
8254	Invalid data type at the DEST_VARIABLE parameter.
8382	The value at parameter POS is outside the limits of the array.
*You can view the error codes as either integer or hexadecimal in the program editor.	

Example: Serialize instruction

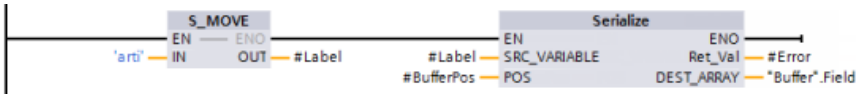
The following example shows how the instruction works:

Network 1:



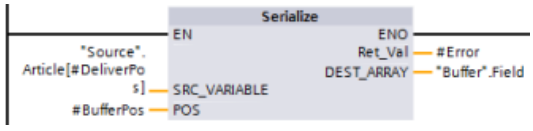
The "MOVE" instruction moves the value "0" to the "#BufferPos" parameter. The "Serialize" instruction serializes the customer data from the "Source" data block and writes it in sequential representation to the "Buffer" data block. The instruction stores the number of bytes used by the sequential representation in the "#BufferPos" parameter.

Network 2:



The logic now inserts some separator text to make it easier to deserialize the sequential representation later. The "S_MOVE" instruction moves the text string "arti" to the "#Label" parameter. The "Serialize" instruction writes these characters after the source client data to the "Buffer" data block. The instruction adds the number of bytes in the text string "arti" to the number already stored in the "#BufferPos" parameter.

Network 3:



The "Serialize" instruction serializes the data of a specific article, which is calculated in runtime, from the "Source" data block and writes it in sequential representation to the "Buffer" data block after the "arti" characters

Block Interface:

Name	Data type
Input	
DeliverPos	Int
Output	
InOut	
Static	
Temp	
BufferPos	DInt
Error	Int
Label	String[4]

Custom PLC data types:

The structure of the two PLC data types (UDTs) for this example are as follows:

Article

		Name	Data type
1		Number	DInt
2		Declaration	String
3		Colli	Int

Client

		Name	Data type
1		Title	Int
2		Firstname	String[10]
3		Surname	String[10]

Data blocks:

The two data blocks for this example are as follows:

Source

		Name	Data type
1		Static	
2		Client	"Client"
3		Article	Array[0..10] of "Article"

Buffer

		Name	Data type
1		Static	
2		Field	Array[0..294] of Byte

9.6.4 FILL_BLK (Fill block) and UFILL_BLK (Fill block uninterruptible)

Table 9-80 FILL_BLK and UFILL_BLK instructions

LAD / FBD	SCL	Description
FILL_BLK EN ENO IN OUT COUNT	**FILL_BLK(** **in:=_variant_in,** **count:=int,** **out=>_variant_out);**	Interruptible fill instruction: Fills an address range with copies of a specified data element
UFILL_BLK EN ENO IN OUT COUNT	**UFILL_BLK(** **in:=_variant_in,** **count:=int,** **out=>_variant_out);**	Uninterruptible fill instruction: Fills an address range with copies of a specified data element

Table 9-81 Data types for parameters

Parameter	Data type	Description
IN	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, Char, WChar	Data source address
COUNT	UDint, USInt, UInt	Number of data elements to copy
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, Char, WChar	Data destination address

NOTE

Rules for data fill operations

- To fill with the BOOL data type, use SET_BF, RESET_BF, R, S, or output coil (LAD)
- To fill with a single elementary data type, use MOVE
- To fill an array with an elementary data type, use FILL_BLK or UFILL_BLK
- To fill a single character in a string, use MOVE
- The FILL_BLK and UFILL_BLK instructions cannot be used to fill arrays in the I, Q, or M memory areas.

The FILL_BLK and UFILL_BLK instructions copy the source data element IN to the destination where the initial address is specified by the parameter OUT. The copy process repeats and a block of adjacent addresses is filled until the number of copies is equal to the COUNT parameter.

FILL_BLK and UFILL_BLK instructions differ in how interrupts are handled:

- Interrupt events are **queued and processed** during FILL_BLK execution. Use the FILL_BLK instruction when the data at the move destination address is not used within an interrupt OB subprogram or, if used, the destination data does not have to be consistent.
- Interrupt events are **queued but not processed** until UFILL_BLK execution is complete. Use the UFILL_BLK instruction when the move operation must be completed and the destination data consistent, before the execution of an interrupt OB subprogram.

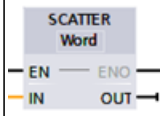
Table 9-82 ENO status

ENO	Condition	Result
1	No error	The IN element was successfully copied to all COUNT destinations.
0	The destination (OUT) range exceeds the available memory area	Elements that fit are copied. No partial elements are copied.

9.6.5 SCATTER

SCATTER: Parse the bit sequence into individual bits

Table 9-83 SCATTER

LAD/FBD	SCL	Description
	**SCATTER** **(IN := #SourceWord,** **OUT => #DestinationArray};**	SCATTER: The "Parse the bit sequence into individual bits" instruction parses a tag of the Byte, Word, or DWord data type into individual bits and saves them in an Array of Bool, a Struct or a PLC data type exclusively with Boolean elements. You can, for example, parse a status Word, and read and change the status of the individual bits using the index. Using GATHER, you can merge the bits once again into a bit sequence.

Data types for the SCATTER instruction

The following table shows the parameters of the instruction:

Parameter	Declaration	Data type	Memory area	Description
EN	Input	Bool	I, Q, M, D, L or constant	Enable input
ENO	Output	Bool	I, Q, M, D, L	Enable output The enable output ENO returns signal state "0" if one of the following conditions applies: • Enable input EN has signal state "0". • The Array, Struct or PLC data type does not provide enough Bool elements.
IN	Input	Byte, Word, DWord	I, Q, M, D, L	Bit sequence that is parsed. The values must not be located in the I/O area or in the DB of a technology object.
OUT	Output	Array[*] of Bool, Struct or PLC data type *: 8, 16, 32 or 64 elements	I, Q, M, D, L	Array, Struct or PLC data type in which the individual bits are stored.

NOTE

Multi-dimensional Array of Bool

With the "Parse the bit sequence into individual bits" instruction, the use of a multidimensional Array of Bool is not permitted.

NOTE

Length of the Array, Struct or PLC data type

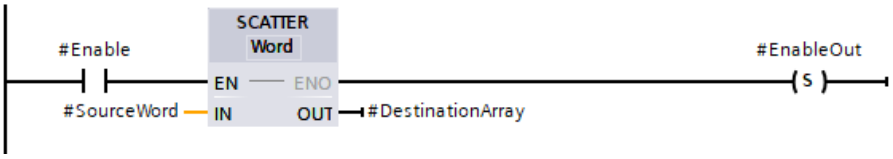
The Array, the Struct or the PLC data type must have the exact number of elements specified by the bit sequence. This means for the data type Byte, for example, the Array, Struct or the PLC data type must have exactly 8 elements (Word = 16, and DWord = 32).

Example: SCATTER instruction with an Array

Create the following tags in the block interface:

Tag	Section	Data type
Enable	Input	Bool
SourceWord		Word
EnableOut	Output	Bool
DestinationArray		Array[0..15] of Bool

The following example shows how the instruction works:



The following table shows how the instruction works using specific operand values:

Parameter	Operand	Data type
IN	SourceWord	Word (16 bits)
OUT	DestinationUDT	The "DestinationUDT" operand has the PLC data type (UDT). It consists of 16 elements and is therefore just as large as the Word that is to be parsed.

If the operand #Enable returns the signal state "1" at the enable input EN, the instruction is executed. The #SourceWord operand of the data type Word is parsed into its individual bits (16) and assigned to the individual elements of the #DestinationArray operand. If an error occurs during the execution of the instruction, the operand #EnableOut returns the signal state "0" at the enable output ENO.

Example: SCATTER instruction with a PLC data type (UDT)

Create the following PLC data type "myBits":

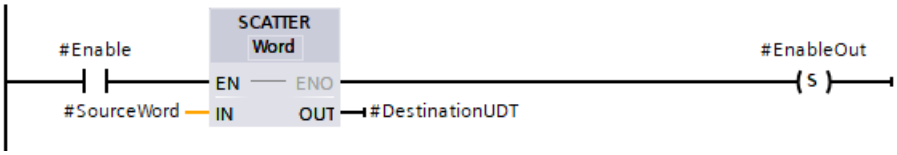
myBits

	Name	Data type
1	GeneralError	Bool
2	DeviceError	Bool
3	CommError	Bool
4	myError1	Bool
5	myError2	Bool
6	myError3	Bool
7	myError4	Bool
8	myError5	Bool
9	myError6	Bool
10	myError7	Bool
11	myError8	Bool
12	myError9	Bool
13	myError10	Bool
14	myError11	Bool
15	myError12	Bool
16	myError13	Bool

Create the following tags in the block interface:

Tag	Section	Data type
Enable	Input	Bool
SourceWord		Word
EnableOut	Output	Bool
DestinationUDT		"myBits"

The following example shows how the instruction works:



The following table shows how the instruction works using specific operand values:

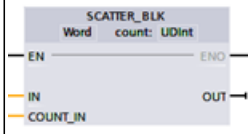
Parameter	Operand	Data type
IN	SourceWord	Word (16 bits)
OUT	DestinationUDT	The "DestinationUDT" operand has the PLC data type (UDT). It consists of 16 elements and is therefore just as large as the Word that is to be parsed.

If the operand #Enable returns the signal state "1" at the enable input EN., the instruction is executed. The #SourceWord operand of the data type Word is parsed into its individual bits (16) and assigned to the individual elements of the #DestinationArray operand. If an error occurs during the execution of the instruction, the operand #EnableOut returns the signal state "0" at the enable output ENO.

9.6.6 SCATTER_BLK

SCATTER_BLK: Parse elements of an ARRAY of <bit sequence> into individual bits

Table 9-84 SCATTER_BLK

LAD/FBD	SCL	Description
	**SCATTER_BLK (IN:=_byte_in_, COUNT_IN:=_uint_in_, OUT=>_bool_out_);_IN:=_uint_in_,**	The "Parse elements of an ARRAY of <bit sequence> into individual bits" instruction parses one or more elements of an array and saves them into a Struct, PLC data type, or Array of Boolean elements. You can, for example, parse status words, and read and change the status of the individual bits using the index. Using GATHER, you can merge the bits once again into a bit sequence.

Data types for the SCATTER_BLK instruction

The following table shows the parameters of the instruction:

Parameter	Declaration	Data type	Memory area	Description
EN	Input	Bool	I, Q, M, D, L or constant	Enable input
ENO	Output	Bool	I, Q, M, D, L	Enable output. If ENO is FALSE, no data is written to the output. The enable output ENO returns signal state "0" if one of the following conditions applies: • Enable input EN has signal state "0". • The source array has fewer elements than specified at the COUNT_IN parameter. • The index of the destination array does not start at a Byte, Word, or DWord limit. In this case, no result is written to the Array of Bool. • The Array of Bool, Struct or PLC data type does not provide the required number of elements.
IN	Input	Element of one of the following: • Array [*] of Byte • Array [*] of Word • Array [*] of DWord • Array [*] of LWord	I, Q, M, D, L	The values must not be located in the I/O area or in the DB of a technology object. You provide the data type (Page 95) of the input array (IN parameter) below and left of the instruction name. The source array at the IN parameter can have more elements than the COUNT_IN parameter specifies.
COUNT_IN	Input	USInt, UInt, UDInt	I, Q, M, D, L	Counter for the number of elements of the source array that are going to be parsed into the OUT parameter. You provide the data type of the COUNT_IN parameter after "count:" under the instruction name. The COUNT_IN value must not be in the I/O area or in the database of a technology object.
OUT	Output	Element of one of the following: • Array [*] of Bool • Array [*] of Struct • Array [*] of <PLC data type>	I, Q, M, D, L	Array, Struct or PLC data type in which the individual bits are stored

NOTE
Multi-dimensional Array of Bool
If the array is a multi-dimensional Array of Bool, all bits in the dimensions are counted.
Example 1: An Array[1..10,0..4,1..2] of Bool has 10x5x2 bits that can be parsed for a total of 100 bits.
Example 2: An Array[0..399] of Bool has 400 bits that can be parsed.

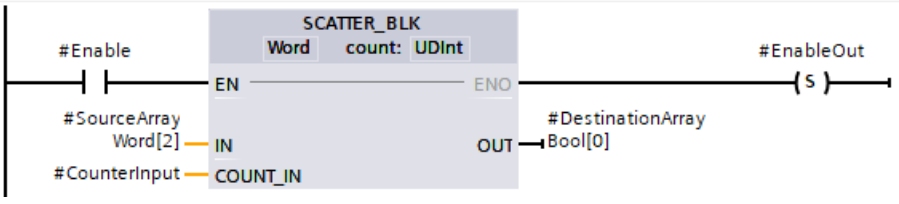
NOTE
If the Array low limit of the target array is not "0", note the following:
For performance reasons the index must always start at a Byte, Word, or DWord boundary limit. This means the array index must be calculated starting at the low limit of the array.

Example: A destination array with the low limit "0"

Create the following tags in the block interface:

Tag	Section	Data type
Enable	Input	Bool
SourceArrayWord		Array[0..5] of Word
CounterInput		UDInt
EnableOut	Output	Bool
DestinationArrayBool		Array[0..95] of Bool

The following example shows how the instruction works:



The following table shows how the instruction works using specific operand values:

Parameter	Operand	Data type
IN	SourceArrayWord[2]	Array[0..5] of Word (96 bits can be parsed.)
COUNT_IN	CounterInput = 3	A CounterInput value of 3 means that 3 Words or 48 bits are to be parsed. This means at least 48 bits must be available in the destination array.
OUT	DestinationArrayBool[0]	The operand "DestinationArrayBool" is of the data type Array[0..95] of Bool. This means it provides 96 Bool elements. The OUT parameter must have sufficient elements to save the bits of the parsed bit sequences; however, the destination memory area may also be larger.

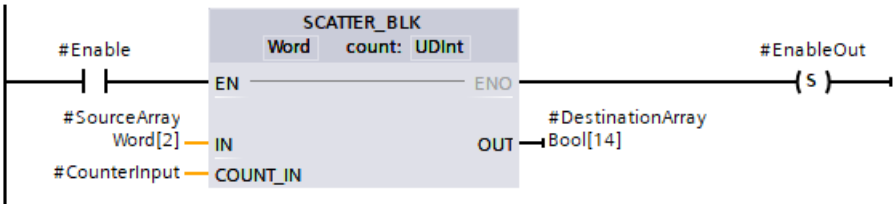
If the operand #Enable returns the signal state "1" at the enable input EN, the instruction is executed. The 3rd, 4th and 5th Word of the #SourceArrayWord operand is parsed into its individual bits (48) and as of the 1st element assigned to the individual elements of the #DestinationArrayBool operand. If an error occurs during the execution of the instruction, the operand #EnableOut returns the signal state "0" at the enable output ENO.

Example: A destination array with a low limit "-2"

This example repeats the previous example, but sets the lower limit of the destination array to a negative and outputs into #DestinationArrayBool[14].
The block interface is the same as in the previous example, except for the DestinationArrayBool dimensions.

Tag	Section	Data type
DestinationArrayBool	Output	Array[-2..93] of Bool

The following example shows how the instruction works:



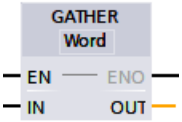
The parameter table is the same as in the previous example, except for the OUT parameter.

Parameter	Operand	Data type
OUT	DestinationArrayBool[14]	The operand "DestinationArrayBool" is of the data type Array[-2..93] of Bool. This means it provides 96 BOOL elements. Since the lower limit of DestinationArrayBool is -2, then DestinationArrayBool[14] is the 16th element of the array.

9.6.7 GATHER

GATHER: Merge individual bits into a bit sequence

Table 9-85 GATHER

LAD/FBD	SCL	Description
	**GATHER** **(IN := #SourceArray,** **OUT => #DestinationArray};**	GATHER: The "Merge individual bits into a bit sequence" instruction merges the bits from an Array of Bool, a Struct or a PLC data type exclusively with Boolean elements into a bit sequence. The bit sequence is saved in a tag of the data type Byte, Word, or DWord.

Data types for the GATHER instruction

The following table shows the parameters of the instruction:

Parameter	Declaration	Data type	Memory area	Description
EN	Input	Bool	I, Q, M, D, L or constant	Enable input
ENO	Output	Bool	I, Q, M, D, L	Enable output The enable output ENO returns signal state "0" if one of the following conditions applies: • Enable input EN has signal state "0". • The Array, Struct or the PLC data type (UDT) has fewer or more Bool elements than specified by the bit sequence. In this case the Bool elements are not transferred. • Fewer than the necessary number of bits are available.
IN	Input	Array[*] of Bool, Struct or PLC data type *: 8, 16, 32 or 64 elements	I, Q, M, D, L	Array, Struct or PLC data type, the bits of which are merged into a bit sequence. The values must not be located in the I/O area or in the DB of a technology object.
OUT	Output	Byte, Word, DWord	I, Q, M, D, L	Merged bit sequence, saved in a tag

NOTE

Multi-dimensional Array of Bool

With the "Merge individual bits into a bit sequence" instruction, the use of a multidimensional Array of Bool is not permitted.

NOTE

Length of the Array, Struct or PLC data type

The Array, Struct or the PLC data type must have exactly the number of elements that is specified by the bit sequence.

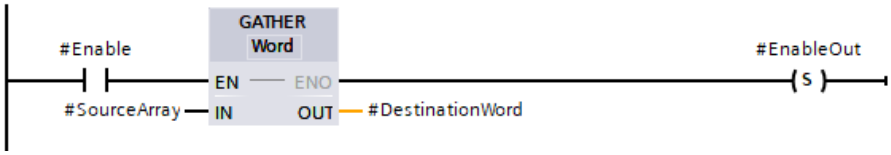
This means for the data type Byte, for example, the Array, Struct or the PLC data type must have exactly 8 elements (Word = 16, and DWord = 32).

Example: GATHER instruction with an Array

Create the following tags in the block interface:

Tag	Section	Data type
Enable	Input	Bool
SourceArray		Array[0..15] of Bool
EnableOut	Output	Bool
DestinationWord		Word

The following example shows how the instruction works:



The following table shows how the instruction works using specific operand values:

Parameter	Operand	Data type
IN	SourceArray	The operand "SourceArray" is of the data type Array[0..15] of Bool. It consists of 16 elements and is therefore just as large as the Word in which the bits are to be merged.
OUT	DestinationWord	Word (16 bits)

If the operand #Enable returns the signal state "1" at the enable input EN, the instruction is executed. The bits of the #SourceArray operand are merged into a Word. If an error occurs during the execution of the instruction, the operand #EnableOut returns the signal state "0" at the enable output ENO.

Example: GATHER instruction with a PLC data type (UDT)

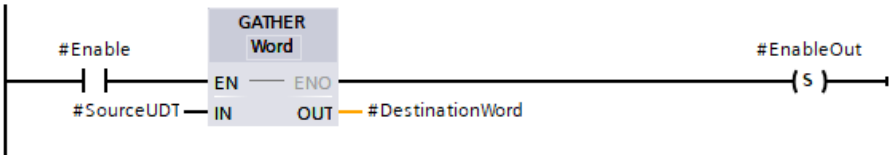
Create the following PLC data type "myBits":

myBits		
	Name	Data type
1	GeneralError	Bool
2	DeviceError	Bool
3	CommError	Bool
4	myError1	Bool
5	myError2	Bool
6	myError3	Bool
7	myError4	Bool
8	myError5	Bool
9	myError6	Bool
10	myError7	Bool
11	myError8	Bool
12	myError9	Bool
13	myError10	Bool
14	myError11	Bool
15	myError12	Bool
16	myError13	Bool

Create the following tags in the block interface:

Tag	Section	Data type
Enable	Input	Bool
SourceUDT		"myBits"
EnableOut	Output	Bool
DestinationWord		Word

The following example shows how the instruction works:



The following table shows how the instruction works using specific operand values:

Parameter	Operand	Data type
IN	SourceUDT	The "SourceUDT" operand has the PLC data type (UDT). It consists of 16 elements and is therefore just as large as the Word in which the bits are to be merged.
OUT	DestinationWord	Word (16 bits)

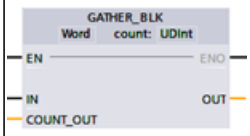
If the operand #Enable returns the signal state "1" at the enable input EN, the instruction is executed. The bits of the #SourceUDT operand are merged into a Word. If an error occurs during the execution of the instruction, the operand #EnableOut returns the signal state "0" at the enable output ENO.

9.6.8 GATHER_BLK

GATHER_BLK: Merge individual bits into multiple elements of an ARRAY of <bit sequence>

Table 9-86 GATHER_BLK

LAD/FBD	SCL	Description

	GATHER_BLK
	(IN := #SourceArrayBool[0],
	COUNT_OUT := #CounterOutput,
	OUT => #DestinationArrayWord[2]);
		The "Merge individual bits into multiple elements of an ARRAY of <bit sequence>" instruction merges the bits from an Array of Bool, a Struct or a PLC data type exclusively with Boolean elements into one or multiple elements of an ARRAY of <bit sequence>.

Data types for the GATHER_BLK instruction

The following table shows the parameters of the instruction:

Parameter	Declaration	Data type	Memory area	Description
EN	Input	Bool	I, Q, M, D, L or constant	Enable input
ENO	Output	Bool	I, Q, M, D, L	Enable output. If ENO is FALSE, no data is written to the output. The enable output ENO returns signal state "0" if one of the following conditions applies: • Enable input EN has signal state "0". • The index of the source Array does not start at a Byte, Word, or DWord limit. In this case, no result is written to the ARRAY of <bit sequence>. • The ARRAY[*] of <bit sequence> does not provide the required number of elements.
IN	Input	Element of one of the following: • Array [*] of Bool • Array [*] of Struct • Array [*] of <PLC data type>	I, Q, M, D, L	Array of Bool, Struct or PLC data type whose bits are merged into the OUT parameter. The values must not be located in the I/O area or in the DB of a technology object. The data type of the input array (IN parameter) is indicated below and left of the instruction name.

Parameter	Declaration	Data type	Memory area	Description
COUNT_OUT	Input	USInt, UInt, UDInt	I, Q, M, D, L	Count how many elements of the target Array are to be described. At the COUNT_OUT parameter, you specify how many elements of the destination Array are going to be written. With this step you also implicitly specify how many elements of the Array of Bool, the Struct or the PLC data type are required. The value must not be in the I/O area or in the database of a technology object. The data type of the COUNT_OUT parameter is indicated below and right of the instruction name.
OUT	Output	Element of one of the following: • Array [*] of Byte • Array [*] of Word • Array [*] of DWord • Array [*] of LWord	I, Q, M, D, L	Array to which the bits are saved. The destination Array at the OUT parameter may have more elements than specified at the COUNT_OUT parameter.

NOTE

Multi-dimensional Array of Bool

If the array is a multi-dimensional Array of Bool, all bits in the dimensions are counted.

Example 1: An Array[1..10,0..4,1..2] of Bool has 10x5x2 bits that can be parsed for a total of 100 bits.

Example 2: An Array[0..399] of Bool has 400 bits that can be parsed.

NOTE

If the Array low limit of the target array is not "0", note the following:

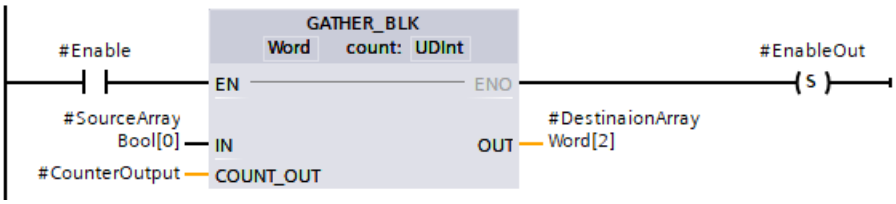
For performance reasons the index must always start at a Byte, Word, or DWord boundary limit. This means the array index must be calculated starting at the low limit of the array.

Example: A source Array with the low limit "0"

Create the following tags in the block interface:

Tag	Section	Data type
Enable	Input	Bool
SourceArrayBool		Array[0..95] of Bool
CounterOutput		UDInt
EnableOut	Output	Bool
DestinationArrayWord		Array[0..5] of Word

The following example shows how the instruction works:



The following table shows how the instruction works using specific operand values:

Parameter	Operand	Data type
IN	SourceArrayBool[0]	The operand "SourceArrayBool" is of the data type Array[0..95] of Bool. This means it provides 96 Bool elements that can merged into words once again.
COUNT_OUT	CounterOutput = 3	A CounterInput value of 3 means that 3 Words or 48 bits are to be parsed. This means at least 48 bits must be available in the destination array.
OUT	DestinationArrayWord[2]	The operand "DestinationArrayWord" is of the data type Array[0..5] of Word. This means 6 Word elements are available. The ARRAY of <bit sequence> must have sufficient elements to save the bits that are going to be merged. However, the destination Array may also be larger.

If the operand #Enable returns the signal state "1" at the enable input EN, the instruction is executed. As of the 1st element of the #SourceArrayBool operand, 48 bits are merged in the #DestinationArrayWord operand. The starting point in the destination Array is the 3rd element. This means that the first 16 bits are written into the 3rd word, the second 16 bits into the 4th word and the third 16 bits into the 5th word of the destination Array. If an error occurs during the execution of the instruction, the operand #EnableOut returns the signal state "0" at the enable output ENO.

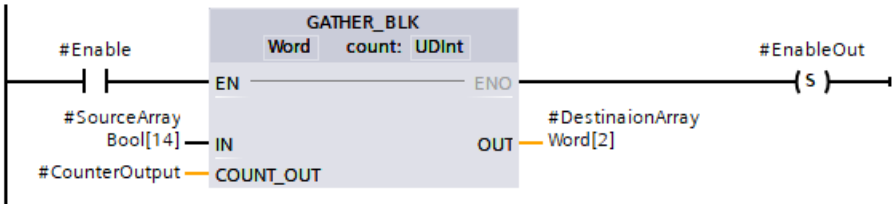
Example: A source Array with the low limit "-2"

This example repeats the previous example, but sets the lower limit of the source array to a negative and outputs into #DestinationArrayWord[2].

The block interface is the same as in the previous example, except for the SourceArrayBool dimensions.

Tag	Section	Data type
SourceArrayBool	Input	Array[-2..93] of Bool

The following example shows how the instruction works:

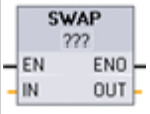


The parameter table is the same as in the previous example, except for the IN parameter.

Parameter	Operand	Data type
IN	SourceArrayBool[14]	The operand "SourceArrayBool" is of the data type Array[-2..93] of Bool. Since the starting point is the 16th element, only 80 Bool elements that can be merged into words again are available.

9.6.9 SWAP (Swap bytes)

Table 9-87 SWAP instruction

LAD / FBD	SCL	Description
	**out := SWAP(in);**	Reverses the byte order for two-byte and four-byte data elements. No change is made to the bit order within each byte. ENO is always TRUE following execution of the SWAP instruction.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-88 Data types for the parameters

Parameter	Data type	Description
IN	Word, DWord	Ordered data bytes IN
OUT	Word, DWord	Reverse ordered data bytes OUT

Example 1	Parameter IN = MB0 (before execution)		Parameter OUT = MB4, (after execution)	
Address	MW0	MB1	MW4	MB5
W#16#1234	12	34	34	12
WORD	MSB	LSB	MSB	LSB

Example 2	Parameter IN = MB0 (before execution)				Parameter OUT = MB4, (after execution)			
Address	MD0	MB1	MB2	MB3	MD4	MB5	MB6	MB7
DW#16#12345678	12	34	56	78	78	56	34	12
DWORD	MSB			LSB	MSB			LSB

9.6.10 Read / Write memory instructions

9.6.10.1 PEEK and POKE (SCL only)

SCL provides PEEK and POKE instructions that allow you to read from or write to data blocks, I/O, or memory. You provide parameters for specific byte offsets or bit offsets for the operation.

NOTE

To use the PEEK and POKE instructions with data blocks, you must use standard (not optimized) data blocks. Also note that the PEEK and POKE instructions merely transfer data. They have no knowledge of data types at the addresses.

`PEEK(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_);`
	Reads the byte referenced by byteOffset of the referenced data block, I/O or memory area.
	Example referencing data block:
	`%MB100 := PEEK(area:=16#84, dbNumber:=1, byteOffset:=#i);`
	Example referencing IB3 input:
	`%MB100 := PEEK(area:=16#81, dbNumber:=0, byteOffset:=#i); // when #i = 3`

`PEEK_WORD(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_);`
	Reads the word referenced by byteOffset of the referenced data block, I/O or memory area.
	Example:
	`%MW200 := PEEK_WORD(area:=16#84, dbNumber:=1, byteOffset:=#i);`

`PEEK_DWORD(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_);`
	Reads the double word referenced by byteOffset of the referenced data block, I/O or memory area.
	Example:
	`%MD300 := PEEK_DWORD(area:=16#84, dbNumber:=1, byteOffset:=#i);`

`PEEK_BOOL(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_,`
`bitOffset:=_in_);`
	Reads a Boolean referenced by the bitOffset and byteOffset of the referenced data block, I/O or memory area
	Example:
	`%MB100.0 := PEEK_BOOL(area:=16#84, dbNumber:=1, byteOffset:=#ii, bitOffset:=#j);`

`POKE(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_,`
`value:=_in_);`
	Writes the value (Byte, Word, or DWord) to the referenced byteOffset of the referenced data block, I/O or memory area
	Example referencing data block:
	`POKE(area:=16#84, dbNumber:=2, byteOffset:=3, value:="Tag_1");`
	Example referencing QB3 output:
	`POKE(area:=16#82, dbNumber:=0, byteOffset:=3, value:="Tag_1");`

`POKE_BOOL(area:=_in_,`
`dbNumber:=_in_,`
`byteOffset:=_in_,`
`bitOffset:=_in_,`
`value:=_in_);`
	Writes the Boolean value to the referenced bitOffset and byteOffset of the referenced data block, I/O or memory area
	Example:
	`POKE_BOOL(area:=16#84, dbNumber:=2, byteOffset:=3, bitOffset:=5, value:=0);`

`POKE_BLK(area_src:=_in_,`
`dbNumber_src:=_in_,`
`byteOffset_src:=_in_,`
`area_dest:=_in_,`
`dbNumber_dest:=_in_,`
`byteOffset_dest:=_in_,`
`count:=_in_);`
	Writes "count" number of bytes starting at the referenced byte Offset of the referenced source data block, I/O or memory area to the referenced byteOffset of the referenced destination data block, I/O or memory area
	Example:
	`POKE_BLK(area_src:=16#84, dbNumber_src:=#src_db, byteOffset_src:=#src_byte, area_dest:=16#84, dbNumber_dest:=#src_db, byteOffset_dest:=#src_byte, count:=10);`

For PEEK and POKE instructions, the following values for the "area", "area_src" and "area_dest" parameters are applicable. For areas other than data blocks, the dbNumber parameter must be 0.

16#81	I
16#82	Q
16#83	M
16#84	DB

9.6.10.2 Read and write big and little Endian instructions (SCL)

The S7-1200 CPU provides SCL instructions for reading and writing data in little endian format and in big endian format. Little endian format means that the byte with the least significant bit is in the lowest memory address. Big endian format means that the byte with the most significant bit is in the lowest memory address.

The four SCL instructions for reading and writing data in little endian and big endian format are as follows:

- READ_LITTLE (Read data in little endian format)
- WRITE_LITTLE (Write data in little endian format)
- READ_BIG (Read data in big endian format)
- WRITE_BIG (Write data in big endian format)

Table 9-89 Read and write big and little endian instructions

LAD / FBD	SCL	Description
Not available	**READ_LITTLE(src_array:=_variant_in_, dest_Variable =>_out_, pos:=_dint_inout)**	Reads data from a memory area and writes it to a single tag in little endian byte format.
Not available	**WRITE_LITTLE(src_variable:=_in_, dest_array =>_variant_inout_, pos:=_dint_inout)**	Writes data from a single tag to a memory area in little endian byte format.
Not available	**READ_BIG(src_array:=_variant_in_, dest_Variable =>_out_, pos:=_dint_inout)**	Reads data from a memory area and writes it to a single tag in big endian byte format.
Not available	**WRITE_BIG(src_variable:=_in_, dest_array =>_variant_inout_, pos:=_dint_inout)**	Writes data from a single tag to a memory area in big endian byte format.

Table 9-90 Parameters for the READ_LITTLE and READ_BIG instructions

Parameter	Data type	Description
src_array	Array of Byte	Memory area from which to read data
dest_Variable	Bit strings, integers, floating-point numbers, timers, date and time, character strings	Destination variable at which to write data
pos	DINT	Zero-based position from which to start reading data from the src_array input.

Table 9-91 Parameters for the WRITE_LITTLE and WRITE_BIG instructions

Parameter	Data type	Description
src_variable	Bit strings, integers, floating-point numbers, TOD, DATA, Char, WChar	Source data from tag
dest_array	Array of Byte	Memory area at which to write data
pos	DINT	Zero-based position at which to start writing data into the dest_array output.

Table 9-92 RET_VAL parameter

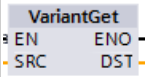
RET_VAL* (W#16#...)	Description
0000	No error
80B4	The SRC_ARRAY or DEST_ARRAY is not an Array of Byte
8382	The value at parameter POS is outside the limits of the array.
8383	The value at parameter POS is within the limits of the Array but the size of the memory area exceeds the high limit of the array.
*You can view the error codes as either integer or hexadecimal in the program editor.	

9.6.11 Variant instructions

9.6.11.1 VariantGet (Read VARIANT tag value)

You can use the "Read out Variant tag value" instruction to read the value of the tag to which the Variant pointer at the SRC parameter points and write it in the tag at the DST parameter.
The SRC parameter has the Variant data type. Any data type except for Variant can be specified at the DST parameter.
The data type of the tag at the DST parameter must match the data type to which the Variant points.

Table 9-93 VariantGet instruction

LAD / FBD	SCL	Description
	**VariantGet(** **SRC:=_variant_in_,** **DST=>_variant_out_);**	Reads the tag pointed to by the SRC parameter and writes it to the tag at the DST parameter

NOTE

To copy structures and arrays, you can use the "MOVE_BLK_VARIANT: Move block" instruction.

Table 9-94 Parameters for the VariantGet instruction

Parameter	Data type	Description
SRC	Variant	Pointer to source data
DST	Bit strings, integers, floating-point numbers, timers, date and time, character strings, ARRAY elements, PLC data types	Destination at which to write data

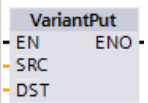
Table 9-95 ENO status

ENO	Condition	Result
1	No error	Instruction copied the tag data pointed to by SRC to the DST tag.
0	Enable input EN has the signal state "0" or the data types do not correspond.	Instruction copied no data.

9.6.11.2 VariantPut (Write VARIANT tag value)

You can use the "Write VARIANT tag value" instruction to write the value of the tag at the SRC parameter to the tag at the DST parameter to which the VARIANT points.
The DST parameter has the VARIANT data type. Any data type except for VARIANT can be specified at the SRC parameter.
The data type of the tag at the SRC parameter must match the data type to which the VARIANT points.

Table 9-96 VariantPut instruction

LAD / FBD	SCL	Description
	**VariantPut(** **SRC:=_variant_in_,** **DST=>_variant_in_);**	Writes the tag referenced by the SRC parameter to the variant pointed to by the DST parameter

NOTE

To copy structures and ARRAYs, you can use the "MOVE_BLK_VARIANT: Move block" instruction.

Table 9-97 Parameters for the VariantPut instruction

Parameter	Data type	Description
SRC	Bit strings, integers, floating-point numbers, timers, date and time, character strings, ARRAY elements, PLC data types	Pointer to source data
DST	Variant	Destination at which to write data

Table 9-98 ENO status

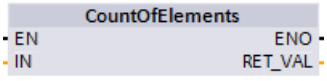
ENO	Condition	Result
1	No error	Instruction copied the SRC tag data to the DST tag.
0	Enable input EN has the signal state "0" or the data types do not correspond.	Instruction copied no data.

9.6.11.3 CountOfElements (Get number of ARRAY elements)

You can use the "Get number of ARRAY elements" instruction to query how many Array elements are in a tag pointed to by a Variant.

If it is a one-dimensional ARRAY, the instruction returns the difference between the high and low limit +1 is output. If it is a multi-dimensional ARRAY, the instruction returns the product of all dimensions.

Table 9-99 CountOfElements instruction

LAD / FBD	SCL	Description
	**Result := CountOfElements(_variant_in_);**	Counts the number of array elements at the array pointed to by the IN parameter.

NOTE

If the Variant points to an Array of Bool, the instruction counts the fill elements to the nearest byte boundary. For example, the instruction returns 8 as the count for an Array[0..1] of Bool.

Table 9-100 Parameters for the CountOfElements instruction

Parameter	Data type	Description
IN	Variant	Tag with array elements to be counted
RET_VAL	UDint	Instruction result

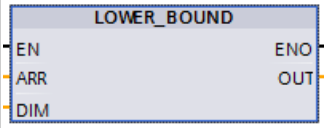
Table 9-101 ENO status

ENO	Condition	Result
1	No error	Instruction returns the number of array elements.
0	Enable input EN has the signal state "0" or the Variant does not point to an array.	Instruction returns 0.

9.6.12 Array instructions

9.6.12.1 LOWER_BOUND: (Read out ARRAY low limit)

Table 9-102 LOWER_BOUND instruction

LAD / FBD	SCL	Description
	**out := LOWER_BOUND(ARR:=_variant_in_, DIM:=_udint_in_);**	You can declare tags with ARRAY[*] in the block interface. For these local tags, you can read out the limits of the ARRAY. You will need to specify the required dimension at the DIM parameter. The LOWER_BOUND (Read out ARRAY low limit). instruction lets you read out the variable low limit of the ARRAY.

Parameters

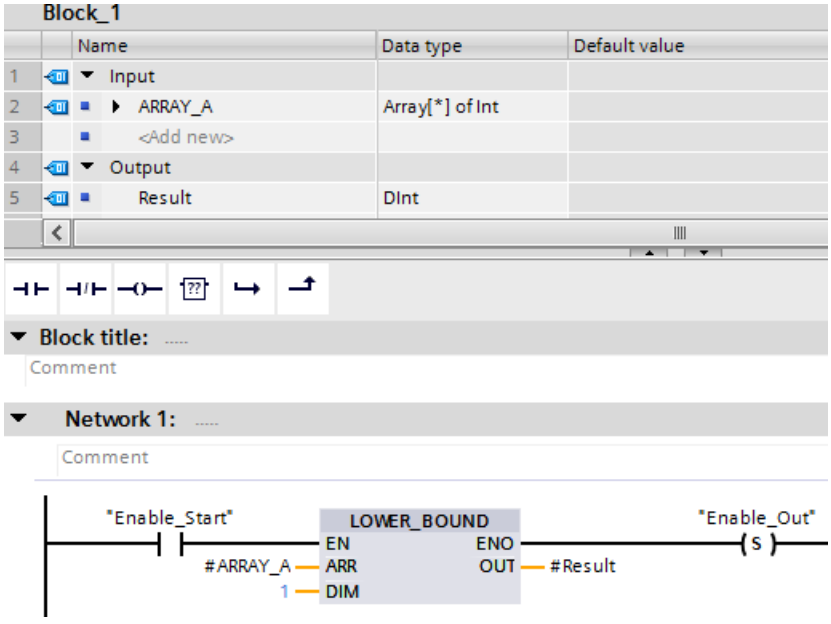
The following table shows the parameters of the instruction "LOWER_BOUND: Read out ARRAY low limit":

Parameters	Declaration	Data type	Memory area	Description
EN	Input	BOOL	I, Q, M, D, L	Enable input
ENO	Output	BOOL	I, Q, M, D, L	Enable output ENO has the signal state "0" if one of the following conditions applies: • The EN enable input has the signal state "0". • The dimension specified at input DIM does not exist.
ARR	Input	ARRAY [*]	FB: Section InOut FC: Sections Input and InOut	ARRAY of which the variable low limit is to be read.
DIM	Input	UDINT	I, Q, M, D, L or constant	Dimension of the ARRAY of which the variable low limit is to be read.
OUT	Output	DINT	I, Q, M, D, L	Result

You can find additional information on valid data types under "Data types (Page 95)":

Example

In the function (FC) block interface, the input parameter ARRAY_A is a one-dimensional array with variable dimensions.



If the "Enable_Start" operand returns signal state "1", the CPU executes the LOWER_BOUND instruction. It reads out the variable low limit of the ARRAY #ARRAY_A from the one-dimensional array. If the instruction executes without errors, it sets operand "Enable_Out" and sets the "Result" operand to the low limit of the array.

9.6.12.2 UPPER_BOUND: (Read out ARRAY high limit)

Table 9-103 LOWER_BOUND instruction

LAD / FBD	SCL	Description
UPPER_BOUND EN ENO ARR OUT DIM	**out := UPPER_BOUND(ARR:=_variant_in_, DIM:=_udint_in_);**	You can declare tags with ARRAY[*] in the block interface. For these local tags, you can read out the limits of the ARRAY. You will need to specify the required dimension at the DIM parameter. The UPPER_BOUND (Read out ARRAY high limit) instruction lets you read out the variable high limit of the ARRAY.

Parameters

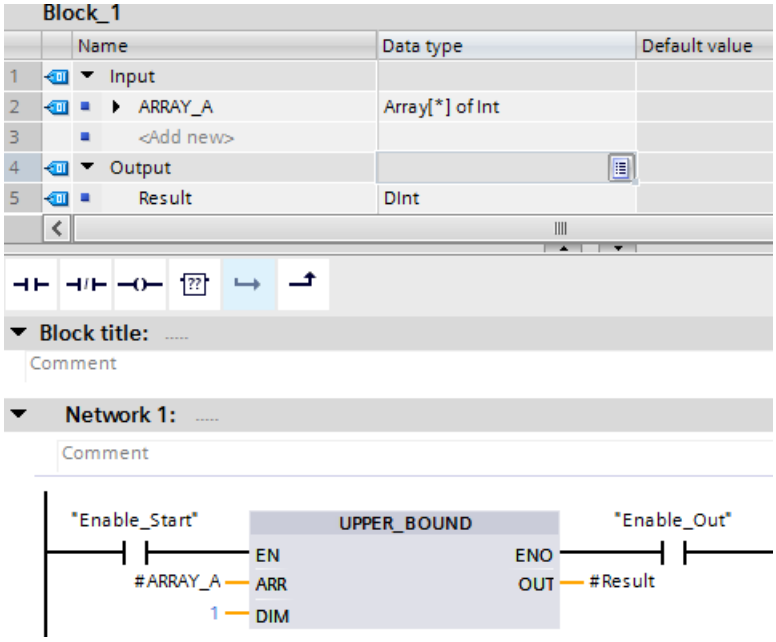
The following table shows the parameters of the instruction "UPPER_BOUND: Read out ARRAY high limit":

Parameters	Declaration	Data type	Memory area	Description
EN	Input	BOOL	I, Q, M, D, L	Enable input
ENO	Output	BOOL	I, Q, M, D, L	Enable output
ARR	Input	ARRAY [*]	FB: Section InOut FC: Sections Input and InOut	ARRAY of which the variable high limit is to be read.
DIM	Input	UDINT	I, Q, M, D, L or constant	Dimension of the ARRAY of which the variable high limit is to be read.
OUT	Output	DINT	I, Q, M, D, L	Result

You can find additional information on valid data types under "Data types (Page 95)":

Example

In the function (FC) block interface, the input parameter ARRAY_A is a one-dimensional array with variable dimensions.

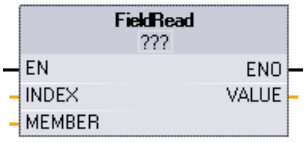


If the "Enable_Start" operand returns signal state "1", the CPU executes the instruction. It reads out the variable high limit of the ARRAY #ARRAY_A from the one-dimensional array. If the instruction executes without errors, it sets operand "Enable_Out" and sets the "Result" operand.

9.6.13 Legacy instructions

9.6.13.1 FieldRead (Read field) and FieldWrite (Write field) instructions

Table 9-104 FieldRead and FieldWrite instructions

LAD / FBD	SCL	Description
	**value := member[index];**	FieldRead reads the array element with the index value INDEX from the array whose first element in specified by the MEMBER parameter. The value of the array element is transferred to the location specified at the VALUE parameter.
	member[index] := value;	WriteField transfers the value at the location specified by the VALUE parameter to the array whose first element is specified by the MEMBER parameter. The value is transferred to the array element whose array index is specified by the INDEX parameter.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-105 Data types for parameters

Parameter and type		Data type	Description
Index	Input	DInt	The index number of the array element to be read or written to
Member [1]	Input	Binary numbers, integers, floating-point numbers, timers, DATE, TOD, CHAR and WCHAR as components of an ARRAY tag	Location of the first element in a one- dimension array defined in a global data block or block interface. For example: If the array index is specified as [-2..4], then the index of the first element is -2 and not 0.
Value [1]	Out	Binary numbers, integers, floating-point numbers, timers, DATE, TOD, CHAR, WCHAR	Location to which the specified array element is copied (FieldRead) Location of the value that is copied to the specified array element (FieldWrite)

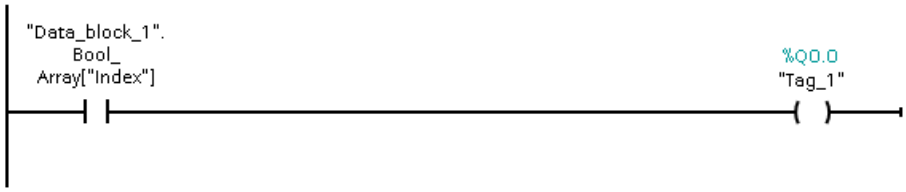
[1] The data type of the array element specified by the MEMBER parameter and the VALUE parameter must have the same data type.

The enable output ENO = 0, if one of the following conditions applies:

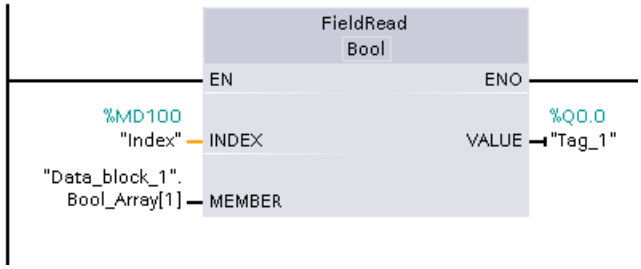
- The EN input has signal state "0"
- The array element specified at the INDEX parameter is not defined in the array referenced at MEMBER parameter
- Errors such as an overflow occur during processing

Example: Accessing data by array indexing

To access elements of an array with a variable, simply use the variable as an array index in your program logic. For example, the network below sets an output based on the Boolean value of an array of Booleans in "Data_block_1" referenced by the PLC tag "Index".



The logic with the variable array index is equivalent to the FieldRead instruction:



FieldWrite and FieldRead instructions can be replaced with variable array indexing logic.

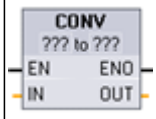
SCL has no FieldRead or FieldWrite instructions, but supports indirect addressing of an array with a variable:

```
#Tag_1 := "Data_block_1".Bool_Array[#Index];
```

9.7 Conversion operations

9.7.1 CONV (Convert value)

Table 9-106 Convert (CONV) instruction

LAD / FBD	SCL	Description
	**out := <data type in>_TO_<data type out>(in);**	Converts a data element from one data type to another data type.

[1] For LAD and FBD: Click the "???" and select the data types from the drop-down menu.

[2] For SCL: Construct the conversion instruction by identifying the data type for the input parameter (in) and output parameter (out). For example, DWORD_TO_REAL converts a DWord value to a Real value.

Table 9-107 Data types for the parameters

Parameter	Data type	Description
IN	Bit string[1], SInt, USInt, Int, UInt, DInt, UDInt, Real, LReal, BCD16, BCD32, Char, WChar	Input value
OUT	Bit string[1], SInt, USInt, Int, UInt, DInt, UDInt, Real, LReal, BCD16, BCD32, Char, WChar	Input value converted to a new data type

[1] The instruction does not allow you to select Bit strings (Byte, Word, DWord). To enter an operand of data type Byte, Word, or DWord for a parameter of the instruction, select an unsigned integer with the same bit length. For example, select USInt for a Byte, UInt for a Word, or UDInt for a DWord.

After you select the (convert from) data type, a list of possible conversions is shown in the (convert to) dropdown list. Conversions from and to BCD16 are restricted to the Int data type. Conversions from and to BCD32 are restricted to the DInt data type.

Table 9-108 ENO status

ENO	Description	Result OUT
1	No error	Valid result
0	IN is +/- INF or +/- NaN	+/- INF or +/- NaN
0	Result exceeds valid range for OUT data type	OUT is set to the IN value

9.7.2 Conversion instructions for SCL

SCL instructions to convert from one data type to another follow this syntax:
out := <data type in>_TO_<data type out>(in);

Conversion instructions for SCL

Table 9-109 Conversion from a Bool, Byte, Word, or DWord

Data type	Instruction	Result
Bool	**BOOL_TO_BYTE, BOOL_TO_WORD, BOOL_TO_DWORD, BOOL_TO_INT, BOOL_TO_DINT**	The value is transferred to the least significant bit of the target data type.
Byte	**BYTE_TO_BOOL**	The least significant bit is transferred into the destination data type.
	BYTE_TO_WORD, BYTE_TO_DWORD	The value is transferred to the least significant byte of the target data type.
	BYTE_TO_SINT, BYTE_TO_USINT	The value is transferred to the target data type.
	BYTE_TO_INT, BYTE_TO_UINT, BYTE_TO_DINT, BYTE_TO_UDINT	The value is transferred to the least significant byte of the target data type.
Word	**WORD_TO_BOOL**	The least significant bit is transferred into the destination data type.
	WORD_TO_BYTE	The least significant byte of the source value is transferred to the target data type
	WORD_TO_DWORD	The value is transferred to the least significant word of the target data type.
	WORD_TO_SINT, WORD_TO_USINT	The least significant byte of the source value is transferred to the target data type.
	WORD_TO_INT, WORD_TO_UINT	The value is transferred to the target data type.

Data type	Instruction	Result
Word	**WORD_TO_DINT, WORD_TO_UDINT**	The value is transferred to the least significant word of the target data type.
DWord	**DWORD_TO_BOOL**	The least significant bit is transferred into the destination data type.
	DWORD_TO_BYTE, DWORD_TO_WORD, DWORD_TO_SINT	The least significant byte of the source value is transferred to the target data type.
	DWORD_TO_USINT, DWORD_TO_INT, DWORD_TO_UINT	The least significant word of the source value is transferred to the target data type.
	DWORD_TO_DINT, DWORD_TO_UDINT, DWORD_TO_REAL	The value is transferred to the target data type.

Table 9-110 Conversion from a short integer (SInt or USInt)

Data type	Instruction	Result
SInt	**SINT_TO_BOOL**	The least significant bit is transferred into the destination data type.
	SINT_TO_BYTE	The value is transferred to the target data type
	SINT_TO_WORD, SINT_TO_DWORD	The value is transferred to the least significant byte of the target data type.
	SINT_TO_INT, SINT_TO_DINT, SINT_TO_USINT, SINT_TO_UINT, SINT_TO_UDINT, SINT_TO_REAL, SINT_TO_LREAL, SINT_TO_CHAR, SINT_TO_STRING	The value is converted.
USInt	**USINT_TO_BOOL**	The least significant bit is transferred into the destination data type.
	USINT_TO_BYTE	The value is transferred to the target data type
	USINT_TO_WORD, USINT_TO_DWORD, USINT_TO_INT, USINT_TO_UINT, USINT_TO_DINT, USINT_TO_UDINT	The value is transferred to the least significant byte of the target data type.
	USINT_TO_SINT, USINT_TO_REAL, USINT_TO_LREAL, USINT_TO_CHAR, USINT_TO_STRING	The value is converted.

Table 9-111 Conversion from an integer (Int or UInt)

Data type	Instruction	Result
Int	**INT_TO_BOOL**	The least significant bit is transferred into the destination data type.
	INT_TO_BYTE, INT_TO_DWORD, INT_TO_SINT, INT_TO_USINT, INT_TO_UINT, INT_TO_UDINT, INT_TO_REAL, INT_TO_LREAL, INT_TO_CHAR, INT_TO_STRING	The value is converted.
	INT_TO_WORD	The value is transferred to the target data type.
	INT_TO_DINT	The value is transferred to the least significant byte of the target data type.
UInt	**UINT_TO_BOOL**	The least significant bit is transferred into the destination data type.

Data type	Instruction	Result
UInt	**UINT_TO_BYTE, UINT_TO_SINT, UINT_TO_USINT, UINT_TO_INT, UINT_TO_REAL, UINT_TO_LREAL, UINT_TO_CHAR, UINT_TO_STRING**	The value is converted.
	UINT_TO_WORD, UINT_TO_DATE	The value is transferred to the target data type.
	UINT_TO_DWORD, UINT_TO_DINT, UINT_TO_UDINT	The value is transferred to the least significant byte of the target data type.

Table 9-112 Conversion from a double integer (Dint or UDInt)

Data type	Instruction	Result
DInt	**DINT_TO_BOOL**	The least significant bit is transferred into the destination data type.
	DINT_TO_BYTE, DINT_TO_WORD, DINT_TO_SINT, DINT_TO_USINT, DINT_TO_INT, DINT_TO_UINT, DINT_TO_UDINT, DINT_TO_REAL, DINT_TO_LREAL, DINT_TO_CHAR, DINT_TO_STRING	The value is converted.
	DINT_TO_DWORD, DINT_TO_TIME	The value is transferred to the target data type.
UDInt	**UDINT_TO_BOOL**	The least significant bit is transferred into the destination data type.
	UDINT_TO_BYTE, UDINT_TO_WORD, UDINT_TO_SINT, UDINT_TO_USINT, UDINT_TO_INT, UDINT_TO_UINT, UDINT_TO_DINT, UDINT_TO_REAL, UDINT_TO_LREAL, UDINT_TO_CHAR, UDINT_TO_STRING	The value is converted.
	UDINT_TO_DWORD, UDINT_TO_TOD	The value is transferred to the target data type.

Table 9-113 Conversion from a Real number (Real or LReal)

Data type	Instruction	Result
Real	**REAL_TO_DWORD, REAL_TO_LREAL**	The value is transferred to the target data type.
	REAL_TO_SINT, REAL_TO_USINT, REAL_TO_INT, REAL_TO_UINT, REAL_TO_DINT, REAL_TO_UDINT, REAL_TO_STRING	The value is converted.
LReal	**LREAL_TO_SINT, LREAL_TO_USINT, LREAL_TO_INT, LREAL_TO_UINT, LREAL_TO_DINT, LREAL_TO_UDINT, LREAL_TO_REAL, LREAL_TO_STRING**	The value is converted.

Table 9-114 Conversion from Time, DTL, TOD or Date

Data type	Instruction	Result
Time	**TIME_TO_DINT**	The value is transferred to the target data type.
DTL	**DTL_TO_DATE, DTL_TO_TOD**	The value is converted.
TOD	**TOD_TO_UDINT**	The value is converted.
Date	**DATE_TO_UINT**	The value is converted.

Table 9-115 Conversion from a Char or String

Data type	Instruction	Result
Char	**CHAR_TO_SINT, CHAR_TO_USINT, CHAR_TO_INT, CHAR_TO_UINT, CHAR_TO_DINT, CHAR_TO_UDINT**	The value is converted.
	CHAR_TO_STRING	The value is transferred to the first character of the string.
String	**STRING_TO_SINT, STRING_TO_USINT, STRING_TO_INT, STRING_TO_UINT, STRING_TO_DINT, STRING_TO_UDINT, STRING_TO_REAL, STRING_TO_LREAL**	The value is converted.
	STRING_TO_CHAR	The first character of the string is copied to the Char.

9.7.3 ROUND (Round numerical value) and TRUNC (Truncate numerical value)

Table 9-116 ROUND and TRUNC instructions

LAD / FBD	SCL	Description
	out := ROUND (in);	Converts a real number to an integer. For SCL, the default data type for the output of the ROUND instruction is DINT. To round to another output data type, enter the instruction name with the explicit name of the data type, for example, ROUND_REAL or ROUND_LREAL. The real number fraction is rounded to the nearest integer value (IEEE - round to nearest). If the number is exactly one-half the span between two integers (for example, 10.5), then the number is rounded to the even integer. For example: • ROUND (10.5) = 10 • ROUND (11.5) = 12
	out := TRUNC(in);	TRUNC converts a real number to an integer. The fractional part of the real number is truncated to zero (IEEE - round to zero).

[1] For LAD and FBD: Click the "???" (by the instruction name) and select a data type from the drop-down menu.

Table 9-117 Data types for the parameters

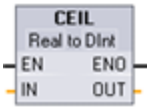
Parameter	Data type	Description
IN	Real, LReal	Floating point input
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal	Rounded or truncated output

Table 9-118 ENO status

ENO	Description	Result OUT
1	No error	Valid result
0	IN is +/- INF or +/- NaN	+/- INF or +/- NaN

9.7.4 CEIL and FLOOR (Generate next higher and lower integer from floating-point number)

Table 9-119 CEIL and FLOOR instructions

LAD / FBD	SCL	Description
	**out := CEIL(in);**	Converts a real number (Real or LReal) to the closest integer greater than or equal to the selected real number (IEEE "round to +infinity").
	out := FLOOR(in);	Converts a real number (Real or LReal) to the closest integer smaller than or equal to the selected real number (IEEE "round to -infinity").

[1] For LAD and FBD: Click the "???" (by the instruction name) and select a data type from the drop-down menu.

Table 9-120 Data types for the parameters

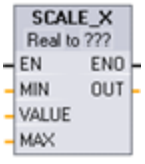
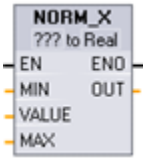
Parameter	Data type	Description
IN	Real, LReal	Floating point input
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal	Converted output

Table 9-121 ENO status

ENO	Description	Result OUT
1	No error	Valid result
0	IN is +/- INF or +/- NaN	+/- INF or +/- NaN

9.7.5 SCALE_X (Scale) and NORM_X (Normalize)

Table 9-122 SCALE_X and NORM_X instructions

LAD / FBD	SCL	Description
	**out :=SCALE_X(min:=_in_, value:=_in_, max:=_in_);**	Scales the normalized real parameter VALUE where (0.0 <= VALUE <= 1.0) in the data type and value range specified by the MIN and MAX parameters: OUT = VALUE (MAX - MIN) + MIN
	**out :=NORM_X(min:=_in_, value:=_in_, max:=_in_);**	Normalizes the parameter VALUE inside the value range specified by the MIN and MAX parameters: OUT = (VALUE - MIN) / (MAX - MIN), where (0.0 <= OUT <= 1.0)

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-123 Data types for the parameters

Parameter	Data type[1]	Description
MIN	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal	Input minimum value for range
VALUE	SCALE_X: Real, LReal NORM_X: SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal	Input value to scale or normalize
MAX	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal	Input maximum value for range
OUT	SCALE_X: SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal NORM_X: Real, LReal	Scaled or normalized output value

1 For SCALE_X: Parameters MIN, MAX, and OUT must be the same data type.
For NORM_X: Parameters MIN, VALUE, and MAX must be the same data type.

NOTE

SCALE_X parameter VALUE should be restricted to (0.0 <= VALUE <= 1.0)

If parameter VALUE is less than 0.0 or greater than 1.0:

- The linear scaling operation can produce OUT values that are less than the parameter MIN value or above the parameter MAX value for OUT values that fit within the value range of the OUT data type. SCALE_X execution sets ENO = TRUE for these cases.
- It is possible to generate scaled numbers that are not within the range of the OUT data type. For these cases, the parameter OUT value is set to an intermediate value equal to the least-significant portion of the scaled real number prior to final conversion to the OUT data type. SCALE_X execution sets ENO = FALSE in this case.

NORM_X parameter VALUE should be restricted to (MIN <= VALUE <= MAX)

If parameter VALUE is less than MIN or greater than MAX, the linear scaling operation can produce normalized OUT values that are less than 0.0 or greater than 1.0. NORM_X execution sets ENO = TRUE in this case.

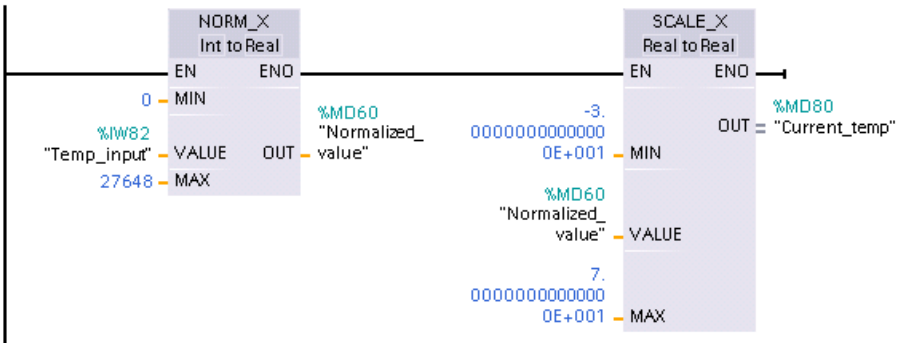
Table 9-124 ENO status

ENO	Condition	Result OUT
1	No error	Valid result
0	Result exceeds valid range for the OUT data type	Intermediate result: The least-significant portion of a real number prior to final conversion to the OUT data type.
0	Parameters MAX <= MIN	SCALE_X: The least-significant portion of the Real number VALUE to fill up the OUT size. NORM_X: VALUE in VALUE data type extended to fill a double word size.
0	Parameter VALUE = +/- INF or +/- NaN	VALUE is written to OUT

Example (LAD): normalizing and scaling an analog input value

An analog input from an analog signal module or signal board using input in current is in the range 0 to 27648 for valid values. Suppose an analog input represents a temperature where the 0 value of the analog input represents -30.0 degrees C and 27648 represents 70.0 degrees C.

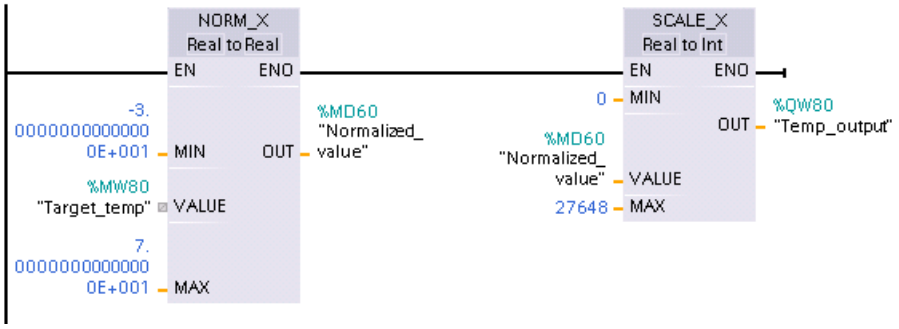
To transform the analog value to the corresponding engineering units, normalize the input to a value between 0.0 and 1.0, and then scale it between -30.0 and 70.0. The resulting value is the temperature represented by the analog input in degrees C:



Note that if the analog input was from an analog signal module or signal board using voltage, the MIN value for the NORM_X instruction would be -27648 instead of 0.

Example (LAD): normalizing and scaling an analog output value

An analog output to be set in an analog signal module or signal board using output in current must be in the range 0 to 27648 for valid values. Suppose an analog output represents a temperature setting where the 0 value of the analog input represents -30.0 degrees C and 27648 represents 70.0 degrees C. To convert a temperature value in memory that is between -30.0 and 70.0 to a value for the analog output in the range 0 to 27648, you must normalize the value in engineering units to a value between 0.0 and 1.0, and then scale it to the range of the analog output, 0 to 27648:



Note that if the analog output was for an analog signal module or signal board using voltage, the MIN value for the SCALE_X instruction would be -27648 instead of 0.

Additional information on analog input representations (Page 1195) and analog output representations (Page 1196) in both voltage and current can be found in the Technical Specifications.

9.7.6 Variant conversion instructions

9.7.6.1 VARIANT_TO_DB_ANY (Convert VARIANT to DB_ANY)

You use the "VARIANT to DB_ANY" instruction to read the operand at the IN parameter and convert it to the data type DB_ANY. The IN parameter is of the Variant data type and represents either an instance data block or an ARRAY data block. When you create the program, you do not need to know which data block corresponds to the IN parameter. The instruction reads the data block number during runtime and writes it to the operand at the RET_VAL parameter.

Table 9-125 VARIANT_TO_DB_ANY instruction

LAD / FBD	SCL	Description
Not available	**RET_VAL := VARIANT_TO_DB_ANY(in := _variant_in_, err => _int_out_);**	Reads the operand from the Variant IN parameter and stores it in the function result, which is of the type DB_ANY

Table 9-126 Parameters for the VARIANT_TO_DB_ANY instruction

Parameter	Data type	Description
IN	Variant	Variant that represents and instance data block or an array data block
RET_VAL	DB_ANY	Output DB_ANY data type that contains the converted data block number
ERR	Int	Error information

Table 9-127 ENO status

ENO	Condition	Result
1	No error	Instruction converts the input Variant and stores it in the DB_ANY function output
0	Enable input EN has the signal state "0" or the IN parameter is invalid.	Instruction does nothing.

Table 9-128 Error output codes for the VARIANT_TO_DB_ANY instruction

Err (W#16#...)	Description
0000	No error
252C	The Variant data type at IN parameter has the value 0. The CPU changes to STOP mode.
8131	The data block does not exist or is too short (first access).
8132	The data block is too short and not an Array data block (second access).
8134	The data block is write-protected

Err (W#16#...)	Description
8150	The data type Variant at parameter IN provides the value "0". To receive this error message, the "Handle errors within block" block property must be activated. Otherwise the CPU changes to STOP mode and sends the error code 16#252C
8154	The data block has the incorrect data type.
*You can display error codes in the program editor as integer or hexadecimal values.	

9.7.6.2 DB_ANY_TO_VARIANT (Convert DB_ANY to VARIANT)

You use the "DB_ANY to VARIANT" instruction to read the number of a data block that meets the requirements listed below. The operand at the IN parameter has the data type DB_ANY, which means you do not need to know during program creation which data block is to be read. The instruction reads the data block number during runtime and writes it to the function result RET_VAL by means of a VARIANT pointer.

Table 9-129 DB_ANY_TO_VARIANT instruction

LAD / FBD	SCL	Description
Not available	**RET_VAL := DB_ANY_TO_VARIANT(in := _db_any_in_, err => _int_out_);**	Reads the data block number from the Variant IN parameter and stores it in the function result, which is of the type Variant

Table 9-130 Parameters for the DB_ANY_TO_VARIANT instruction

Parameter	Data type	Description
IN	DB_ANY	Variant that contains the data block number
RET_VAL	Variant	Output DB_ANY data type that contains the converted data block number
ERR	Int	Error information

Table 9-131 ENO status

ENO	Condition	Result
1	No error	Instruction converts the data block number in the variant and stores it in the function DB_ANY output
0	Enable input EN has the signal state "0" or the IN parameter is invalid.	Instruction does nothing.

Table 9-132 Error output codes for the DB_ANY_TO_VARIANT instruction

Err (W#16#...)	Description
0000	No error
8130	The number of the data block is 0.
8131	The data block does not exist or is too short.
8132	The data block is too short and not an Array data block.
8134	The data block is write-protected.

Err (W#16#...)	Description
8154	The data block has the incorrect data type.
8155	Unknown type code
*You can display error codes in the program editor as integer or hexadecimal values.	

9.8 Program control operations

9.8.1 JMP (Jump if RLO = 1), JMPN (Jump if RLO = 0), and Label (Jump label) instructions

Table 9-133 JMP, JMPN, and LABEL instruction

LAD	FBD	SCL	Description
Label_name —(JMP)—	Label_name JMP	See the GOTO (Page 286) statement.	Jump if RLO (result of logic operation) = 1: If there is power flow to a JMP coil (LAD), or if the JMP box input is true (FBD), then program execution continues with the first instruction following the specified label.
Label_name —(JMPN)—	Label_name JMPN		Jump if RLO = 0: If there is no power flow to a JMPN coil (LAD), or if the JMPN box input is false (FBD), then program execution continues with the first instruction following the specified label.
Label_name	Label_name		Destination label for a JMP or JMPN jump instruction.

[1] You create your label names by typing in the LABEL instruction directly. Use the parameter helper icon to select the available label names for the JMP and JMPN label name field. You can also type a label name directly into the JMP or JMPN instruction.

Table 9-134 Data types for the parameters

Parameter	Data type	Description
Label_name	Label identifier	Identifier for Jump instructions and the corresponding jump destination program label

- Each label must be unique within a code block.
- You can jump within a code block, but you cannot jump from one code block to another code block.
- You can jump forward or backward.
- You can jump to the same label from more than one place in the same code block.

9.8.2 JMP_LIST (Define jump list)

Table 9-135 JMP_LIST instruction

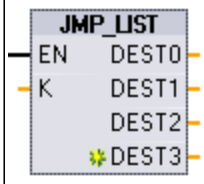
LAD / FBD	SCL	Description
	**CASE k OF** **0: GOTO dest0;** **1: GOTO dest1;** **2: GOTO dest2;** **[n: GOTO destn;]** **END_CASE;**	The JMP_LIST instruction acts as a program jump distributor to control the execution of program sections. Depending on the value of the K input, a jump occurs to the corresponding program label. Program execution continues with the program instructions that follow the destination jump label. If the value of the K input exceeds the number of labels - 1, then no jump occurs and processing continues with the next program network.

Table 9-136 Data types for parameters

Parameter	Data type	Description
K	UInt	Jump distributor control value
DEST0, DEST1, .., DESTn.	Program Labels	Jump destination labels corresponding to specific K parameter values: If the value of K equals 0, then a jump occurs to the program label assigned to the DEST0 output. If the value of K equals 1, then a jump occurs to the program label assigned to the DEST1 output, and so on. If the value of the K input exceeds the (number of labels - 1), then no jump occurs and processing continues with the next program network.

For LAD and FBD: When you first place a JMP_LIST instruction in your program, there are two jump label outputs. You can add or delete jump destinations.

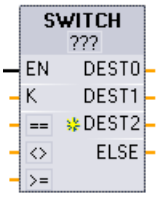
To insert a jump destination, click the create icon inside the box to add a new destination output.

You can also right-click an output and select the "Insert output" command.

To delete a jump destination right-click an output stub and select the "Delete" command.

9.8.3 SWITCH (Jump distributor)

Table 9-137 SWITCH instruction

LAD / FBD	SCL	Description
	**Not available**	The SWITCH instruction acts as a program jump distributor to control the execution of program sections. Depending on the result of comparisons between the value of the K input and the values assigned to the specified comparison inputs, a jump occurs to the program label that corresponds to the first comparison test that is true. If none of the comparisons is true, then a jump to the label assigned to ELSE occurs. Program execution continues with the program instructions that follow the destination jump label.

[1] For LAD and FBD: Click below the box name and select a data type from the drop-down menu.

[2] For SCL: Use a CASE statement or set of IF-THEN comparisons.

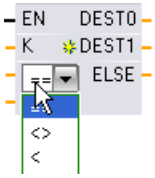
Table 9-138 Data types for parameters

Parameter	Data type[1]	Description
K	UInt	Common comparison value input
==, <>, <, <=, >. >=	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, TOD, Date	Separate comparison value inputs for specific comparison types
DEST0, DEST1, .., DESTn, ELSE	Program Labels	Jump destination labels corresponding to specific comparisons: The comparison input below and next to the K input is processed first and causes a jump to the label assigned to DEST0, if the comparison between the K value and this input is true. The next comparison test uses the next input below and causes a jump to the label assigned to DEST1, if the comparison is true, The remaining comparisons are processed similarly and if none of the comparisons are true, then a jump to the label assigned to the ELSE output occurs.

[1] The K input and comparison inputs (==, <>, <, <=, >, >=) must be the same data type.

Adding inputs, deleting inputs, and specifying comparison types

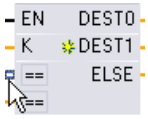
When you first place an LAD or FBD SWITCH instruction in your program, there are two comparison inputs. You can assign comparison types and add inputs/jump destinations, as shown below.



Click a comparison operator inside the box and select a new operator from the drop-down list.

To insert a new comparison input and output, click the create icon inside the box.

You can also right-click any output parameter and select the "Insert input and output" command.



To delete a comparison from the SWITCH instruction, right-click an input or output and select the "Delete" command.

The instruction has a minimum of two comparisons.

Table 9-139 SWITCH box data type selection and allowed comparison operations

Data type	Comparison	Operator syntax
Byte, Word, DWord	Equal	==
	Not equal	<>
SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Time, TOD, Date	Equal	==
	Not equal	<>
	Greater than or equal	>=
	Less than or equal	<=
	Greater than	>
	Less than	<

SWITCH box placement rules

- No LAD/FBD instruction connection in front of the compare input is allowed.
- There is no ENO output, so only one SWITCH instruction is allowed in a network and the SWITCH instruction must be the last operation in a network.

9.8.4 RET (Return)

The optional RET instruction is used to terminate the execution of the current block. If and only if there is power flow to the RET coil (LAD) or if the RET box input is true (FBD), then program execution of the current block will end at that point and instructions beyond the RET instruction will not be executed. If the current block is an OB, the "Return_Value" parameter is ignored. If the current block is a FC or FB, the value of the "Return_Value" parameter is passed back to the calling routine as the ENO value of the called box.

You are not required to use a RET instruction as the last instruction in a block; this is done automatically for you. You can have multiple RET instructions within a single block.

For SCL, see the RETURN (Page 287) statement.

Table 9-140 Return_Value (RET) execution control instruction

LAD	FBD	SCL	Description
"Return_Value" —(RET)—|	"Return_Value" RET	**RETURN;**	Terminates the execution of the current block

Table 9-141 Data types for the parameters

Parameter	Data type	Description
Return_Value	Bool	The "Return_value" parameter of the RET instruction is assigned to the ENO output of the block call box in the calling block.

Sample steps for using the RET instruction inside an FC code block:

1. Create a new project and add an FC.
2. Edit the FC:
   - Add instructions.
   - Add a RET instruction, including one of the following for the "Return_Value" parameter: TRUE, FALSE, or a memory location that specifies the required return value.
   - Add more instructions.
3. Call the FC from MAIN [OB1].

The EN input on the FC box in the MAIN code block must be true to begin execution of the FC.

The value specified by the RET instruction in the FC will be present on the ENO output of the FC box in the MAIN code block following execution of the FC for which power flow to the RET instruction is TRUE.

9.8.5 ENDIS_PW (Enable/disable CPU passwords)

Table 9-142 ENDIS_PW instruction

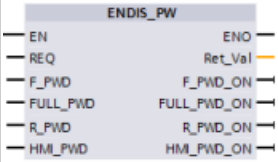
LAD / FBD	SCL	Description
	**ENDIS_PW(** **req:=_bool_in_,** **f_pwd:=_bool_in_,** **full_pwd:=_bool_in_,** **r_pwd:=_bool_in_,** **hmi_pwd:=_bool_in_,** **f_pwd_on=>_bool_out_,** **full_pwd_on=>_bool_out_,** **r_pwd_on=>_bool_out_,** **hmi_pwd_on=>_bool_out_);**	The ENDIS_PW instruction can allow and disallow client connections to a S7-1200 CPU, even when the client can provide the correct password. This instruction does not disallow Web server passwords.

Table 9-143 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Perform function if REQ=1
F_PWD	IN	Bool	Fail-safe password: Allow (=1) or disallow (=0)
FULL_PWD	IN	Bool	Full access password: Allow (=1) or disallow (=0) full access password
R_PWD	IN	Bool	Read access password: Allow (=1) or disallow (=0)
HMI_PWD	IN	Bool	HMI password: Allow (=1) or disallow (=0)
F_PWD_ON	OUT	Bool	Fail-safe password status: Allowed (=1) or disallowed (=0)
FULL_PWD_ON	OUT	Bool	Full access password status: Allowed (=1) or disallowed (=0)
R_PWD_ON	OUT	Bool	Read only password status: Allowed (=1) or disallowed (=0)
HMI_PWD_ON	OUT	Bool	HMI password status: Allowed (=1) or disallowed (=0)
Ret_Val	OUT	Word	Function result

Calling ENDIS_PW with REQ=1 disallows password types where the corresponding password input parameter is FALSE. Each password type can be allowed or disallowed independently. For example, if the fail-safe password is allowed and all other passwords disallowed, then you can restrict CPU access to a small group of employees.

ENDIS_PW is executed synchronously in a program scan and the password output parameters always show the current state of password allowance independent of the input parameter REQ. All passwords that you set to allow must be changeable to disallowed/allowed. Otherwise, an error is returned and all passwords are allowed that were allowed before ENDIS_PW execution. This means that in a standard CPU (where the fail-safe password is not configured) F_PWD must always be set to 1, to result in a return value of 0. In this case, F_PWD_ON is always 1.

NOTE

- ENDIS_PW execution can block the access of HMI devices, if the HMI password is disallowed.
- Client sessions that were authorized prior to ENDIS_PW execution may be terminated by ENDIS_PW execution dependent on the existing legitimization level. For example, a connection legitimized with READ password protection will be aborted by ENDIS_PW (REQ=1, R_PWD=0). Other lower protection level connections are also aborted under this scenario. Accordingly, connections legitimized with FULL access are retained.

After a power-up, CPU access is restricted by passwords previously defined in the regular CPU protection configuration. The ability to disallow a valid password must be re-established with a new ENDIS_PW execution. However, if ENDIS_PW is immediately executed and necessary passwords are disallowed, then TIA portal access can be locked out. You can use a timer instruction to delay ENDIS_PW execution and allow time to enter passwords, before the passwords become disallowed.

NOTE

Restoring a CPU that locks out TIA portal communication

Refer to the "Recovery from a lost password (Page 119)" topic for details about how to erase the internal load memory of a PLC using a memory card.

An operating mode change to STOP caused by errors, STP execution or STEP 7 does not abolish the protection. The protection is valid until the CPU is power cycled. See the following table for details.

Action	Operating mode	ENDIS_PW password control
After memory reset from STEP 7	STOP	Active: Disallowed passwords remain disallowed.
After powering on, or changing a memory card	STOP	Off: No passwords are disallowed.
After ENDIS_PW execution in a program cycle or startup OB	STARTUP, RUN	Active: Passwords are disallowed according to ENDIS_PW parameters
After change of the operating mode from RUN or STARTUP to STOP through STP instruction, error, or STEP 7	STOP	Active: Disallowed passwords remain disallowed

WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server or OPC UA users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

- Enable Access control (Page 147) under "Protection & Security > Access control".
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Enable the setting "Only allow secure PG/PC and HMI communication" under "Protection & Security > Connection mechanisms".
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC from a location outside your protected network.
- Enable access to the Web server only with the HTTPS protocol.
- Perform error-checking and range-checking on your variables in your program logic because Web server or OPC UA users can change PLC variables to invalid values.
- For the OPC UA server: In your STEP 7 Device configuration, navigate to "Properties > OPC UA > Server > Security" and deselect "No security" in "Security policies available on the server for the secure channel".

Disruption of process operations can result in death, severe personal injury, and/or property damage.

Table 9-144 Condition codes

RET_VAL (W#16#...)	Description
0000	No error
8090	The instruction is not supported.
80D0	The password for fail-safe is not configured.
80D1	The password for read/write access is not configured.
80D2	The password for read access is not configured.
80D3	The password for HMI access is not configured.

9.8.6 RE_TRIGR (Restart cycle monitoring time)

Table 9-145 RE_TRIGR instruction

LAD / FBD	SCL	Description
	RE_TRIGR();	RE_TRIGR (Re-trigger scan time watchdog) is used to extend the maximum time allowed before the scan cycle watchdog timer generates an error.

Use the RE_TRIGR instruction to restart the scan cycle monitoring timer during a single scan cycle. This has the effect of extending the allowed maximum scan cycle time by one maximum cycle time period, from the last execution of the RE_TRIGR function.

NOTE

RE_TRIGR can be executed from any OB (including start up, interrupt, and error OBs). The PLC scan can only be extended by a maximum of 10x the configured maximum cycle time.

Setting the PLC maximum cycle time

Configure the value for maximum scan cycle time in the Device configuration for "Cycle time".

Table 9-146 Cycle time values

Cycle time monitor	Minimum value	Maximum value	Default value
Maximum cycle time	1 ms	6000 ms	150 ms

Watchdog timeout

If the maximum scan cycle timer expires before the scan cycle has been completed, an error is generated. If the user program includes a time error interrupt OB (OB 80), the CPU executes the time error interrupt OB, which can include program logic to create a special reaction.

If a time error interrupt OB has never been downloaded, the first timeout condition is ignored and the CPU remains in RUN mode. If a second maximum scan time timeout occurs in the same program scan (2 times the maximum cycle time value), then an error is triggered that causes a transition to STOP mode.

In STOP mode, your program execution stops while CPU system communications and system diagnostics continue.

9.8.7 STP (Exit program)

Table 9-147 STP instruction

LAD / FBD	SCL	Description
	STP();	STP puts the CPU in STOP mode. When the CPU is in STOP mode, the execution of your program and physical updates from the process image are stopped.

For more information see: Configuring the outputs on a RUN-to-STOP transition (Page 88).

If EN = TRUE, then the CPU goes to STOP mode, the program execution stops, and the ENO state is meaningless. Otherwise, EN = ENO = 0.

9.8.8 GET_ERROR and GET_ERROR_ID (Get error and error ID locally) instructions

The get error instructions provide information about program block execution errors. If you add a GET_ERROR or GET_ERROR_ID instruction to your code block, you can handle program errors within your program block.

GET_ERROR

Table 9-148 GET_ERROR instruction

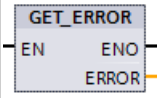
LAD / FBD	SCL	Description
	**GET_ERROR(_out_);**	Indicates that a local program block execution error has occurred and fills a predefined error data structure with detailed error information.

Table 9-149 Data types for the parameters

Parameter	Data type	Description
ERROR	ErrorStruct	Error data structure: You can rename the structure, but not the members within the structure.

Table 9-150 Elements of the ErrorStruct data structure

Structure components		Data type	Description
ERROR_ID		Word	Error ID
FLAGS		Byte	Shows if an error occurred during a block call. • 16#01: Error during a block call. • 16#00: No error during a block call.
REACTION		Byte	Default reaction: • 0: Ignore (write error), • 1: Continue with substitute value "0" (read error), • 2: Skip instruction (system error)
CODE_ADDRESS		CREF	Information about the address and type of block
	BLOCK_TYPE	Byte	Type of block where the error occurred: • 1: OB • 2: FC • 3: FB
	CB_NUMBER	UInt	Number of the code block
	OFFSET	UDInt	Reference to the internal memory
MODE		Byte	Access mode: Depending on the type of access, the following information can be output:

Mode	(A)	(B)	(C)	(D)	(E)
0					
1					Offset
2			Area		
3	Location	Scope		Number	
4			Area		Offset
5			Area	DB no.	Offset

Structure components		Data type	Description					
MODE		Byte	6	PtrNo. /Acc		Area	DB no.	Offset
			7	PtrNo. / Acc	Slot No. / Scope	Area	DB no.	Offset
OPERAND_NUMBER		UInt	Operand number of the machine command					
POINTER_NUMBER_ LOCATION		UInt	(A) Internal pointer					
SLOT_NUMBER_SCOPE		UInt	(B) Storage area in internal memory					
DATA_ADDRESS		NREF	Information about the address of an operand					
	AREA	Byte	(C) Memory area: • L: 16#40 – 4E, 86, 87, 8E, 8F, C0 – CE • I: 16#81 • Q: 16#82 • M: 16#83 • DB: 16#84, 85, 8A, 8B					
	DB_NUMBER	UInt	(D) Number of the data block					
	OFFSET	UDInt	(E) Relative address of the operand					

GET_ERROR_ID

Table 9-151 GetErrorID instruction

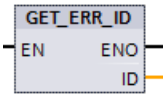
LAD / FBD	SCL	Description
	**GET_ERR_ID();**	Indicates that a program block execution error has occurred and reports the ID (identifier code) of the error.

Table 9-152 Data types for the parameters

Parameter	Data type	Description
ID	Word	Error identifier values for the ErrorStruct ERROR_ID member

Table 9-153 Error_ID values

ERROR_ID hexadecimal	ERROR_ID decimal	Program block execution error
0	0	No error
2520	9504	Corrupted string
2522	9506	Operand out of range read error
2523	9507	Operand out of range write error
2524	9508	Invalid area read error
2525	9509	Invalid area write error
2528	9512	Data alignment read error (incorrect bit alignment)
2529	9513	Data alignment write error (incorrect bit alignment)
252C	9516	Uninitialized pointer error
2530	9520	DB write protected
2533	9523	Invalid pointer used

ERROR_ID hexadecimal	ERROR_ID decimal	Program block execution error
2538	9528	Access error: DB does not exist
2539	9529	Access error: Wrong DB used
253A	9530	Global DB does not exist
253C	9532	Wrong version or FC does not exist
253D	9533	Instruction does not exist
253E	9534	Wrong version or FB does not exist
253F	9535	Instruction does not exist
2550	9552	Access error: DB does not exist
2575	9589	Program nesting depth error
2576	9590	Local data allocation error
2942	10562	Physical input point does not exist
2943	10563	Physical output point does not exist

Operation

By default, the CPU responds to a block execution error by logging an error in the diagnostics buffer. However, if you place one or more GET_ERROR or GET_ERROR_ID instructions within a code block, this block is now set to handle errors within the block. In this case, the CPU does not log an error in the diagnostics buffer. Instead, the error information is reported in the output of the GET_ERROR or GET_ERROR_ID instruction. You can read the detailed error information with the GET_ERROR instruction, or read just the error identifier with GET_ERROR_ID instruction. Normally the first error is the most important, with the following errors only consequences of the first error.

The first execution of a GET_ERROR or GET_ERROR_ID instruction within a block returns the first error detected during block execution. This error could have occurred anywhere between the start of the block and the execution of either GET_ERROR or GET_ERROR_ID. Subsequent executions of either GET_ERROR or GET_ERROR_ID return the first error since the previous execution of GET_ERROR or GET_ERROR_ID. The history of errors is not saved, and execution of either instruction will re-arm the PLC system to catch the next error.

The ErrorStruct data type used by the GET_ERROR instruction can be added in the data block editor and block interface editors, so your program logic can access these values. Select ErrorStruct from the data type drop-down list to add this structure. You can create multiple ErrorStruct elements by using unique names. The members of an ErrorStruct cannot be renamed.

Error condition indicated by ENO

If EN = TRUE and GET_ERROR or GET_ERROR_ID executes, then:

- ENO = TRUE indicates a code block execution error occurred and error data is present
- ENO = FALSE indicates no code block execution error occurred

You can connect error reaction program logic to ENO which activates after an error occurs. If an error exists, then the output parameter stores the error data where your program has access to it.

GET_ERROR and GET_ERROR_ID can be used to send error information from the currently executing block (called block) to a calling block. Place the instruction in the last network of the called block program to report the final execution status of the called block.

9.8.9 RUNTIME (Measure program runtime)

Table 9-154 RUNTIME instruction

LAD / FBD	SCL	Description
RUNTIME EN ENO MEM Ret_Val	**Ret_Val := RUNTIME(_lread_inout_);**	Measures the runtime of the entire program, individual blocks, or command sequences.

To measure the runtime of your entire program, call the instruction "Measure program runtime" in OB 1. Measurement of the runtime starts with the first call and the output RET_VAL returns the runtime of the program after the second call. The measured runtime includes all CPU processes that can occur during the program execution, for example, interruptions caused by higher-level events or communication. The instruction "Measure program runtime" reads an internal counter of the CPU and write the value to the IN-OUT parameter MEM. The instruction calculates the current program runtime according to the internal counter frequency and writes it to output RET_VAL.

If you want to measure the runtime of individual blocks or individual command sequences, you need three separate networks. Call the instruction "Measure program runtime" in an individual network within your program. You set the starting point of the runtime measurement with this first call of the instruction. Then you call the required program block or the command sequence in the next network. In another network, call the "Measure program runtime" instruction a second time and assign the same memory to the IN-OUT parameter MEM as you did during the first call of the instruction. The "Measure program runtime" instruction in the third network reads an internal CPU counter and calculates the current runtime of the program block or the command sequence according to the internal counter frequency and writes it to the output RET_VAL.

The Measure program runtime" instruction uses an internal high-frequency counter to calculate the time. If the counter overruns, the instruction returns values <= 0.0. Ignore these runtime values.

NOTE

The CPU cannot exactly determine the runtime of a command sequence, because the sequence of instructions within a command sequence changes during optimized compilation of the program.

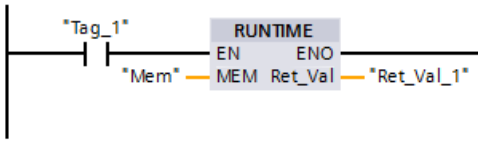
Table 9-155 Data types for the parameters

Parameter	Data type	Description
MEM	LReal	Starting point of the runtime measurement
RET_VAL	LReal	Measured runtime in seconds

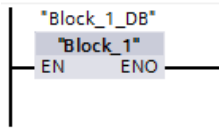
Example: RUNTIME instruction

The following example shows the use of the RUNTIME instruction to measure the execution time of a function block:

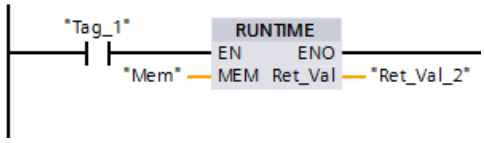
Network 1:



Network 2:



Network 3:



When the "Tag_1" operand in network 1 has the signal state "1", the RUNTIME instruction executes. The starting point for the runtime measurement is set with the first call of the instruction and buffered as reference for the second call of the instruction in the "Mem" operand.

The function block FB1 executes in network 2.

When the FB1 program block completes and the "Tag_1" operand has the signal state "1", the RUNTIME instruction in network 3 executes. The second call of the instruction calculates the runtime of the program block and writes the result to the output RET_VAL_2.

9.8.10 SCL program control statements

Structured Control Language (SCL) provides three types of program control statements for structuring your user program:

- Selective statements: A selective statement enables you to direct program execution into alternative sequences of statements.
- Loops: You can control loop execution using iteration statements. An iteration statement specifies which parts of a program should be iterated depending on certain conditions.
- Program jumps: A program jump means an immediate jump to a specified jump destination and therefore to a different statement within the same block.

These program control statements use the syntax of the PASCAL programming language.

Table 9-156 Types of SCL program control statements

Program control statement		Description
Selective	IF-THEN (Page 281)	Enables you to direct program execution into one of two alternative branches, depending on a condition being TRUE or FALSE
	CASE (Page 282)	Enables the selective execution into 1 of *n* alternative branches, based on the value of a variable
Loop	FOR (Page 283)	Repeats a sequence of statements for as long as the control variable remains within the specified value range
	WHILE-DO (Page 284)	Repeats a sequence of statements while an execution condition continues to be satisfied
	REPEAT-UNTIL (Page 284)	Repeats a sequence of statements until a terminate condition is met
Program jump	CONTINUE (Page 285)	Stops the execution of the current loop iteration

Program control statement		Description
Program jump	EXIT (Page 286)	Exits a loop at any point regardless of whether the terminate condition is satisfied or not
	GOTO (Page 286)	Causes the program to jump immediately to a specified label
	RETURN (Page 287)	Causes the program to exit the block currently being executed and to return to the calling block

9.8.10.1 IF-THEN

The IF-THEN statement is a conditional statement that controls program flow by executing a group of statements, based on the evaluation of a Bool value of a logical expression. You can also use brackets to nest or structure the execution of multiple IF-THEN statements.

Table 9-157 Elements of the IF-THEN statement

SCL	Description
IF "condition" THEN **statement_A;** **statement_B;** **statement_C;** **;**	If "condition" is TRUE or 1, then execute the following statements until encountering the END_IF statement. If "condition" is FALSE or 0, then skip to END_IF statement (unless the program includes optional ELSIF or ELSE statements).
ELSIF "condition-n" THEN **statement_N;** **;**	The optional ELSEIF[1] statement provides additional conditions to be evaluated. For example: If "condition" in the IF-THEN statement is FALSE, then the program evaluates "condition-n". If "condition-n" is TRUE, then execute "statement_N".
ELSE **statement_X;** **;**	The optional ELSE statement provides statements to be executed when the "condition" of the IF-THEN statement is FALSE.
END_IF;	The END_IF statement terminates the IF-THEN instruction.

[1] You can include multiple ELSIF statements within one IF-THEN statement.

Table 9-158 Variables for the IF-THEN statement

Variables	Description
"condition"	Required. The logical expression is either TRUE (1) or FALSE (0).
"statement_A"	Optional. One or more statements to be executed when "condition" is TRUE.
"condition-n"	Optional. The logical expression to be evaluated by the optional ELSIF statement.
"statement_N"	Optional. One or more statements to be executed when "condition-n" of the ELSIF statement is TRUE.
"statement_X"	Optional. One or more statements to be executed when "condition" of the IF-THEN statement is FALSE.

An IF statement is executed according to the following rules:

- The first sequence of statements whose logical expression = TRUE is executed. The remaining sequences of statements are not executed.
- If no Boolean expression = TRUE, the sequence of statements introduced by ELSE is executed (or no sequence of statements if the ELSE branch does not exist).
- Any number of ELSIF statements can exist.

NOTE

Using one or more ELSIF branches has the advantage that the logical expressions following a valid expression are no longer evaluated in contrast to a sequence of IF statements. The runtime of a program can therefore be reduced.

9.8.10.2 CASE

Table 9-159 Elements of the CASE statement

SCL	Description
CASE "Test_Value" OF **"ValueList": Statement[; Statement, ...]** **"ValueList": Statement[; Statement, ...]** **ELSE** **Else-statement[; Else-statement, ...]** **END_CASE;**	The CASE statement executes one of several groups of statements, depending on the value of an expression. Additional statements for each test case and additional else-statements are optional.

Table 9-160 Parameters

Parameter	Description
"Test_Value"	Value to be tested
"ValueList"	Required. A single value or a comma-separated list of values or ranges of values. (Use two periods to define a range of values: 2..8) The following example illustrates the different variants of the value list: 1: Statement_A; 2, 4: Statement _B; 3, 5..7,9: Statement _C;
Statement	Required. One or more statements that are executed when "Test_Value" matches any value in the value list
Else-statement	Optional. One or more statements that are executed if no match with a value of the "ValueList" stated matches

The CASE statement is executed according to the following rules:

- The program checks whether the value of the Test_value expression is contained within a specified list of values. If a match is found, the statement component assigned to the list is executed.
- If no match is found, the program section following ELSE is executed. If the ELSE branch does not exist, no statement is executed.

Example: Nested CASE statements

CASE statements can be nested. Each nested case statement must have an associated END_CASE statement.

```
CASE "var1" OF
       1 : #var2 := 'A';
       2 : #var2 := 'B';
ELSE
       CASE "var3" OF

          65..90: #var2 := 'UpperCase';
          97..122: #var2 := 'LowerCase';
       ELSE

          #var2:= 'SpecialCharacter';
       END_CASE;
END_CASE;
```

9.8.10.3 FOR

Table 9-161 Elements of the FOR statement

SCL	Description
FOR "control_variable" := "begin" TO "end" **BY "increment" DO** **statement;** **;** **END_FOR;**	A FOR statement is used to repeat a sequence of statements as long as a control variable is within the specified range of values. The definition of a loop with FOR includes the specification of an initial and an end value. Both values must be the same type as the control variable. You can nest FOR loops. The END_FOR statement refers to the last executed FOR instruction. The BY clause is optional.

Table 9-162 Parameters

Parameter	Description
"control_variable"	Required. An integer that serves as a loop counter
"begin"	Required. Simple expression that specifies the initial value of the control variables
"end"	Required. Simple expression that determines the final value of the control variables
"increment"	Optional. Amount by which a "control variable" is changed after each loop. The "increment" has the same data type as "control variable". If the "increment" value is not specified, then the value of the run tags will be increased by 1 after each loop. You cannot change "increment" during the execution of the FOR statement.

The FOR statement executes as follows:

- At the start of the loop, the control variable is set to the initial value (initial assignment) and each time the loop iterates, it is incremented by the specified increment (positive increment) or decremented (negative increment) until the final value is reached.
- Following each run through of the loop, the condition is checked (final value reached) to establish whether or not it is satisfied. If the end condition is not satisfied, the sequence of statements is executed again, otherwise the loop terminates and execution continues with the statement immediately following the loop.

You can omit the statement BY [increment]. If no increment is specified, the increment is +1.

To end the loop regardless of the state of the "condition" expression, use EXIT (Page 286). The EXIT statement executes the statement immediately following the END_FOR statement.

Use the CONTINUE (Page 285) to skip the subsequent statements of a FOR loop and to continue the loop with the examination of whether the condition is met for termination.

9.8.10.4 WHILE-DO

Table 9-163 WHILE statement

SCL	Description
WHILE "condition" DO **Statement;** **Statement;** **...;** **END_WHILE;**	The WHILE statement performs a series of statements until a given condition is TRUE. You can nest WHILE loops. The END_WHILE statement refers to the last executed WHILE instruction.

Table 9-164 Parameters

Parameter	Description
"condition"	A logical expression that evaluates to TRUE or FALSE. (A "null" condition is interpreted as FALSE.)
Statement	One or more statements that are executed until the condition evaluates to TRUE.

NOTE

The WHILE statement evaluates the state of "condition" before executing any of the statements. To execute the statements at least one time regardless of the state of "condition", use the REPEAT statement (Page 284).

The WHILE statement executes according to the following rules:

- Prior to each iteration of the loop body, the execution condition is evaluated.
- The loop body following DO iterates as long as the execution condition has the value TRUE.
- Once the condition is FALSE, the loop is skipped and the statement following the loop is executed.

To end the loop regardless of the state of the "condition" expression, use EXIT (Page 286). The EXIT statement executes the statement immediately following the END_WHILE statement.

Use the CONTINUE (Page 285) statement to skip the subsequent statements of a WHILE loop and to continue the loop with the examination of whether the condition is met for termination.

9.8.10.5 REPEAT-UNTIL

Table 9-165 REPEAT instruction

SCL	Description
REPEAT **Statement;** **;** **UNTIL "condition"** **END_REPEAT;**	The REPEAT statement executes a group of statements until a given condition is TRUE. You can nest REPEAT loops. The END_REPEAT statement always refers to the last executed REPEAT instruction.

Table 9-166 Parameters

Parameter	Description
Statement	One or more statements that are executed until the condition is TRUE.
"condition"	One or more expressions of the two following ways: A numeric expression or string expression that evaluates to TRUE or FALSE. A "null" condition is interpreted as FALSE.

NOTE

Before evaluating the state of "condition", the REPEAT statement executes the statements during the first iteration of the loop (even if "condition" is FALSE). To review the state of "condition" before executing the statements, use the WHILE statement (Page 284).

To end the loop regardless of the state of the "condition" expression, use the EXIT (Page 286). The EXIT statement executes the statement immediately following the END_REPEAT statement.

Use the CONTINUE (Page 285) to skip the subsequent statements of a REPEAT loop and to continue the loop with the examination of whether the condition is met for termination.

9.8.10.6 CONTINUE

Table 9-167 CONTINUE statement

SCL	Description
CONTINUE **Statement;** **;**	The CONTINUE statement skips the subsequent statements of a program loop (FOR, WHILE, REPEAT) and continues the loop with the examination of whether the condition is met for termination. If this is not the case, the loop continues.

The CONTINUE statement executes according to the following rules:

- This statement immediately terminates execution of a loop body.
- Depending on whether the condition for repeating the loop is satisfied or not the body is executed again or the iteration statement is exited and the statement immediately following is executed.
- In a FOR statement, the control variable is incremented by the specified increment immediately after a CONTINUE statement.

Use the CONTINUE statement only within a loop. In nested loops CONTINUE always refers to the loop that includes it immediately. CONTINUE is typically used in conjunction with an IF statement.

If the loop is to exit regardless of the termination test, use the EXIT statement.

Example: CONTINUE statement

The following example shows the use of the CONTINUE statement to avoid a division-by-0 error when calculating the percentage of a value:

```
FOR i := 0 TO 10 DO
IF value[i] = 0 THEN CONTINUE; END_IF;
    p := part / value[i] * 100;
    s := INT_TO_STRING(p);
    percent := CONCAT(IN1:=s, IN2:="%");
END_FOR;
```

9.8.10.7 EXIT

Table 9-168 EXIT instruction

SCL	Description
`EXIT;`	An EXIT statement is used to exit a loop (FOR, WHILE or REPEAT) at any point, regardless of whether the terminate condition is satisfied.

The EXIT statement executes according to the following rules:

- This statement causes the repetition statement immediately surrounding the exit statement to be exited immediately.
- Execution of the program is continued after the end of the loop (for example after END_FOR).

Use the EXIT statement within a loop. In nested loops, the EXIT statement returns the processing to the next higher nesting level.

Example: EXIT statement

```
FOR i := 0 TO 10 DO
CASE value[i, 0] OF
    1..10: value [i, 1]:="A";
    11..40: value [i, 1]:="B";
    41..100: value [i, 1]:="C";
ELSE
EXIT;
END_CASE;
END_FOR;
```

9.8.10.8 GOTO

Table 9-169 GOTO statement

SCL	Description

`GOTO JumpLabel;`
`Statement;`
`... ;`
`JumpLabel: Statement;`
	The GOTO statement skips over statements by jumping to a label in the same block. The jump label ("JumpLabel") and the GOTO statement must be in the same block. The name of a jump label can only be assigned once within a block. Each jump label can be the target of several GOTO statements.

It is not possible to jump to a loop section (FOR, WHILE or REPEAT). It is possible to jump from within a loop.

Example: GOTO statement

In the following example: Depending on the value of the "Tag_value" operand, the execution of the program resumes at the point defined by the corresponding jump label. If "Tag_value" equals 2, the program execution resumes at the jump label "MyLabel2" and skips "MyLabel1".

```
CASE "Tag_value" OF
1 : GOTO MyLabel1;
2 : GOTO MyLabel2;
ELSE GOTO MyLabel3;
END_CASE;
MyLabel1: "Tag_1" := 1;
MyLabel2: "Tag_2" := 1;
MyLabel3: "Tag_4" := 1;
```

9.8.10.9 RETURN

Table 9-170 RETURN instruction

SCL	Description
`RETURN;`	The Return instruction exits the code block being executed without conditions. Program execution returns to the calling block or to the operating system (when exiting an OB).

Example: RETURN instruction:

```
IF "Error" <> 0 THEN
RETURN;
END_IF;
```

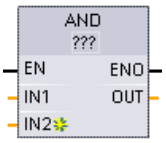
NOTE

After executing the last instruction, the code block automatically returns to the calling block. Do not insert a RETURN instruction at the end of the code block.

9.9 Word logic operations

9.9.1 AND, OR, and XOR logic operation instructions

Table 9-171 AND, OR, and XOR logic operation instructions

LAD / FBD	SCL	Description
	**out := in1 AND in2;**	AND: Logical AND
	out := in1 OR in2;	OR: Logical OR
	out := in1 XOR in2;	XOR: Logical EXCLUSIVE OR

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

To add an input, click the "Create" icon or right-click on an input stub for one of the existing IN parameters and select the "Insert input" command.

To remove an input, right-click on an input stub for one of the existing IN parameters (when there are more than the original two inputs) and select the "Delete" command.

Table 9-172 Data types for the parameters

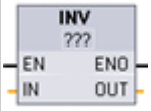
Parameter	Data type	Description
IN1, IN2	Byte, Word, DWord	Logical inputs
OUT	Byte, Word, DWord	Logical output

[1] The data type selection sets parameters IN1, IN2, and OUT to the same data type.

The corresponding bit values of IN1 and IN2 are combined to produce a binary logic result at parameter OUT. ENO is always TRUE following the execution of these instructions.

9.9.2 INV (Create ones complement)

Table 9-173 INV instruction

LAD / FBD	SCL	Description
	**Not available**	Calculates the binary one's complement of the parameter IN. The one's complement is formed by inverting each bit value of the IN parameter (changing each 0 to 1 and each 1 to 0). ENO is always TRUE following the execution of this instruction.

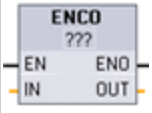
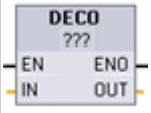
[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-174 Data types for the parameters

Parameter	Data type	Description
IN	SInt, Int, DInt, USInt, UInt, UDInt, Byte, Word, DWord	Data element to invert
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Byte, Word, DWord	Inverted output

9.9.3 DECO (Decode) and ENCO (Encode) instructions

Table 9-175 ENCO and DECO instruction

LAD / FBD	SCL	Description
	**out := ENCO(_in_);**	Encodes a bit pattern to a binary number The ENCO instruction converts parameter IN to the binary number corresponding to the bit position of the least-significant set bit of parameter IN and returns the result to parameter OUT. If parameter IN is either 0000 0001 or 0000 0000, then a value of 0 is returned to parameter OUT. If the parameter IN value is 0000 0000, then ENO is set to FALSE.
	**out := DECO(_in_);**	Decodes a binary number to a bit pattern The DECO instruction decodes a binary number from parameter IN, by setting the corresponding bit position in parameter OUT to a 1 (all other bits are set to 0). ENO is always TRUE following execution of the DECO instruction. Note: The default data type for the DECO instruction is DWORD. In SCL, change the instruction name to DECO_BYTE or DECO_WORD to decode a byte or word value, and assign to a byte or word tag or address.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

Table 9-176 Data types for the parameters

Parameter	Data type	Description
IN	ENCO: Byte, Word, DWord DECO: UInt	ENCO: Bit pattern to encode DECO: Value to decode
OUT	ENCO: Int DECO: Byte, Word, DWord	ENCO: Encoded value DECO: Decoded bit pattern

Table 9-177 ENO status

ENO	Condition	Result (OUT)
1	No error	Valid bit number
0	IN is zero	OUT is set to zero

The DECO parameter OUT data type selection of a Byte, Word, or DWord restricts the useful range of parameter IN. If the value of parameter IN exceeds the useful range, then a modulo operation is performed to extract the least significant bits shown below.

DECO parameter IN range:

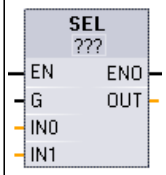
- 3 bits (values 0-7) IN are used to set 1 bit position in a Byte OUT
- 4-bits (values 0-15) IN are used to set 1 bit position in a Word OUT
- 5 bits (values 0-31) IN are used to set 1 bit position in a DWord OUT

Table 9-178 Examples

DECO IN value			DECO OUT value (Decode single bit position)
Byte OUT 8 bits	Min. IN	0	00000001
	Max. IN	7	10000000
Word OUT 16 bits	Min. IN	0	0000000000000001
	Max. IN	15	1000000000000000
DWord OUT 32 bits	Min. IN	0	00000000000000000000000000000001
	Max. IN	31	10000000000000000000000000000000

9.9.4 SEL (Select), MUX (Multiplex), and DEMUX (Demultiplex) instructions

Table 9-179 SEL (select) instruction

LAD / FBD	SCL	Description
	**out := SEL(** **g:=_bool_in,** **in0:-_variant_in,** **in1:=_variant_in);**	SEL assigns one of two input values to parameter OUT, depending on the parameter G value.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

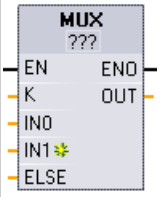
Table 9-180 Data types for the SEL instruction

Parameter	Data type [1]	Description
G	Bool	• 0 selects IN0 • 1 selects IN1
IN0, IN1	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, Char, WChar	Inputs
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, Char, WChar	Output

[1] Input variables and the output variable must be of the same data type.

Condition codes: ENO is always TRUE following execution of the SEL instruction.

Table 9-181 MUX (multiplex) instruction

LAD / FBD	SCL	Description
	**out := MUX(** **k:=_unit_in,** **in1:=variant_in,** **in2:=variant_in,** **[...in32:=variant_in,]** **inelse:=variant_in);**	MUX copies one of many input values to parameter OUT, depending on the parameter K value. If the parameter K value exceeds (IN*n* - 1), then the parameter ELSE value is copied to parameter OUT.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

To add an input, click the "Create" icon or right-click on an input stub for one of the existing IN parameters and select the "Insert input" command.

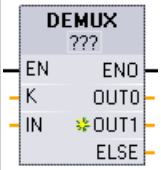
To remove an input, right-click on an input stub for one of the existing IN parameters (when there are more than the original two inputs) and select the "Delete" command.

Table 9-182 Data types for the MUX instruction

Parameter	Data type	Description
K	UInt	• 0 selects IN1 • 1 selects IN2 • *n* selects IN*n*
IN0, IN1, .. INn	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, Char, WChar	Inputs
ELSE	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, Char, WChar	Input substitute value (optional)
OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, Char, WChar	Output

[1] Input variables and the output variable must be of the same data type.

Table 9-183 DEMUX (Demultiplex) instruction

LAD / FBD	SCL	Description
	**DEMUX(** **k:=_unit_in,** **in:=variant_in,** **out1:=variant_in,** **out2:=variant_in,** **[...out32:=variant_in,]** **outelse:=variant_in);**	DEMUX copies the value of the location assigned to parameter IN to one of many outputs. The value of the K parameter selects which output selected as the destination of the IN value. If the value of K is greater than the number (OUT*n* - 1) then the IN value is copied to location assigned to the ELSE parameter.

[1] For LAD and FBD: Click the "???" and select a data type from the drop-down menu.

To add an output, click the "Create" icon or right-click on an output stub for one of the existing OUT parameters and select the "Insert output" command.

To remove an output, right-click on an output stub for one of the existing OUT parameters (when there are more than the original two outputs) and select the "Delete" command.

Table 9-184 Data types for the DEMUX instruction

Parameter	Data type [1]	Description
K	UInt	Selector value: • 0 selects OUT1 • 1 selects OUT2 • n selects OUTn
IN	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, Char, WChar	Input
OUT0, OUT1, .. OUTn	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, Char, WChar	Outputs
ELSE	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal, Byte, Word, DWord, Time, Date, TOD, Char, WChar	Substitute output when K is greater than (OUTn - 1)

[1] The input variable and the output variables must be of the same data type.

Table 9-185 ENO status for the MUX and DEMUX instructions

ENO	Condition	Result OUT
1	No error	MUX: Selected IN value is copied to OUT DEMUX: IN value is copied to selected OUT
0	MUX: K is greater than the number of inputs -1	• No ELSE provided: OUT is unchanged, • ELSE provided, ELSE value assigned to OUT
	DEMUX: K is greater than the number of outputs -1	• No ELSE provided: outputs are unchanged, • ELSE provided, IN value copied to ELSE

9.10 Shift and rotate

9.10.1 SHR (Shift right) and SHL (Shift left) instructions

Table 9-186 SHR and SHL instructions

LAD / FBD	SCL	Description
	out := SHR(**in:=_variant_in_,** **n:=_uint_in);** **out := SHL(** **in:=_variant_in_,** **n:=_uint_in);**	Use the shift instructions (SHL and SHR) to shift the bit pattern of parameter IN. The result is assigned to parameter OUT. Parameter N specifies the number of bit positions shifted: • SHR: Shift bit pattern right • SHL: Shift bit pattern left

[1] For LAD and FBD: Click the "???" and select the data types from the drop-down menu.

Table 9-187 Data types for the parameters

Parameter	Data type	Description
IN	Integers	Bit pattern to shift
N	USInt, UDint	Number of bit positions to shift
OUT	Integers	Bit pattern after shift operation

- For N=0, no shift occurs. The IN value is assigned to OUT.
- Zeros are shifted into the bit positions emptied by the shift operation.
- If the number of positions to shift (N) exceeds the number of bits in the target value (8 for Byte, 16 for Word, 32 for DWord), then all original bit values will be shifted out and replaced with zeros (zero is assigned to OUT).
- ENO is always TRUE for the shift operations.

Table 9-188 Example: SHL for Word data

Shift the bits of a Word to the left by inserting zeroes from the right (N = 1)			
IN	1110 0010 1010 1101	OUT value before first shift:	1110 0010 1010 1101
		After first shift left:	1100 0101 0101 1010
		After second shift left:	1000 1010 1011 0100
		After third shift left:	0001 0101 0110 1000

9.10.2 ROR (Rotate right) and ROL (Rotate left) instructions

Table 9-189 ROR and ROL instructions

LAD / FBD	SCL	Description
	out := ROL(**in:=_variant_in_,** **n:=_uint_in);** **out := ROR(** **in:=_variant_in_,** **n:=_uint_in);**	Use the rotate instructions (ROR and ROL) to rotate the bit pattern of parameter IN. The result is assigned to parameter OUT. Parameter N defines the number of bit positions rotated. • ROR: Rotate bit pattern right • ROL: Rotate bit pattern left

[1] For LAD and FBD: Click the "???" and select the data types from the drop-down menu.

Table 9-190 Data types for the parameters

Parameter	Data type	Description
IN	Integers	Bit pattern to rotate
N	USInt, UDint	Number of bit positions to rotate
OUT	Integers	Bit pattern after rotate operation

- For N=0, no rotate occurs. The IN value is assigned to OUT.
- Bit data rotated out one side of the target value is rotated into the other side of the target value, so no original bit values are lost.
- If the number of bit positions to rotate (N) exceeds the number of bits in the target value (8 for Byte, 16 for Word, 32 for DWord), then the rotation is still performed.
- ENO is always TRUE following execution of the rotate instructions.

Table 9-191 Example: ROR for Word data

Rotate bits out the right -side into the left -side (N = 1)			
IN	0100 0000 0000 0001	OUT value before first rotate:	0100 0000 0000 0001
		After first rotate right:	1010 0000 0000 0000
		After second rotate right:	0101 0000 0000 0000

Extended instructions 10

10.1 Date, time-of-day, and clock functions

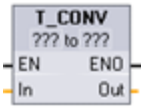
10.1.1 Date and time-of-day instructions

Use the date and time instructions for calendar and time calculations.

- T_CONV converts a value to or from (date and time data types) and (byte, word, and dword size data types)
- T_ADD adds Time and DTL values: (Time + Time = Time) or (DTL + Time = DTL)
- T_SUB subtracts Time and DTL values: (Time - Time = Time) or (DTL - Time = DTL)
- T_DIFF provides the difference between two DTL values as a Time value: DTL - DTL = Time
- T_COMBINE combines a Date value and a Time_and_Date value to create a DTL value

For information about the format of DTL and Time data, refer to the section on the Time and Date data types (Page 98).

Table 10-1 T_CONV (Convert times and extract) instruction

LAD / FBD	SCL example	Description
	**out := DINT_TO_TIME(in:=_variant_in);** **out := TIME_TO_DINT(in:=_variant_in);**	T_CONV converts a value to or from (date and time data types) and (byte, word, and dword size data types).

[1] For LAD and FBD boxes: Click "???" and select the source/target data types from the drop-down menu.

[2] For SCL: Drag T_CONV from instruction tree and drop into the program editor, then select the source/target data types.

Table 10-2 Valid data types for T_CONV conversions

Data type IN (or OUT)	Data types OUT (or IN)
TIME (milliseconds)	DInt, Int, SInt, UDInt, UInt, USInt, TOD SCL only: Byte, Word, Dword
DATE (number of days since Jan. 1 1990)	DInt, Int, SInt, UDInt, UInt, USInt, DTL SCL only: Byte, Word, Dword
TOD (milliseconds since midnight- 24:00:00.000)	DInt, Int, SInt, UDInt, UInt, USInt, TIME, DTL SCL only: Byte, Word, Dword

NOTE

Using T_CONV to convert a larger data size to a smaller data size

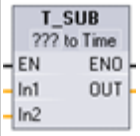
Data values can be truncated when you convert a larger data type with more bytes to a smaller data type with less bytes. If this error occurs, then ENO is set to 0.

Conversion to/from DTL data type

DTL (Date and Time Long) contains year, month, date, and time data. DTL data can be converted to/from DATE and TOD data types.
However, DTL conversion with DATE data only affects the year, month, and day values. DTL conversion with TOD data only affects the hour, minutes, and seconds values.

When T_CONV converts to DTL, the unaffected data elements in the DTL format are left unchanged.

Table 10-3 T_ADD (Add times) and T_SUB (Subtract times) instructions

LAD / FBD	SCL	Description
	out := T_ADD(in1:=_variant_in, in2:=_time_in);	T_ADD adds the input IN1 value (DTL or Time data types) with the input IN2 Time value. Parameter OUT provides the DTL or Time value result. Two data type operations are possible: • Time + Time = Time • DTL + Time = DTL
	**out := T_SUB(in1:=_variant_in, in2:=_time_in);**	T_SUB subtracts the IN2 Time value from IN1 (DTL or Time value). Parameter OUT provides the difference value as a DTL or Time data type. Two data type operations are possible. • Time - Time = Time • DTL - Time = DTL

[1] For LAD and FBD: Click the "???" and select the data types from the drop-down menu.

Table 10-4 Data types for the T_ADD and T_SUB parameters

Parameter and type		Data type	Description
IN1[1]	IN	DTL, Time	DTL or Time value
IN2	IN	Time	Time value to add or subtract
OUT	OUT	DTL, Time	DTL or Time sum or difference

[1] Select the IN1 data type from the drop-down list available below the instruction name. The IN1 data type selection also sets the data type of parameter OUT.

Table 10-5 T_DIFF (Time difference) instruction

LAD / FBD	SCL	Description
	out := T_DIFF(in1:=_DTL_in, in2:=_DTL_in);	T_DIFF subtracts the DTL value (IN2) from the DTL value (IN1). Parameter OUT provides the difference value as a Time data type. • DTL - DTL = Time

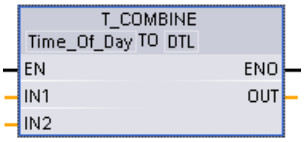
Table 10-6 Data types for the T_DIFF parameters

Parameter and type		Data type	Description
IN1	IN	DTL	DTL value
IN2	IN	DTL	DTL value to subtract
OUT	OUT	Time	Time difference

Condition codes: ENO = 1 means no error occurred. ENO = 0 and parameter OUT = 0 errors:

- Invalid DTL value
- Invalid Time value

Table 10-7 T_COMBINE (Combine times) instruction

LAD / FBD	SCL	Description
	**out := CONCAT_DATE_TOD(In1 := _date_in, In2 := _tod_in);**	T_COMBINE combines a Date value and a Time_of_Day value to create a DTL value.

[1] Note that the T_COMBINE instruction in the Extended Instructions equates to the CONCAT_DATE_TOD function in SCL.

Table 10-8 Data types for the T_COMBINE parameters

Parameter and type		Data type	Description
IN1	IN	Date	Date value to be combined must be between DATE#1990-01-01 and DATE#2089-12-31
IN2	IN	Time_of_Day	Time_of_Day values to be combined
OUT	OUT	DTL	DTL value

10.1.2 Clock functions

WARNING

Risk of attacker accessing your networks through Network Time Protocol (NTP) synchronization

If an attacker can access your networks through Network Time Protocol (NTP) synchronization, the attacker can possibly disrupt control of your process by shifting the CPU system time.

The NTP client feature of the S7-1200 CPU is disabled by default, and, when enabled, only allows configured IP addresses to act as an NTP server. The CPU disables this feature by default, and you must configure this feature to allow remotely-controlled CPU system time corrections.

The S7-1200 CPU supports "time of day" interrupts and clock instructions that depend upon accurate CPU system time. If you configure NTP and accept time synchronization from a server, you must ensure that the server is a trusted source. Failure to do so can cause a security breach that allows an unknown user to disrupt control of your process by shifting the CPU system time.

Disruptions to process control can possibly cause death, severe injury, or property damage.

For security information and recommendations, see the "Operational Guidelines" white paper on the Siemens Industrial Cybersecurity Web site (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

Use the clock instructions to set and read the CPU system clock. The data type DTL (Page 98) is used to provide date and time values.

Table 10-9 System time instructions

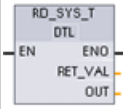
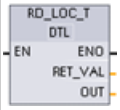
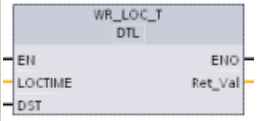
LAD / FBD	SCL	Description
	ret_val := WR_SYS_T(in:=_DTL_in_);	WR_SYS_T (Set time-of-day) sets the CPU time of day clock with a DTL value at parameter IN. This time value does not include local time zone or daylight saving time offsets.
	**ret_val := RD_SYS_T(out=>_DTL_out);**	RD_SYS_T (Read time-of-day) reads the current system time from the CPU. This time value does not include local time zone or daylight saving time offsets.
	**ret_val := RD_LOC_T(out=>_DTL_out);**	RD_LOC_T (Read local time) provides the current local time of the CPU as a DTL data type. This time value reflects the local time zone adjusted appropriately for daylight saving time (if configured).
	**ret_val := WR_LOC_T(LOCTIME:=DTL_in_, DST:_in_;**	WR_LOC_T (Write local time) sets the date and time of the CPU clock. You assign the date and time information as local time at LOCTIME with DTL data type. The instruction uses the "TimeTransformationRule (Page 297)" DB structure to calculate the system time. The granularity of the time information for local time and system time is product-specific and is at least one millisecond. Input values at the LOCTIME parameter which are less than those supported by the CPU are rounded up during system time calculation. **Note**: You must use the CPU device configuration to set the "Time of day" properties (time zone, DST activation, DST start, and DST stop). Otherwise, WR_LOC_T cannot interpret the DST time change.

Table 10-10 Data types for the parameters

Parameter and type		Data type	Description
IN	IN	DTL	Time of day to set in the CPU system clock
OUT	OUT	DTL	RD_SYS_T: Current CPU system time RD_LOC_T: Current local time, including any adjustment for daylight saving time, if configured
LOCTIME	IN	DTL	WR_LOC_T: Local time
DST	IN	BOOL	WR_LOC_T: **D**aylight **S**aving **T**ime only evaluated during the "double hour" when the clocks change to daylight saving time. • TRUE = daylight saving time (first hour) • FALSE = standard time (second hour)
RET_VAL	OUT	Int	Execution condition code

- The local time is calculated by using the time zone and daylight saving time offsets that you set in the device configuration general tab "Time of day" parameters.
- Time zone configuration is an offset to UTC or GMT time.
- Daylight saving time configuration specifies the month, week, day, and hour when daylight saving time begins.
- Standard time configuration also specifies the month, week, day, and hour when standard time begins.

- The time zone offset is always applied to the system time value. The daylight saving time offset is only applied when daylight saving time is in effect.

NOTE
Daylight saving and standard start time configuration
The "Time of day" properties for "Start for daylight saving time" of the CPU device configuration must be your local time.

Condition codes: ENO = 1 means no error occurred. ENO = 0 means an execution error occurred, and a condition code is provided at the RET_VAL output.

RET_VAL (W#16#....)	Description
0000	The current local time is in standard time.
0001	Daylight saving time has been configured, and the current local time is in daylight saving time.
8080	Local time not available or LOCTIME value is invalid.
8081	Illegal year value or time value assigned by the LOCTIME parameter is invalid
8082	Illegal month value (byte 2 in DTL format)
8083	Illegal day value (byte 3 in DTL format)
8084	Illegal hour value (byte 5 in DTL format)
8085	Illegal minute value (byte 6 in DTL format)
8086	Illegal second value (byte 7 in DTL format)
8087	Illegal nanosecond value (bytes 8 to 11 in DTL format)
8089	Time value does not exist (hour already passed upon changeover to daylight saving time)
80B0	The real-time clock has failed
80B1	The "TimeTransformationRule" structure has not been defined.

10.1.3 SET_TIMEZONE (Set timezone)

Table 10-11 SET_TIMEZONE instruction

LAD / FBD	SCL	Description
	"SET_TIMEZONE_DB"(REQ:=_bool_in, Timezone:=_struct_in, DONE=>_bool_out_, BUSY=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);	Sets the local time zone and daylight saving parameters that are used to transform the CPU system time to local time.

[1] In the SCL example, "SET_TIMEZONE_DB" is the name of the instance DB.

Table 10-12 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	REQ=1: execute function
Timezone	IN	TimeTransformationRule	Rules for the transformation from system time to local time
DONE	OUT	Bool	Function complete
BUSY	OUT	Bool	Function busy
ERROR	OUT	Bool	Error detected
STATUS	OUT	Word	Function result / error message

To manually configure the time zone parameters for the CPU, use the "Time of day" properties of the "General" tab of the device configuration.

Use the SET_TIMEZONE instruction to set the local time configuration. The parameters of the "TimeTransformationRule" data structure assign the local time zone and timing for automatic switching between standard time and daylight saving time.

NOTE

Effect of the SET_TIMEZONE instruction on flash memory

The SET_TIMEZONE instruction performs write operations in flash memory (internal load memory or memory card). To avoid reducing the lifetime of the flash memory, use the SET_TIMEZONE instruction for infrequent updates.

Condition codes: ENO = 1 means no error occurred. ENO = 0 means an execution error occurred, and a condition code is provided at the STATUS output.

STATUS (W#16#....)	Description
0	No error
7000	No job processing active
7001	Start of job processing. Parameter BUSY = 1, DONE = 0
7002	Intermediate call (REQ irrelevant): Instruction already active; BUSY has the value "1".
808x	Error at x-th component: For example 8084 indicates that DaylightStartWeekif is not a value from 1to 5.

TimeTransformationRule data structure

The changeover rules for standard and daylight saving time are defined in the TimeTransformationRule data structure:

Name		Data type	Description
TimeTransformationRule		STRUCT	
	Bias	INT	Time difference between local time and UTC [minutes] Range: -1439 to 1439
	DaylightBias	INT	Time difference between daylight saving and standard time [minutes] Range: 0 to 120
	DaylightStartMonth	USINT	Month of conversion to daylight saving time Range: 1 to 12

Name		Data type	Description
	DaylightStartWeek	USINT	Week of conversion to daylight saving time 1 = First occurrence of the weekday in the month, ..., 5 = Last occurrence of the weekday in the month
	DaylightStartWeekday	USINT	Weekday of daylight saving time changeover: 1 = Sunday
	DaylightStartHour	USINT	Hour of daylight saving time changeover: Range: 0 to 23
	DaylightStartMinute	USINT	Minute of daylight saving time changeover Range: 0 to 59
	StandardStartMonth	USINT	Month of conversion to standard time Range: 1 to 12
	StandardStartWeek	USINT	Week of conversion to standard time 1 = First occurrence of the weekday in the month, ..., 5 = Last occurrence of the weekday in the month
	StandardStartWeekday	USINT	Weekday of standard time changeover: 1 = Sunday
	StandardStartHour	USINT	Hour of standard time changeover Range: 0 to 23
	StandardStartMinute	USINT	Minute of standard time changeover Range: 0 to 59
	TimeZoneName	STRING[80]	Name of time zone: "(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna"

10.1.4 RTM (Runtime meters)

Table 10-13 RTM instruction

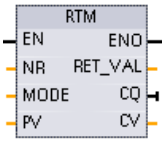
LAD / FBD	SCL	Description
	**RTM(NR:=_uint_in_, MODE:=_byte_in_, PV:=_dint_in_, CQ=>_bool_out_, CV=>_dint_out_);**	The RTM (Runtime Meters) instruction can set, start, stop, and read the runtime hour meters in the CPU.

Table 10-14 Data types for the parameters

Parameter and type		Data type	Description
NR	IN	UInt	Runtime meter number: (possible values: 0..9)
MODE	IN	Byte	RTM Execution mode number: • 0 = Fetch values (the status is then written to CQ and the current value to CV) • 1 = Start (at the last counter value) • 2 = Stop • 4 = Set (to the value specified in PV) • 5 = Set (to the value specified in PV) and then start • 6 = Set (to the value specified in PV) and then stop • 7 = Save all RTM values in the CPU to the SIMATIC MC (memory card)
PV	IN	DInt	Preset hours value for the specified runtime meter

Parameter and type		Data type	Description
RET_VAL	OUT	Int	Function result / error message
CQ	OUT	Bool	Runtime meter status (1 = running)
CV	OUT	DInt	Current runtime hours value for the specified meter

The CPU operates up to 10 runtime hour meters to track the runtime hours of critical control subsystems. You must start the individual hour meters with one RTM execution for each timer. All runtime hour meters are stopped when the CPU makes a run-to-stop transition. You can also stop individual timers with RTM execution mode 2.

When a CPU makes a stop-to-run transition, you must restart the hour timers with one RTM execution for each timer that is started. After a runtime meter value is greater than 2147483647 hours, counting stops and the "Overflow" error is sent. You must execute the RTM instruction once for each timer to reset or modify the timer.

A CPU power failure or power cycle causes a power-down process that saves the current runtime meter values in retentive memory. Upon CPU power-up, the stored runtime meter values are reloaded to the timers and the previous runtime hour totals are not lost. The runtime meters must be restarted to accumulate additional runtime.

Your program can also use RTM execution mode 7 to save the runtime meter values in a memory card. The states of all timers at the instant RTM mode 7 is executed are stored in the memory card. These stored values can become incorrect over time as the hour timers are started and stopped during a program run session. You must periodically update the memory card values to capture important runtime events.

The advantage that you get from storing the RTM values in the memory card is that you can insert the memory card in a substitute CPU where your program and saved RTM values will be available. After you insert the memory card, perform a memory reset or reset to factory defaults to use the saved RTM values. This ensures that the RTM values stored in the memory card are properly loaded and used in the program. If you did not save the RTM values in the memory card, then the timer values would be lost in the substitute CPU.

NOTE

Avoid excessive program calls for memory card write operations

Minimize flash memory card write operations to extend the life of the memory card.

Table 10-15 Condition codes

RET_VAL (W#16#....)	Description
0	No error
8080	Incorrect runtime meter number
8081	A negative value was passed to the parameter PV
8082	Overflow of the operating hours counter
8091	The input parameter MODE contains an illegal value
80B1	Value cannot be saved to memory card (MODE=7)

10.2 String and character

10.2.1 String data overview

String data type

String data is stored as a 2-byte header followed by up to 254 character bytes of ASCII character codes. A String header contains two lengths. The first byte is the maximum length that is given in square brackets when you initialize a string, or 254 by default. The second header byte is the current length that is the number of valid characters in the string. The current length must be smaller than or equal to the maximum length. The number of stored bytes occupied by the String format is 2 bytes greater than the maximum length.

Initialize your String data

String input and output data must be initialized as valid strings in memory, before execution of any string instructions.

Valid String data

A valid string has a maximum length that must be greater than zero but less than 255. The current length must be less than or equal to the maximum length.

Strings cannot be assigned to I or Q memory areas.

For more information see: Format of the String data type (Page 99).

10.2.2 S_MOVE (Move character string)

Table 10-16 String move instruction

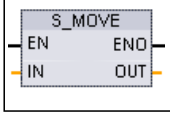
LAD / FBD	SCL	Description
	**out := in;**	Copy the source IN string to the OUT location. S_MOVE execution does not affect the contents of the source string.

Table 10-17 Data types for the parameters

Parameter	Data type	Description
IN	String	Source string
OUT	String	Target address

If the actual length of the string at the input IN exceeds the maximum length of a string stored at output OUT, then the part of the IN string that can fit in the OUT string is copied.

10.2.3 String conversion instructions

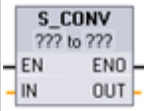
10.2.3.1 S_CONV, STRG_VAL, and VAL_STRG (Convert to/from character string and number) instructions

You can convert number character strings to number values or number values to number character strings with these instructions:

- S_CONV converts (number string to a number value) or (number value to a number string)
- STRG_VAL converts a number string to a number value with format options
- VAL_STRG converts a number value to a number string with format options

S_CONV (convert character string)

Table 10-18 String conversion instruction

LAD / FBD	SCL	Description
	**out := <Type>_TO_<Type>(in);**	Converts a character string to the corresponding value, or a value to the corresponding character string. The S_CONV instruction has no output formatting options. This makes the S_CONV instruction simpler, but less flexible than the STRG_VAL and VAL_STRG instructions.

[1] For LAD / FBD: Click the "???" and select the data type from the drop-down list.

[2] For SCL: Select S_CONV from the Extended Instructions, and answer the prompts for the data types for the conversion. STEP 7 then provides the appropriate conversion instruction.

Table 10-19 Data types (string to value)

Parameter and type		Data type	Description
IN	IN	String, WString	Input character string
OUT	OUT	String, WString, Char, WChar, SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal	Output number value

Conversion of the string parameter IN starts at the first character and continues until the end of the string, or until the first character is encountered that is not "0" through "9", "+", "-", or ".". The result value is provided at the location specified in parameter OUT. If the output number value does not fit in the range of the OUT data type, then parameter OUT is set to 0 and ENO is set to FALSE. Otherwise, parameter OUT contains a valid result and ENO is set to TRUE.

Input String format rules:

- If a decimal point is used in the IN string, you must use the "." character.
- Comma characters "," used as a thousands separator to the left of the decimal point are allowed and ignored.
- Leading spaces are ignored.

S_CONV (value to string conversion)

Table 10-20 Data types (value to string)

Parameter and type		Data type	Description
IN	IN	String, WString, Char, WChar, SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal	Input number value
OUT	OUT	String, WString	Output character string

An integer, unsigned integer, or floating point value IN is converted to the corresponding character string at OUT. The parameter OUT must reference a valid string before the conversion is executed. A valid string consists of a maximum string length in the first byte, the current string length in the second byte, and the current string characters in the next bytes. The converted string replaces characters in the OUT string starting at the first character and adjusts the current length byte of the OUT string. The maximum length byte of the OUT string is not changed.

How many characters are replaced depends on the parameter IN data type and number value. The number of characters replaced must fit within the parameter OUT string length. The maximum string length (first byte) of the OUT string should be greater than or equal to the maximum expected number of converted characters. The following table shows S_CONV value to string conversion examples:

Output String format rules:

- Values written to parameter OUT do not use a leading "+" sign.
- Fixed-point representation is used (no exponential notation).
- The period character "." is used to represent the decimal point when parameter IN is the Real data type.
- Values are right-justified in the output string and are preceded by space characters that fill empty character positions.

Table 10-21 Maximum string lengths for each data type

IN data type	Character positions allocated by S_CONV	Converted string example[1]	Total string length including maximum and current length bytes
USInt	4	"x255"	6
SInt	4	"-128"	6
UInt	6	"x65535"	8
Int	6	"-32768"	8
UDInt	11	"x4294967295"	13
DInt	11	"-2147483648"	13
Real	14	"x-3.402823E+38" "x-1.175495E-38" "x+1.175495E-38" "x+3.402823E+38"	16
LReal	21	"-1.7976931348623E+308" "-2.2250738585072E-308" "+2.2250738585072E-308" "+1.7976931348623E+308"	23

[1] The "x" characters represent space characters that fill empty positions in the right-justified field that is allocated for the converted value.

STRG_VAL (convert character string to numerical value)

Table 10-22 String-to-value instruction

LAD / FBD	SCL	Description
	"STRG_VAL"(in:=_string_in, format:=_word_in, p:=uint_in, out=>_variant_out);	Converts a number character string to the corresponding integer or floating point representation.

[1] For LAD / FBD: Click the "???" and select the data type from the drop-down list.

Table 10-23 Data types for the STRG_VAL instruction

Parameter and type		Data type	Description
IN	IN	String, WString	The ASCII character string to convert
FORMAT	IN	Word	Output format options
P	IN	UInt, Byte, USInt	IN: Index to the first character to be converted (first character = 1)
OUT	OUT	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal	Converted number value

Conversion begins in the string IN at character offset P and continues until the end of the string, or until the first character is encountered that is not "+", "-", ".", ",", "e", "E", or "0" to "9". The result is placed at the location specified in parameter OUT.

String data must be initialized before execution as a valid string in memory.

The FORMAT parameter for the STRG_VAL instruction is defined below. The unused bit positions must be set to zero.

Table 10-24 Format of the STRG_VAL instruction

Bit 16							Bit 8	Bit 7							Bit 0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	f	r

f = Notation format — 1= Exponential notation
0 = Fixed point notation

r = Decimal point format — 1 = "," (comma character)
0 = "." (period character)

Table 10-25 Values of the FORMAT parameter

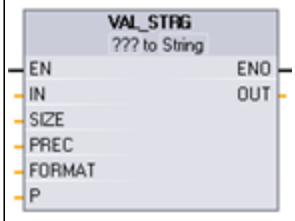
FORMAT (W#16#)	Notation format	Decimal point representation
0000 (default)	Fixed point	"."
0001		","
0002	Exponential	"."
0003		","
0004 to FFFF	Illegal values	

Rules for STRG_VAL conversion:

- If the period character "." is used for the decimal point, then commas "," to the left of the decimal point are interpreted as thousands separator characters. The comma characters are allowed and ignored.
- If the comma character "," is used for the decimal point, then periods "." to the left of the decimal point are interpreted as thousands separator characters. These period characters are allowed and ignored.
- Leading spaces are ignored.

VAL_STRG (convert numerical value to string)

Table 10-26 Value-to-string operation

LAD / FBD	SCL	Description
	**"VAL_STRG"(in:=_variant_in, size:=_usint_in, prec:=_usint_in, format:=_word_in, p:=uint_in, out=>_string_out);**	Converts an integer, unsigned integer, or floating point value to the corresponding character string representation.

[1] For LAD / FBD: Click the "???" and select the data type from the drop-down list.

Table 10-27 Data types for the VAL_STRG instruction

Parameter and type		Data type	Description
IN	IN	SInt, Int, DInt, USInt, UInt, UDInt, Real, LReal	Value to convert
SIZE	IN	USInt	Number of characters to be written to the OUT string
PREC	IN	USInt	The precision or size of the fractional portion. This does not include the decimal point.
FORMAT	IN	Word	Output format options
P	IN	UInt, Byte, USInt	IN: Index to the first OUT string character to be replaced (first character = 1)
OUT	OUT	String, WString	The converted string

This instruction converts the value represented by parameter IN to a string referenced by parameter OUT. The parameter OUT must be a valid string before the conversion is executed.

The converted string replaces characters in the OUT string starting at character offset count P to the number of characters specified by parameter SIZE. The number of characters in SIZE must fit within the OUT string length, counting from character position P. If the SIZE parameter is zero, then the characters overwrite at position P in the OUT string without limitation. This instruction is useful for embedding number characters into a text string. For example, you can put the numbers "120" into the string "Pump pressure = 120 psi".

Parameter PREC specifies the precision or number of digits for the fractional part of the string. If the parameter IN value is an integer, then PREC specifies the location of the decimal point. For example, if the data value is 123 and PREC = 1, then the result is "12.3". The maximum supported precision for the Real data type is 7 digits.

If parameter P is greater than the current size of the OUT string, then spaces are added, up to position P, and the result is appended to the end of the string. The conversion ends if the maximum OUT string length is reached.

The FORMAT parameter for the VAL_STRG instruction is defined below. The unused bit positions must be set to zero.

Table 10-28 Format of the VAL_STRG instruction

Bit 16							**Bit 8**	**Bit 7**							**Bit 0**
0	0	0	0	0	0	0	0	0	0	0	0	0	s	f	r

s = Number sign character	1= use sign character "+" and "-" 0 = use sign character "-" only
f = Notation format	1= Exponential notation 0 = Fixed point notation
r = Decimal point format	1 = "," (comma character) 0 = "." (period character)

Table 10-29 Values of the FORMAT parameter

FORMAT (WORD)	**Number sign character**	**Notation format**	**Decimal point representation**
W#16#0000	"-" only	Fixed point	"."
W#16#0001			","
W#16#0002		Exponential	"."
W#16#0003			","
W#16#0004	"+" and "-"	Fixed Point	"."
W#16#0005			","
W#16#0006		Exponential	"."
W#16#0007			","
W#16#0008 to W#16#FFFF	Illegal values		

Parameter OUT string format rules:

- Leading space characters are added to the leftmost part of the string when the converted string is smaller than the specified size.
- When the FORMAT parameter sign bit is FALSE, unsigned and signed integer data type values are written to the output buffer without the leading "+" sign. The "-" sign is used if required.
  <leading spaces><digits without leading zeroes>'.'<PREC digits>
- When the sign bit is TRUE, unsigned and signed integer data type values are written to the output buffer always with a leading sign character.
  <leading spaces><sign><digits without leading zeroes>'.'<PREC digits>
- When the FORMAT is set to exponential notation, Real data type values are written to the output buffer as:
  <leading spaces><sign><digit> '.' <PREC digits>'E' <sign><digits without leading zero>
- When the FORMAT is set to fixed point notation, integer, unsigned integer, and real data type values are written to the output buffer as:
  <leading spaces><sign><digits without leading zeroes>'.'<PREC digits>

- Leading zeros to the left of the decimal point (except the digit adjacent to the decimal point) are suppressed.
- Values to the right of the decimal point are rounded to fit in the number of digits to the right of the decimal point specified by the PREC parameter.
- The size of the output string must be a minimum of three bytes more than the number of digits to the right of the decimal point.
- Values are right-justified in the output string.

Conditions reported by ENO

When the conversion operation encounters an error, the instruction returns the following results:

- ENO is set to 0.
- OUT is set to 0, or as shown in the examples for string to value conversion.
- OUT is unchanged, or as shown in the examples when OUT is a string.

Table 10-30 ENO status

ENO	Description
1	No error
0	Illegal or invalid parameter; for example, an access to a DB that does not exist
0	Illegal string where the maximum length of the string is 0 or 255
0	Illegal string where the current length is greater than the maximum length
0	The converted number value is too large for the specified OUT data type.
0	The OUT parameter maximum string size must be large enough to accept the number of characters specified by parameter SIZE, starting at the character position parameter P.
0	Illegal P value where P=0 or P is greater than the current string length
0	Parameter SIZE must be greater than parameter PREC.

Table 10-31 Example of S_CONV string to value conversion

IN string	OUT data type	OUT value	ENO
"123"	Int or DInt	123	TRUE
"-00456"	Int or DInt	-456	TRUE
"123.45"	Int or DInt	123	TRUE
"+2345"	Int or DInt	2345	TRUE
"00123AB"	Int or DInt	123	TRUE
"123"	Real	123.0	TRUE
"123.45"	Real	123.45	TRUE
"1.23e-4"	Real	1.23	TRUE
"1.23E-4"	Real	1.23	TRUE
"12,345.67"	Real	12345.67	TRUE
"3.4e39"	Real	3.4	TRUE
"-3.4e39"	Real	-3.4	TRUE
"1.17549e-38"	Real	1.17549	TRUE

IN string	OUT data type	OUT value	ENO
"12345"	SInt	0	FALSE
"A123"	N/A	0	FALSE
""	N/A	0	FALSE
"++123"	N/A	0	FALSE
"+-123"	N/A	0	FALSE

Table 10-32 Examples of S_CONV value to string conversion

Data type	IN value	OUT string [1]	ENO
UInt	123	"xxx123"	TRUE
UInt	0	"xxxxx0"	TRUE
UDInt	12345678	"xxx12345678"	TRUE
Real	+9123.456	"xx+9.123456E+3"	TRUE
LReal	+9123.4567890123	"xx+9.1234567890123E+3"	TRUE
Real	-INF	"xxxxxxxxxxxINF"	FALSE
Real	+INF	"xxxxxxxxxxxINF"	FALSE
Real	NaN	"xxxxxxxxxxxNaN"	FALSE

[1] The "x" characters represent space characters that fill empty positions in the right-justified field that is allocated for the converted value.

Table 10-33 Example: STRG_VAL conversion

IN string	FORMAT (W#16#....)	OUT data type	OUT value	ENO
"123"	0000	Int or DInt	123	TRUE
"-00456"	0000	Int or DInt	-456	TRUE
"123.45"	0000	Int or DInt	123	TRUE
"+2345"	0000	Int or DInt	2345	TRUE
"00123AB"	0000	Int or DInt	123	TRUE
"123"	0000	Real	123.0	TRUE
"-00456"	0001	Real	-456.0	TRUE
"+00456"	0001	Real	456.0	TRUE
"123.45"	0000	Real	123.45	TRUE
"123.45"	0001	Real	12345.0	TRUE
"123.45"	0000	Real	12345.0	TRUE
"123.45"	0001	Real	123.45	TRUE
".00123AB"	0001	Real	123.0	TRUE
"1.23e-4"	0000	Real	1.23	TRUE
"1.23E-4"	0000	Real	1.23	TRUE
"1.23E-4"	0002	Real	1.23E-4	TRUE
"12,345.67"	0000	Real	12345.67	TRUE
"12,345.67"	0001	Real	12.345	TRUE

IN string	FORMAT (W#16#....)	OUT data type	OUT value	ENO
"3.4e39"	0002	Real	+INF	TRUE
"-3.4e39"	0002	Real	-INF	TRUE
"1.1754943e-38" (and smaller)	0002	Real	0.0	TRUE
"12345"	N/A	SInt	0	FALSE
"A123"	N/A	N/A	0	FALSE
""	N/A	N/A	0	FALSE
"++123"	N/A	N/A	0	FALSE
"+-123"	N/A	N/A	0	FALSE

The following examples of VAL_STRG conversions are based on an OUT string initialized as follows:

"`Current Temp = xxxxxxxxxx C`"

where the "`x`" character represents space characters allocated for the converted value.

Table 10-34 Example: VAL_STRG conversion

Data type	IN value	P	SIZE	FORMAT (W#16#....)	PREC	OUT string	ENO
UInt	123	16	10	0000	0	`Current Temp = xxxxxxx123 C`	TRUE
UInt	0	16	10	0000	2	`Current Temp = xxxxxx0.00 C`	TRUE
UDInt	12345678	16	10	0000	3	`Current Temp = x12345.678 C`	TRUE
UDInt	12345678	16	10	0001	3	`Current Temp = x12345,678 C`	TRUE
Int	123	16	10	0004	0	`Current Temp = xxxxxx+123 C`	TRUE
Int	-123	16	10	0004	0	`Current Temp = xxxxxx-123 C`	TRUE
Real	-0.00123	16	10	0004	4	`Current Temp = xxx-0.0012 C`	TRUE
Real	-0.00123	16	10	0006	4	`Current Temp = -1.2300E-3 C`	TRUE
Real	-INF	16	10	N/A	4	`Current Temp = xxxxxx-INF C`	FALSE
Real	+INF	16	10	N/A	4	`Current Temp = xxxxxx+INF C`	FALSE
Real	NaN	16	10	N/A	4	`Current Temp = xxxxxxxNaN C`	FALSE
UDInt	12345678	16	6	N/A	3	`Current Temp = xxxxxxxxxx C`	FALSE

10.2.3.2 Strg_TO_Chars and Chars_TO_Strg (Convert to/from character string and array of CHAR) instructions

Strg_TO_Chars copies an ASCII character string into an array of character bytes.
Chars_TO_Strg copies an array of ASCII character bytes into a character string.

NOTE

You can only use zero-based array types (Array [0..n] of Char) or (Array [0..n] of Byte) for the following:

- Chars input parameter for the Chars_TO_Strg instruction
- Chars IN_OUT parameter for the Strg_TO_Chars instruction

Table 10-35 Strg_TO_Chars instruction

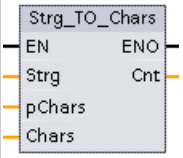
LAD / FBD	SCL	Description
	**Strg_TO_Chars(** **Strg:=_string_in_,** **pChars:=_dint_in_,** **Cnt=>_uint_out_,** **Chars:=_variant_inout_);**	Copies complete input string Strg to an array of characters at IN_OUT parameter Chars The operation overwrites bytes starting at array element number specified by the pChars parameter. Strings of all supported max lengths (1..254) may be used. An end delimiter is not written; this is your responsibility. To set an end delimiter just after the last written array character, use the next array element number [pChars+Cnt].

Table 10-36 Data types for the parameters (Strg_TO_Chars)

Parameter and type		Data type	Description
Strg	IN	String, WString	Source string
pChars	IN	DInt	Array element number for the first string character written to the target array
Chars	IN_OUT	Variant	Pointer to a zero-based array [0..n] of characters copied from the input string The array can be declared in a DB or as local variables in the block interface. Example: "DB1".MyArray points to MyArray [0..10] of Char element values in DB1.
Cnt	OUT	UInt	Count of characters copied

Table 10-37 Chars_TO_Strg instruction

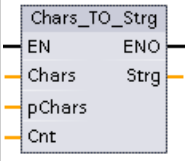
LAD / FBD	SCL	Description
	**Chars_TO_Strg(** **Chars:=_variant_in_,** **pChars:=_dint_in_,** **Cnt:=_uint_in_,** **Strg=>_string_out_);**	Copies all or part of an array of characters to a string The output string must be declared before Chars_TO_Strg is executed. The string is then overwritten by the Chars_TO_Strg operation. Strings of all supported maximum lengths (1..254) may be used. The string maximum length value is not changed by Chars_TO_Strg operation. Copying from array to string stops when the maximum string length is reached. A null character '$00' or 16#00 value in the character array works as a delimiter and ends copying of characters into the string.

Table 10-38 Data types for the parameters (Chars_TO_Strg)

Parameter and type		Data type	Description
Chars	IN	Variant	Pointer to zero based array [0..n] of characters to be converted into a string The array can be declared in a DB or as local variables in the block interface. Example: "DB1".MyArray points to MyArray [0..10] of Char element values in DB1.
pChars	IN	Dint	Element number for the first character in the array to copy Array element [0] is the default value.
Cnt	IN	UInt	Count of characters to copy: 0 means all
Strg	OUT	String, WString	Target string

Table 10-39 ENO status

ENO	Description
1	No error
0	Chars_TO_Strg: Attempt to copy more character bytes to the output string than allowed by the maximum length byte in the string declaration
0	Chars_TO_Strg: Nul character (16#00) value was found in the input character byte array
0	Strg_TO_Chars: Attempt to copy more character bytes to the output array than are allowed by the element number limit

10.2.3.3 ATH and HTA (Convert to/from ASCII string and hexadecimal number) instructions

Use the ATH (ASCII to hexadecimal) and HTA (hexadecimal to ASCII) instructions for conversions between ASCII character bytes (characters 0 to 9 and uppercase A to F only) and the corresponding 4-bit hexadecimal nibbles.

Table 10-40 ATH instruction

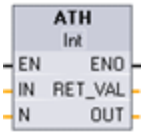
LAD / FBD	SCL	Description
	**ret_val := ATH(in:=_variant_in_, n:=_int_in_, out=>_variant_out_);**	Converts ASCII characters into packed hexadecimal digits.

Table 10-41 Data types for the ATH instruction

Parameter type		Data Type	Description
IN	IN	Variant	Pointer to ASCII character byte array
N	IN	UInt	Number of ASCII character bytes to convert
RET_VAL	OUT	Word	Execution condition code
OUT	OUT	Variant	Pointer to the converted hexadecimal byte array

Conversion begins at the location specified by parameter IN and continues for N bytes. The result is placed at the location specified by OUT. Only valid ASCII characters 0 to 9, lower case a to f, and uppercase A to F can be converted. Any other character will be converted to zero.

8-bit ASCII coded characters are converted to 4-bit hexadecimal nibbles. Two ASCII characters can converted into a single byte containing two 4-bit hexadecimal nibbles.

The IN and OUT parameters specify byte arrays and not hexadecimal String data. ASCII characters are converted and placed in the hexadecimal output in the same order as they are read. If there are an odd number of ASCII characters, then zeros are put in the right-most nibble of the last converted hexadecimal digit.

Table 10-42 Examples: ASCII-to-hexadecimal (ATH) conversion

IN character bytes	N	OUT value	ENO
'0a23'	4	W#16#0A23	TRUE
'123AFx1a23'	10	16#123AF01023	FALSE
'a23'	3	W#16#A230	TRUE

Table 10-43 HTA instruction

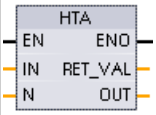
LAD / FBD	SCL	Description
	**ret_val := HTA(in:=_variant_in_, n:=_uint_in_, out=>_variant_out_);**	Converts packed hexadecimal digits to their corresponding ASCII character bytes.

Table 10-44 Data types for the HTA instruction

Parameter and type		Data Type	Description
IN	IN	Variant	Pointer to input byte array
N	IN	UInt	Number of bytes to convert (each input byte has two 4-bit nibbles and produces 2N ASCII characters)
RET_VAL	OUT	Word	Execution condition code
OUT	OUT	Variant	Pointer to ASCII character byte array

Conversion begins at the location specified by parameter IN and continues for N bytes. Each 4-bit nibble converts to a single 8-bit ASCII character and produces 2N ASCII character bytes of output. All 2N bytes of the output are written as ASCII characters 0 to 9 through uppercase A to F. The parameter OUT specifies a byte array and not a string.

Each nibble of the hexadecimal byte is converted into a character in the same order as they are read in (left-most nibble of a hexadecimal digit is converted first, followed by the right-most nibble of that same byte).

Table 10-45 Examples: Hexadecimal -to- ASCII (HTA) conversion

IN value	N	OUT character bytes	ENO (ENO always TRUE after HTA execution)
W#16#0123	2	'0123'	TRUE
DW#16#123AF012	4	'123AF012'	TRUE

Table 10-46 ATH and HTA condition codes

RET_VAL (W#16#....)	Description	ENO
0000	No error	TRUE
0007	Invalid ATH input character: A character was found that was not an ASCII character 0-9, lowercase a to f, or uppercase A to F	FALSE
8101	Illegal or invalid input pointer, for example, an access to a DB that does not exist.	FALSE
8120	Input string is an invalid format, i.e., max= 0, max=255, current>max, or grant length in pointer < max	FALSE
8182	Input buffer is too small for N	FALSE

RET_VAL (W#16#....)	Description	ENO
8151	Data type not allowed for input buffer	FALSE
8301	Illegal or invalid output pointer, for example, an access to a DB that does not exist.	FALSE
8320	Output string is an invalid format, i.e., max= 0, max=255, current>max, or grant length in pointer < max	FALSE
8382	Output buffer is too small for N	FALSE
8351	Data type not allowed for output buffer	FALSE

10.2.4 String operation instructions

10.2.4.1 MAX_LEN (Maximum length of a character string)

Table 10-47 Maximum length instruction

LAD / FBD	SCL	Description
	out := MAX_LEN(in);	MAX_LEN (Maximum length of string) provides the maximum length value assigned to string IN at output OUT. If errors occur during processing of the instruction, then an empty string length will be output. The String and WString data types contain two lengths: the first byte (or word) gives the maximum length and the second byte (or word) gives the current length (this is the current number of valid characters). • The maximum length of the character string is assigned for each String or WString declaration in square brackets. The number of bytes occupied by a String is 2 bytes greater than the maximum length. The number of words occupied by a WString is 2 words greater than the maximum length. • The current length represents the number of the characters actually used. The current length must be less than or equal to the maximum length. The current length is in bytes for a String and in words for a WString. Use the MAX_LEN instruction to get the maximum length of the character string and the LEN instruction to get the current length of a string.

Table 10-48 Data types for the parameters

Parameter and type		Data type	Description
IN	IN	String, WString	Input string
OUT	OUT	DInt	Maximum number of characters allowed for IN string

10.2.4.2 LEN (Determine the length of a character string)

Table 10-49 Length instruction

LAD / FBD	SCL	Description
	out := LEN(in);	LEN (length) provides the current length of the string IN at output OUT. An empty string has a length of zero.

Table 10-50 Data types for the parameters

Parameter and type		Data type	Description
IN	IN	String, WString	Input string
OUT	OUT	Int, DInt, Real, LReal	Number of valid characters of IN string

Table 10-51 ENO status

ENO	Condition	OUT
1	No invalid string condition	Valid string length
0	Current length of IN exceeds maximum length of IN	Current length is set to 0
	Maximum length of IN does not fit within allocated memory range	
	Maximum length of IN is 255 (illegal length)	

10.2.4.3 CONCAT (Combine character strings)

Table 10-52 Concatenate strings instruction

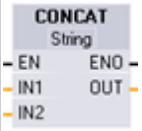
LAD / FBD	SCL	Description
	**out := CONCAT(in1, in2);**	CONCAT (concatenate strings) joins string parameters IN1 and IN2 to form one string provided at OUT. After concatenation, String IN1 is the left part and String IN2 is the right part of the combined string.

Table 10-53 Data types for the parameters

Parameter and type		Data type	Description
IN1	IN	String, WString	Input string 1
IN2	IN	String, WString	Input string 2
OUT	OUT	String, WString	Combined string (string 1 + string 2)

Table 10-54 ENO status

ENO	Condition	OUT
1	No errors detected	Valid characters
0	Resulting string after concatenation is larger than maximum length of OUT string	Resulting string characters are copied until the maximum length of the OUT is reached
	Current length of IN1 exceeds maximum length of IN1, current length of IN2 exceeds maximum length of IN2, or current length of OUT exceeds maximum length of OUT (invalid string)	Current length is set to 0
	Maximum length of IN1, IN2 or OUT does not fit within allocated memory range	
	Maximum length of IN1 or IN2 is 255, or the maximum length of OUT is 0 or 255 (String data type)	
	Maximum length of IN1 or IN2 is 65534, or the maximum length of OUT is 0 or 65534 (WString data type)	

10.2.4.4 LEFT, RIGHT, and MID (Read substrings in a character string) instructions

Table 10-55 Left, right and middle substring operations

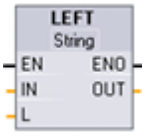
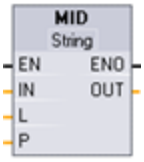
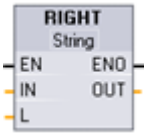
LAD / FBD	SCL	Description
	**out := LEFT(in, L);**	LEFT (Left substring) provides a substring made of the first L characters of string parameter IN. • If L is greater than the current length of the IN string, then the entire IN string is returned in OUT. • If an empty string is the input, then an empty string is returned in OUT.
	**out := MID(in, L, p);**	MID (Middle substring) provides the middle part of a string. The middle substring is L characters long and starts at character position P (inclusive) If the sum of L and P exceeds the current length of the string parameter IN, then a substring is returned that starts at character position P and continues to the end of the IN string.
	**out := RIGHT(in, L);**	RIGHT (Right substring) provides the last L characters of a string. • If L is greater than the current length of the IN string, then the entire IN string is returned in parameter OUT. • If an empty string is the input, then an empty string is returned in OUT.

Table 10-56 Data types for the parameters

Parameter and type		Data type	Description
IN	IN	String, WString	Input string
L	IN	Int	Length of the substring to be created: • LEFT uses the left-most characters number of characters in the string • RIGHT uses the right-most number of characters in the string • MID uses the number of characters starting at position P within the string
P	IN	Int	MID only: Position of first substring character to be copied P= 1, for the initial character position of the IN string
OUT	OUT	String, WString	Output string

Table 10-57 ENO status

ENO	Condition	OUT
1	No errors detected	Valid characters
0	• L or P is less than or equal to 0 • P is greater than maximum length of IN • Current length of IN exceeds maximum length of IN, or current length of OUT exceeds maximum length of OUT • Maximum length of IN or OUT does not fit within allocated memory • Maximum length of IN or OUT is 0 or 255 (String data type) or 0 or 65534 (WString data type)	Current length is set to 0
	Substring length (L) to be copied is larger than maximum length of OUT string.	Characters are copied until the maximum length of OUT is reached
	MID only: L or P is less than or equal to 0	Current length is set to 0
	MID only: P is greater than maximum length of IN	

ENO	Condition	OUT
0	Current length of IN1 exceeds maximum length of IN1, or current length of IN2 exceeds maximum length of IN2 (invalid string)	Current length is set to 0
	Maximum length of IN1, IN2 or OUT does not fit within allocated memory range	
	Maximum length of IN1, IN2 or OUT is illegal length: 0 or 255 (String data type) or 0 or 65534 (WString data type)	

10.2.4.5 DELETE (Delete characters in a character string)

Table 10-58 Delete substring instruction

LAD / FBD	SCL	Description
	out := DELETE(in, L, p);	Deletes L characters from string IN. Character deletion starts at character position P (inclusive), and the remaining substring is provided at parameter OUT. • If L is equal to zero, then the input string is returned in OUT. • If the sum of L and P is greater than the length of the input string, then the string is deleted to the end.

Table 10-59 Data types for the parameters

Parameter and type		Data type	Description
IN	IN	String, WString	Input string
L	IN	Int	Number of characters to be deleted
P	IN	Int	Position of the first character to be deleted: The first character of the IN string is position number 1
OUT	OUT	String, WString	Output string

Table 10-60 ENO status

ENO	Condition	OUT
1	No errors detected	Valid characters
0	P is greater than current length of IN	IN is copied to OUT with no characters deleted
	Resulting string after characters are deleted is larger than maximum length of OUT string	Resulting string characters are copied until the maximum length of OUT is reached
	L is less than 0, or P is less than or equal to 0	Current length is set to 0
	Current length of IN exceeds maximum length of IN, or current length of OUT exceeds maximum length of OUT	
	Maximum length of IN or OUT does not fit within allocated memory	
	Maximum length of IN or OUT is 0 or 255	

10.2.4.6 INSERT (Insert characters in a character string)

Table 10-61 Insert substring instruction

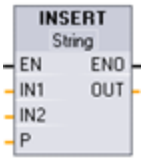
LAD / FBD	SCL	Description
	**out := INSERT(in1, in2, p);**	Inserts string IN2 into string IN1. Insertion begins after the character at position P.

Table 10-62 Data types for the parameters

Parameter and type		Data type	Description
IN1	IN	String, WString	Input string 1
IN2	IN	String, WString	Input string 2
P	IN	Int	Last character position in string IN1 before the insertion point for string IN2 The first character of string IN1 is position number 1.
OUT	OUT	String, WString	Result string

Table 10-63 ENO status

ENO	Condition	OUT
1	No errors detected	Valid characters
0	P is greater than length of IN1	IN2 is concatenated with IN1 immediately following the last IN1 character
	P is less than 0	Current length is set to 0
	Resulting string after insertion is larger than maximum length of OUT string	Resulting string characters are copied until the maximum length of OUT is reached
	Current length of IN1 exceeds maximum length of IN1, current length of IN2 exceeds maximum length of IN2, or current length of OUT exceeds maximum length of OUT (invalid string)	Current length is set to 0
	Maximum length of IN1, IN2 or OUT does not fit within allocated memory range	
	Maximum length of IN1 or IN2 is 255, or maximum length of OUT is 0 or 255 (String data type)	
	Maximum length of IN1 or IN2 is 65534, or maximum length of OUT is 0 or 65534 (WString data type)	

10.2.4.7 REPLACE (Replace characters in a character string)

Table 10-64 Replace substring instruction

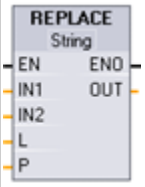
LAD / FBD	SCL	Description
	**out := REPLACE(in1:=_string_in_, in2:=_string_in_, L:=_int_in_, p:=_int_in);**	Replaces L characters in the string parameter IN1. Replacement starts at string IN1 character position P (inclusive), with replacement characters coming from the string parameter IN2.

Table 10-65 Data types for the parameters

Parameter and type		Data type	Description
IN1	IN	String, WString	Input string
IN2	IN	String, WString	String of replacement characters
L	IN	Int	Number of characters to replace
P	IN	Int	Position of first character to be replaced
OUT	OUT	String, WString	Result string

If parameter L is equal to zero, then the string IN2 is inserted at position P of string IN1 without deleting any characters from string IN1.

If P is equal to one, then the first L characters of string IN1 are replaced with string IN2 characters.

Table 10-66 ENO status

ENO	Condition	OUT
1	No errors detected	Valid characters
0	P is greater than length of IN1	IN2 is concatenated with IN1 immediately following the last IN1 character
	P points within IN1, but fewer than L characters remain in IN1	IN2 replaces the end characters of IN1 beginning at position P
	Resulting string after replacement is larger than maximum length of OUT string	Resulting string characters are copied until the maximum length of OUT is reached
	Maximum length of IN1 is 0	IN2 characters are copied to OUT
	L is less than 0, or P is less than or equal to 0	Current length is set to 0
	Current length of IN1 exceeds maximum length of IN1, current length of IN2 exceeds maximum length of IN2, or current length of OUT exceeds maximum length of OUT	
	Maximum length of IN1, IN2 or OUT does not fit within allocated memory range	
	Maximum length of IN1 or IN2 is 255, or maximum length of OUT is 0 or 255 (String data type)	
	Maximum length of IN1 or IN2 is 65534, or maximum length of OUT is 0 or 65534 (WString data type)	

10.2.4.8 FIND (Find characters in a character string)

Table 10-67 Find substring instruction

LAD / FBD	SCL	Description
	out := FIND(**in1:=_string_in_,** **in2:=_string_in);**	Provides the character position of the substring specified by IN2 within the string IN1. The search starts on the left. The character position of the first occurrence of IN2 string is returned at OUT. If the string IN2 is not found in the string IN1, then zero is returned.

Table 10-68 Data types for the parameters

Parameter and type		Data type	Description
IN1	IN	String, WString	Search inside this string
IN2	IN	String, WString	Search for this string
OUT	OUT	Int	Character position in string IN1 of the first search match

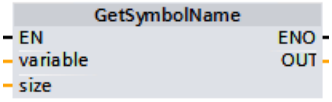
Table 10-69 ENO status

ENO	Condition	OUT
1	No errors detected	Valid character position
0	IN2 is larger than IN1	Character position is set to 0
	Current length of IN1 exceeds maximum length of IN1, or current length of IN2 exceeds maximum length of IN2 (invalid string)	
	Maximum length of IN1 or IN2 does not fit within allocated memory range	
	Maximum length of IN1 or IN2 is 255 (String data type) or 65535 (WString data type)	

10.2.5 Runtime information

10.2.5.1 GetSymbolName (Read out a tag on the input parameter)

Table 10-70 GetSymbolName instruction

LAD / FBD	SCL	Description
	**OUT := GetSymbolName(** **variable:=_parameter_in_,** **size:=_dint_in_);**	The GetSymbolName instruction returns a string corresponding to the name of a variable from the block interface. Your program can call the instruction multiple times with different tags. The process value of the tag is irrelevant. The instruction returns the name read at the OUT parameter.

Parameter

The following table shows the parameters of the GetSymbolName instruction:

Parameter	Declaration	Data type	Memory area	Description
VARIABLE	Input	PARAMETER	Parameter sections Input, Output, InOut	Variable from the local block interface for which you want a string value of the name returned
SIZE	Input	DINT	I, Q, M, D, L	Limits the number of characters output at the OUT parameter: • SIZE > 0: GetSymbolName returns the first SIZE characters of the name. • SIZE = 0: GetSymbolName returns the entire name. • SIZE < 0: GetSymbolName returns the last SIZE characters of the name.
OUT	Return	WSTRING	D, L	Output of the tag name supplied by the input parameter

You specify the input parameters of the block interface at the VARIABLE parameter. Use only an interface parameter for this parameter and not a PLC or data block tag.

To limit the length of the read tag name, use the SIZE parameter. If the instruction truncates the name, it indicates the truncation by the characters "..." (Unicode character 16#2026) appears at the end of the name. Note that this character has the length 1.

You can find additional information on valid data types under "Data types (Page 95)".

Example: Meaning of SIZE parameter

The following example illustrates the meaning of the SIZE parameter. The following tag name is read from the block interface: "MyPLCTag" (The double quotes at the start and end belong to the name.)

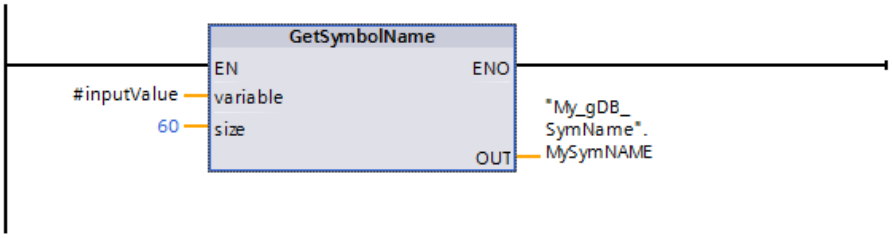
SIZE	GetSymbolName returns	Explanation
1	'...'	• First character of WSTRING:' • Identifier that the name was truncated: ... • Last character of WSTRING:'
2	'"...'	• First character of WSTRING:' • The first character of the name and identifier that the name was truncated:"... • Last character of WSTRING:'
3	'"M...'	• First character of WSTRING:' • The first two characters of the name and identifier that the name was truncated:"... "M... • Last character of WSTRING:'
6	'"MyPL...'	• First character of WSTRING:' • The first five characters of the name and identifier that the name was truncated: "MyPL... • Last character of WSTRING:'
0	'"MyPLCTag"'	• First character of WSTRING:' • All characters of the name: "MyPLCTag" • Last character of WSTRING:'

Example: Reading a symbol name

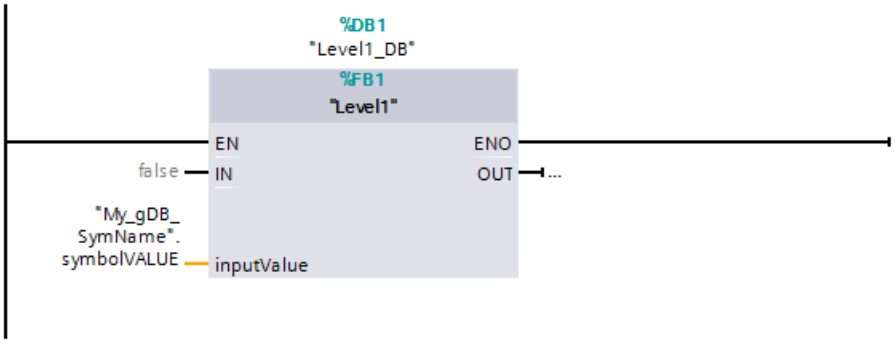
In the following example, you read out the name of a tag that is interconnected via the input parameter of a block.
Create two tags in a global data block for storing the data.

My_gDB_SymName			
	Name	Data type	Start value
1	Static		
2	MySymNAME	WString	WSTRING#''
3	symbolVALUE	Byte	16#42

Create an input parameter inputValue with the BYTE data type in the Level1 block. Call the GetSymbolName instruction in the Level1 block. Interconnect the parameters of the instruction as follows.



Interconnect the inputValue parameter of the Level1 block as follows.

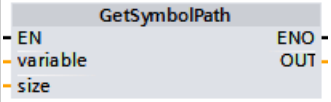


The GetSymbolName instruction is executed in the Level1 block. Input parameter inputValue of the Level1 block is examined for its interconnection using input parameter VARIABLE of the instruction. In doing so, the symbolVALUE tag is read out and output as a character string at output parameter OUT ("MySymNAME"). According to the value of input parameter SIZE, the length of the character string is limited to 60 characters.

My_gDB_SymName				
	Name	Data type	Start value	Monitor value
1	Static			
2	MySymNAME	WString	WSTRING#''	WSTRING#'"My_gDB_SymName".symbolVALUE'
3	symbolVALUE	Byte	16#42	16#42

10.2.5.2 GetSymbolPath (Query composite global name of the input parameter assignment)

Table 10-71 GetSymbolPath instruction

LAD / FBD	SCL	Description
	**OUT := GetSymbolPath(variable:=_parameter_in_, size:=_dint_in_);**	The GetSymbolPath instruction reads the composite global name of an input parameter at the local interface of a block (FB or FC). The name consists of the storage path and the tag name. Your program can call the instruction multiple times with different tags. The process value of the tag is irrelevant. The instruction returns the name read at the OUT parameter.

Parameter

The following table shows the parameters of the GetSymbolPath instruction:

Parameter	Declaration	Data type	Memory area	Description
VARIABLE	Input	PARAMETER	Parameter sections Input, Output, InOut	Selection of the formal parameter for which you want to read out the name of the corresponding actual parameter at the beginning of the call path.
SIZE	Input	DINT	I, Q, M, D, L or constant	Limits the number of characters output at the OUT parameter. • SIZE > 0: GetSymbolPath returns the first SIZE characters of the name. • SIZE = 0: GetSymbolPath returns the entire name. • SIZE < 0: GetSymbolPath returns the last SIZE characters of the name.
OUT	Output	WSTRING	D, L	Output of the tag name of the input parameters supply.

You can find additional information on valid data types under "Data types (Page 95)".

Usage

Note the following tips on using the GetSymbolPath instruction:

- Specify the block interface through which the name of the input tag is read at the VARIABLE parameter of the instruction:
  - If a data block tag supplies the input parameter, GetSymbolPath outputs the name of the DB, contained structures and the name of the tag.
  - If a PLC tag supplies the input parameters GetSymbolPath outputs the name of the PLC tag.
  - If a constant supplies the input parameter, GetSymbolPath outputs the constant value.
- To limit the length of the read tag name, use the SIZE parameter. If the name has been truncated, this is indicated by the character "..." (Unicode character 16#2026) at the end of the name. Note that this character has the length 1.

Example: Meaning of the SIZE parameter

The following example illustrates the meaning of the SIZE parameter. GetSymbolPath has read out the following tag name is read out from the block interface: "MyPLCTag" (The double quotes at the start and end belong to the name.)

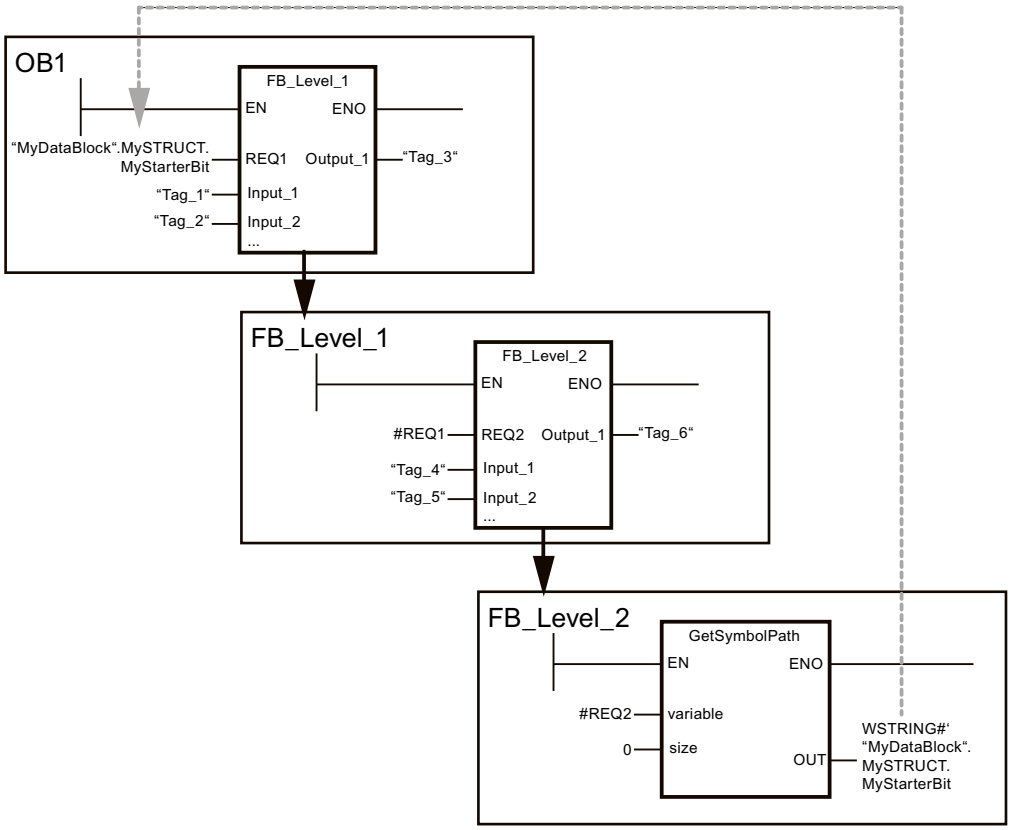
SIZE	GetSymbolPath returns	Explanation
1	'...'	• First character of WSTRING:' • Identifier that the name was truncated: ... • Last character of WSTRING:'
2	'"...'	• First character of WSTRING:' • The first character of the name and identifier that the name was truncated:"... • Last character of WSTRING:'
3	'"M...'	• First character of WSTRING:' • The first two characters of the name and identifier that the name was truncated:"... "M... • Last character of WSTRING:'
6	'"MyPL...'	• First character of WSTRING:' • The first five characters of the name and identifier that the name was truncated: "MyPL... • Last character of WSTRING:'
0	'"MyPLCTag"'	• First character of WSTRING:' • All characters of the name: "MyPLCTag" • Last character of WSTRING:'

Example: Calling GetSymbolPath over multiple block call levels

The following example shows the use of GetSymbolPath over several call levels:

- Organization block OB1 calls the FB_Level_1 block, which in turn calls the FB_Level_2 block.
- The FB_Level_2 block executes GetSymbolPath to read the path of the parameter at the REQ2 interface.
- Since the REQ1 interface supplies REQ2, the instruction determines the path of the input parameter of REQ1.
- The MyStarterBit tag is the REQ1 input parameter. The bit is located in the MySTRUCT structure in the MyDatablock data block.

  GetSymbolPath reads this information and outputs the path ("MyDataBlock".MySTRUCT.MyStarterBit) at the OUT parameter.



10.2.5.3 GetInstanceName (Read out name of the block instance)

Table 10-72 GetInstanceName instruction

LAD / FBD	SCL	Description
GetInstanceName - EN ENO - - size OUT -	**OUT := GetInstanceName(size:=_dint_in_);**	You can use the GetInstanceName instruction to read the name of the instance data block within a function block.

Parameter

The following table shows the parameters of the GetInstanceName instruction:

Parameter	Declaration	Data type	Memory area	Description
SIZE	Input	DINT	I, Q, M, D, L or constant	Limits the number of characters output at the OUT parameter. • SIZE > 0: GetInstanceName returns the first SIZE characters of the name. • SIZE = 0: GetInstanceName returns the entire name. • SIZE < 0: GetInstanceName returns the last SIZE characters of the name.
OUT	Output	WSTRING	D, L	Read name of the instance data block

You can find additional information on valid data types under "Data types (Page 95)".

Example: Meaning of SIZE parameter

To limit the length of the read instance name, use the SIZE parameter. If the instruction has truncated the name, it indicates the truncation by the character "..." (Unicode character 16#2026) at the end of the name. Note that this character has the length 1.

The following example illustrates the meaning of the SIZE parameter. GetInstanceName has read out the following instance name from the block interface: "Level1_DB" (The double quotes at the start and end belong to the name.)

SIZE	GetSymbolPath returns	Explanation
1	'...'	• First character of WSTRING:' • Identifier that the name was truncated: ... • Last character of WSTRING:'
2	'"...'	• First character of WSTRING:' • The first character of the name and identifier that the name was truncated:"... • Last character of WSTRING:'
3	'"L...'	• First character of WSTRING:' • The first two characters of the name and identifier that the name was truncated:"... "L... • Last character of WSTRING:'
6	'"Leve...'	• First character of WSTRING:' • The first five characters of the name and identifier that the name was truncated: "Leve... • Last character of WSTRING:'
0	'"Level1_DB"'	• First character of WSTRING:' • All characters of the name: "Level1_DB" • Last character of WSTRING:'

GetInstanceName writes out the name of the instance data block to the OUT parameter. The instruction truncates the name if the name of the instance data block is longer than the maximum length of WSTRING.

Example: Reading the name of an instance data block

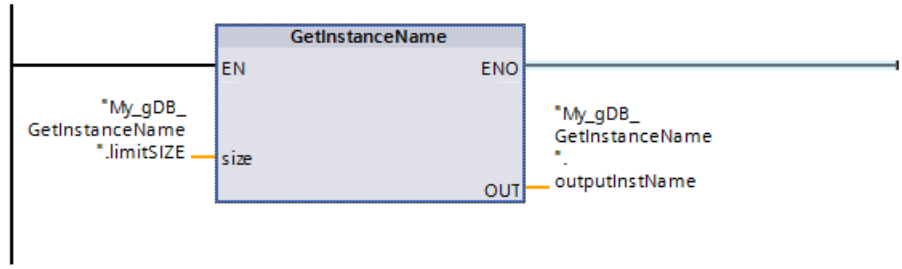
The following example shows how to read out the name of an instance data block.

Create two tags in a global data block for storing the data.

Define the parameters of the instruction as follows.

My_gDB_GetInstanceName				
		Name	Datentyp	Startwert
1		Static		
2		limitSIZE	DInt	0
3		outputInsName	WString	WSTRING#''

The Level1_gin block executes the GetInstanceName instruction, which determines the associated instance data block of the Level1_gin block and outputs the name as a character string at output parameter OUT (outputInstName). According to the value 0 of parameter SIZE (limitSIZE), the length of the character string is unlimited.



My_gDB_GetInstanceName

		Name	Data type	Start value	Monitor value
1		Static			
2		limitSIZE	DInt	0	0
3		outputInstName	WString	WSTRING#''	WSTRING#'"Level1_DB"'

10.2.5.4 GetInstancePath (Query composite global name of the block instance)

Table 10-73 GetInstancePath instruction

LAD / FBD	SCL	Description
GetInstancePath EN ENO size OUT	**OUT := GetInstancePath(size:=_dint_in_);**	You use the GetInstancePath instruction to read the composed global name of the block instance within a function block. The composed global name of the block instance is the path of the complete call hierarchy when the program calls multiple instances.

Parameter

The following table shows the parameters of the GetInstancePath instruction:

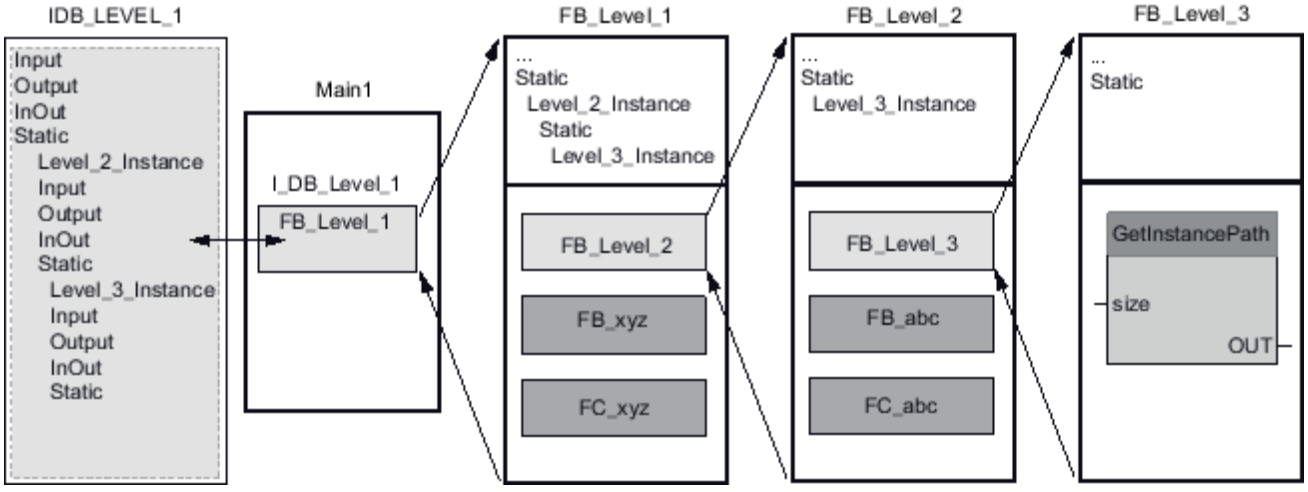
Parameter	Declaration	Data type	Memory area	Description
SIZE	Input	DINT	I, Q, M, D, L or constant	Limits the number of characters output at the OUT parameter. • SIZE > 0: GetInstancePath returns the first SIZE characters of the name. • SIZE = 0: GeInstancePath returns the entire name. • SIZE < 0: GetInstancePath returns the last SIZE characters of the name.
OUT	Output	WSTRING	D, L	Read global name of the block instance. If the global name of the block instance is longer than the maximum length of WSTRING (254 characters), GetInstancePath truncates the name.

You can find additional information on valid data types under "Data types (Page 95)".

Example: Calling GetInstancePath to get the path of a multi-instance FB call

In the following example, the FB_Level_3 function block calls the GetInstancePath instruction.

- The FB_Level_3 function block stores its data in the calling FB_Level_2 function block.
- The FB_Level_2 function block in turn stores its data in the calling FB_Level_1 function block.
- The FB_Level_1 function block in turn stores its data in its instance data block IDB_LEVEL_1. Through the use of multi-instances, the instance data block of FB_Level_1 contains all data of the three function blocks.



The GetInstancePath instruction returns the following values for this example, depending on the value of the SIZE parameter:

SIZE	GetInstancePath returns	Explanation
1	'...'	• First character of WSTRING:' • Identifier that the name was truncated: ... • Last character of WSTRING:'
2	'"...'	• First character of WSTRING:' • The first character of the name and identifier that the name was truncated:"... • Last character of WSTRING:'
3	'"I...'	• First character of WSTRING:' • The first two characters of the name and identifier that the name was truncated:"... "I... • Last character of WSTRING:'
6	'"IDB_...'	• First character of WSTRING:' • The first five characters of the name and identifier that the name was truncated: "IDB_... • Last character of WSTRING:'
0	'"IDB_LEVEL_1".Level_2_Instance.Level_3_Instance'	• First character of WSTRING:' • All characters of the name: "IDB_LEVEL_1".Level_2_Instance.Level_3_Instance • Last character of WSTRING:'

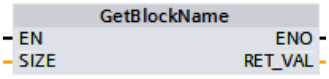
NOTE

Use of GetInstancePath in function blocks with single instance

If the function block in which you call GetInstancePath saves data in its own instance data block, GetInstancePath outputs the name of the single instance as the global name. The result at parameter OUT corresponds in this case to the GetInstanceName (Page 324) instruction.

10.2.5.5 GetBlockName (Read out name of the block)

Table 10-74 GetBlockName instruction

LAD / FBD	SCL	Description
	**RET_VAL := GetBlockName(size:=_dint_in_);**	You use the GetBlockName instruction to read the name of the block in which the instruction is called.

Parameter

The following table shows the parameters of the GetBlockName instruction:

Parameter	Declaration	Data type	Memory area	Description
SIZE	Input	UINT	I, Q, M, D, L or constant	Limits the number of characters output at the RET_VAL parameter. • SIZE > 0: GetBlockName returns the first SIZE characters of the name. • SIZE = 0: GetBlockName returns the entire name. • SIZE < 0: GetBlockName returns the last SIZE characters of the name.
RET_VAL	Output	WSTRING	D, L	Read name of the instance data block

You can find additional information on valid data types under "Data types (Page 95)".

Example: Meaning of the SIZE parameter

To limit the length of the block name to a certain number of characters, specify the maximum length at the SIZE parameter. If GetBlockName truncates the name, it indicates the truncation by the character "..." (Unicode character 16#2026) at the end of the name. Note that this character has the length 1.

The following example illustrates the meaning of the SIZE parameter. GetBlockName has read out the following block name: Level1_gbn (The double quotes at the start and end belong to the name.)

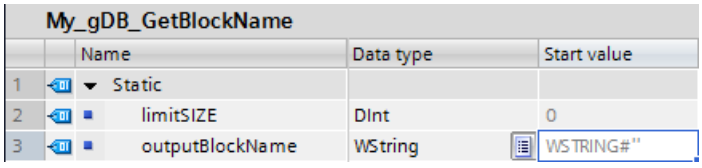
SIZE	GetBlockName returns	Explanation
1	'...'	• First character of WSTRING:' • Identifier that the name was truncated: ... • Last character of WSTRING:'
2	'"...'	• First character of WSTRING:' • The first character of the name and identifier that the name was truncated:"... • Last character of WSTRING:'
3	'"L...'	• First character of WSTRING:' • The first two characters of the name and identifier that the name was truncated:"... "L... • Last character of WSTRING:'
6	'"Leve...'	• First character of WSTRING:' • The first five characters of the name and identifier that the name was truncated: "Leve... • Last character of WSTRING:'
0	'"Level1_gbn"'	• First character of WSTRING:' • All characters of the name: "Level1_gbn" • Last character of WSTRING:'

GetBlockName writes the name of the block at the RET_VAL parameter. If the name of the block is longer than the maximum length of WSTRING, it truncates the name.

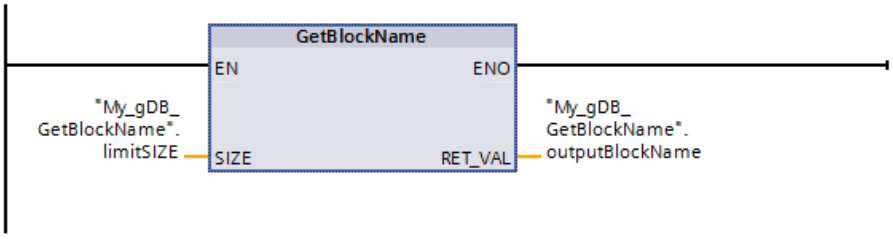
Example: Reading a block name

The following example shows how to read out a block name.

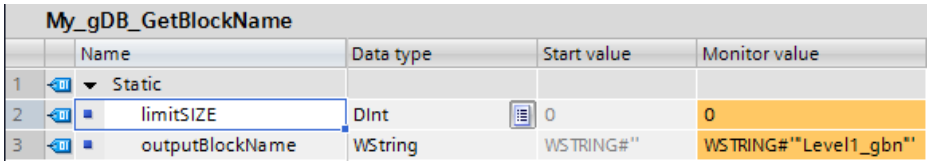
1. Create two tags in a global data block for storing the data.



2. Define the parameters of the instruction as follows:



The Level1_gbn block executes the GetBlockName instruction. GetBlockName reads out the name of the Level1_gbn block and outputs the name as a character string at output parameter RET_VAL(outputBlockName). Because the SIZE parameter is 0 (limitSIZE), the length of the character string is unlimited.



My_gDB_GetBlockName

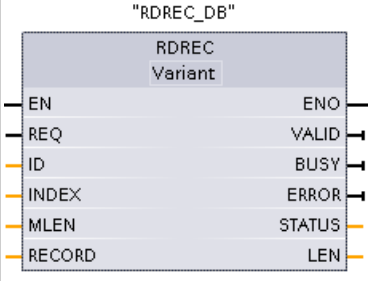
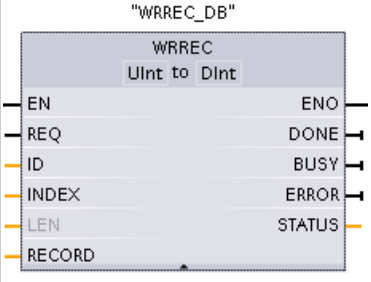
		Name	Data type	Start value	Monitor value
1		Static			
2		limitSIZE	DInt	0	0
3		outputBlockName	WString	WSTRING#''	WSTRING#'"Level1_gbn"'

10.3 Distributed I/O (PROFINET, PROFIBUS, or AS-i)

10.3.1 RDREC and WRREC (Read/write data record)

You can use the RDREC (Read data record) and WRREC (Write data record) instructions with PROFINET, PROFIBUS, and AS-i.

Table 10-75 RDREC and WRREC instructions

LAD / FBD	SCL	Description
	**"RDREC_DB"(** **req:=_bool_in_,** **ID:=_word_in_,** **index:=_dint_in_,** **mlen:=_uint_in_,** **valid=>_bool_out_,** **busy=>_bool_out_,** **error=>_bool_out_,** **status=>_dword_out_,** **len=>_uint_out_,** **record:=_variant_inout_);**	Use the RDREC instruction to read a data record with the number INDEX from the component addressed by the ID, such as a central rack or a distributed component (PROFIBUS DP or PROFINET IO). Assign the maximum number of bytes to read in MLEN. The selected length of the target area RECORD should have at least the length of MLEN bytes.
	**"WRREC_DB"(** **req:=_bool_in_,** **ID:=_word_in_,** **index:=_dint_in_,** **len:=_uint_in_,** **done=>_bool_out_,** **busy=>_bool_out_,** **error=>_bool_out_,** **status=>_dword_out_,** **record:=_variant_inout_);**	Use the WRREC instruction to transfer a data RECORD with the record number INDEX to a DP slave/PROFINET IO device component addressed by ID, such as a module in the central rack or a distributed component (PROFIBUS DP or PROFINET IO). Assign the byte length of the data record to be transmitted. The selected length of the source area RECORD should, therefore, have at least the length of LEN bytes.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL examples, "RDREC_DB" and "WRREC_DB" are the names of the instance DBs.

Table 10-76 RDREC and WRREC data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	REQ = 1: Transfer data record
ID	IN	HW_IO (Word)	Logical address of the DP slave/PROFINET IO component (module or submodule): • For an output module, bit 15 must be set (for example, for address 5: ID:= DW#16#8005). • For a combination module, the smaller of the two addresses should be specified. **Note**: In V3.0, the device ID can be determined in one of two ways: • By making the following "Network view" selections: – Device (gray box) – "Properties" of the device – "Hardware identifier" **Note**: Not all devices display their Hardware identifiers, however. • By making the following "Project tree" menu selections: – PLC tags – Default tag table – System constants tab All configured device Hardware identifiers are displayed. **Note**: In V4.0, the device ID (hardware identifier) for the interface module is determined by going to the tag table and locating the "Device Name [HEAD]" parameter under System Constants.
INDEX	IN	Byte, Word, USInt, UInt, SInt, Int, DInt	Data record number
MLEN	IN	Byte, USInt, UInt	Maximum length in bytes of the data record information to be fetched (RDREC)
VALID	OUT	Bool	New data record was received and valid (RDREC). The VALID bit is TRUE for one scan, after the last request was completed with no error.
DONE	OUT	Bool	Data record was transferred (WRREC). The DONE bit is TRUE for one scan, after the last request was completed with no error.
BUSY	OUT	Bool	• BUSY = 1: The read (RDREC) or write (WRREC) process is not yet terminated. • BUSY = 0: Data record transmission is completed.
ERROR	OUT	Bool	ERROR = 1: A read (RDREC) or write (WRREC) error has occurred. The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	DWord	Block status (Page 345) or error information (Page 473)
LEN	OUT (RDREC) IN (WRREC)	UInt	• Length of the fetched data record information (RDREC) • Maximum byte length of the data record to be transferred (WRREC)
RECORD	IN_OUT	Variant	• Target area for the fetched data record (RDREC) • Data record (WRREC)

The RDREC and WRREC instructions operate asynchronously, that is, processing covers multiple instruction calls. Start the job by calling RDREC or WRREC with REQ = 1.

The job status is displayed via output parameter BUSY and the two central bytes of output parameter STATUS. The transfer of the data record is complete when the output parameter BUSY has been set to FALSE

A value of TRUE (only for one scan) on the output parameter VALID (RDREC) or DONE (WRREC) verifies that the data record has been successfully transferred into the target area RECORD (RDREC) or to the target device (WRREC). In the case of the RDREC, the output parameter LEN contains the length of the fetched data in bytes.

The output parameter ERROR (only for one scan when ERROR = TRUE) indicates that a data record transmission error has occurred. In this case, the output parameter STATUS (only for the one scan when ERROR = TRUE) contains the error information.

Data records are defined by the hardware device manufacturer. Refer to the hardware manufacturer's device documentation for details about a data record.

You can have up to four RDREC instructions and four WRREC instructions in use at the same time.

NOTE

If you configure a DPV1 slave with a GSD file (GSD rev. 3 and higher) and the DP interface of the DP master is set to "S7 compatible", then you might not read any data records from the I/O modules in the user program with "RDREC" or write to the I/O modules with "WRREC". In this case, the DP master addresses the wrong slot (configured slot + 3).

Remedy: set the interface of the DP master to "DPV1".

NOTE

The interfaces of the "RDREC" and "WRREC" instructions are identical to the "RDREC" and "WRREC" FBs defined in "PROFIBUS Guideline PROFIBUS Communication and Proxy Function Blocks according to IEC 61131-3".

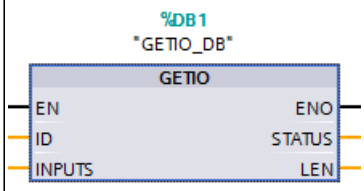
NOTE

If you use "RDREC" or "WRREC" to read or write a data record for PROFINET IO, then the CPU interprets negative values in the INDEX, MLEN, and LEN parameters as unsigned 16-bit integers.

10.3.2 GETIO (Read process image)

You use the instruction "GETIO" to consistently read inputs of modules or submodules of DP slaves and PROFINET IO devices. The instruction "GETIO" calls the instruction "DPRD_DAT (Page 348)". If there is no error during the data transmission, the data that has been read is entered in the destination area indicated by INPUTS.

Table 10-77 GETIO (Read process image) instruction

LAD / FBD	SCL	Description
	**"GETIO_DB"(id:=_uint_in_, status=>_dword_out_, len=>_int_out_, inputs:=_variant_inout_);**	Use the instruction "GETIO" to consistently read out all inputs of a DP standard slave / PROFINET IO device.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "GETIO_DB" is the name of the instance DB.

The destination area must have a length that is greater than or equal to the length of the selected component.
If you read from a DP standard slave with a modular configuration or with several DP identifiers, you only access the data of one component / DP identifier at the configured start address with a "GETIO" call.

Parameters

The following table shows the parameters of the "GETIO" instruction:

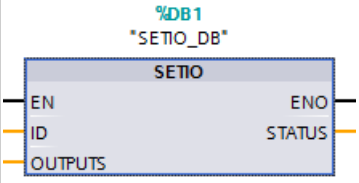
Parameter	Declaration	Data type	Description
ID	IN	HW_SUBMODULE	Hardware ID of the DP standard slave / PROFINET IO device
STATUS[1]	OUT	DWord	Contains the error information of "DPRD_DAT (Page 348)" in the form DW#16#40xxxx00
LEN	OUT	Int	Amount of data read in bytes
INPUTS	IN_OUT	Variant	Destination area for the read data: The destination area must have a length that is greater than or equal to the length of the selected DP standard slave / PROFINET IO device. You can use the following data types: • System data types and array of system data types: BYTE, CHAR, SINT, USINT, WORD, INT, UINT, DWORD, DINT, UDINT, REAL, LREAL, LWORD, LINT • User Defined Types (UDT) • Structures (STRUCT), but only in non-optimized data blocks (DB)

[1] When displaying the "GETIO" error codes, use the DWord data type.

10.3.3 SETIO (Transfer process image)

You use the instruction "SETIO" to consistently transfer data from the source range defined by the OUTPUTS parameter to the addressed modules or submodules of DP slaves and PROFINET IO devices. If you have configured the relevant address area of the DP standard slave / PROFINET IO device as a consistent range in a process image, the data is transferred to the process image. "SETIO" calls the "DPWR_DAT (Page 348)" instruction during this transfer.

Table 10-78 SETIO (Read process image) instruction

LAD / FBD	SCL	Description
	**"SETIO_DB"(id:=_uint_in_, status=>_dword_out_, outputs:=_variant_inout_);**	Use the instruction "SETIO" to consistently transfer data from the source range defined by the parameter OUTPUTS to the addressed DP standard slave / PROFINET IO device.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "SETIO_DB" is the name of the instance DB.

The source range must have a length that is greater than or equal to the length of the selected component.

In the case of a DP standard slave / PROFINET IO device with modular configuration or with several DP identifiers, you can only access one DP identifier / component per "SETIO" call.

Parameters

The following table shows the parameters of the "SETIO" instruction:

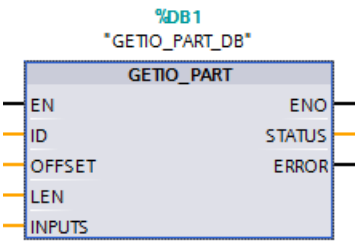
Parameter	Declaration	Data type	Description
ID	IN	HW_SUBMODULE	Hardware ID of the DP standard slave / PROFINET IO device
STATUS[1]	OUT	DWord	Contains the error information of "DPWR_DAT (Page 348)" in the form DW#16#40xxxx00
OUTPUTS	IN_OUT	Variant	Source range for the data to be written: The source range must have a length that is greater than or equal to the length of the selected DP standard slave / PROFINET IO device. You can use the following data types: • System data types and array of system data types: BYTE, CHAR, SINT, USINT, WORD, INT, UINT, DWORD, DINT, UDINT, REAL, LREAL, LWORD, LINT • User Defined Types (UDT) • Structures (STRUCT), but only in non-optimized data blocks (DB)

[1] When displaying the "SETIO"error codes, use the DWord data type.

10.3.4 GETIO_PART (Read process image area)

You use the instruction "GETIO_PART" to consistently read a related part of the inputs of modules or submodules of DP slaves and PROFINET IO devices. GETIO_PART calls the instruction "DPRD_DAT (Page 348)".

Table 10-79 GETIO_PART (Read process image area) instruction

LAD / FBD	SCL	Description
	**"GETIO_PART_DB"(id:=_uint_in_, offset:=_int_in_, len:=_int_in_, status=>_dword_out_, error=>_bool_out_, inputs:=_variant_inout_);**	Use the instruction GETIO_PART to consistently read out a related part of the inputs of an IO module.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "GETIO_PART_DB" is the name of the instance DB.

Use the ID input parameter to select the IO module by means of the hardware ID.

Use the OFFSET and LEN parameters to specify the portion of the process image area to be read. If the input area spanned by OFFSET and LEN is not completely covered by the module, the block returns the error code DW#16#40**80B7**00.

The length of the destination area must be larger than or equal to the amount of bytes to be read:

- If there is no error during the data transmission, ERROR receives the value FALSE. The data that is read is written to the destination area defined at the INPUTS parameter.
- If there is an error during the data transmission, ERROR receives the value TRUE. The STATUS parameter receives the error information from DPRD_DAT.
- If the destination area is greater than LEN, the instruction writes to the first LEN bytes of the destination area. ERROR receives the value FALSE.

Parameters

The following table shows the parameters of the GETIO_PART instruction:

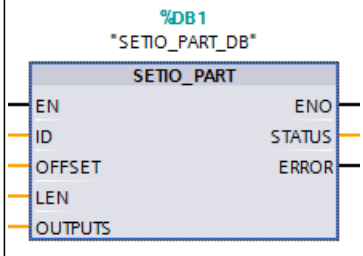
Parameter	Declaration	Data type	Description
ID	IN	HW_SUBMOD-ULE	Hardware identifier of the module
OFFSET	IN	Int	Number of the first byte to be read in the process image for the component (smallest possible value: 0)
LEN	IN	Int	Number of bytes to be read
STATUS[1]	OUT	DWord	Contains the error information of DPRD_DAT (Page 348) in the form DW#16#40xxxx00, if ERROR = TRUE
ERROR	OUT	Bool	Error display: ERROR = TRUE if an error occurs when DPRD_DAT (Page 348) is called
INPUTS	IN_OUT	Variant	Destination area for read data: If the destination area is greater than LEN, the instruction writes to the first LEN bytes of the destination area. You can use the following data types: • System data types and array of system data types: BYTE, CHAR, SINT, USINT, WORD, INT, UINT, DWORD, DINT, UDINT, REAL, LREAL, LWORD, LINT • User Defined Types (UDT) • Structures (STRUCT), but only in non-optimized data blocks (DB)

[1] When displaying the GETIO_PART error codes, use the DWord data type.

10.3.5 SETIO_PART (Transfer process image area)

You can use the "SETIO_PART" instruction to consistently write data from the source area spanned by OUTPUTS to the outputs of modules or submodules of DP slaves and PROFINET IO devices. SETIO_PART calls the instruction "DPWR_DAT (Page 348)".

Table 10-80 SETIO_PART (Transfer process image area) instruction

LAD / FBD	SCL	Description
	**"SETIO_PART_DB"(id:=_uint_in_, offset:=_int_in_, len:=_int_in_, status=>_dword_out_, error=>_bool_out_, outputs:=_variant_inout_);**	Use the instruction SETIO_PART to consistently write data from the source area spanned by OUTPUTS to the outputs of an IO module.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "SETIO_PART_DB" is the name of the instance DB.

With the input parameter ID, you select the I/O module based on the hardware identified.

With the parameters OFFSET and LEN, you assign the portion of the process image area to be written for the component addressed by ID. If the output area spanned by OFFSET and LEN is not completely covered by the module, the block returns the error code DW#16#40**80B7**00.

The length of the destination area must be larger than or equal to the amount of bytes to be read:

- If there is no error during the data transmission, ERROR receives the value FALSE.
- If there is an error during the data transmission, ERROR receives the value TRUE, and STATUS receives the error information of DPWR_DAT.
- If the source area is greater than LEN, the instruction transfers the first LEN bytes from OUTPUTS. ERROR receives the value FALSE.

Parameters

The following table shows the parameters of the SETIO_PART instruction:

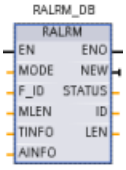
Parameter	Declaration	Data type	Description
ID	IN	HW_SUBMODULE	Hardware identifier of the IO module
OFFSET	IN	Int	Number of the first byte to be written in the process image for the component (smallest possible value: 0)
LEN	IN	Int	Number of bytes to be written
STATUS[1]	OUT	DWord	Contains the error information of DPWR_DAT (Page 348) in the form DW#16#40xxxx00, if ERROR = TRUE
ERROR	OUT	Bool	Error display: ERROR = TRUE if an error occurs when DPWR_DAT (Page 348) is called
OUTPUTS	IN_OUT	Variant	Source range for the data to be written: If the source area is greater than LEN, the first LEN bytes are transferred from OUTPUTS. You can use the following data types: • System data types and array of system data types: BYTE, CHAR, SINT, USINT, WORD, INT, UINT, DWORD, DINT, UDINT, REAL, LREAL, LWORD, LINT • User Defined Types (UDT) • Structures (STRUCT), but only in non-optimized data blocks (DB)

[1] When displaying the SETIO_PART error codes, use the DWord data type.

10.3.6 RALRM (Receive interrupt)

You can use the RALRM (Read alarm) instruction with PROFINET and PROFIBUS.

Table 10-81 RALRM instruction

LAD / FBD	SCL	Description
	**"RALRM_DB"(** **mode:=_int_in_,** **f_ID:=_word_in_,** **mlen:=_uint_in_,** **new=>_bool_out_,** **status=>_dword_out_,** **ID=>_word_out_,** **len=>_uint_out_,** **tinfo:=_variant_inout_,** **ainfo:=_variant_inout_);**	Use the RALRM (read alarm) instruction to read diagnostic interrupt information from PROFIBUS or PROFINET I/O modules/devices. The information in the output parameters contains the start information of the called OB as well as information of the interrupt source. Call RALRM in an interrupt OB to return information regarding the event(s) that caused the interrupt. In the S7-1200. The following Diagnostic OB interrupts are supported: Status, Update, Profile, Diagnostic error interrupt, Pull or plug of modules, Rack or station failure.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "RALRM_DB" is the name of the instance DB.

Table 10-82 Data types for the parameters

Parameter and type		Data type	Description
MODE	IN	Byte, USInt, SInt, Int	Operating mode
F_ID	IN	HW_IO (Word)	Logical start address of the component (module) from which interrupts are to be received **Note**: The device ID can be determined in one of two ways: • By making the following "Network view" selections: – Device (gray box) – "Properties" of the device – "Hardware identifier" **Note**: Not all devices display their Hardware identifiers. • By making the following "Project tree" menu selections: – PLC tags – Default tag table – System constants tab – All configured device Hardware identifiers are displayed.
MLEN	IN	Byte, USInt, UInt	Maximum length in bytes of the data interrupt information to be received. MLEN of 0 will allow receipt of as much data interrupt information as is available in the AINFO Target Area.
NEW	OUT	Bool	A new interrupt was received.
STATUS	OUT	DWord	Status of the RALRM instruction. Refer to "STATUS parameter for RDREC, WRREC, and RALRM" (Page 345) for more information.
ID	OUT	HW_IO (Word)	Hardware identifier of the I/O module that caused the diagnostic interrupt **Note**: Refer to the F_ID parameter for an explanation of how to determine the device ID.
LEN	OUT	DWord, UInt, UDInt, DInt, Real, LReal	Length of the received AINFO interrupt information
TINFO	IN_OUT	Variant	Task information: Target range for OB start and management information. The TINFO length is always 32 bytes.
AINFO	IN_OUT	Variant	Interrupt information: Target area for header information and additional interrupt information. For AINFO, provide a length of at least the MLEN bytes, if MLEN is greater than 0. The AINFO length is variable.

NOTE

If you call "RALRM" in an OB whose start event is not an I/O interrupt, the instruction will provide correspondingly reduced information in its outputs.

Make sure to use different instance DBs when you call "RALRM" in different OBs. If you evaluate data from an "RALRM" call outside of the associated interrupt OB, use a separate instance DB per OB start event.

NOTE

The interface of the "RALRM" instruction is identical to the "RALRM" FB defined in "PROFIBUS Guideline PROFIBUS Communication and Proxy Function Blocks according to IEC 61131-3".

Calling RALRM

You can call the RALRM instruction in three different operating modes (MODE).

Table 10-83 RALRM instruction operating modes

MODE	Description
0	• ID contains the hardware identifier of the I/O module that triggered the interrupt. • Output parameter NEW is set to TRUE. • LEN produces an output of 0. • AINFO and TINFO are not updated with any information.
1	• ID contains the hardware identifier of the I/O module that triggered the interrupt. • Output parameter NEW is set to TRUE. • LEN produces an output of the amount in bytes of AINFO data that is returned. • AINFO and TINFO are updated with interrupt-related information.
2	If the hardware identifier assigned to input parameter F_ID has triggered the interrupt then: • ID contains the hardware identifier of the I/O module that triggered the interrupt. Should be the same as the value at F_ID. • Output parameter NEW is set to TRUE. • LEN produces an output of the amount in bytes of AINFO data that is returned. • AINFO and TINFO are updated with interrupt-related information.

NOTE

If you assign a destination area for TINFO or AINFO that is too short, RALRM cannot return the full information.

MLEN can limit the amount of AINFO data that is returned.

Refer to the AINFO parameters and TINFO parameters of the online information system of STEP 7 for information on how to interpret the TINFO and AINFO data.

TInfo organization block data

The table below shows how the TInfo data is arranged for the RALRM instruction:

Same for OBs: Status, Update, Profile, Diagnostic error interrupt, Pull or plug of modules, Rack or station failure	0	SI_Format	OB_Class	OB_Nr	
	4	LADDR			
TI_Submodule - OBs: Status, Update, Profile	4			Slot	
	8	Specifier		0	
TI_DiagnosticInterrupt - OB: Diagnostic error interrupt	4			IO_State	
	8	Channel		MultiError	0
TI_PlugPullModule - OB: Pull or plug of modules	4			Event_Class	Fault_ID

	8	0		0	
TI_StationFailure - OB: Rack or station failure	4			Event_Class	Fault_ID
	8	0		0	
Same for OBs: Status, Update, Profile, Diagnostic error interrupt, Pull or plug of modules, Rack or station failure	12	0			
	16				
	20	address		slv_prfl	intr_type
	24	flags1	flags2	id	
	28[1]	manufacturer		instance	

[1] Bytes 28 - 31 (manufacturer and instance) are not used with PROFIBUS.

NOTE

Refer to the online information system of STEP 7 for more detailed information on TINFO data.

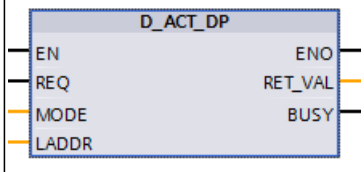
10.3.7 D_ACT_DP (Enable/disable PROFINET IO devices)

With the "D_ACT_DP" instruction, you can disable and enable configured PROFINET IO devices in a targeted manner. In addition, you can determine whether each assigned PROFINET IO device is currently activated or deactivated.

NOTE

You can only use the D_ACT_DP instruction with PROFINET IO devices. You cannot use the instruction with PROFIBUS DP slaves.

Table 10-84 D_ACT_DP instruction

LAD / FBD	SCL	Description
	**"D_ACT_DP_DB"(req:=_bool_in_, mode:=_usint_in_, laddr:=_uint_in_, ret_val=>_int_out_, busy=>_bool_out_);**	Use the D_ACT_DP instruction to disable and enable configured PROFINET IO devices and determine whether each assigned PROFINET IO device is currently activated or deactivated.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "D_ACT_DP_SFB_DB" is the name of the instance DB.

You cannot disable/enable an IE/PB Link PN IO type of gateway using the D_ACT_DP instruction. If you nevertheless use D_ACT_DP on the gateway named, the CPU returns the value W#16#8093 (there is no hardware object that can be activated or deactivated for the address specified in LADDR).

NOTE

The disabling or enabling job requires several runs through the cycle control point. Therefore, you cannot wait for the end of such a job in a programmed loop.

Functional description

D_ACT_DP is an asynchronous instruction, which means that the job processing extends over multiple D_ACT_DP instruction executions. You start the job by calling D_ACT_DP with REQ = 1.

The output parameters RET_VAL and BUSY indicate the status of the job.

Application

If you configure PROFINET IO devices in a CPU which are not actually present or not currently required, the CPU nevertheless continues to access these PROFINET IO devices at regular intervals. After the devices are deactivated, further CPU accessing stops. The corresponding error events no longer occur.

Examples

From a machine OEM's point of view, there are numerous device options possible in series production of machines. However, each delivered machine includes only one combination of selected options.

The manufacturer configures every one of these possible machine options as a PROFINET IO device. The manufacturer does this in order to create and maintain a common user program having all possible options. Use D_ACT_DP to deactivate all PROFINET IO devices not present at machine startup.

A similar situation exists for machine tools having numerous tooling options available, but actually using only a few of them at any given time. These tools are implemented as PROFINET IO devices. With D_ACT_DP, the user program activates the tools currently needed and deactivates those required later.

Identification of a job

If you have started a deactivation or activation job and you call D_ACT_DP again before the job is complete, the behavior of the instruction depends on whether or not the new call involves the same job. If the input parameter LADDR matches, the call is interpreted as a follow-on call.

Deactivating PROFINET IO devices

When you deactivate a PROFINET IO device with D_ACT_DP, its process outputs are set to the configured substitute values or to "0" (safe state). The assigned PROFINET IO controller does not continue to address this component. The error LEDs on the PROFINET IO controller or CPU do not identify the deactivated PROFINET IO devices as faulty or missing.

The CPU updates the process image inputs of deactivated PROFINET IO devices with "0". Therefore, the CPU treats the deactivated PROFINET IO devices just like failed PROFINET IO devices.

If you directly access the user data of a previously deactivated PROFINET IO device from your program, the system behavior depends on the block's error handling selection:

- If global error handling is enabled, the system enters an access error start event into the diagnostics buffer and stays in RUN.
- If block-local error handling is enabled, the system enters an error cause in the error structure. You can access the error cause using the GET_ERROR_ID (Page 276) instruction.

  An error for a read access returns "0". Refer to "Event execution priorities and queuing" (Page 77) for further information on error handling.

If you attempt to access a deactivated PROFINET IO device using an instruction (such as "RD_REC (Page 330)"), you receive the same error information in RET_VAL as for an unavailable PROFINET IO device.

If a PROFINET IO station fails after you have deactivated it with D_ACT_DP, the operating system does not detect the failure.

Activating PROFINET IO devices

When you reactivate a PROFINET IO device with D_ACT_DP, the associated PROFINET IO controller configures the component and assigns parameters (as with the return of a failed PROFINET IO station). This activation is complete when the component is able to transfer user data.

If you try to activate a PROFINET IO device that cannot be accessed (for example, because it was physically separated from the bus) with a D_ACT_DP instruction, the instruction returns the error code W#16#80A7 after expiration of the configured parameter assignment time for distributed I/O. The PROFINET IO device is activated and the fact that the activated PROFINET IO device cannot be accessed results in a corresponding display in the system diagnostics.

If the PROFINET IO device is accessible again afterwards, this results in standard system behavior.

NOTE

Activating a PROFINET IO device can be time-consuming. If you want to cancel a currently running activation job, start D_ACT_DP with the same value for LADDR and MODE = 2. You repeat the call for D_ACT_DP with MODE = 2 until the successful cancellation of the activation job is displayed with RET_VAL = 0.

Parameters

The following table shows the parameters of the D_ACT_DP instruction:

Parameter	Declaration	Data type	Description
REQ	IN	Bool	Level-triggered control parameter REQ = 1: Run activation or deactivation
MODE	IN	USInt	Job identifier Possible values: • 0: Request information on whether the addressed component is activated or deactivated (output using RET_VAL parameter) • 1: Activate the PROFINET IO device • 2: Deactivate the PROFINET IO device
LADDR	IN	HW_DEVICE	Hardware identifier of the PROFINET IO device (HW_Device) The number can be taken from the properties of the PROFINET IO device in the Network view or from the "System constants" tab of the standard tag table. If both the identifier for the device diagnostics as well as the ID for operating state transitions are specified there, you must use the code for the device diagnostics.
RET_VAL	OUT	Int	If an error occurs while the program executes the instruction, the return value contains an error code.
BUSY	OUT	Bool	Active code: • BUSY = 1: The job is still active. • BUSY = 0: The job was terminated.

Parameter RET_VAL

Error code* (W#16#...)	Explanation
0000	Job completed without error.
0001	The PROFINET IO device is active (this error code is only possible with MODE = 0.)
0002	The PROFINET IO device is deactivated (this error code is only possible with MODE = 0.)
7000	First call with REQ = 0: The job specified in LADDR is not active; BUSY has the value "0".
7001	First call with REQ = 1. The program triggered the job specified in LADDR. BUSY has the value "1".
7002	Intermediate call (REQ irrelevant). The activated job is still active; BUSY has the value "1".
8090	• You have not configured a module with the address specified in LADDR. • You operate your CPU as I-slave / I-device, and you have specified an address of this I-slave/I-device in LADDR.
8092	The deactivation of the currently addressed PROFINET IO device (MODE = 2) cannot be canceled by being activated (MODE = 1). Activate the component at a later time.
8093	The address specified in LADDR does not belong to any PROFINET IO device that can be activated or deactivated, or the MODE parameter is unknown.

Error code* (W#16#...)	Explanation
8094	You have attempted to activate a device which is a potential partner for a tool change port. However, another device is already activated on this tool change port at this time. The activated device remains activated.
80A0	Error during the communication between the CPU and the IO controller.
80A1	Parameters cannot be assigned for the addressed component. (This error code is only possible when MODE = 1.) Note: If this component fails again during parameter assignment of the activated device, the D_ACT_DP instruction supplies the error information. If the parameter assignment of a single module is unsuccessful, D_ACT_DP returns the error information W#16#0000.
80A3	The PROFINET IO controller concerned does not support this function.
80A4	The CPU does not support this function for an external PROFINET IO controller.
80A6	Slot error in the PROFINET IO device; not all user data can be accessed (this error code is only available when MODE = 1). Note: D_ACT_DP returns this error information only if the activated component fails again after parameter assignment and before the end of the D_ACT_DP instruction execution. If only a single module is unavailable, D_ACT_DP returns the error information W#16#0000.
80A7	A timeout occurred during activation: The remote device is unreachable, or you have set the parameter assignment time for central and distributed I/O too short. The status of the remote device is "activated", but it is not accessible.
80AA	Activation with errors in the PROFINET IO device: Differences in the configuration
80AB	Activation with errors in the PROFINET IO device: Parameter assignment error
80AC	Activation with errors in the PROFINET IO device: Maintenance required
80C1	D_ACT_DP has started and is being continued with another address (this error code is possible when MODE = 1 and MODE = 2).
80C3	• Temporary resource error: The CPU is currently processing the maximum possible activation and deactivation jobs (8). (This error code is only possible when MODE = 1 and MODE = 2.) • The CPU is busy receiving a modified configuration. Currently, you cannot enable/disable PROFINET IO devices.
80C6	PROFINET: Jobs not collected by the user are discarded at restart.
General error information	See the GET_ERROR_ID (Page 276) instruction for information on how to access the error.
* The error codes in the program editor can be displayed as integer or hexadecimal values.	

10.3.8 STATUS parameter for RDREC, WRREC, and RALRM

The output parameter STATUS contains error information that is interpreted as ARRAY[1...4] OF BYTE, with the following structure:

Table 10-85 STATUS output array

Array element	Name	Description
STATUS[1]	Function_Num	• B#16#00, if no error • Function ID from DPV1-PDU: If an error occurs, B#16#80 is OR'ed (for read data record: B#16#DE; for write data record: B#16#DF). If no DPV1 protocol element is used, then B#16#C0 will be output.
STATUS[2]	Error_Decode	Location of the error ID
STATUS[3]	Error_Code_1	Error ID
STATUS[4]	Error_Code_2	Manufacturer-specific error ID expansion

Table 10-86 STATUS[2] values

Error_decode (B#16#....)	Source	Description
00 to 7F	CPU	No error or no warning
80	DPV1	Error according to IEC 61158-6
81 to 8F	CPU	B#16#8x shows an error in the "xth" call parameter of the instruction.
FE, FF	DP Profile	Profile-specific error

Table 10-87 STATUS[3] values

Error_decode (B#16#....)	Error_code_1 (B#16#....)	Explanation (DVP1)	Description
00	00		No error, no warning
70	00	Reserved, reject	Initial call; no active data record transfer
	01	Reserved, reject	Initial call; data record transfer has started
	02	Reserved, reject	Intermediate call; data record transfer already active
80	90	Reserved, pass	Invalid logical start address
	92	Reserved, pass	Illegal type for Variant pointer
	93	Reserved, pass	The DP component addressed via ID or F_ID is not configured.
	96		The "RALRM (Page 337)" cannot supply the OB start information, management information, header information, or additional interrupt information. For the following OBs, you can use the "DPNRM_DG (Page 355)" instruction to read the current diagnostics message frame of the relevant DP slave asynchronously (address information from OB start information): • Hardware interrupt (Page 69) • Status (Page 74), Update (Page 74) or Profile (Page 75) • Diagnostic error interrupt (Page 71) • Pull or plug of modules (Page 72)
	A0	Read error	Negative acknowledgement while reading from the module
	A1	Write error	Negative acknowledgement while writing to the module

Error_decode (B#16#....)	Error_code_1 (B#16#....)	Explanation (DVP1)	Description
80	A2	Module failure	DP protocol error at layer 2 (for example, slave failure or bus problems)
	A3	Reserved, pass	• PROFIBUS DP: DP protocol error with Direct-Data-Link-Mapper or User-Interface/User • PROFINET IO: General CM error
	A4	Reserved, pass	Communication on the communication bus disrupted
	A5	Reserved, pass	-
	A7	Reserved, pass	DP slave or modules is occupied (temporary error).
	A8	Version conflict	DP slave or module reports non-compatible versions.
	A9	Feature not supported	Feature not supported by DP slave or module
	AA to AF	User specific	DP slave or module reports a manufacturer-specific error in its application. Please check the documentation from the manufacturer of the DP slave or module.
	B0	Invalid index	Data record not known in module; illegal data record number ≥ 256
	B1	Write length error	The length information in the RECORD parameter is incorrect. • With "RALRM": Length error in AINFO **Note**: Refer to the online information system of STEP 7 for immediate access to information on how to interpret the "AINFO" returned buffers. • With "RDREC (Page 330)" and "WRREC (Page 330)": Length error in "MLEN"
	B2	Invalid slot	The configured slot is not occupied.
	B3	Type conflict	Actual module type does not match specified module type.
	B4	Invalid area	DP slave or module reports access to an invalid area.
	B5	Status conflict	DP slave or module not ready
	B6	Access denied	DP slave or module denies access.
	B7	Invalid range	DP slave or module reports an invalid range for a parameter or value.
	B8	Invalid parameter	DP slave or module reports an invalid parameter.
	B9	Invalid type	DP slave or module reports an invalid type: • With "RDREC (Page 330)": Buffer too small (subsets cannot be read) • With "WRREC (Page 330)": Buffer too small (subsets cannot be written)
	BA to BF	User specific	DP slave or module reports a manufacturer-specific error when accessing. Please check the documentation from the manufacturer of the DP slave or module.
	C0	Read constraint conflict	• With "WRREC (Page 330)": The data can only be written when the CPU is in STOP mode. **Note**: This means that data cannot be written by the user program. You can only write the data online with a PG/PC.

Error_decode (B#16#....)	Error_code_1 (B#16#....)	Explanation (DVP1)	Description
80			• With "RDREC (Page 330)": The module routes the data record, but either no data is present or the data can only be read when the CPU is in STOP mode. **Note**: If data can only be read when the CPU is in STOP mode, no evaluation by the user program is possible. In this case, you can only read the data online with a PG/PC.
	C1	Write constraint conflict	The data of the previous write request to the module for the same data record has not yet been processed by the module.
	C2	Resource busy	The module is currently processing the maximum possible number of jobs for a CPU.
	C3	Resource unavailable	The required operating resources are currently occupied.
	C4		Internal temporary error. Job could not be carried out. Repeat the job. If this error occurs often, check your installation for sources of electrical interference.
	C5		DP slave or module not available
	C6		Data record transfer was cancelled due to priority class cancellation.
	C7		Job aborted due to warm or cold restart on the DP master.
	C8 to CF		DP slave or module reports a manufacturer-specific resource error. Please check the documentation from the manufacturer of the DP slave or module.
	Dx	User specific	DP Slave specific. Refer to the description of the DP Slave.
81	00 to FF		Error in the initial call parameter (with "RALRM (Page 337)": MODE)
	00		Illegal operating mode
82	00 to FF		Error in the second call parameter
88	00 to FF		Error in the eighth call parameter (with "RALRM (Page 337)": TINFO) **Note**: Refer to the online information system of STEP 7 for immediate access to information on how to interpret the "TINFO" returned buffers.
	01		Wrong syntax ID
	23		Quantity structure exceeded or destination area too small
	24		Wrong range ID
	32		DB/DI number out of user range
	3A		DB/DI number is NULL for area ID DB/DI, or specified DB/DI does not exist.
89	00 to FF		Error in the ninth call parameter (with "RALRM (Page 337)": AINFO) **Note**: Refer to the online information system of STEP 7 for immediate access to information on how to interpret the "AINFO" returned buffers.
	01		Wrong syntax ID
	23		Quantity structure exceeded or destination area too small

Error_decode (B#16#....)	Error_code_1 (B#16#....)	Explanation (DVP1)	Description
89	24		Wrong range ID
	32		DB/DI number out of user range
	3A		DB/DI number is NULL for area ID DB/DI, or specified DB/DI does not exist.
8A	00 to FF		Error in the 10th call parameter
8F	00 to FF		Error in the 15th call parameter
FE, FF	00 to FF		Profile-specific error

Array element STATUS[4]

With DPV1 errors, the DP Master passes on STATUS[4] to the CPU and to the instruction. Without a DPV1 error, this value is set to 0, with the following exceptions for the RDREC:

- STATUS[4] contains the target area length from RECORD, if MLEN > the destination area length from RECORD.
- STATUS[4]=MLEN, if the actual data record length < MLEN < the destination area length from RECORD.
- STATUS[4]=0, if STATUS[4] > 255; would have to be set

In PROFINET IO, STATUS[4] has the value 0.

10.3.9 Others

10.3.9.1 DPRD_DAT and DPWR_DAT (Read/write consistent data)

Use the DPRD_DAT (Read consistent data) instruction to read one or more bytes of data consistently, and use the DPWR_DAT (Write consistent data) instruction to transfer one or more bytes of data consistently. You can use the DPRD_DAT and DPWR_DAT instructions with PROFINET and PROFIBUS.

Table 10-88 DPRD_DAT and DPWR_DAT instructions

LAD / FBD	SCL	Description
	ret_val := DPRD_DAT(laddr:=_word_in_, record=>_variant_out_);	Use the DPRD_DAT instruction to read one or more bytes of data from modules or submodules of one of the following locations: • Local base I/O • DP slave • PROFINET I/O device The CPU transfers the data read consistently. If no errors occur during the data transfer, the CPU enters the read data into the target area set up by the RECORD parameter. The target area must have the same length as you configured with STEP 7 for the selected module. When you execute the DPRD_DAT instruction, you can only access the data of one module or submodule. The transfer starts at the configured start address.

LAD / FBD	SCL	Description
DPWR_DAT EN — ENO LADDR — RET_VAL RECORD	**ret_val := DPWR_DAT(laddr:=_word_in_, record:=_variant_in_);**	Use the DPWR_DAT instruction to transfer the data in RECORD consistently to the following locations: • Addressed module or submodule in the local base • DP standard slave • PROFINET I/O device The source area must have the same length as you configured with STEP 7 for the selected module or submodule.

- The S7-1200 CPU supports consistent peripheral I/O read or write of 1, 2, or 4 bytes. Use the DPRD_DAT instruction to consistently read and the DPWR_DAT instruction to consistently write data of lengths other than 1, 2, or 4 bytes.
- You can use these instructions for data areas of 1 or more bytes. If the access is rejected, error code W#16#8090 results.
- PROFINET supports up to 1024 bytes of consistent data. You do not need to use these instructions for consistent transfers between the S7-1200 and PROFINET devices.

NOTE

If you are using the DPRD_DAT and DPWR_DAT instructions with consistent data, you must remove this consistent data from the process-image automatic update. Refer to "PLC concepts: Execution of the user program" (Page 61) for more information.

Table 10-89 Parameters

Parameter	Declaration	Data type	Description
LADDR	IN	HW_IO (Word)	Hardware ID of the module from which the data is to be read. (DPRD_DAT) Hardware ID of the module to which the data is to be written. (DPWR_DAT) The hardware ID can be found in the properties of the module in the device view or system constants.
RECORD	OUT	Variant	Destination area for the user data that were read (DPRD_DAT) or source area for the user data to be written (DPWR_DAT). This must be exactly as large as you configured for the selected module with STEP 7.
RET_VAL	OUT	Int	If an error occurs while the function is active, the return value contains an error code.

DPRD_DAT operations

Use the parameter LADDR to select the module of the DP standard slave / PROFINET IO device. If an access error occurs on the addressed module, the error code W#16#8090 is output.

Use the parameter RECORD to define the target range of the read data:

- The target range has to be at least as long as the inputs of the selected module. Only the inputs are transferred; the other bytes are not considered. If you read from a DP standard slave with a modular configuration or with several DP identifiers, you can only access the data of a module of the configured hardware identifier for each DPRD_DAT instruction call. If you select a target range that is too small, the error code W#16#80B1 is output at the RET_VAL parameter.
- The following data types can be used: Byte, Char, Word, DWord, Int, UInt, USInt, SInt, DInt, UDInt. The use of these data types in a User Defined Type (UDT) data structure of the type ARRAY or STRUCT is permissible.

- The data type STRING is not supported.
- If there was no error during the data transmission, the data that have been read are entered in the target range defined at the parameter RECORD.

DPWR_DAT operations

Use the parameter LADDR to select the module of the DP standard slave / PROFINET IO device. If an access error occurs on the addressed module, the error code W#16#8090 is output.

Use the parameter RECORD to define the source range of the data to be written:

- The source range has to be at least as long as the outputs of the selected module. Only the outputs are transferred; the other bytes are not considered. If the source range at the parameter RECORD is longer than the outputs of the configured module, only the data up to the maximum length of the outputs is transferred. If the source range at the parameter RECORD is shorter than the outputs of the configured module, the error code W#16#80B1 is output at the RET_VAL parameter.
- The following data types can be used: Byte, Char, Word, DWord, Int, UInt, USInt, SInt, DInt, UDInt. The use of these data types in a User Defined Type (UDT) data structure of the type ARRAY or STRUCT is permissible.
- The data type STRING is not supported.
- The data is transferred synchronously, that is, the write process is completed when the instruction is completed.

Error codes

Table 10-90 DPRD_DAT and DPWR_DAT error codes

Error code [1]	Description
0000	No error occurred
8090	One of the following cases apply: • You have not configured a module for the specified logical base address. • You have ignored the restriction concerning the length of consistent data. • You have not entered the start address in the LADDR parameter in hexadecimal format.
8092	The RECORD parameter supports the following data types: Byte, Char, Word, DWord, Int, UInt, USInt, SInt, DInt, UDInt, and arrays of these types.
8093	No DP module/PROFINET IO device from which you can read (DPRD_DAT) or to which you can write (DPWR_DAT) consistent data exists at the logical address specified in LADDR.
80A0	Access error detected while the I/O devices were being accessed (DPRD_DAT).
80B1	The length of the specified destination (DPRD_DAT) or source (DPWR_DAT) area is not identical to the user data length configured with STEP 7 Basic.
80B2	System error with external DP interface module (DPRD_DAT) and (DPWR_DAT)

[1] When displaying the DPRD_DAT and DPWR_DAT error codes, use the Word data type.

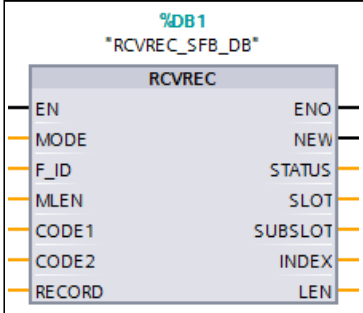
NOTE

If you access DPV1 slaves, error information from these slaves can be forwarded from the DP master to the instruction.

10.3.9.2 RCVREC (Receive data record)

An I-device can receive a data record from a higher-level controller. The receipt takes place in the user program with the RCVREC instruction (receive data record).

Table 10-91 RCVREC instruction

LAD / FBD	SCL	Description
	**"RCVREC_SFB_DB"(mode:=_int_in_, F_ID:=_uint_in_, mlen:=_uint_in_, code1:=_byte_in_, code2:=_byte_in_, new=>_bool_out_, status=>_dword_out_, slot=>_uint_out_, subslot=>_uint_out_, index=>_uint_out_ len=>_uint_out_, record:=_variant_inout_);**	Use the RCVREC instruction to receive a data record from a higher-level controller.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "RCVREC_SFB_DB" is the name of the instance DB.

The instruction has the following operating modes:

- Check whether the I-device has a request for a data record receipt
- Make the data record available to the output parameters
- Send an answer to the higher-level controller

You can determine the operating mode executed by the instruction using the input parameter MODE.

The I-device must be in the RUN or STARTUP mode.

With MLEN, you specify the maximum number of bytes you want to receive. The selected length of the target range RECORD should have at least the length of MLEN bytes.

If a data record is received (MODE = 1 or MODE = 2), the output parameter NEW indicates that the data record is stored in RECORD. Note that RECORD has a sufficient length. The output parameter LEN contains the actual length of the data record received in bytes.

Set CODE1 and CODE2 to zero for the positive answer to the higher-level controller. If the received data record is to be rejected, enter the negative answer to the higher-level controller in Error Code 1 of the CODE1 and in Error Code 2 of the CODE2.

NOTE

If the I-device has received a request for a data record receipt, you must recognize the delivery of this request within a certain duration. After recognition, you must send an answer to the higher-level controller within this time period. Otherwise, the I-device experiences a timeout error which causes the operating system of the I-device to send a negative answer to the higher-level controller. For information on the value for the time period, refer to the specifications of your CPU.

The STATUS output parameter receives the error information after the occurrence of an error.

Operating modes

You can determine the operating mode of the RCVREC instruction with the input parameter MODE. This step is explained in the following table:

MODE	Meaning
0	Check whether a request for a data record receipt exists If a data record from a higher-level controller exists on the I-device, the instruction only writes to the NEW, SLOT, SUBSLOT, INDEX, and LEN output parameters. If you call the instruction several times with MODE = 0, then the output parameter only refers to one and the same request.
1	Receiving a data record for any subslot of the I-device If a data record from a higher-level controller exists on the I-device for any subslot of the I-device, the instruction writes to the output parameter and transfers the data record to the parameter RECORD.
2	Receiving a data record for a specific subslot of the I-device If a data record from a higher-level controller exists on the I-device for a specific subslot of the I-device, the instruction writes to the output parameter and transfers the data record to the parameter RECORD.
3	Sending a positive answer to the higher-level controller The instruction checks the request of the higher-level controller to receive a data record, accepts the existing data record, and sends a positive acknowledgment to the higher-level controller.
4	Sending a negative answer to the higher-level controller The instruction checks the request of the higher-level controller to receive a data record, rejects the existing data record, and sends a negative acknowledgment to the higher-level controller. Enter the reason for the rejection in the input parameters CODE1 and CODE2.

NOTE

After the receipt of a data record (NEW = 1), you must call the RCVREC instruction twice to ensure complete processing. You must do this in the following order:

- First call with MODE = 1 or MODE = 2
- Second call with MODE = 3 or MODE = 4

Parameters

The following table shows the parameters of the RCVREC instruction:

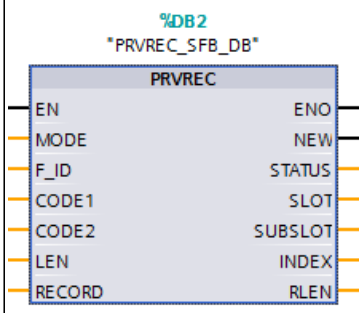
Parameter	Declaration	Data type	Description
MODE	IN	Int	Mode
F_ID	IN	HW_SUBMODULE	Subslot in the transfer area of the I-device for the data record to be received (only relevant for MODE = 2). The high word is always set to zero.
MLEN	IN	Int	Maximum length of the data record to be received in bytes
CODE1	IN	Byte	Zero (for MODE = 3) and/or Error Code 1 (for MODE = 4)
CODE2	IN	Byte	Zero (for MODE = 3) and/or Error Code 2 (for MODE = 4)
NEW	OUT	Bool	• MODE = 0: New data record was received • MODE = 1 or 2: Data record was transferred to RECORD
STATUS	OUT	DWord	Error information. Refer to "STATUS parameter" (Page 345) for more information.
SLOT	OUT	HW_SUBMODULE	Identical to F_ID

Parameter	Declaration	Data type	Description
SUBSLOT	OUT	HW_SUBMODULE	Identical to F_ID
INDEX	OUT	UInt	Number of the data record received
LEN	OUT	UInt	Length of the data record received
RECORD	IN_OUT	Variant	Target range for the data record received

10.3.9.3 PRVREC (Make data record available)

An I-device can receive a request from a higher-level controller to make a data record available. The I-device makes the data record available in the user program with the PRVREC instruction (make data record available).

Table 10-92 PRVREC instruction

LAD / FBD	SCL	Description
	**"PRVREC_SFB_DB"(mode:=_int_in_, F_ID:=_uint_in_, code1:=_byte_in_, code2:=_byte_in_, len:=_uint_in_, new=>_bool_out_, status=>_dword_out_, slot=>_uint_out_, subslot=>_uint_out_, index=>_uint_out_ rlen=>_uint_out_, record:=_variant_inout_);**	Use the PRVREC instruction to receive a request from a higher-level controller to make a data record available.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "PRVREC_SFB_DB" is the name of the instance DB.

The instruction has the following operating modes:

- Check whether the I-device has a request for making a data record available
- Transfer the requested data record to the higher-level controller
- Sending an answer to the higher-level controller

You can determine the operating mode executed by the instruction using the input parameter MODE.

The I-device must be in the RUN or STARTUP mode.

Enter the maximum number of bytes the data record to be sent should have with LEN. The selected length of the target range RECORD should have at least the length of LEN bytes.

If a request to make a data record available exists, (MODE = 0), the output parameter NEW is set to TRUE.

If the request for making a data record available is accepted, write RECORD for the positive answer to the higher-level controller with the requested data record and write zero for CODE1 and CODE2. If the request for making a data record available is to be rejected, enter the negative answer to the higher-level controller in Error Code 1 of the CODE1 and in Error Code 2 of the CODE2.

NOTE

If the I-device has received a request for making a data record available, you must recognize the delivery of this request within a certain time period. After recognition, you must send an answer to the higher-level controller within this time period. Otherwise, the I-device experiences a timeout error which causes the operating system of the I-device to send a negative answer to the higher-level controller. For information on the value for the time period, refer to the specifications of your CPU.

The STATUS output parameter receives the error information after the occurrence of an error.

Operating modes

You can determine the operating mode of the PRVREC instruction with the input parameter MODE. This step is explained in the following table:

MODE	Meaning
0	Check whether a request for making a data record available exists If a request from a higher-level controller for making a data record available exists on the I-device, the instruction only writes to the NEW, SLOT, SUBSLOT, INDEX, and RLEN output parameters. If you call the instruction several times with MODE = 0, then the output parameter only refers to one and the same request.
1	Receiving a request for making a data record available for any subslot of the I-device If such a request from a higher-level controller for any subslot of the I-device exists on the I-device, the instruction writes to the output parameter.
2	Receiving a request for making a data record available for a specific subslot of the I-device If such a request from a higher-level controller for a specific subslot of the I-device exists on the I-device, the instruction writes to the output parameter.
3	Make the data record available and send a positive answer to the higher-level controller The instruction checks the request of the higher-level controller to make a data record available, makes the request data record available to RECORD, and sends a positive acknowledgement to the higher-level controller.
4	Sending a negative answer to the higher-level controller The instruction checks the request of the higher-level controller to make a data record available, rejects this request, and sends a negative acknowledgement to the higher-level controller. Enter the reason for the rejection in the input parameters CODE1 and CODE2.

NOTE

After the receipt of a request (NEW = 1), you must call the PRVREC instruction twice to ensure complete processing. You must do this in the following order:

- First call with MODE = 1 or MODE = 2
- Second call with MODE = 3 or MODE = 4

Parameters

The following table shows the parameters of the PRVREC instruction:

Parameter	Declaration	Data type	Description
MODE	IN	Int	Mode
F_ID	IN	HW_SUBMODULE	Subslot in the transfer area of the I-device for the data record to be sent (only relevant for MODE = 2). The high word is always set to zero.
CODE1	IN	Byte	Zero (for MODE = 3) and/or Error Code 1 (for MODE = 4)
CODE2	IN	Byte	Zero (for MODE = 3) and/or Error Code 2 (for MODE = 4)
LEN	IN	UInt	Maximum length of the data record to be sent in bytes
NEW	OUT	Bool	The new data record was requested by the higher-level controller.
STATUS	OUT	DWord	Error information. Refer to "STATUS parameter" (Page 345) for more information.
SLOT	OUT	HW_SUBMODULE	Identical to F_ID
SUBSLOT	OUT	HW_SUBMODULE	Identical to F_ID
INDEX	OUT	UInt	Number of the data record to be sent
RLEN	OUT	UInt	Length of the data record to be sent
RECORD	IN_OUT	Variant	Data record made available

10.3.9.4 DPNRM_DG (Read diagnostic data from a PROFIBUS DP slave)

You can use the DPNRM_DG (Read diagnostic data) instruction with PROFIBUS.

Table 10-93 DPNRM_DG instruction

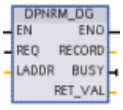
LAD / FBD	SCL	Description
	**ret_val := DPNRM_DG(req:=_bool_in_, laddr:=_word_in_, record=>_variant_out_, busy=>_bool_out_);**	Use the DPNRM_DG instruction to read the current diagnostic data of a DP slave in the format specified by EN 50 170 Volume 2, PROFIBUS. The data that has been read is entered in the destination area indicated by RECORD following error-free data transfer.

Table 10-94 DPNRM_DG instruction data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	REQ=1: Read request
LADDR	IN	HW_DPSLAVE	Configured diagnostic address of the DP slave: Must be the address of the station and not for the I/O device. Select the station (and not the image of the device) in the "Network" view of the "Device configuration" to determine the diagnostic address. Enter the addresses in hexadecimal format. For example, diagnostic address 1022 means LADDR:=W#16#3FE.

Parameter and type		Data type	Description
RET_VAL	OUT	Int	If an error occurs while the function is active, the return value contains an error code. If no error occurs, the length of the data actually transferred is entered in RET_VAL.
RECORD	OUT	Variant	Destination area for the diagnostic data that were read. The minimum length of the data record to be read (or the destination area) is 6 bytes. The maximum length of the data record to be sent is 240 bytes. Standard slaves can provide more than 240 bytes of diagnostic data up to a maximum of 244 bytes. In this case, the first 240 bytes are transferred to the destination area, and the overflow bit is set in the data.
BUSY	OUT	Bool	BUSY=1: The read job is not yet completed

You start the read job by assigning 1 to the input parameter REQ in the DPNRM_DG instruction call. The read job is executed asynchronously, in other words, it requires several DPNRM_DG instruction calls. The status of the job is indicated by the output parameters RET_VAL and BUSY.

Table 10-95 Slave diagnostic data structure

Byte	Description
0	Station status 1
1	Station status 2
2	Station status 3
3	Master station number
4	Vendor ID (high byte)
5	Vendor ID (low byte)
6 ...	Additional slave-specific diagnostic information

Table 10-96 DPNRM_DG instruction error codes

Error code	Description	Restriction
0000	No error	-
7000	First call with REQ=0: No data transfer active; BUSY has the value 0.	-
7001	First call with REQ =1: No data transfer active; BUSY has the value 1.	Distributed I/Os
7002	Interim call (REQ irrelevant): Data transfer already active; BUSY has the value 1.	Distributed I/Os
8090	Specified logical base address invalid: There is no base address.	-
8092	The RECORD parameter supports the following data types: Byte, Char, Word, DWord, Int, UInt, USInt, SInt, DInt, UDInt, and arrays of these types.	-
8093	• This instruction is not permitted for the module specified by LADDR (S7-DP modules for S7-1200 are permitted). • LADDR specifies the I/O device instead of specifying the station. Select the station (and not the image of the device) in the "Network" view of the "Device configuration" to determine the diagnostic address for LADDR.	-
80A2	• DP protocol error at layer 2 (for example, slave failure or bus problems) • For ET200S, data record cannot be read in DPV0 mode.	Distributed I/Os
80A3	DP protocol error with user interface/user	Distributed I/Os

Error code	Description	Restriction
80A4	Communication problem on the communication bus	The error occurs between the CPU and the external DP interface module.
80B0	• The instruction is not possible for module type. • The module does not recognize the data record. • Data record number 241 is not permitted.	-
80B1	The length specified in the RECORD parameter is incorrect.	Specified length > record length
80B2	The configured slot is not occupied.	-
80B3	Actual module type does not match the required module type.	-
80C0	There is no diagnostic information.	-
80C1	The data of the previous write job for the same data record on the module have not yet been processed by the module.	-
80C2	The module is currently processing the maximum possible number of jobs for a CPU.	-
80C3	The required resources (memory, etc.) are currently occupied.	-
80C4	Internal temporary error. The job could not be processed. Repeat the job. If this error occurs frequently, check your system for electrical disturbance sources.	-
80C5	Distributed I/Os not available	Distributed I/Os
80C6	Data record transfer was stopped due to a priority class abort (restart or background)	Distributed I/Os
8xyy[1]	General error codes	

Refer to "Extended instructions, Distributed I/O: Error information for RDREC, WRREC, and RALRM" (Page 345) for more information on general error codes.

10.4 PROFIenergy

PROFIenergy is a manufacturer- and device-neutral profile for energy management with PROFINET. To reduce electricity consumption during breaks in production and unplanned interruptions, it is possible to shut down equipment in a coordinated and centralized manner using PROFIenergy.

The PROFINET IO controller switches off the PROFINET devices/power modules using special commands in the user program. You require no additional hardware. The PROFINET devices interpret the PROFIenergy commands directly.

The S7-1200 CPU does not support the PE controller functionality. The S7-1200 CPU can only act as a PROFIenergy entity (with I-device functionality).

PROFIenergy controller (PE controller)

The PE controller is a higher-level CPU (for example, an S7-1500) that activates or deactivates the idle state of lower-level devices. The PE controller deactivates and reactivates specific production components or complete production lines using the user program. Lower-level devices receive commands from the user program through corresponding instructions (function blocks).

The user program sends the commands using the PROFINET communication protocol. The PE command can be either a control command to switch a PE entity to the energy-saving mode, or a command to read a status or measured value.

You use the PE_I_DEV instruction to request data from a module. The user program has to determine what information is being requested by the PE controller and retrieve it from the energy module using data records. The module itself does not directly support the PE commands. The module stores the energy measurement information in a shared area, and the lower-level CPU (for example, an S7-1200) triggers the PE_I_DEV instruction to return it to the PE controller.

PROFIenergy entity (PE entity)

The PE entity (for example, an S7-1200) receives the PROFIenergy commands of the PE controller (for example, an S7-1500) and executes these accordingly (for example, by returning a measured value or activating an energy saving mode). Implementation of the PE entity in a PROFIenergy-capable device is device- and manufacturer-specific.

Reference information

You can find further information on PROFIenergy in the TIA Portal STEP 7 online help. You can find examples that use the PROFIenergy instructions in the Industry Online Support in the entry "PROFIenergy - Saving Energy with SIMATIC S7 (http://support.automation.siemens.com/WW/view/en/41986454)".

10.5 Interrupts

10.5.1 ATTACH and DETACH (Attach/detach an OB and an interrupt event) instructions

You can activate and deactivate interrupt event-driven subprograms with the ATTACH and DETACH instructions.

Table 10-97 ATTACH and DETACH instructions

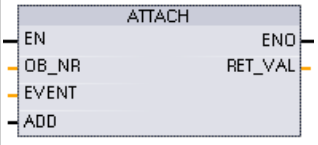
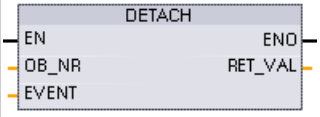
LAD / FBD	SCL	Description
	**ret_val := ATTACH(** **ob_nr:=_int_in_,** **event:=_event_att_in_,** **add:=_bool_in_);**	ATTACH enables interrupt OB subprogram execution for a hardware interrupt event.
	**ret_val := DETACH(** **ob_nr:=_int_in_,** **event:=_event_att_ in);**	DETACH disables interrupt OB subprogram execution for a hardware interrupt event.

Table 10-98 Data types for the parameters

Parameter and type		Data type	Description
OB_NR	IN	OB_ATT	Organization block identifier: Select from the available hardware interrupt OBs that were created using the "Add new block" feature. Double-click on the parameter field, then click on the helper icon to see the available OBs.
EVENT	IN	EVENT_ATT	Event identifier: Select from the available hardware interrupt events that were enabled in PLC device configuration for digital inputs or high-speed counters. Double-click on the parameter field, then click on the helper icon to see the available events.
ADD (ATTACH only)	IN	Bool	• ADD = 0 (default): This event replaces all previous event attachments for this OB. • ADD = 1: This event is added to previous event attachments for this OB.
RET_VAL	OUT	Int	Execution condition code

Hardware interrupt events

The following hardware interrupt events are supported by the CPU:

- Rising edge events: first 12 built-in CPU digital inputs (DIa.0 to DIb.3) and all SB digital inputs
  - A rising edge occurs when the digital input transitions from OFF to ON as a response to a change in the signal from a field device connected to the input.
- Falling edge events: first 12 built-in CPU digital inputs (DIa.0 to DIb.3) and all SB digital inputs
  - A falling edge occurs when the digital input transitions from ON to OFF.
- High-speed counter (HSC) current value = reference value (CV = RV) events (HSC 1 through 6)
  - A CV = RV interrupt for a HSC is generated when the current count transitions from an adjacent value to the value that exactly matches a reference value that was previously established.
- HSC direction changed events (HSC 1 through 6)
  - A direction changed event occurs when the HSC is detected to change from increasing to decreasing, or from decreasing to increasing.
- HSC external reset events (HSC 1 through 6)
  - Certain HSC modes allow the assignment of a digital input as an external reset that is used to reset the HSC count value to zero. An external reset event occurs for such a HSC, when this input transitions from OFF to ON.

Enabling hardware interrupt events in the device configuration

Hardware interrupts must be enabled during the device configuration. You must check the enable-event box in the device configuration for a digital input channel or a HSC, if you want to attach this event during configuration or run time.

Check box options within the PLC device configuration:

- Digital input
  - Enable rising edge detection
  - Enable falling edge detection
- High-speed counter (HSC)
  - Enable this high-speed counter for use
  - Generate interrupt for counter value equals reference value count
  - Generate interrupt for external reset event
  - Generate interrupt for direction change event

Adding new hardware interrupt OB code blocks to your program

By default, no OB is attached to an event when the event is first enabled. This is indicated by the "HW interrupt:" device configuration "<not connected>" label. Only hardware-interrupt OBs can be attached to a hardware interrupt event. All existing hardware-interrupt OBs appear in the "HW interrupt:" drop-down list. If no OB is listed, then you must create an OB of type "Hardware interrupt" as follows. Under the project tree "Program blocks" branch:

1. Double-click "Add new block", select "Organization block (OB)" and choose "Hardware interrupt".
2. Optionally, you can rename the OB, select the programming language (LAD, FBD or SCL), and select the block number (switch to manual and choose a different block number than that suggested).
3. Edit the OB and add the programmed reaction that you want to execute when the event occurs. You can call FCs and FBs from this OB, up to the maximum nesting depth. The maximum nesting depth is four for safety programs. For other programs, the maximum nesting depth is six.

OB_NR parameter

All existing hardware-interrupt OB names appear in the device configuration "HW interrupt:" drop-down list and in the ATTACH / DETACH parameter OB_NR drop-list.

EVENT parameter

When a hardware interrupt event is enabled, a unique default event name is assigned to this particular event. You can change this event name by editing the "Event name:" edit box, but it must be a unique name. These event names become tag names in the "Constants" tag table, and appear on the EVENT parameter drop-down list for the ATTACH and DETACH instruction boxes. The value of the tag is an internal number used to identify the event.

General operation

Each hardware event can be attached to a hardware-interrupt OB which will be queued for execution when the hardware interrupt event occurs. The OB-event attachment can occur at configuration time or at run time.

You have the option to attach or detach an OB to an enabled event at configuration time. To attach an OB to an event at configuration time, you must use the "HW interrupt:" drop-down list (click on the down arrow on the right) and select an OB from the list of available hardware-interrupt OBs. Select the appropriate OB name from this list, or select "<not connected>" to remove the attachment.

You can also attach or detach an enabled hardware interrupt event during run time. Use the ATTACH or DETACH program instructions during run time (multiple times if you wish) to attach or detach an enabled interrupt event to the appropriate OB. If no OB is currently attached (either from a "<not connected>" selection in device configuration, or as a result of executing a DETACH instruction), the enabled hardware interrupt event is ignored.

DETACH operation

Use the DETACH instruction to detach either a particular event or all events from a particular OB. If an EVENT is specified, then only this one event is detached from the specified OB_NR; any other events currently attached to this OB_NR will remain attached. If no EVENT is specified, then all events currently attached to OB_NR will be detached.

Condition codes

Table 10-99 Condition codes

RET_VAL (W#16#....)	ENO	Description
0000	1	No error
0001	1	Nothing to Detach (DETACH only)
8090	0	OB does not exist
8091	0	OB is wrong type
8093	0	Event does not exist

10.5.2 Cyclic interrupts

10.5.2.1 SET_CINT (Set cyclic interrupt parameters)

Table 10-100 SET_CINT (Set cyclic interrupt parameters)

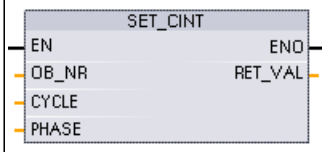
LAD / FBD	SCL	Description
	**ret_val := SET_CINT(ob_nr:=_int_in_, cycle:=_udint_in_, phase:=_udint_in_);**	Set the specified interrupt OB to begin cyclic execution that interrupts the program scan.

Table 10-101 Data types for the parameters

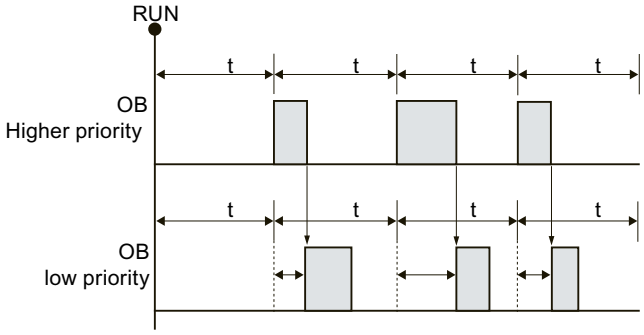
Parameter and type		Data type	Description
OB_NR	IN	OB_CYCLIC	OB number (accepts symbolic name)
CYCLE	IN	UDInt	Time interval, in microseconds
PHASE	IN	UDInt	Phase shift, in microseconds
RET_VAL	OUT	Int	Execution condition code

Examples: time parameter

- If the CYCLE time = 100 us, then the interrupt OB referenced by OB_NR interrupts the cyclic program scan every 100 us. The interrupt OB executes and then returns execution control to the program scan, at the point of interruption.
- If the CYCLE time = 0, then the interrupt event is deactivated and the interrupt OB is not executed.
- The PHASE (phase shift) time is a specified delay time that occurs before the CYCLE time interval begins. You can use the phase shift to control the execution timing of lower priority OBs.

If lower and higher priority OBs are called in the same time interval, the lower priority OB is only called after the higher priority OB has finished processing. The execution start time for the low priority OB can shift depending on the processing time of higher priority OBs.

OB call without phase shift



If you want to start the execution of a lower priority OB on a fixed time cycle, then phase shift time should be greater then the processing time of higher priority OBs.

OB-call with phase shift

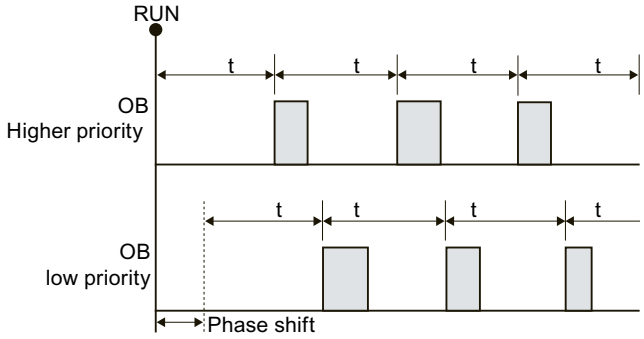


Table 10-102 Condition codes

RET_VAL (W#16#....)	Description
0000	No error
8090	OB does not exist or is of wrong type
8091	Invalid cycle time
8092	Invalid phase shift time
80B2	OB has no attached event

10.5.2.2 QRY_CINT (Query cyclic interrupt parameters)

Table 10-103 **QRY_CINT (Query cyclic interrupt)**

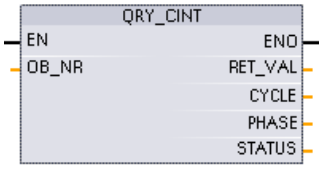
LAD / FBD	SCL	Description
	**ret_val := QRY_CINT(ob_nr:=_int_in_, cycle=>_udint_out_, phase=>_udint_out__, status=>_word_out_);**	Get parameter and execution status from a cyclic interrupt OB. The values that are returned existed at the time QRY_CINT was executed.

Table 10-104 Data types for the parameters

Parameter and type		Data type	Description
OB_NR	IN	OB_CYCLIC	OB number (accepts symbolic name like OB_MyOBName)
RET_VAL	OUT	Int	Execution condition code
CYCLE	OUT	UDInt	Time interval, in microseconds
PHASE	OUT	UDInt	Phase shift, in microseconds
STATUS	OUT	Word	Cyclic interrupt status code: • Bits 0 to 4, see the STATUS table below • Other bits, always 0

Table 10-105 STATUS parameter

Bit	Value	Description
0	0	During CPU RUN
	1	During startup
1	0	The interrupt is enabled.
	1	Interrupt is disabled via the DIS_IRT instruction.
2	0	The interrupt is not active or has elapsed.
	1	The interrupt is active.
4	0	The OB identified by OB_NR does not exist.
	1	The OB identified by OB_NR exists.
Other Bits		Always 0

If an error occurs, RET_VAL displays the appropriate error code and the parameter STATUS = 0.

Table 10-106 RET_VAL parameter

RET_VAL (W#16#....)	Description
0000	No error
8090	OB does not exist or is of wrong type.
80B2	OB has no attached event.

10.5.3 Time of day interrupts

WARNING

Risk of network attack through Network Time Protocol (NTP) synchronization

If an attacker can access your networks through Network Time Protocol (NTP) synchronization, the attacker can possibly disrupt control of your process by shifting the CPU system time.

The NTP client feature of the S7-1200 CPU is disabled by default, and, when enabled, only allows configured IP addresses to act as an NTP server. The CPU disables this feature by default, and you must configure this feature to allow remotely-controlled CPU system time corrections.

The S7-1200 CPU supports "time of day" interrupts and clock instructions that depend upon accurate CPU system time. If you configure NTP and accept time synchronization from a server, you must ensure that the server is a trusted source. Failure to do so can cause a security breach that allows an unknown user to take limited control of your process by shifting the CPU system time.

Disruptions to process control can possibly cause death, severe injury, or property damage.

For security information and recommendations, see the "Operational Guidelines" white paper on the Siemens Industrial Cybersecurity Web site (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

10.5.3.1 SET_TINTL (Set time of day interrupt)

Table 10-107 SET_TINTL (Set date and time of day interrupt with DTL data type)

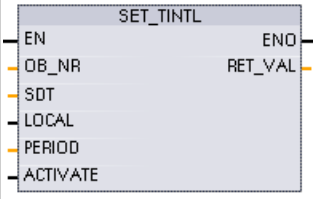
LAD / FBD	SCL	Description
	**ret_val := SET_TINTL(** **OB_NR:=_int_in_,** **SDT:=_dtl_in_,** **LOCAL:=_bool_in_** **PERIOD:=_word_in_** **ACTIVATE:=_bool_in_);**	Set a date and time of day interrupt. The program interrupt OB can be set for one execution, or for recurring execution with an assigned time period.

Table 10-108 Data types for the parameters

Parameter and type		Data type	Description
OB_NR	IN	OB_TOD (INT)	OB number (accepts symbolic name)
SDT	IN	DTL	Start date and time: Seconds and milliseconds are ignored and can be set to 0.
LOCAL	IN	Bool	0 = Use system time 1 = Use local time (if the CPU is configured for local time, otherwise use system time)
PERIOD	IN	Word	The period from the starting date and time for recurring interrupt event. • W#16#0000 = Once • W#16#0201 = Every minute • W#16#0401 = Every hour • W#16#1001 = Daily • W#16#1201 = Weekly • W#16#1401 = Monthly • W#16#1801 = yearly • W#16#2001 = End of month
ACTIVATE	IN	Bool	0 = ACT_TINT must be executed to activate the interrupt event. 1 = The interrupt event is activated.
RET_VAL	OUT	Int	Execution condition code

Your program can use SET_TINTL to set a date and time of day interrupt event that will execute the assigned interrupt OB. The start date and time is set by parameter SDT and the time period for recurring interrupts (for example, daily or weekly) is set by parameter PERIOD. If you set the repetition period to monthly, then you must set the start date to a day from 1 to 28. The days 29 to 31 may not be used because they do not occur in February. If you want an interrupt event at the end of each month, then use end of month for parameter PERIOD.

The DTL data weekday value in parameter SDT is ignored. Set a CPU's current date and time using the "Set time of day" function in the "Online & diagnostics" view of an online CPU. You must set the month, day of month, and year. STEP 7 calculates the interrupt period based on the CPU date and time clock.

NOTE

The first hour of the day does not exist when changing from summer to winter (daylight saving time). Use a start time within the second hour or use an additional time delay interrupt within the first hour.

Table 10-109 Condition code

RET_VAL (W#16#....)	Description
0000	No error
8090	Invalid OB_NR parameter
8091	Invalid SDT start time parameter: (for example, a start time within the skipped hour at the start of daylight savings time)
8092	Invalid PERIOD parameter
80A1	The start time is in the past. (This error code only occurs with PERIOD = W #16#0000.)

10.5.3.2 CAN_TINT (Cancel time of day interrupt)

Table 10-110 CAN_TINT (Cancel date and time of day interrupt)

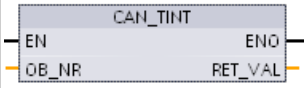
LAD / FBD	SCL	Description
	**ret_val:=CAN_TINT(_int_in);**	Cancels the start date and time of day interrupt event for the specified interrupt OB.

Table 10-111 Data types for the parameters

Parameter and type		Data type	Description
OB_NR	IN	OB_TOD (INT)	OB number (accepts symbolic name)
RET_VAL	OUT	Int	Execution condition code

Table 10-112 Condition codes

RET_VAL (W#16#....)	Description
0000	No error
8090	Invalid OB_NR parameter
80A0	No start date / time set for that interrupt OB

10.5.3.3 ACT_TINT (Activate time of day interrupt)

Table 10-113 ACT_TINT (Activate date and time of day interrupt)

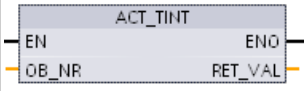
LAD / FBD	SCL	Description
	**ret_val:=ACT_TINT(_int_in_);**	Activates the start date and time of day interrupt event for the specified interrupt OB.

Table 10-114 Data types for the parameters

Parameter and type		Data type	Description
OB_NR	IN	OB_TOD (INT)	OB number (accepts symbolic name)
RET_VAL	OUT	Int	Execution condition code

Table 10-115 Condition codes

RET_VAL (W#16#....)	Description
0000	No error
8090	Invalid OB_NR parameter
80A0	Start date and time-of day not set, for the relevant time-of-day interrupt OB
80A1	The activated time is in the past. The error only occurs when the interrupt OB is set to execute once only.

10.5.3.4 QRY_TINT (Query status of time of day interrupt)

Table 10-116 QRY_TINT (Query date and time of day interrupt)

LAD / FBD	SCL	Description
	ret_val:=QRY_TINT(OB_NR:=_int_in_, STATUS=>_word_out_);	Queries the date and time of day interrupt status for the specified interrupt OB.

Table 10-117 Data types for the parameters

Parameter and type		Data type	Description
OB_NR	IN	OB_TOD (INT)	OB number (accepts symbolic name) of the interrupt OB to query
RET_VAL	OUT	Int	Execution condition code
STATUS	OUT	Word	Status of the specified interrupt OB

Table 10-118 STATUS parameter

Bit	Value	Description
0	0	In Run
	1	In Startup
1	0	The interrupt is enabled.
	1	The interrupt is disabled.
2	0	The interrupt is not active or has expired.
	1	The interrupt is active.
4	0	The assigned OB_NR does not exist.
	1	An OB with the assigned OB_NR exists.
6	1	The date and time of day interrupt uses local time.
	0	The date and time of day interrupt uses system time.
Others		Always 0

Table 10-119 Condition code

RET_VAL (W#16#....)	Description
0000	No error
8090	Invalid OB_NR parameter

10.5.4 Time delay interrupts

You can start and cancel time delay interrupt processing with the SRT_DINT and CAN_DINT instructions, or query the interrupt status with the QRY_DINT instruction. Each time delay interrupt is a one-time event that occurs after the specified delay time. If the time delay event is cancelled before the time delay expires, the program interrupt does not occur.

Table 10-120 SRT_DINT, CAN_DINT, and QRY_DINT instructions

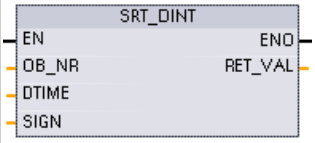
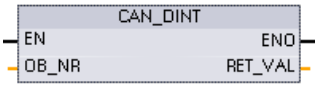
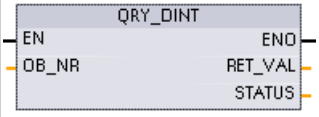
LAD / FBD	SCL	Description
	**ret_val := SRT_DINT(ob_nr:=_int_in_, dtime:=_time_in_, sign:=_word_in_);**	SRT_DINT starts a time delay interrupt that executes an OB when the delay time specified by parameter DTIME has elapsed.
	**ret_val := CAN_DINT(ob_nr:=_int_in_);**	CAN_DINT cancels a time delay interrupt that has already started. The time delay interrupt OB is not executed in this case.
	**ret_val := QRY_DINT(ob_nr:=_int_in_, status=>_word_out_);**	QRY_DINT queries the status of the time delay interrupt specified by the OB_NR parameter.

Table 10-121 Data types for the parameters

Parameter and type		Data type	Description
OB_NR	IN	OB_DELAY	Organization block (OB) to be started after a time-delay: Select from the available time-delay interrupt OBs that were created using the "Add new block" project tree feature. Double-click on the parameter field, then click on the helper icon to see the available OBs.
DTIME [1]	IN	Time	Time delay value (1 to 60000 ms)
SIGN [1]	IN	Word	Not used by the S7-1200: Any value is accepted. A value must be assigned to prevent errors.
RET_VAL	OUT	Int	Execution condition code
STATUS	OUT	Word	QRY_DINT instruction: Status of the specified time-delay interrupt OB, see the table below

[1] Only for SRT_DINT

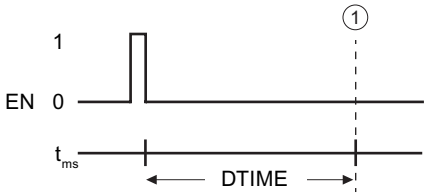
Operation

When EN=1, the SRT_DINT instruction starts the internal time delay timer (DTIME). When the time delay elapses, the CPU generates a program interrupt that triggers the execution of the associated time delay interrupt OB. You can cancel an in-process time delay interrupt before the specified time delay occurs by executing the CAN_DINT instruction. The total number of active time delay interrupt events must not exceed four.

NOTE

The SRT_DINT starts the time delay timer on every scan when EN=1. Assert EN=1 as a one-shot rather than just setting EN=1 to begin your time delay.

Timing diagram for the SRT_DINT instruction:



① Time delay interrupt executes

Adding time delay interrupt OBs to your project

You can only assign time delay interrupt OBs to the SRT_DINT and CAN_DINT instructions. No time delay interrupt OB exists in a new project. You must add time delay interrupt OBs to your project. To create a time-delay interrupt OB, follow these steps:

1. Double-click the "Add new block" item in the "Program blocks" branch of the project tree, select "Organization block (OB)", and choose "Time delay interrupt".
2. You have the option to rename the OB, select the programming language, or select the block number. Switch to manual numbering if you want to assign a different block number than the number that was assigned automatically.
3. Edit the time delay interrupt OB subprogram and create programmed reaction that you want to execute when the time delay timeout event occurs. You can call other FC and FB code blocks from the time delay interrupt OB. The maximum nesting depth is four for safety programs. For other programs, the maximum nesting depth is six.
4. The newly assigned time delay interrupt OB names will be available when you edit the OB_NR parameter of the SRT_DINT and CAN_DINT instructions.

QRY_DINT parameter STATUS

Table 10-122 If there is an error (REL_VAL <> 0), then STATUS = 0.

Bit	Value	Description
0	0	In RUN
	1	In startup
1	0	The interrupt is enabled.
	1	The interrupt is disabled.
2	0	The interrupt is not active or has elapsed.
	1	The interrupt is active.
4	0	An OB with an OB number given in OB_NR does not exist.
	1	An OB with an OB number given in OB_NR exists.
Other bits		Always 0

Condition codes

Table 10-123 Condition codes for SRT_DINT, CAN_DINT, and QRY_DINT

RET_VAL (W#16#...)	Description
0000	No error occurred
8090	Incorrect parameter OB_NR
8091	Incorrect parameter DTIME
80A0	Time delay interrupt has not started.

10.5.5 DIS_AIRT and EN_AIRT (Delay/enable execution of higher priority interrupts and asynchronous error events) instructions

Use the DIS_AIRT and EN_AIRT instructions to disable and enable alarm interrupt processing.

Table 10-124 DIS_AIRT and EN_AIRT instructions

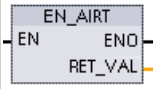
LAD / FBD	SCL	Description
	DIS_AIRT();	DIS_AIRT delays the processing of new interrupt events. You can execute DIS_AIRT more than once in an OB.
	**EN_AIRT();**	EN_AIRT enables the processing of interrupt events that you previously disabled with the DIS_AIRT instruction. Each DIS_AIRT execution must be cancelled by an EN_AIRT execution. The EN_AIRT executions must occur within the same OB, or any FC or FB called from the same OB, before interrupts are enabled again for this OB.

Table 10-125 Data types for the parameters

Parameter and type		Data type	Description
RET_VAL	OUT	Int	Number of delays = number of DIS_AIRT executions in the queue.

The DIS_AIRT executions are counted by the operating system. Each of these remains in effect until it is cancelled again specifically by an EN_AIRT instruction, or until the current OB has been completely processed. For example: if you disabled interrupts five times with five DIS_AIRT executions, you must cancel these with five EN_AIRT executions before interrupts become enabled again.

After the interrupt events are enabled again, the interrupts that occurred while DIS_AIRT was in effect are processed, or the interrupts are processed as soon as the current OB has been executed.

Parameter RET_VAL indicates the number of times that interrupt processing was disabled, which is the number of queued DIS_AIRT executions. Interrupt processing is only enabled again when parameter RET_VAL = 0.

10.6 Alarms

10.6.1 Gen_UsrMsg (Generate user diagnostic alarms)

Table 10-126 Gen_UsrMsg instruction

LAD / FBD	SCL	Description
	ret_val :=Gen_UsrMsg(**Mode:=_uint_in_,** **TextID:=_uint_in_,** **TextListID:=_uint_in_,** **AssocValues:=_struct_inout_);**	You use the "Gen_UsrMsg" instruction to generate a user diagnostic alarm that can be either an incoming or outgoing alarm. By means of user diagnostic alarms, you can write a user entry to the diagnostics buffer and send a corresponding alarm. The entry in the diagnostics buffer is created synchronously. Alarm transmission is asynchronous. If an error occurs during the execution of an instruction, it is output via the parameter RET_VAL.

Content of the alarm

A text list defines the content of the alarm:

- Define the text list you want to use with the parameter TextListID. For this purpose open the dialog "Text lists" in the project navigation. Show the column "ID" in the dialog "Text lists". Apply the ID at the parameter TextListID.
- Use the parameter TextID to select the text list entry you want to write in the diagnostics buffer. For this purpose select an entry from the "Text lists entries" dialog by applying a number from the columns "Range from / range to" at the parameter TextID. You must use the same number from both the "Range from" and "Range to" columns for the text list entry.

Refer to the STEP 7 Information System for detailed information about text lists.

Defining associated values

The text list entry defines new associated values to be added to the alarm:

- Add the following information to the text list entry to define associated values:
  @<No. of the associated value><Element type><Format specification>@
- Use the system data type AssocValues to specify which associated value to add when generating the alarm.

Refer to the STEP 7 Information System for detailed information about the structure of associated values.

Parameters

The following table shows the parameters of the "Gen_UsrMsg" instruction:

Parameter	Declaration	Data type	Memory area	Description
Mode	Input	UInt	I, Q, M, D, L or constant	Parameters for selecting the status of the alarm: • 1: incoming alarm • 2: outgoing alarm
TextID	Input	UInt	I, Q, M, D, L or constant	ID of the text list entry that should be used for the alarm text.
TextListID	Input	UInt	I, Q, M, D, L or constant	ID of the text list that contains text list entry.
Ret_Val	Return	Int	I, Q, M, D, L	Error code of the instruction.
AssocValues	InOut	VARIANT	D, L	Pointer to the system data type AssocValues that allows you to define the associated values.

For additional information on valid data types, refer to "Data types (Page 95)".

Parameter AssocValues

Use the system data type AssocValues to define which associated values will be sent. A maximum of eight associated values are possible. Enter the data type "AssocValues" as a data block to create the structure.

You select associated values by entering the numbers of the associated values for the parameters Value[x]. Note the following:

- The Gen_UsrMsg instruction treats the values for TextID and TextListID as associated values to be sent. As a result, "1" and "2" are pre-assigned as numbers for addressing associated values. Do not use the numbers "1" or "2" to address associated values.
- Address the associated value at parameter Value [1] as number "3", at parameter Value [2] as number "4", and so forth.

Byte	Parameter	Data type	Start value	Description	Number of the associated value
0..1	Value[1]	UINT	0	First associated value of the alarm.	3
2..3	Value[2]	UINT	0	Second associated value of the alarm.	4
4..5	Value[3]	UINT	0	...	5
6..7	Value[4]	UINT	0	...	6
8..9	Value[5]	UINT	0	...	7
10..11	Value[6]	UINT	0	...	8
12..13	Value[7]	UINT	0	...	9
14..15	Value[8]	UINT	0	Eighth associated value of the alarm.	10

Parameter RET_VAL

The following table defines output values for the RET_VAL parameter. See also Common error codes for the Extended instructions (Page 473).

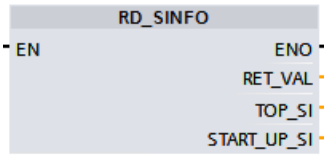
Error code* (W#16#...)	Explanation
0000	No error
8080	Value in the MODE parameter is not supported.
80C1	Resource bottleneck due to too many parallel calls.
8528	Parameter 5 (AssocValues) is not byte-aligned.
853A	Parameter 5 (AssocValues) references an invalid point.
* You can display the error code as either integer or hexadecimal in the program editor.	

10.7 Diagnostics (PROFINET or PROFIBUS)

10.7.1 RD_SINFO (Read current OB start information)

Description

Table 10-127 RD_SINFO instruction

LAD / FBD	SCL	Description
	**ret_val := RD_SINFO(TOP_SI=>_variant_out_, START_UP_SI=>_variant_out_);**	You use the instruction "RD_SINFO" to read the start information of the following OBs: • Last OB called that has not yet been completely executed • Last startup OB that the CPU started There is no time stamp in either case. If the call is in OB 100, OB 101 or OB 102, two identical start information messages will be returned.

Parameter

The following table shows the parameters of the "RD_SINFO" instruction:

Parameter	Declaration	Data type	Memory area	Description
RET_VAL	Return	INT	I, Q, M, D, L	Error information
TOP_SI	Output	VARIANT	D, L	Start information of the current OB
START_UP_SI	Output	VARIANT	D, L	Start information of the startup OB last started

You will find more detailed information on valid data types in "Data types (Page 95)".

SDTs of the TOP_SI parameter

The following table shows the possible SDTs for the TOP_SI parameter:

Organization blocks (OB)	System data types (SDT)	System data type numbers
Any	SI_classic*	592*
	SI_none	593
ProgramCycleOB	SI_ProgramCycle	594
TimeOfDayOB	SI_TimeOfDay	595
TimeDelayOB	SI_Delay	596
CyclicOB	SI_Cyclic	597
ProcessEventOB	SI_HWInterrupt	598
ProfileEventOB StatusEventOB UpdateEventOB	SI_Submodule	601
SynchronousCycleOB	SI_SynchCycle	602
IOredundancyErrorOB	SI_IORedundancyError	604
CPUredundancyErrorOB	SI_CPURedundancyError	605
TimeErrorOB	SI_TimeError	606
DiagnosticErrorOB	SI_DiagnosticInterrupt	607
PullPlugEventOB	SI_PlugPullModule	608
PeripheralAccessErrorOB	SI_AccessError	609
RackStationFailureOB	SI_StationFailure	610
ServoOB	SI_Servo	611
IpoOB	SI_Ipo	612
StartupOB	SI_Startup	613
ProgrammingErrorOB IOaccessErrorOB	SI_ProgIOAccessError	614
CPURedundancyErrorOB	SI_CPURedundancyError_V2	617

*The SI_classic SDT is not applicable for the S7-1200. The S7-1200 CPU returns a RET_VAL of #16#8081 if the TOP_SI parameter is of type SI_classic.

SDTs of the START_UP_SI parameter

The following table shows the possible SDTs for the START_UP_SI parameter:

System data types (SDT)	System data type numbers
SI_classic*	592
SI_none	593
SI_Startup	613

*The SI_classic SDT is not applicable for the S7-1200. The S7-1200 CPU returns a RET_VAL of #16#8083 if the START_UP_SI parameter is of type SI_classic.

Structures

The following tables define the structure elements of the individual structures:

Table 10-128 SI_classic structure

Structure element	Data type	Description
EV_CLASS	BYTE	• Bits 0 to 3: Event ID • Bits 4 to 7: Event class
EV_NUM	BYTE	Event number
PRIORITY	BYTE	Priority class number (Meaning of B#16#FE: OB not available or disabled or cannot be started in current operating mode)
NUM	BYTE	OB number
TYP2_3	BYTE	Data ID 2_3: Identifies the information entered in ZI2_3
TYP1	BYTE	Data ID 1: Identifies the information entered in ZI1
ZI1	WORD	Additional information 1
ZI2_3	DWORD	Additional information 2_3

Table 10-129 SI_none structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)

Table 10-130 SI_ProgramCycle structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 1	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
Initial_Call	BOOL	For OB_Class = 1, 30, 52, 61, 65
Remanence	BOOL	For OB_Class = 1

Table 10-131 SI_TimeOfDay structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 10	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
CaughtUp	BOOL	For OB_Class = 10
SecondTime	BOOL	For OB_Class = 10

Table 10-132 SI_Delay structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 20	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
Sign	WORD	For OB_Class = 20

Table 10-133 SI_Cyclic structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 30	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
Initial_Call	BOOL	For OB_Class = 1, 30, 52, 61, 65
Event_Count	INT	For OB_Class = 30, 51, 52, 61, 65, 91, 92

Table 10-134 SI_HWInterrupt structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 40	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
LADDR	HW_IO	For OB_Class = 40, 51, 55, 56, 57, 70, 82, 83, 85, 86, 91, 92
USI	WORD	For OB_Class = 40
IChannel	USINT	For OB_Class = 40
EventType	BYTE	For OB_Class = 40

Table 10-135 SI_Submodule structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
LADDR	HW_IO	For OB_Class = 40, 51, 55, 56, 57, 70, 82, 83, 85, 86, 91, 92
Slot	UINT	For OB_Class = 55, 56, 57
Specifier	WORD	For OB_Class = 55, 56, 57

Table 10-136 SI_SynchCycle structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 61	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
Initial_Call	BOOL	For OB_Class = 1, 30, 52, 61, 65
PIP_Input	BOOL	For OB_Class = 61, 91, 92
PIP_Output	BOOL	For OB_Class = 61, 91, 92
IO_System	USINT	For OB_Class = 61, 91, 92
Event_Count	INT	For OB_Class = 30, 51, 52, 61, 65, 91, 92
SyncCycleTime	LTIME	Calculated cycle time

Table 10-137 SI_IORedundancyError structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 70	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
LADDR	HW_ANY	For OB_Class = 40, 51, 55, 56, 57, 70, 82, 83, 85, 86, 91, 92
Event_Class	BYTE	For OB_Class = 70, 83, 85, 86
Fault_ID	BYTE	For OB_Class = 70, 80, 83, 85, 86

Table 10-138 SI_CPURedundancyError structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 72	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
Switch_Over	BOOL	For OB_Class = 72

Table 10-139 SI_TimeError structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 80	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
Fault_ID	BYTE	For OB_Class = 70, 80, 83, 85, 86
Csg_OBnr	OB_ANY	For OB_Class = 80
Csg_Prio	UINT	For OB_Class = 80

Table 10-140 SI_DiagnosticInterrupt structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 82	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
IO_State	WORD	For OB_Class = 82
LADDR	HW_ANY	For OB_Class = 40, 51, 55, 56, 57, 70, 82, 83, 85, 86, 91, 92
Channel	UINT	For OB_Class = 82
MultiError	BOOL	For OB_Class = 82

Table 10-141 SI_PlugPullModule structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 83	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
LADDR	HW_IO	For OB_Class = 40, 51, 55, 56, 57, 70, 82, 83, 85, 86, 91, 92
Event_Class	BYTE	For OB_Class = 70, 83, 85, 86
Fault_ID	BYTE	For OB_Class = 70, 80, 83, 85, 86

Table 10-142 SI_AccessError structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 85	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
LADDR	HW_IO	For OB_Class = 40, 51, 55, 56, 57, 70, 82, 83, 85, 86, 91, 92
Event_Class	BYTE	For OB_Class = 70, 83, 85, 86
Fault_ID	BYTE	For OB_Class = 70, 80, 83, 85, 86
IO_Addr	UINT	For OB_Class = 85
IO_LEN	UINT	For OB_Class = 85

Table 10-143 SI_StationFailure structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 86	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
LADDR	HW_IO	For OB_Class = 40, 51, 55, 56, 57, 70, 82, 83, 85, 86, 91, 92
Event_Class	BYTE	For OB_Class = 70, 83, 85, 86
Fault_ID	BYTE	For OB_Class = 70, 80, 83, 85, 86

Table 10-144 SI_Servo structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 91	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
Initial_Call	BOOL	For OB_Class = 1, 30, 52, 61, 65
PIP_Input	BOOL	For OB_Class = 61, 91, 92
PIP_Output	BOOL	For OB_Class = 61, 91, 92
IO_System	USINT	For OB_Class = 61, 91, 92
Event_Count	INT	For OB_Class = 30, 51, 52, 61, 65, 91, 92
Synchronous	BOOL	

Table 10-145 SI_Ipo structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 92	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
Initial_Call	BOOL	For OB_Class = 1, 30, 52, 61, 65
PIP_Input	BOOL	For OB_Class = 61, 91, 92
PIP_Output	BOOL	For OB_Class = 61, 91, 92
IO_System	USINT	For OB_Class = 61, 91, 92
Event_Count	INT	For OB_Class = 30, 51, 52, 61, 65, 91, 92
Reduction	UINT	For OB_Class = 92

Table 10-146 SI_Startup structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT := 100	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
LostRetentive	BOOL	For OB_Class = 100
LostRTC	BOOL	For OB_Class = 100

Table 10-147 SI_ProgIOAcessError structure

Structure element	Data type	Description
SI_Format	USINT	• 16#FF = No information • 16#FE = Optimized start information
OB_Class	USINT	OB class for "No information" or "Optimized start information"
OB_Nr	UINT	OB number (1 ... 32767)
BlockNr	UINT	For OB_Class = 121, 122
Reaction	USINT	For OB_Class = 121, 122

Structure element	Data type	Description
Fault_ID	BYTE	For OB_Class = 121, 122
BlockType	USINT	For OB_Class = 121, 122
Area	USINT	For OB_Class = 121, 122
DBNr	DB_ANY	For OB_Class = 121, 122
Csg_OBNr	OB_ANY	For OB_Class = 121, 122
Csg_Prio	USINT	For OB_Class = 121, 122
Width	USINT	For OB_Class = 121, 122

NOTE

If this was created with the block property "Standard", the structure elements specified for the SI_classic structure are identical in content to the temporary tags of an OB.

Note, however, that temporary tags of the individual OBs can have different names and different data types. Also note that the call interface of each OB includes additional information regarding the date and the time of the OB request.

Bits 4 to 7 of the EV_CLASS structure element contain the event class. The following values are possible here:

- 1: Start events from standard OBs
- 2: Start events from synchronous error OBs
- 3: Start events from asynchronous error OBs

The PRIORITY structure element supplies the priority class belonging to the current OB.

Apart from these two elements, NUM is also relevant. NUM contains the number of the current OB or the startup OB that was started last.

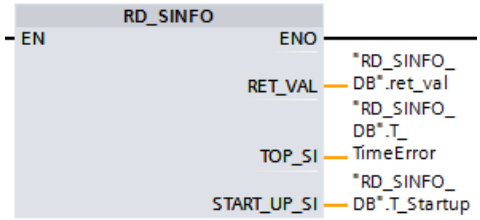
RET_VAL parameter

The following table shows the meaning of the values of the RET_VAL parameter:

Error code* (W#16#...)	Explanation
8081	Start information of the current OB does not correspond to the specified system data type
8083	Start information of the last startup OB started does not correspond to the specified system data type
* You can display the error code as either integer or hexadecimal values in the program editor.	

Example

A time error interrupt OB (OB 80) is the OB that was called last and that has not yet been completely processed. Startup OB (OB 100) is the startup OB that was started last. The instruction call to read the startup information is as follows, where RD_SINFO_DB is the data block that contains tags of the SDTs for types of OBs:



The following table shows the assignment between the structure elements of the TOP_SI parameter of the "RD_SINFO" instruction and the associated local tags of OB 80.

TOP_SI structure element	Data type	OB 80 - Associated local tag	Data type
EV_CLASS	BYTE	OB80_EV_CLASS	BYTE
EV_NUM	BYTE	OB80_FLT_ID	BYTE
PRIORITY	BYTE	OB80_PRIORITY	BYTE
NUM	BYTE	OB80_OB_NUMBR	BYTE
TYP2_3	BYTE	OB80_RESERVED_1	BYTE
TYP1	BYTE	OB80_RESERVED_2	BYTE
ZI1	WORD	OB80_ERROR_INFO	WORD
ZI2_3	DWORD	OB80_ERR_EV_CLASS	BYTE
		OB80_ERR_EV_NUM	BYTE
		OB80_OB_PRIORITY	BYTE
		OB80_OB_NUM	BYTE

The following table shows the assignment between the structure elements of the START_UP_SI parameter of the "RD_SINFO" instruction and the associated local tags of OB 100.

START_UP_SI structure element	Data type	OB 100 - Local tag	Data type
EV_CLASS	BYTE	OB100_EV_CLASS	BYTE
EV_NUM	BYTE	OB100_STRTUP	BYTE
PRIORITY	BYTE	OB100_PRIORITY	BYTE
NUM	BYTE	OB100_OB_NUMBR	BYTE
TYP2_3	BYTE	OB100_RESERVED_1	BYTE
TYP1	BYTE	OB100_RESERVED_2	BYTE
ZI1	WORD	OB100_STOP	WORD
ZI2_3	DWORD	OB100_STRT_INFO	DWORD

10.7.2 LED (Read LED status)

Table 10-148 LED instruction

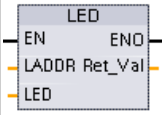
LAD / FBD	SCL	Description
	**ret_val := LED(** **laddr:=_word_in_,** **LED:=_uint_in_);**	Use the LED instruction to read the state of the LEDs on the CPU (Page 1047). The specified LED state is returned by the RET_VAL output.

Table 10-149 Data types for the parameters

Parameter and type		Data type	Description		
LADDR	IN	HW_IO	Identifier of the CPU[1]		
LED	IN	UInt	LED identifier number		
			1	RUN/STOP	Color 1 = green, color 2 = yellow
			2	Error	Color 1 = red
			3	Maintenance	Color 1 = yellow
RET_VAL	OUT	Int	Status of the LED		

[1] For the identifier of the connected CPU, select Local~Common from the drop-down list of the parameter.

Table 10-150 Status of RET_VAL

RET_VAL (W#16#...)	Description	
0 to 9 LED state	0	LED does not exist
	1	Off
	2	Color 1 On (solid)
	3	Color 2 On (Solid)
	4	Color 1 flashing at 2 Hz
	5	Color 2 flashing 2 Hz
	6	Color 1 & 2 flashing alternatively at 2 Hz
	9	State of the LED is not available
8091	Device identified by LADDR does not exist	
8092	Device identified by LADDR does not support LEDs	
8093	LED identifier not defined	
80Bx	CPU identified by LADDR does not support the LED instruction	

10.7.3 Get_IM_Data (Read the identification and maintenance data)

You use the Get_IM_Data instruction to check the identification and maintenance (I&M) data for the specified module or sub-module.

Table 10-151 Get_IM_Data instruction

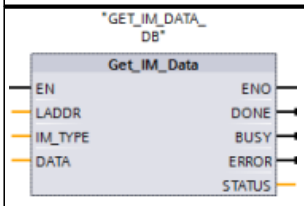
LAD / FBD	SCL	Description
	**"GET_IM_DATA_DB"(LADDR:=16#0, IM_TYPE:=0, DONE=>_bool_out_, BUSY=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, DATA:=_variant_inout_);**	Use the Get_IM_Data instruction to check the identification and maintenance (I&M) data for the specified module or sub-module.

Table 10-152 Data types for the parameters

Parameter and type		Data type	Description
LADDR	Input	HW_IO	Identifier of the module
IM_TYPE	Input	UInt	Identification and maintenance (I&M) data number: • 0: I&M0 (MLFB, serial number, version, and other information) • 1: I&M1 (Designators) • 2: I&M2 (Installation date) • 3: I&M3 (Descriptor) • 4: I&M4 (Signature)
RET_VAL	Output	Int	Status (condition code)
DATA	InOut	Variant	I&M data (STRING or an array of BYTE); recommend use of the SDT "IM0_Data" for IM_TYPE = 0.

Identification and maintenance (I&M) data can help you to check the system configuration, detect hardware changes, or view maintenance data. Module identification data (I data) is read only. Module maintenance data (M data) depends on system information, such as the installation date. M data are created during maintenance planning and written to the module:

- If the data type used at the parameter DATA is a string, then the current length of the string is set according to the length of the I&M data.
- If the data type used at the parameter DATA is an array of Byte or Char, then the I&M data are copied in as a sequence of bytes.
- If the data type used at the parameter DATA is a structure, then the I&M data are copied in as a sequence of bytes.
- If the given array of byte/char at DATA is longer than the requested I&M data, then the byte value 16#00 is appended.
- Other data types are not supported and error 8093 is returned.

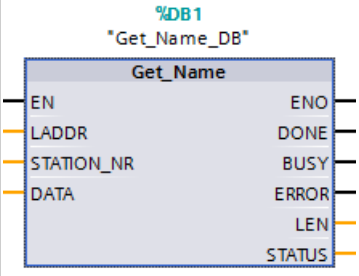
Table 10-153 Condition codes

RET_VAL (W#16#...)	Description
0	No error
8091	LADDR does not exist
8092	LADDR does not address a HW object which supports I&M data
8093	Data type given at parameter DATA is not supported
80B1	DATA instruction not supported by the CPU for this LADDR
80B2	IM_TYPE not supported by the CPU
8452	The complete I&M information does not fit into the variable given at the DATA parameter. A partial result up to the byte length of the variable is returned.

10.7.4 Get_Name (Read the name of a PROFINET IO device)

The "Get_Name" instruction reads the name of a PROFINET IO device, PROFIBUS slave, or AS-i slave. The name is displayed in the network view and in the properties of the IO device.

Table 10-154 Get_Name instruction

LAD / FBD	SCL	Description
	**"Get_Name_DB"(LADDR:=_uint_in_, STATION_NR:=_uint_in_, DONE=>_bool_out_, BUSY=>_bool_out_, ERROR=>_bool_out_, LEN=>_dint_out_, STATUS=>_word_out_, DATA:=_variant_inout_);**	Use the Get_Name instruction to read the name of a PROFINET IO device or PROFIBUS slave.

1 STEP 7 automatically creates the DB when you insert the instruction.

2 In the SCL example, "Get_Name_DB" is the name of the instance DB.

You select the IO device by using the hardware identifier of the distributed IO system (at the LADDR parameter) and the device number of the PROFINET IO device or the PROFIBUS address of the PROFIBUS slave (at the STATION_NR parameter).

Once the instruction has been executed, the program writes the name of the IO device to the area addressed with the DATA parameter.

The name that is read depends on the type of IO device:

- DP slave or IO device: Name of the head module
- I-slave or I-device: Name of the interface module
- HMI panel: Name of the interface
- PC station: Name of the interface module
- GSD devices: Displays the name of the Device Access Point (DAP) (name of the interface or head module)

The instruction writes the length of the name at the LEN parameter. If the name is longer than the area specified at the DATA parameter, the program writes only that section which corresponds to the maximum length of the addressed area.

The maximum length for a name is 128 characters.

NOTE
Name of the CPU readout (Version 1.1)
If you assign a "0" at each of the parameters LADDR and STATION_NR, the instruction writes the name of the CPU.

Parameters

The following table shows the parameters of the Get_Name instruction:

Parameter	Declaration	Data type	Description
LADDR	IN	HW_IOSYSTEM	Hardware identifier (HW-IoSystem) of the distributed IO system. The number is taken from the system constants or the properties of the IO system.
STATION_NR	IN	UInt	• PROFINET IO device: Device number is applied in the Network view from the properties of the IO device under "Ethernet addresses". • PROFIBUS slave: PROFIBUS address is applied in the Network view from the properties of the PROFIBUS slave under "PROFIBUS address".
DATA	IN_OUT	Variant	Pointer to the area where the name is written.
DONE	OUT	Bool	The instruction executes successfully. Name of the module transfers to the area at the DATA parameter.
BUSY	OUT	Bool	Status parameter: • 0: Execution of the instruction complete. • 1: Execution of the instruction not yet complete.
ERROR	OUT	Bool	Status parameter: • 0: No error • 1: An error occurred during execution of the instruction. The STATUS parameter contains detailed information.
LEN	OUT	DInt	Length of the name of the IO device (number of characters).
STATUS	OUT	Word	Status parameter: The parameter is only set for the duration of one call. To display the status, you should therefore copy STATUS to a free data area.

STATUS parameter

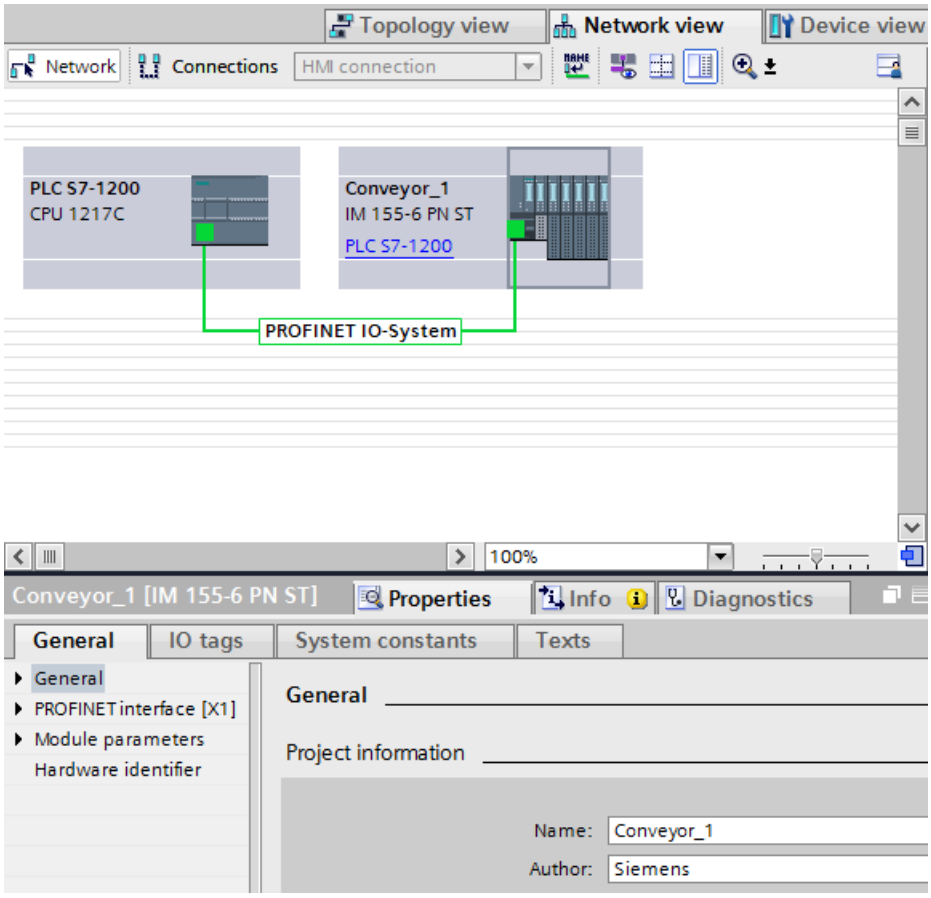
Error code* (W#16#...)	Explanation
0	No error
7000	No job in progress
7001	First call of the asynchronous Get_Name instruction. Execution of the instruction not yet complete (BUSY = 1, DONE = 0).
7002	Additional call of the asynchronous Get_Name instruction. Execution of the instruction not yet complete (BUSY = 1, DONE = 0).
8090	The hardware identifier specified at the LADDR parameter does not exist in the project.
8092	The value at the LADDR parameter does not address a PROFINET IO system.

Error code* (W#16#...)	Explanation
8093	Instruction does not support data type at the DATA parameter.
8095	Device number (STATION_NR parameter) does not exist in the selected PROFINET IO system or does not address an IO device.
80B1	The CPU used does not support the instruction.
80C3	Temporary resource error: The CPU is currently processing the maximum possible number of simultaneous block calls. Get_Name cannot be executed until at least one of the block calls is finished.
8852	The area specified at the DATA parameter is too short for the full name of the IO device. The name can be written up to the maximum possible length. To read the full name, use a longer data area at the DATA parameter. The area must have at least as many characters as there are at the LEN parameter.
* The error codes in the program editor can be displayed as integer or hexadecimal values.	

Example

The following example shows how you can read the station name of an ET 200SP PROFINET IO device:

1. Configuring the ET 200SP:
   - Create the ET 200SP with the station name "Conveyor_1" in the network view and assign it to the same PROFINET IO system as the CPU.
   - Assign the CPU as the IO controller for the ET 200SP.
   - Use the default device number "1" located in the Properties under "Ethernet addresses".

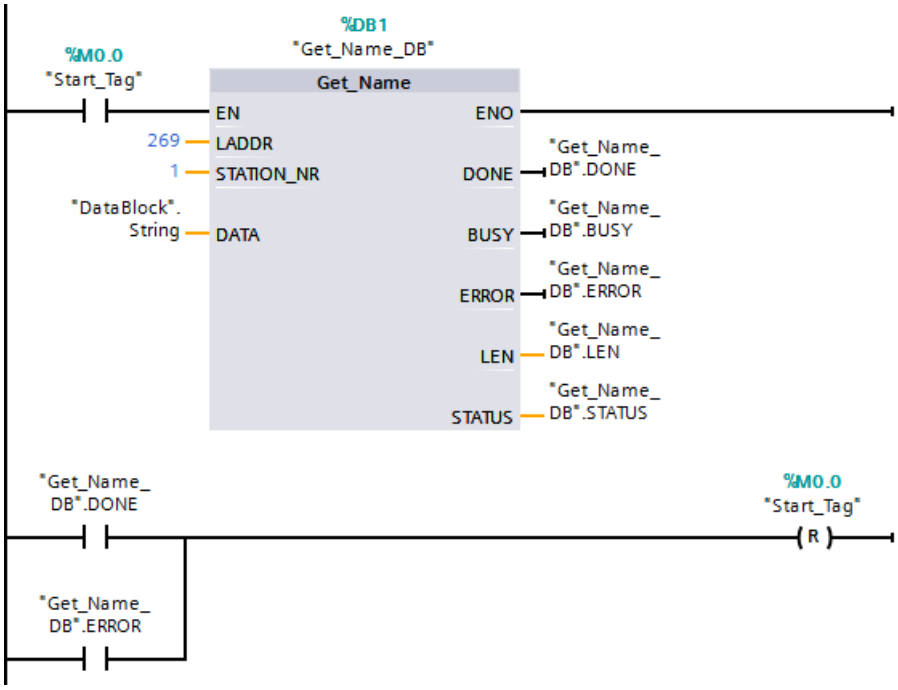


2. Assigning parameters for the Get_Name instruction:
   - Enter the hardware ID of the IO system at the LADDR parameter. In this example, the hardware ID is "269". You can find the hardware ID at the following location: PLC tags > Show all tags > System constants tab > Local-PROFINET_IO-System
   - Enter the device number of the ET 200SP at the STATION_NR parameter. In this example, the device number is "1".
   - Connect a tag with the data type STRING of a data block at the DATA parameter.

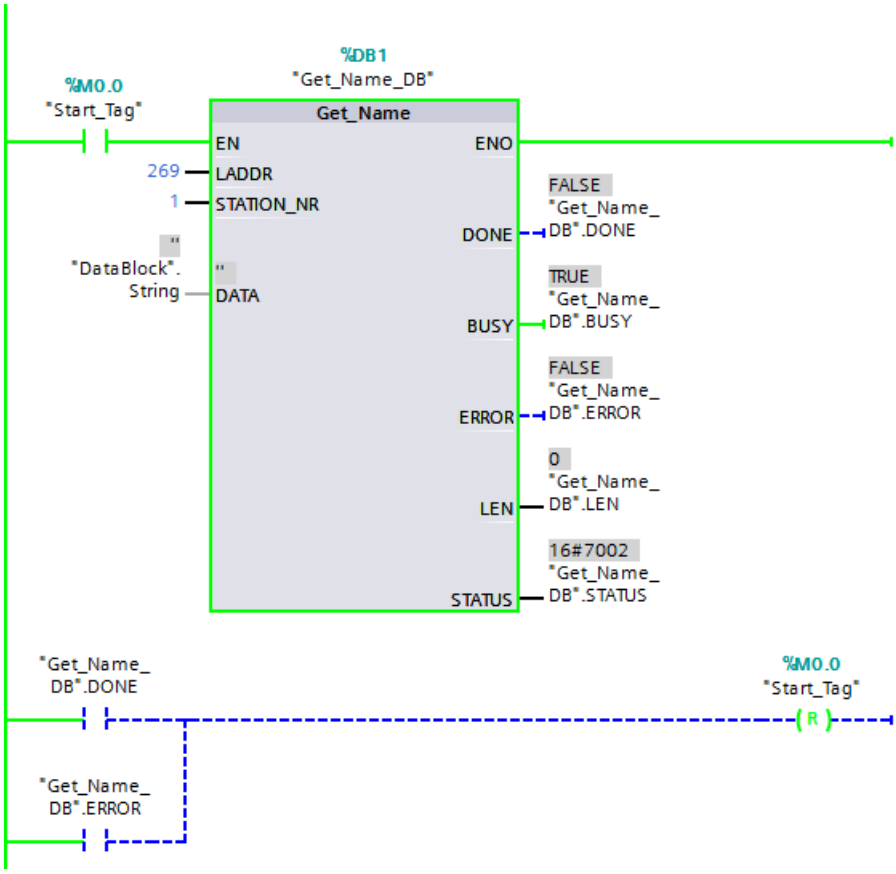
NOTE

When using the dropdown to make your selections for configuring the tag to the DATA parameter, select the DB (in the example, "Datablock") and the tag (in the example, "String[ ]"). In order to read the entire String data type, you must delete the brackets so that the final result is: "Datablock".String

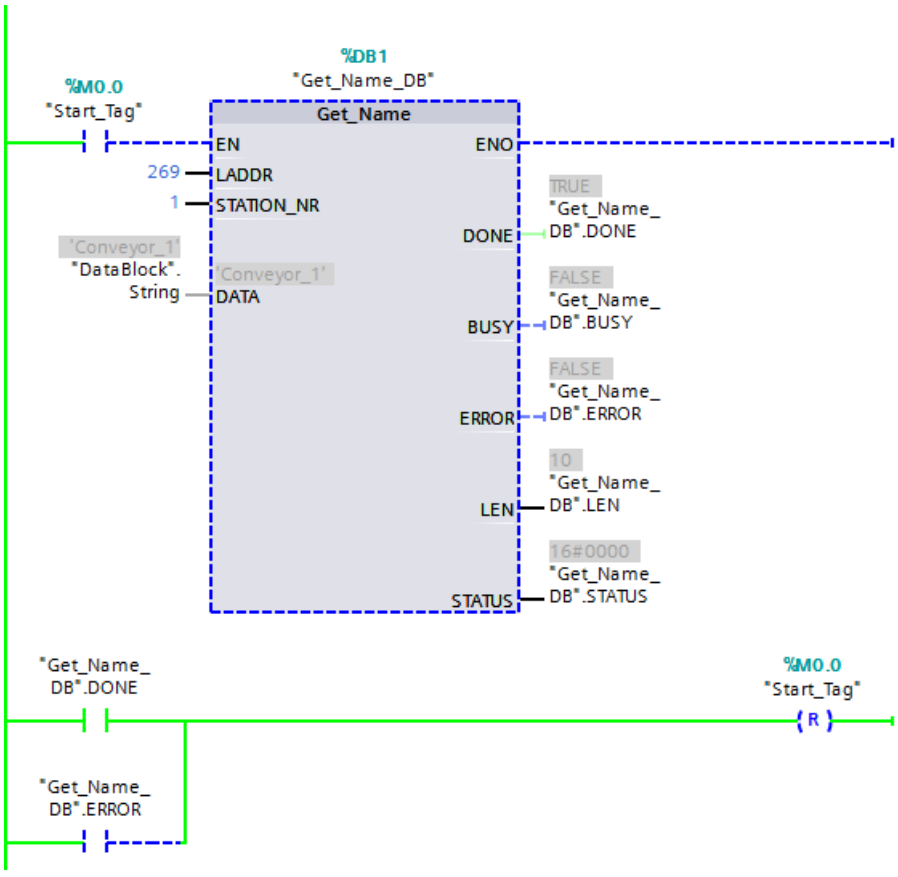
– Define PLC tags (memory area, flags) for the output parameters of the instruction.



3. Executing the Get_Name instruction:
   - As the instruction executes, the BUSY output parameter may get set to "1", and the DONE parameter is then set to "0".
   - Error code information is displayed at the STATUS output parameter.



4. Completing execution of the Get_Name instruction:
   - After execution of the instruction, the program writes "Conveyor_1", the station name of the ET 200SP, into the data block at the DATA parameter.
   - The program writes "10", the number of characters in the station name, to the LEN parameter.



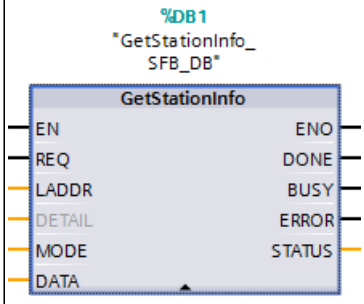
10.7.5 GetStationInfo (Read the IP or MAC address of a PROFINET IO device)

The "GetStationInfo" instruction reads the IP or MAC address of a PROFINET IO device in the local IO system or a PROFINET IO device located in a lower-level IO system (connected using CP/CM modules).

NOTE

You can only use the GetStationInfo instruction with PROFINET IO devices. You cannot use the instruction with PROFIBUS DP devices.

Table 10-155 GetStationInfo instruction

LAD / FBD	SCL	Description
	**"GetStationInfo_SFB_DB"(** **REQ:=_bool_in_,** **LADDR:=_uint_in_,** **DETAIL:=_uint_in_,** **MODE:=_uint_in_,** **DONE=>_bool_out_,** **BUSY=>_bool_out_,** **ERROR=>_bool_out_,** **STATUS=>_word_out_,** **DATA:=_variant_inout_);**	Use the GetStationInfo instruction to read the IP or MAC address of a PROFINET IO device. The instruction also enables you to read the IP or MAC address of an IO device located in a lower-level IO system (connected using CP/CM modules).

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "GetStationInfo_SFB_DB" is the name of the instance DB.

You address the IO device using the hardware identifier of the station at the LADDR parameter. You can find the hardware ID at the following location:
PLC tags > Show all tags > System constants tab. Search for the "IODevice" in the Name column and for "Hw_Device" in the Data type column.

Use the MODE parameter to select the information to be read.

At the DATA parameter, assign the data area to which the instruction writes the read address data. For storing the IP address, use the "IF_CONF_v4" structure. For storing the MAC address, use the "IF_CONF_MAC" structure.

Enable reading of the address data using the REQ control parameter. This requires the IO device to be accessible.

The instruction displays the execution status of the read job using the BUSY, DONE, and ERROR output parameters and the STATUS output parameter.

NOTE

Address the IO device using only the hardware identifier of the station

The station, the IO device, and PROFINET interface have their own hardware identifier. Use only the hardware identifier of the station for the GetStationInfo instruction.

If a PROFINET interface is addressed using the LADDR parameter, for example, the address data is not read and the CPU generates a "8092" error code.

To read the address data of an integrated PROFINET interface or a CM/CP module in the central configuration, use the "RDREC" instruction.

Parameters

The following table shows the parameters of the GetStationInfo instruction:

Parameter	Declaration	Data type	Description
REQ	IN	Bool	Control parameter request Activates the reading of the information with REQ = "1".
LADDR	IN	HW_DEVICE	Hardware identifier of the station of the IO device The number is taken from the properties of the station in the Network view or from the "System constants" tab of the default tag table.
DETAIL	IN	HW_SUBMODULE	The DETAIL parameter is not used. Leave the parameter unconnected.
MODE	IN	UNIT	Selection of address data to be read: • MODE = 1: Address parameter according to IPv4 • MODE = 2: MAC address
DATA	IN_OUT	Variant	Pointer to the area to which the program writes the address data of the IO device. Use the "IF_CONF_v4" structure for MODE = 1, and the "IF_CONF_MAC" structure for MODE = 2.
DONE	OUT	Bool	The program executed the instruction successfully. The program transferred the address data to the DATA parameter.
BUSY	OUT	Bool	STATUS parameter: • 0: Execution of the instruction complete. • 1: Execution of the instruction not yet complete.
ERROR	OUT	Bool	STATUS parameter: • 0: No error. • 1: An error occurred during execution of the instruction. Detailed information is output using the STATUS parameter.
STATUS	OUT	Word	STATUS parameter: The parameter is only set for the duration of one call. To display the status, you should therefore copy STATUS to a free data area.

DATA parameter

- Use the "IF_CONF_v4" structure at the DATA parameter to store the address parameter according to IPv4:

Byte	Parameter	Data type	Start value	Description
0 ... 1	Id	UINT	30	ID of the "IF_CONF_v4" structure
2 ... 3	Length	UNIT	18	Length of data read in BYTE
4 ... 5	Mode	UNIT	0	Not relevant for the "GetStationInfo" instruction (left at "0")
6 ... 9	InterfaceAddress	ARRAY [1..4] of BYTE	-	IP address of the IO device in the format IP_V4 (for example, 192.168.3.10): • addr[1] = 192 • addr[2] = 168 • addr[3] = 3 • addr[4] = 10

Byte	Parameter	Data type	Start value	Description
10 ... 13	SubnetMask	ARRAY [1..4] of BYTE	-	Subnet mask of the IO device in the format IP_V4 (for example, 255.255.255.0): • addr[1] = 255 • addr[2] = 255 • addr[3] = 255 • addr[4] = 0
14 ... 17	DefaultRouter	ARRAY [1..4] of BYTE	-	IP address of the router in the format IP_V4 (for example, 192.168.3.1): • addr[1] = 192 • addr[2] = 168 • addr[3] = 3 • addr[4] = 1

- Use the "IF_CONF_MAC" structure at parameter DATA for storing the MAC address:

Byte	Parameter	Data type	Start value	Description
0 ... 1	Id	UINT	3	ID of the "IF_CONF_MAC" structure
2 ... 3	Length	UNIT	12	Length of data read in BYTE
4 ... 5	Mode	UNIT	0	Not relevant for the "GetStationInfo" instruction (left at "0")
6 ... 11	MACAddress	ARRAY [1..6] of BYTE	-	MAC address of the IO device (for example, 08-00-06-12-34-56): • Mac[1] = 8 • Mac[2] = 0 • Mac[3] = 6 • Mac[4] = 12 • Mac[5] = 34 • Mac[6] = 56

STATUS parameter

Error code* (W#16#...)	Explanation
0	No error
7000	No job in progress
7001	First call of the asynchronous instruction GetStationInfo. Execution of the instruction not yet complete (BUSY = 1, DONE = 0).
7002	Additional call of the asynchronous instruction GetStationInfo. Execution of the instruction not yet complete (BUSY = 1, DONE = 0).
8080	Value at the MODE parameter is not supported.
8090	The hardware identifier specified at the LADDR parameter is not configured.
8092	The LADDR parameter does not address a PROFINET IO device.
8093	Invalid data type at the DATA parameter.
80A0	Requested information is not read.

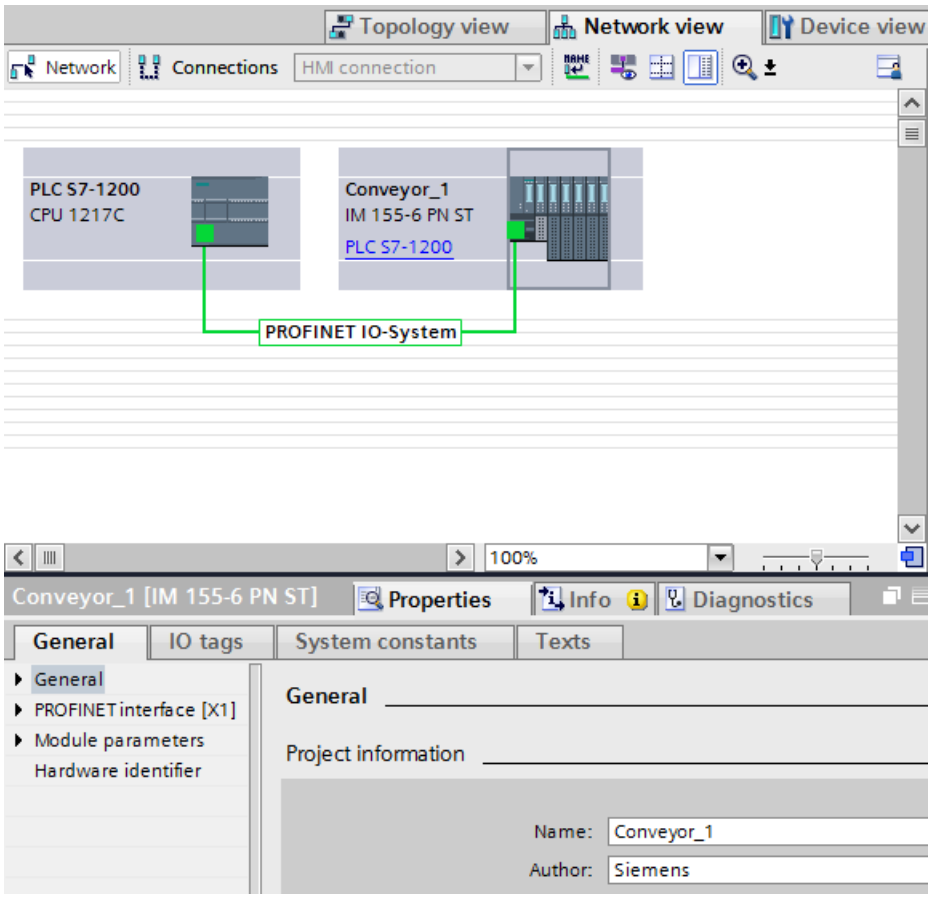
Error code* (W#16#...)	Explanation
80C0	Addressed IO device is not reachable.
80C3	The maximum number of simultaneous calls of the GetStationInfo instruction (10 instances) has been reached.
* The error codes in the program editor are displayed as integer or hexadecimal values.	

Example

In the example below, you use the GetStationInfo instruction to read the IP address data of an IO device and write the information to a data block. The IP address data includes the IP address, subnet mask, and (if used) the address data of the router.

The IO controller executes the GetStationInfo instruction, and the instruction reads the IP address information of a lower-level IO device (in this example, an ET200SP):

1. Configuring the ET 200SP:
   – Create the ET 200SP with the station name "Conveyor_1" in the network view, and assign it to the same PROFINET IO system as the CPU.
   – Assign the CPU as the IO controller for the ET 200SP.



2. Assigning parameters for the GetStationInfo instruction:
   – Create five tags and a structure with the IF_CONF_v4 data type in a global data block for storing the IP address data. Assign any name to the structure. (In the example, the structure name is "IP_Address".)

GetStationInfo_Global_DB

	Name	Data type	Start value
1	Static		
2	Execute	Bool	false
3	IP_address	IF_CONF_v4	
4	Id	UInt	30
5	Length	UInt	18
6	Mode	UInt	0
7	InterfaceAddress	IP_V4	
8	ADDR	Array[1..4] of Byte	
9	ADDR[1]	Byte	16#0
10	ADDR[2]	Byte	16#0
11	ADDR[3]	Byte	16#0
12	ADDR[4]	Byte	16#0
13	SubnetMask	IP_V4	
14	DefaultRouter	IP_V4	
15	Done	Bool	false
16	Busy	Bool	false
17	Error	Bool	false
18	Status	Word	16#0

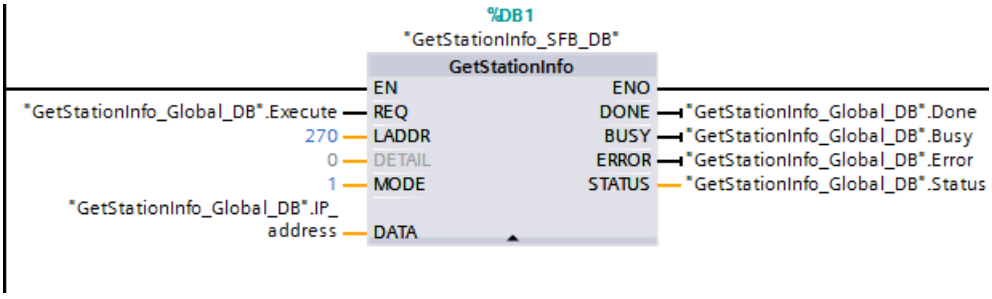
3. Assigning parameters for the GetStationInfo instruction:
   – Enter the hardware ID of the IO device at the LADDR parameter. The hardware identifier uniquely identifies the product, and, in this example, the hardware ID is "270". You can find the hardware ID at the following location: PLC tags > Show all tags > System constants tab

     Search for the IO device in the Name column and for the "Hw_Device" in the Data type column. The associated value is the hardware ID that you enter at the LADDR parameter.
   – Select "1" (read address parameters according to IPv4) for the MODE parameter.
   – Connect the IF_CONF_v4 structure at the DATA parameter.

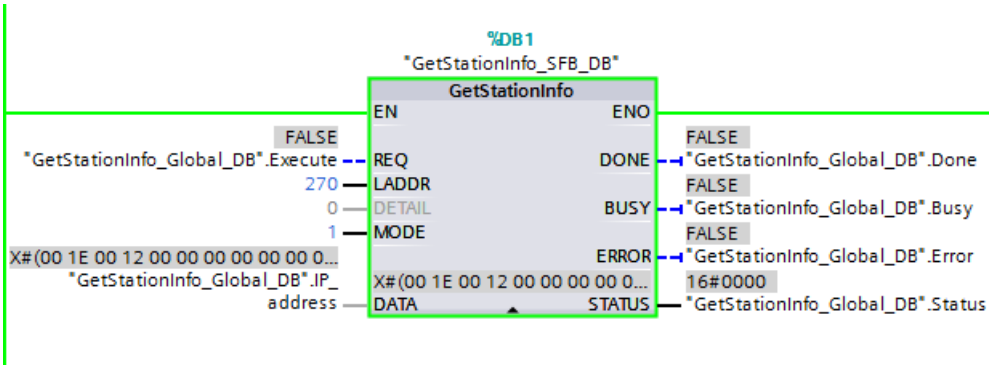
NOTE

When using the dropdown list to make your selections for configuring the tag to the DATA parameter, select the DB (in the example, "GetStationInfo_Global_DB") and the tag (in the example, "IP address"). In order to read the entire IF_CONF_v4 data type, you must delete the period that appears following "IP address" so that the final result is: "GetStationInfo_Global_DB".IP address

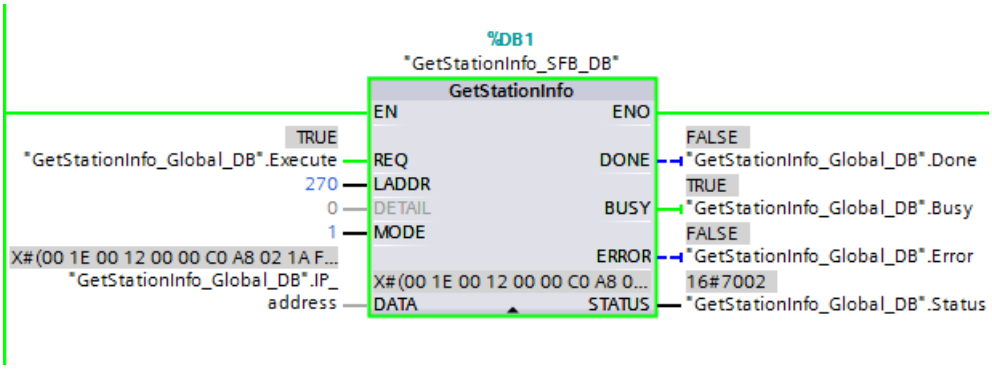
– Define PLC tags from your global DB for the output parameters of the instruction.



4. Executing the GetStationInfo instruction:
   – When the REQ input = 1 (FALSE), the instruction displays no IP address information at the DATA input/output parameter or error code information at the STATUS output parameter.



5. Completing execution of the GetStationInfo instruction:
   – When the REQ input = 1 (TRUE), the program executes the instruction and writes the IP address to the data block. The program writes the IP address, "C0 A8 02 1A" (decimal value of "192.168.2.26"), to the DATA input/output parameter.



GetStationInfo_Global_DB

	Name	Data type	Start value	Monitor value
1	Static			
2	Execute	Bool	false	TRUE
3	IP_address	IF_CONF_v4		
4	Id	UInt	30	30
5	Length	UInt	18	18
6	Mode	UInt	0	0
7	InterfaceAddress	IP_V4		
8	ADDR	Array[1..4] of Byte		
9	ADDR[1]	Byte	16#0	16#C0
10	ADDR[2]	Byte	16#0	16#A8
11	ADDR[3]	Byte	16#0	16#02
12	ADDR[4]	Byte	16#0	16#1A
13	SubnetMask	IP_V4		
14	DefaultRouter	IP_V4		
15	Done	Bool	false	TRUE
16	Busy	Bool	false	FALSE
17	Error	Bool	false	FALSE
18	Status	Word	16#0	16#0000

10.7.6 DeviceStates instruction

You can use the DeviceStates instruction to return the states of all distributed I/O slave devices connected to a specified distributed I/O Master.

Table 10-156 DeviceStates instruction

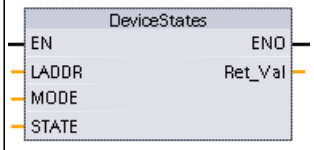
LAD / FBD	SCL	Description
	**ret_val := DeviceStates(** **laddr:=_word_in_,** **mode:=_uint_in_,** **state:=_variant_inout_);**	DeviceStates retrieves the I/O device operational states of an I/O subsystem. After execution, the STATE parameter contains the error state of each I/O device in a bit list (for the assigned LADDR and MODE). This information corresponds with the device status seen in the STEP 7 diagnostics view. The LADDR input of DeviceStates uses the hardware identifier of a distributed I/O interface. In the TIA portal, the hardware identifiers for a PLC can be found by looking for "HW_IOSYSTEM" data types in the system constants tab in the PLC tag table.

Table 10-157 Data types for the parameters

Parameter and type		Data type	Description
LADDR	IN	HW_IOSYSTEM	Logical address: (Identifier for the I/O system)
MODE	IN	UInt	Supports five modes of operation. The MODE input determines which data will be returned to the location specified for STATE information. The modes are as follows:

Parameter and type		Data type	Description
			• 1: Device configuration active • 2: Device defective • 3: Device disabled • 4: Device exists • 5: Problem in Device
RET_VAL	OUT	Int	Execution condition code
STATE[1]	InOut	Variant	Buffer that receives the error status of each device: The data type that you choose for the STATE parameter can be any bit type (Bool, Byte, Word, or DWord) or an array of a bit type • Bit 0 of the first byte of the returned STATE data is a summary bit. When it is set to TRUE, it indicates that other data is available. • The data returned by the STATE parameter shows a one-to-one correlation between a bit location and a distributed I/O address. This device addressing is TRUE for PROFIBUS and PROFINET. For example, Bit 4 in the first Byte correlates to PROFIBUS address 4 or PROFINET device number 4.

[1] For PROFIBUS-DP, the length of the status information is 128 bits. For PROFINET I/O, the length is 1024 bits.

After execution, the STATE parameter contains the error state of each I/O device as a bit list (for the assigned LADDR and MODE).

Table 10-158 Condition codes

RET_VAL (W#16#...)	Description
0	No error
8091	LADDR does not exist.
8092	LADDR does not address an I/O system.
8093	Invalid data type assigned for STATE parameter: Valid data types are (Bool, Byte, Word, or Dword), or an array of (Bools, Bytes, Words, or Dwords)
80Bx	DeviceStates instruction not supported by the CPU for this LADDR.
8452	The complete state data is too large for the assigned STATE parameter. The STATE buffer contains a partial result.

10.7.6.1 DeviceStates example configurations

PROFIBUS example

The PROFIBUS example consists of the following:

- 16 PROFIBUS devices named "DPSlave_10" through "DPSlave_25"
- The 16 PROFIBUS devices use PROFIBUS addresses 10 through 25, respectively.
- Each slave device is configured with multiple I/O modules.
- The first four bytes of the returned STATE parameter information is displayed.

MODE	Example 1: Normal operation with no errors	Example 2: PROFIBUS slave device DPSlave_12 with single module pulled	Example 3: PROFIBUS slave device DPSlave_12 disconnected
1: Device configuration active	0x01FC_FF03	0x01FC_FF03	0x01FC_FF03
2: Device defective	0x0000_0000	0x0110_0000	0x0110_0000
3: Device disabled	0x0000_0000	0x0000_0000	0x0000_0000
4: Device exists	0x01FC_FF03	0x01FC_FF03	0x01EC_FF03
5: Problem in device	0x0000_0000	0x0110_0000	0x0110_0000

The following four tables show a binary breakdown of the four bytes of data that are being analyzed:

Table 10-159 Example 1: No errors: A value of 0x01FC_FF03 is returned for MODE 1 (Device configuration active).

Byte with value	Bit pattern with value	Notes
Byte 1 0x01	Bit 7 0000-0001 Bit 0	Bit 0 is true; data is available.
Byte 2 0xFC	Bit 15 1111-1100 Bit 8	
Byte 3 0xFF	Bit 23 1111-1111 Bit 16	
Byte 4 0x03	Bit 31 0000-0011 Bit 24	

The devices are configured in addresses 10 (Bit 10) through 25 (Bit 25).
No devices are configured in addresses 1 through 9.
MODE 4 (Device exists) data matches MODE 1 (Device configuration active), so the configured devices match the existing devices.

Table 10-160 Example 2: A module has been pulled from PROFIBUS slave device "DPSlave_12". A value of 0x0110_0000 is returned for MODE 2 (Device defective).

Byte with value	Bit pattern with value	Notes
Byte 1 0x01	Bit 7 0000-0001 Bit 0	Bit 0 is true; data is available.
Byte 2 0x10	Bit 15 000**1**-0000 Bit 8	
Byte 3 0x00	Bit 23 0000-0000 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

Device 12 (Bit 12) is marked as defective.
MODE 5 (Problem in device) returns the same information as MODE 2 (Device defective).

Table 10-161 Example 2 (continued): A module has been pulled from PROFIBUS slave device "DPSlave_12". A value of 0x01FC_FF03 is returned for MODE 4 (Device exists).

Byte with value	Bit pattern with value	Notes
Byte 1 0x01	Bit 7 0000-0001 Bit 0	Bit 0 is true; data is available.
Byte 2 0xFC	Bit 15 111**1**-1100 Bit 8	
Byte 3 0xFF	Bit 23 1111-1111 Bit 16	
Byte 4 0x03	Bit 31 0000-0011 Bit 24	

Even though device 12 (Bit 12) has an error as shown in MODE 2 (Device defective) above, the device is still functioning on the network which causes MODE 4 (Device exists) to show the device as an "existing device".

Table 10-162 Example 3: PROFIBUS slave device "DPSlave_12" is disconnected (cable disconnected or power loss) from the PROFIBUS network. "DPSlave_12" is still detected as a defective device as well as an error in the device. The difference is that "DPSlave_12" is no longer detected as a device that exists. A value of 0x01EC_FF03 is returned for MODE 4 (Device exists).

Byte with value	Bit pattern with value	Notes
Byte 1 0x01	Bit 7 0000-0001 Bit 0	Bit 0 is true; data is available.
Byte 2 0xEC	Bit 15 111**0**-1100 Bit 8	
Byte 3 0xFF	Bit 23 1111-1111 Bit 16	
Byte 4 0x03	Bit 31 0000-0011 Bit 24	

Device 12 (Bit 12) is marked as not existing. With this exception, devices 10 through 25 still report as existing.

PROFINET example

The PROFINET example consists of the following:

- 16 PROFINET slave devices named "et200s_1" through "et200s_16"
- The 16 PROFINET devices use PROFINET device numbers 1 through 16, respectively.
- Each slave device is configured with multiple I/O modules.
- The first four bytes of the returned STATE parameter information is displayed.

MODE	Example 1: Normal operation with no errors	Example 2: PROFINET slave et200s_1 module pulled	Example 3: PROFINET slave et200s_1 disconnected
1: Device configuration active	0xFFFF_0100	0xFFFF_0100	0xFFFF_0100
2 - Device defective	0x0000_0000	0x0300_0000	0x0300_0000
3 - Device disabled	0x0000_0000	0x0000_0000	0x0000_0000
4 - Device exists	0xFFFF_0100	0xFFFF_0100	0xFDFF_0100
5 - Problem in device	0x0000_0000	0x0300_0000	0x0300_0000

The following four tables show a binary breakdown of the four bytes of data that are being analyzed:

Table 10-163 Example 1: No errors: A value of 0xFFFF_0100 is returned for MODE 1 (Device configuration active).

Byte with value	Bit pattern with value	Notes
Byte 1 0xFF	Bit 7 1111-1111 Bit 0	Bit 0 is true; data is available.
Byte 2 0xFF	Bit 15 1111-1111 Bit 8	
Byte 3 0x01	Bit 23 0000-0001 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

The devices are configured in addresses 1 (Bit 1) through 16 (Bit 16).
No devices are configured in addresses 1 through 9.
MODE 4 (Device exists) data matches MODE 1 (Device configuration active), so the configured devices match the existing devices.

Table 10-164 Example 2: A module has been pulled from PROFINET slave device "et200s_1". A value of 0x0300_0000 is returned for MODE 2 (Device defective).

Byte with value	Bit pattern with value	Notes
Byte 1 0x03	Bit 7 0000-00**1**1 Bit 0	Bit 0 is true; data is available.
Byte 2 0x00	Bit 15 0000-0000 Bit 8	
Byte 3 0x00	Bit 23 0000-0000 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

Device 1 (Bit 1) is marked as defective. Since the device still exists, MODE 4 (Device exists) shows the same data as when operating normally.
MODE 5 (Problem in device) returns the same information as MODE 2 (Device defective).

Table 10-165 Example 2 (continued): A module has been pulled from PROFIBUS slave device "et200s_1". A value of 0xFFFF_0100 is returned for MODE 4 (Device exists).

Byte with value	Bit pattern with value	Notes
Byte 1 0xFF	Bit 7 1111-11**1**1 Bit 0	Bit 0 is true; data is available.
Byte 2 0xFF	Bit 15 1111-1111 Bit 8	
Byte 3 0x01	Bit 23 0000-0001 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

Even though device 1 (Bit 1) has an error as shown in MODE 2 (Device defective) above, the device is still functioning on the network which causes MODE 4 (Device exists) to show the device as an "existing device".

Table 10-166 Example 3: PROFINET slave device "et200s_1" is disconnected (cable disconnected or power loss) from the PROFINET network. A value of 0xFDFF_0100 is returned for MODE 4 (Device exists).

Byte with value	Bit pattern with value	Notes
Byte 1 0xFD	Bit 7 1111-11**0**1 Bit 0	Bit 0 is true; data is available.
Byte 2 0xFF	Bit 15 1111-1111 Bit 8	
Byte 3 0x01	Bit 23 0000-0001 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

Device 1 (Bit 1) does not exist. Devices 2 (Bit 2) through 16 (Bit 16) do exist.

10.7.7 ModuleStates instruction

You can use the ModuleStates instruction to return the status of all of the modules in a PROFIBUS or PROFINET station.

Table 10-167 ModuleStates instruction

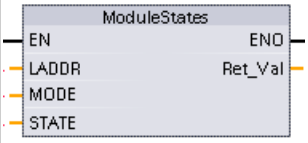
LAD / FBD	SCL	Description
	**ret_val := ModuleStates(laddr:=_word_in_, mode:=_uint_in, state:=_variant_inout);**	ModuleStates retrieves the operational states of I/O modules. After execution, the STATE parameter contains the error state of each I/O module in a bit list (for the assigned LADDR and MODE). This information corresponds with the module status seen in the STEP 7 diagnostics view. The LADDR input of ModuleStates uses is a hardware identifier of a distributed I/O station and not of the head module itself. The hardware identifier can be found by selecting the entire station in the network view and then looking in the hardware identifier section under properties. It can also be found by looking for "Hw_Device" and "Hw_DpSlave" data types in the system constants tab in the PLC tag table.

Table 10-168 Data types for the parameters

Parameter and type		Data type	Description
LADDR	IN	HW_DEVICE	Logical address (Identifier for the I/O modules)
MODE	IN	UInt	Supports five modes of operation. The MODE input determines which data will be returned to the location specified for STATE information. The modes are as follows: • 1: Module configuration active • 2: Module defective • 3: Module disabled • 4: Module exists • 5: Problem in Module
RET_VAL	OUT	Int	Status (condition code)
STATE[1]	InOut	Variant	Buffer that receives the error status of each module: The data type you use for the STATE parameter can be any bit type (Bool, Byte, Word, or DWord) or an array of a bit type. • Bit 0 of the first byte of the returned STATE data is a summary bit. When it is set to TRUE, it indicates that other data is available. • The data returned by the STATE parameter shows a one-to-one correlation between a bit location and a module position. This slot addressing is TRUE for PROFIBUS and PROFINET. For example, for an ET 200SP with a head module, power module, and a pair of I/O modules, Bit 1 in the first Byte correlates to the head module, Bit 2 to the power module, and Bits 3 and 4 to the I/O modules, respectively.

[1] A maximum of 128 bits can be assigned. The number of bits required is dependent on your I/O module usage.

Table 10-169 Condition codes

RET_VAL (W#16#...)	Description
0	No error
8091	Module identified by LADDR does not exist.
8092	Module identified by LADDR does not address an I/O device.
8093	Invalid data type for STATE parameter: Valid data types are (Bool, Byte, Word, or Dword), or an array of (Bools, Bytes, Words, or Dwords).
80Bx	ModuleStates instruction not supported by this CPU for this LADDR.
8452	The complete state data is too large for the assigned STATE parameter. The STATE buffer contains a partial result.

10.7.7.1 ModuleStates example configurations

PROFIBUS example

The PROFIBUS example consists of the following:

- 16 PROFIBUS devices named "DPSlave_10" through "DPSlave_25"
- The 16 PROFIBUS devices use PROFIBUS addresses 10 through 25, respectively.
- Each slave device is configured with multiple I/O modules.
- The example uses the LADDR parameter of PROFIBUS slave "DPSlave_12" which contains a head module, a power module, and two I/O modules.
- The first four bytes of the returned STATE parameter information is displayed.

MODE	Example 1: Normal operation with no errors	Example 2: PROFIBUS slave device DPSlave_12 module pulled	Example 3: PROFIBUS slave device DPSlave_12 disconnected
1: Module configuration active	0x1F00_0000	0x1F00_0000	0x1F00_0000
2: Module defective	0x0000_0000	0x0900_0000	0x1F00_0000
3: Module disabled	0x0000_0000	0x0000_0000	0x0000_0000
4: Module exists	0x1F00_0000	0x1700_0000	0x0000_0000
5: Problem in module	0x0000_0000	0x0900_0000	0x1F00_0000

The following four tables show a binary breakdown of the four bytes of data that are being analyzed:

Table 10-170 Example 1: No errors: A value of 0x1F00_0000 is returned for MODE 1 (Module configuration active).

Byte with value	Bit pattern with value	Notes
Byte 1 0x1F	Bit 7 0001-1111 Bit 0	Bit 0 is true; data is available.
Byte 2 0x00	Bit 15 0000-0000 Bit 8	
Byte 3 0x00	Bit 23 0000-0000 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

Slots 1 (Bit 1) through 4 (Bit 4) contain modules. Slots 5 (Bit 5) and beyond do not contain modules. MODE 4 (Module exists) data matches MODE 1 (Module configuration active), so the configured modules match the existing modules.

Table 10-171 Example 2: A module has been pulled from PROFIBUS slave device "DPSlave_12". A value of 0x0900_0000 is returned for MODE 2 (Module defective).

Byte with value	Bit pattern with value	Notes
Byte 1 0x09	Bit 7 0000-**1**001 Bit 0	Bit 0 is true; data is available.
Byte 2 0x00	Bit 15 0000-0000 Bit 8	
Byte 3 0x00	Bit 23 0000-0000 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

Only module 3 (Bit 3) is marked as defective. All other modules are functional.

Table 10-172 Example 2 (continued): A module has been pulled from PROFIBUS slave device "DPSlave_12". A value of 0x1700_0000 is returned for MODE 4 (Module exists).

Byte with value	Bit pattern with value	Notes
Byte 1 0x17	Bit 7 0001-**0**111 Bit 0	Bit 0 is true; data is available.
Byte 2 0x00	Bit 15 0000-0000 Bit 8	
Byte 3 0x00	Bit 23 0000-0000 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

Module 3 (Bit 3) is shown as missing. Modules 1, 2, and 4 (Bits 1, 2, and 4) are shown as existing.

Table 10-173 Example 3: PROFIBUS slave device "DPSlave_12" is disconnected (cable disconnected or power loss) from the PROFIBUS network. A value of 0x1F00_0000 is returned for MODE 2 (Module defective).

Byte with value	Bit pattern with value	Notes
Byte 1 0x1F	Bit 7 000**1**-1111 Bit 0	Bit 0 is true; data is available.
Byte 2 0x00	Bit 15 0000-0000 Bit 8	
Byte 3 0x00	Bit 23 0000-0000 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

The modules in slots 1 through 4 (Bits 1 through 4) are all marked as defective since the device is missing.
MODE 5 (Problem in module) shows the same information as MODE 2 (Module defective).

PROFINET example

The PROFINET example consists of the following:

- 16 PROFINET slave devices named "et200s_1" through "et200s_16"
- The 16 PROFINET devices use PROFINET device numbers 1 through 16, respectively.
- Each slave device is configured with multiple I/O modules.
- The example uses PROFINET slave "et200s_1" which contains a head module, a power module, and 18 I/O modules.
- The first four bytes of the returned STATE parameter information is displayed.

MODE	Example 1: Normal operation with no errors	Example 2: PROFINET et200s_1 slave module pulled	Example 3: PROFINET et200s_1 slave disconnected
1: Module configuration active	0xFFFF_1F00	0xFFFF_1F00	0xFFFF_1F00
2: Module defective	0x0000_0000	0x0180_0000	0xFFFF_1F00
3: Module disabled	0x0000_0000	0x0000_0000	0x0000_0000
4: Module exists	0xFFFF_1F00	0xFF7F_1F00	0x0000_0000
5: Problem in module	0x0000_0000	0x0180_0000	0xFFFF_1F00

The following four tables show a binary breakdown of the four bytes of data that are being analyzed:

Table 10-174 Example 1: No errors: A value of 0xFFFF_1F00 is returned for MODE 1 (Module configuration active).

Byte with value	Bit pattern with value	Notes
Byte 1 0xFF	Bit 7 1111-1111 Bit 0	Bit 0 is true; data is available.
Byte 2 0xFF	Bit 15 1111-1111 Bit 8	
Byte 3 0x1F	Bit 23 0001-1111 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

Slots 1 (Bit 1) through 20 (Bit 20) contain modules. Slot 21 (Bit 21) and beyond do not contain modules. MODE 4 (Module exists) data matches MODE 1 (Module configuration active), so the configured modules match the existing modules.

Table 10-175 Example 2: A module has been pulled from PROFINET slave device "et200s_1". A value of 0x0180_0000 is returned for MODE 2 (Module defective).

Byte with value	Bit pattern with value	Notes
Byte 1 0x01	Bit 7 0000-0001 Bit 0	Bit 0 is true; data is available.
Byte 2 0x80	Bit 15 **1**000-0000 Bit 8	
Byte 3 0x00	Bit 23 0000-0000 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

Only module 15 (Bit 15) is marked as defective. All other modules are functional.

Table 10-176 Example 2 (continued): A module has been pulled from PROFIBUS slave device "et200s_1". A value of 0xFF7F_1F00 is returned for MODE 4 (Module exists).

Byte with value	Bit pattern with value	Notes
Byte 1 0xFF	Bit 7 1111-1111 Bit 0	Bit 0 is true; data is available.
Byte 2 0x7F	Bit 15 **0**111-1111 Bit 8	
Byte 3 0x1F	Bit 23 0001-1111 Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

Module 15 (Bit 15) is shown as missing. Modules 1 through 14 (Bits 1 through 14) and 16 through 20 (Bits 16 through 20) are shown as existing.

Table 10-177 Example 3: PROFINET slave device "et200s_1" is disconnected (cable disconnected or power loss) from the PROFINET network. A value of 0xFFFF_1F00 is returned for MODE 2 (Module defective).

Byte with value	Bit pattern with value	Notes
Byte 1 0xFF	Bit 7 **1111**-**1111** Bit 0	Bit 0 is true; data is available.
Byte 2 0xFF	Bit 15 **1111**-**1111** Bit 8	
Byte 3 0x1F	Bit 23 000**1**-**1111** Bit 16	
Byte 4 0x00	Bit 31 0000-0000 Bit 24	

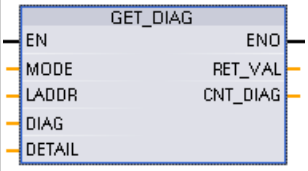
The modules in slots 1 through 20 (Bits 1 through 20) are all marked as defective since the device is missing.
MODE 5 (Problem in module) shows the same information as MODE 2 (Module defective).

10.7.8 GET_DIAG (Read diagnostic information)

Description

You can use the "GET_DIAG" instruction to read out the diagnostic information of a hardware device. The hardware device is selected with the LADDR parameter. With the MODE parameter, you select which diagnostic information to read.

Table 10-178 GET_DIAG instruction

LAD / FBD	SCL	Description
	**ret_val := GET_DIAG(** **mode:=_uint_in_,** **laddr:=_word_in_,** **cnt_diag=>_uint_out_,** **diag:=_variant_inout_,** **detail:=_variant_inout_);**	Reads the diagnostic information from an assigned hardware device.

Parameters

The following table shows the parameters of the "GET_DIAG" instruction:

Table 10-179 Data types for the parameters

Parameter and type		Data type	Description
MODE	IN	UInt	Use the MODE parameter to select which diagnostic data is to be output.
LADDR	IN	HW_ANY (Word)	Hardware ID of the device
RET_VAL	OUT	Int	Status of the instruction
CNT_DIAG	OUT	UInt	Number of output diagnostic details
DIAG	InOut	Variant	Pointer to data area for storage of diagnostic information of the selected mode
DETAILS	InOut	Variant	Pointer to data area for storage of diagnostic details in accordance with the selected mode

MODE parameter

Depending on the value at the MODE parameter, different diagnostics data is output at the DIAG, CNT_DIAG and DETAILS output parameters:

Table 10-180 MODE parameter

MODE	Description	DIAG	CNT_DIAG	DETAILS
0	Output of all supported diagnostic information for a module as DWord, where Bit X=1 indicates that mode X is supported.	Bit string of the supported modes as DWord, where Bit X=1 indicates that mode X is supported. The S7-1200 CPU ignores the LADDR parameter when the MODE parameter is 0.	0	-
1	Output of the inherent status of the addressed hardware object.	Diagnostics status: Output in accordance with the DIS structure. (Note: Refer to the "DIS structure" information below and GET_DIAG instruction example at the end of the section.)	0	-
2	Output of the status of all subordinate modules of the addressed hardware object.	Output of diagnostics data in accordance with the DNN structure. (Note: Refer to the "DNN structure" information below and GET_DIAG instruction example at the end of the section.)	0	-

DIS structure

With the MODE parameter = 1, the diagnostics information is output in accordance with the DIS structure. The following table shows the meaning of the individual parameter values:

Table 10-181 Structure of the Diagnostic Information Source (DIS)

Parameter	Data type	Value	Description
MaintenanceState	DWord	Enum	
		0	No maintenance required
		1	The module or device is disabled.
		2	-
		3	-
		4	-
		5	Maintenance required
		6	Maintenance demanded
		7	Error
		8	Status unknown / error in subordinate module
		9	-
		10	Inputs/outputs are not available.
Componentstate Detail	DWord	Bit array	Status of the module submodules: • Bit 0 to 15: Status message of the module • Bit 16 to 31: Status message of the CPU
		0 to 2 (enum)	Additional information: • Bit 0: No additional information • Bit 1: Transfer not permitted
		3	Bit 3 = 1: At least one channel supports qualifiers for diagnostics.
		4	Bit 4 = 1: Maintenance required for at least one channel or one component
		5	Bit 5 = 1: Maintenance demanded for at least one channel or one component
		6	Bit 6 = 1: Error in at least one channel or one component
		7 to 10	Reserved (always = 0)
		11 to 14	Bit 11 = 1: PNIO - submodule correct Bit 12 = 1: PNIO - replacement module Bit 13 = 1: PNIO - incorrect module Bit 14 = 1: PNIO - module disconnected
		15	Reserved (always = 0)
		16 to 31	Status information for modules generated by the CPU: Bit 16 = 1: Module disabled Bit 17 = 1: CiR operation active Bit 18 = 1: Input not available Bit 19 = 1: Output not available Bit 20 = 1: Overflow diagnostics buffer Bit 21 = 1: Diagnostics not available Bit 22 - 31: Reserved (always 0)
OwnState	Uint16	Enum	The value of the OwnState parameter describes the maintenance status of the module.

Parameter	Data type	Value	Description
OwnState	Uint16	0	No fault
		1	The module or device is disabled.
		2	Maintenance required
		3	Maintenance demanded
		4	Error
		5	The module or the device cannot be reached from the CPU (valid for modules and devices below a CPU).
		6	Inputs/outputs are not available.
		7	-
IO State	Uint16	Bit array	I/O status of the module
		0	Bit 0 = 1: No maintenance required
		1	Bit 1 = 1: The module or device is disabled.
		2	Bit 2 = 1: Maintenance required
		3	Bit 3 = 1: Maintenance demanded
		4	Bit 4 = 1: Error
		5	Bit 5 = 1: The module or the device cannot be reached from the CPU (valid for modules and devices below a CPU).
		6	Qualifier; bit 7 = 1, if bit 0, 2, or 3 are set
		7	Inputs/outputs are not available.
		8 to 15	Reserved (always = 0)
OperatingState	UInt16	Enum	
		0	-
		1	In STOP / firmware update
		2	In STOP / reset memory
		3	In STOP / self start
		4	In STOP
		5	Memory reset
		6	In START
		7	In RUN
		8	-
		9	In HOLD
		10	-
		11	-
		12	Module defective
		13	-
		14	No power
		15	CiR
		16	In STOP / without DIS
		17	In

Parameter	Data type	Value	Description
OperatingState	UInt16	18	
		19	
		20	

DNN structure

With the MODE parameter = 2, the diagnostics information details are output in accordance with the DNN structure. The following table shows the meaning of the individual parameter values:

Table 10-182 Structure of the Diagnostic Navigation Node (DNN)

Parameter	Data type	Value	Description
SubordinateState	UINT	Enum	Status of the subordinate module (See parameter OwnState of the DIS structure.)
SubordinateIOState	WORD	Bitarray	Status of the inputs and outputs of the subordinate module (See parameter IO State of the DIS structure.)
DNNmode	WORD	Bitarray	• Bit 0 = 0: Diagnostics enabled • Bit 0 = 1: Diagnostics disabled • Bit 1 to 15: Reserved

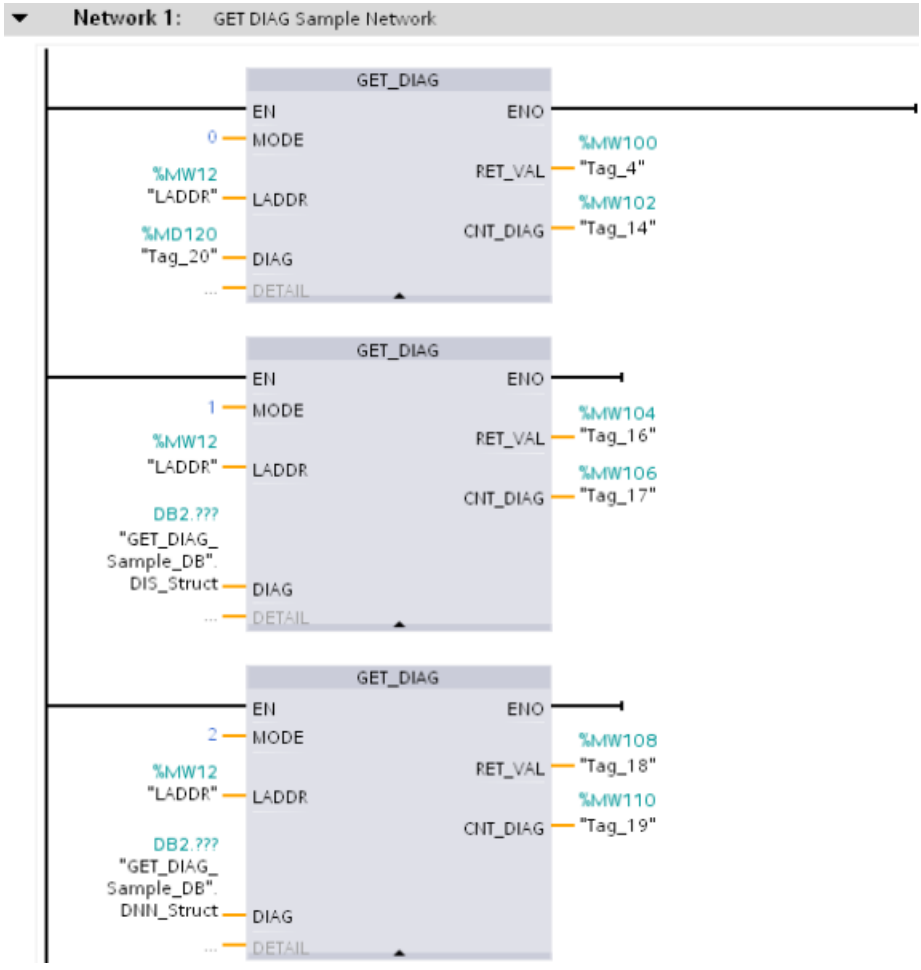
RET_VAL parameter

Table 10-183 Error codes of the RET_VAL parameter

Error code (W#16#...)	Description
0	No error
8080	Value in the MODE parameter is not supported.
8081	Type in the DIAG parameter is not supported with the selected mode (parameter MODE).
8082	Type in the DETAILS parameter is not supported with the selected mode (parameter MODE).
8090	LADDR does not exist.
8091	The selected channel in the CHANNEL parameter does not exist.
80C1	Insufficient resources for parallel execution

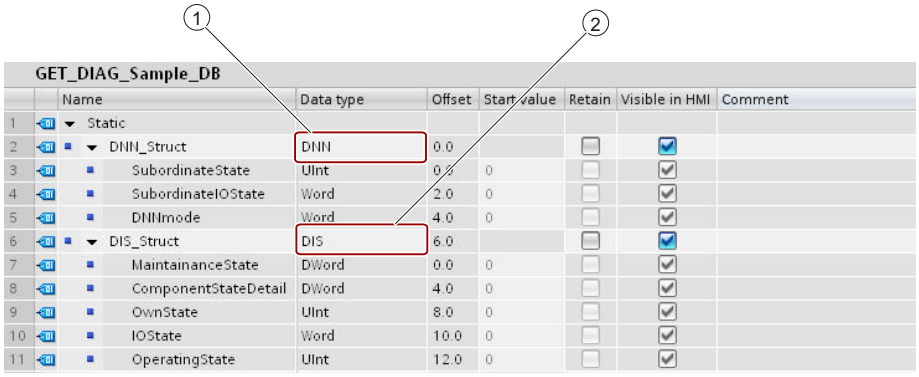
Example

The following ladder logic network and DB show how to use the three modes with the three modes:



Sample data block with the DNN and DIS structures

In the DB, you must type in DNN and DIS for the Data type. They do not appear in the Data type dropdown list.

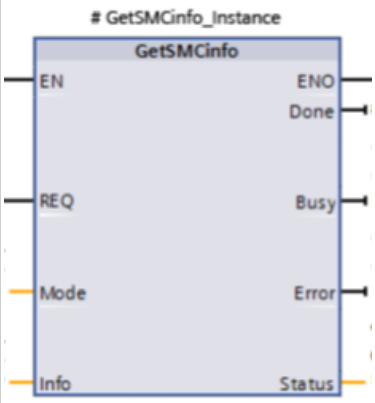


	Name	Data type	Offset	Start value	Retain	Visible in HMI	Comment
1	Static						
2	DNN_Struct	DNN	0.0			☑	
3	SubordinateState	UInt	0.0	0		☑	
4	SubordinateIOState	Word	2.0	0		☑	
5	DNNmode	Word	4.0	0		☑	
6	DIS_Struct	DIS	6.0			☑	
7	MaintainanceState	DWord	0.0	0		☑	
8	ComponentStateDetail	DWord	4.0	0		☑	
9	OwnState	UInt	8.0	0		☑	
10	IOState	Word	10.0	0		☑	
11	OperatingState	UInt	12.0	0		☑	

10.7.9 GetSMCInfo (Reading out information about the memory card)

The "GetSMCinfo" instruction retrieves information about the inserted SIMATIC memory card. The information to be read out is selected with the parameter, "Mode".

Table 10-184 GetSMCinfo instruction

LAD / FBD	SCL	Description
	**ret_val := GetSMCinfo(Mode:=_uint_in_, Info:=_variant_inout_);**	With the “GetSMCinfo“ instruction you read information about the inserted memory card. If no memory card is inserted the instruction returns the error code W#16#8081. You use the "Mode" parameter to select the information to be read.

Parameters

The following table shows the parameters of the "GetSMCinfo" instruction:

Parameter and type		Data type	Description
REQ	IN	Bool	Control parameter Request Activates the reading of the information with REQ = "1".
Mode	IN	UInt	Use the Mode parameter to select the information about the SIMATIC memory card that you want to read out: • 0: Memory size in KiB (1 KiB = 1024 bytes) • 1: Memory in use in KiB • 2: Maintenance information: Previously used up portion of the service life in % Note: – The S7-1200 now provides the maintenance information. With S7-PLCSIM, 0x00 is always entered in Info (no maintenance information available). – If the information is not supported by the SIMATIC Memory Card or the currently installed firmware of your CPU, 0xFF is entered in Info. • 3: When the set service life % threshold is exceeded, the PLC creates a diagnostics buffer entry and activates the maintenance LED. Note: –If you have disabled the generation of diagnostics interrupts, 0xFF is entered in Info. –With the S7-PLCSIM, 0xFF is always entered in Info. • 10 or 20: Corresponds with Mode 0, but reserved for S7-1500-R/H CPUs. • 11 or 21: Corresponds with Mode 1, but reserved for S7-1500-R/H CPUs. • 12 or 22: Corresponds to Mode 2, but reserved for S7-1500-R/H CPUs. • 13 or 23: Corresponds to Mode 3, but reserved for S7-1500-R/H CPUs.

Parameter and type		Data type	Description
Done	OUT	Bool	1: The instruction has been executed successfully. The information that was read is transferred to the Info parameter.
Busy	OUT	Bool	Status parameter • 0: Execution of the instruction complete • 1: Execution of the instruction not yet complete
Error	OUT	Bool	Status parameter • 0: No error. • 1: An error occurred during execution of the instruction Detailed information is output via the Status parameter
Status	OUT	Word	Error code
Info	INOUT	UDInt	Buffer for the information that was read

You can find additional information on valid data types under "Data types (Page 95)".

NOTE

Determining the I&M 0 data

The I&M 0 data of the memory card cannot be determined with the GetSMCinfo instruction. For this use the “Get_IM_Data (Page 383)” instruction.

Parameter status

Error code* (W#16#...)	Explanation
0	No error
7000	No job in progress.
7001	First call: Trigger job (Busy = 1, Done = 0).
7002	Intermediate call: Job already active (Busy = 1, Done = 0).
8080	Invalid value of the “Mode“ parameter
8081	No SIMATIC memory card inserted
8092	No data available, for example, because "GetSMCinfo" is not supported by the CPU
80C3	The maximum number of simultaneous calls of the "GetSMCinfo" instruction has been reached.

* The error codes in the program editor are displayed as integer or hexadecimal values. For information on switching the display formats, refer to "See also".

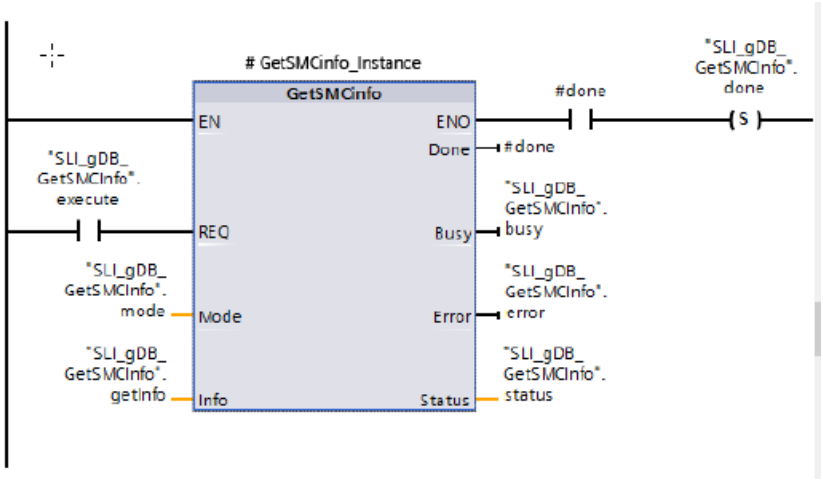
Example: Determine memory size of the SIMATIC memory card used

In the following example, you determine the memory size of the SIMATIC memory card used. Create the following tags for storing the data in a global data block:

SLI_gDB_GetSMCinfo

	Name	Data type	Start value
1	Static		
2	execute	Bool	false
3	mode	UInt	0
4	getInfo	UDInt	0
5	done	Bool	false
6	busy	Bool	false
7	error	Bool	false
8	status	Word	16#0

Create an FB. In the status area of the FB, create a local tag "#done" with the Bool data type. Interconnect the parameters of the "GetSMCinfo" instruction as follows.



The "GetSMCinfo" instruction is executed only when the input parameter REQ ("execute") returns the signal state "TRUE". The mode to be used for reading out the SIMATIC Memory Card is stored in the input parameter MODE ("mode"). In the example below, the memory size of the SIMATIC memory card is read according to the "mode" value being set to "0" and displayed in KB at parameter INFO ("getInfo"). The success status of GetSMCinfo is displayed at the output parameter DONE ("#done") and stored in the tag "done".

Output parameters STATUS ("status") and ERROR ("error") indicate that the processing in the example was completed without error.

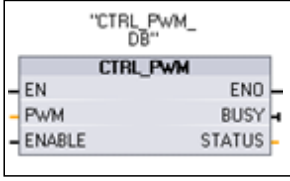
SLI_gDB_GetSMCinfo

	Name	Data type	Start value	Monitor value
1	Static			
2	execute	Bool	false	TRUE
3	mode	UInt	0	0
4	getInfo	UDInt	0	2025008
5	done	Bool	false	TRUE
6	busy	Bool	false	FALSE
7	error	Bool	false	FALSE
8	status	Word	16#0	16#0000

10.8 Pulse

10.8.1 CTRL_PWM (Pulse width modulation)

Table 10-185 CTRL_PWM (Pulse Width Modulation) instruction

LAD / FBD	SCL	Description
	**"CTRL_PWM_DB"(PWM:=_uint_in_, ENABLE:=_bool_in_, BUSY=>_bool_out_, STATUS=>_word_out_);**	Provides a fixed cycle time output with a variable duty cycle. The PWM output runs continuously after being started at the specified frequency (cycle time). The pulse width is varied as required to affect the desired control.

[1] When you insert the instruction, STEP 7 displays the "Call Options" dialog for creating the associated DB.

[2] In the SCL example, "CTRL_PWM_DB" is the name of the instance DB.

Table 10-186 Data types for the parameters

Parameter and type		Data type	Description
PWM	IN	HW_PWM (Word)	PWM identifier: Names of enabled pulse generators will become tags in the "constant" tag table, and will be available for use as the PWM parameter. (Default value: 0)
ENABLE	IN	Bool	1=start pulse generator 0 = stop pulse generator
BUSY	OUT	Bool	Function busy (Default value: 0)
STATUS	OUT	Word	Execution condition code (Default value: 0)

The CTRL_PWM instruction stores the parameter information in the DB. The data block parameters are not separately changed by the user, but are controlled by the CTRL_PWM instruction.

Specify the enabled pulse generator to use, by using its tag name for the PWM parameter.

When the EN input is TRUE, the PWM_CTRL instruction starts or stops the identified PWM based on the value at the ENABLE input. Pulse width is specified by the value in the associated Q word output address.

Because the CPU processes the request when the CTRL_PWM instruction is executed, parameter BUSY will always report FALSE. If an error is detected, then ENO is set to FALSE, and parameter STATUS contains a condition code.

The pulse width will be set to the initial value configured in device configuration when the CPU first enters RUN mode. You write values to the Q-word location specified in device configuration ("Output addresses" / "Start address:") as needed to change the pulse width. You use an instruction such as a move, convert, math, or PID box to write the desired pulse width to the appropriate Q word. You must use the valid range for the Q-word value (percent, thousandths, ten-thousandths, or S7 analog format).

NOTE

Digital I/O points assigned to PWM and PTO cannot be forced

The digital I/O points used by the pulse-width modulation (PWM) and pulse-train output (PTO) devices are assigned during device configuration. When digital I/O point addresses are assigned to these devices, the values of the assigned I/O point addresses cannot be modified by the Watch table force function.

Table 10-187 Value of the STATUS parameter

STATUS	Description
0	No error
80A1	PWM identifier does not address a valid PWM.

10.8.2 CTRL_PTO (Pulse train output)

The PTO instruction provides a square wave with a 50% duty cycle output at a specified frequency. You can use the CTRL_PTO instruction to assign the frequency without a Technology objects (TO) axis data block (DB).

This instruction requires a pulse generator. You must activate the pulse generator and select a signal type in the hardware configuration. Refer to "Configuring a pulse channel for PWM or PTO" (Page 421) for further information.

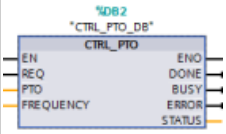
NOTE

The CTRL_PTO instruction cannot be used to select direction

You can use motion control move functions such as MC_MoveAbsolute in the S7-1200 CPU to select direction. You must first create a technology object within the STEP7 program. Configure the technology object as a pulse generator and select the signal type. The Direction or Position input of the motion instruction as either positive (+) or negative (-) values. The technology object outputs these values and allows for the performance of the motion.

You can access the CTRL_PTO instruction in the Task Cards, Extended instructions.

Table 10-188 CTRL_PTO (Pulse Train Output) instruction

LAD / FBD[1]	SCL[2]	Description
	**"CTRL_PTO_DB"(REQ:=_bool_in_, PTO:=_uint_in_, FREQUENCY:=_udint_in_, DONE=>_bool_out_, BUSY=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	The PTO instruction allows the user to control the frequency for a square wave (50% duty cycle) output.

[1] When you insert the instruction, STEP 7 displays the "Call Options" dialog for creating the associated DB.

[2] In the SCL example, "CTRL_PTO_DB" is the name of the instance DB.

Table 10-189 Data types for the parameters

Parameter and type		Data type	Description
EN	IN	Bool	1 = Instruction enabled 0 = Instruction disabled
REQ	IN	Bool	1 = Set PTO output frequency to value in FREQUENCY input 0 = No change to PTO
PTO	IN	HW_PTO (Word)	PTO identifier: Hardware ID of the pulse generator: • Names of the enabled pulse generators become tags in the "constant" tag table, and are available for use as the PTO parameter. (Default value = 0) • You can find the hardware ID in the Properties of the pulse generator in the Device view. The system constants also list the hardware IDs of the pulse generators. (Default value = 0)

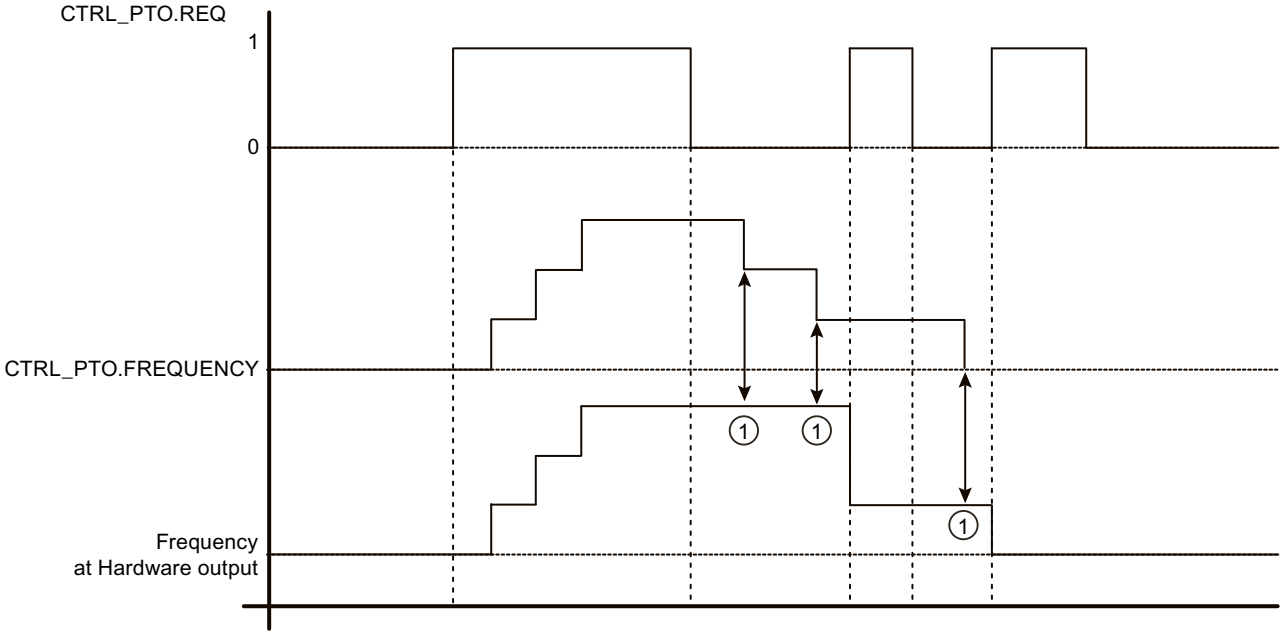
Parameter and type		Data type	Description
FREQUENCY	IN	UDInt	Desired frequency (in Hz) of the PTO. This value is applied only when REQ = 1 (Default value is 0 Hz)
DONE	OUT	Bool	Function completed without error (Default value: 0)
BUSY	OUT	Bool	Function busy (Default value: 0)
ERROR	OUT	Word	Error detected (Default value: 0)
STATUS	OUT	Word	Execution condition code (Default value: 0)

The CTRL_PTO instruction stores the parameter information in the DB. The data block parameters are not separately changed by the user, but are controlled by the CTRL_PTO instruction.

Specify the enabled pulse generator to use, by using its tag name or hardware identifier for the PTO parameter.

When the EN input is TRUE, the CTRL_PTO instruction starts or stops the identified PTO. When the EN input is FALSE, the CTRL_PTO instruction does not execute and the PTO maintains its current state.

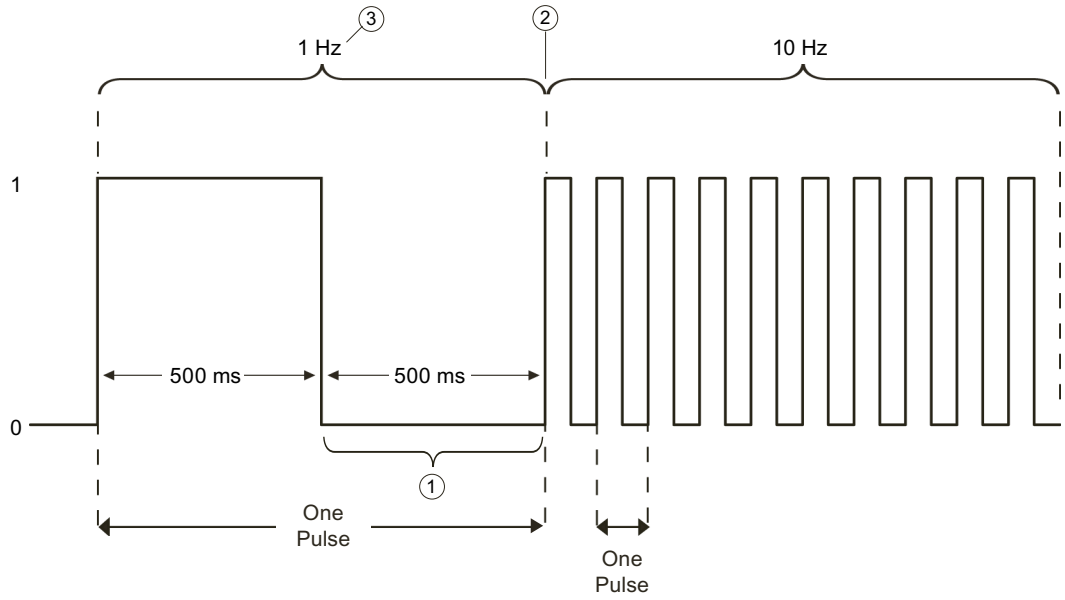
When you set the REQ input to TRUE, the FREQUENCY value takes effect. If REQ is FALSE, the PTO's output frequency cannot be changed, and the PTO continues to output pulses.



1 No change in output frequency while REQ = 0

Since the CTRL_PTO instruction only starts the PTO, the CTRL_PTO instruction finishes immediately. As a result, the BUSY output never turns on. The DONE output comes on as long as no error occurs. If an error is detected, the ERROR parameter is set to TRUE, and the STATUS parameter contains a condition code.

When the user enables the CTRL_PTO instruction with a given frequency, the S7-1200 outputs a pulse train at that given frequency. The user can change the desired frequency at any time. When the frequency is changed, the S7-1200 finishes the current pulse prior to changing frequency to the new desired frequency. For example, if the desired frequency is 1 Hz (which takes 1000ms to complete) and the user changes the frequency to 10 Hz after 500ms, the frequency changes at the end of the 1000ms time period.



① The user changes the frequency to 10 Hz after 500 ms.

② The 1 Hz pulse must finish before the frequency can change to the new 10 Hz frequency.

③ 1 Hz corresponds to 1000 ms

The pulse generator hardware object has the following restriction: Only one instruction can use the pulse generator as PTO, and the hardware configuration editor manages the use of the pulse generator. Other instructions that try to access that PTO return an error: "0x8090" (Pulse generator with the specified hardware ID is in use).

NOTE

Digital I/O points assigned to PWM and PTO cannot be forced

The digital I/O points used by the pulse width modulation (PWM) and pulse train output (PTO) devices are assigned during device configuration. When digital I/O point addresses are assigned to these devices, the values of the assigned I/O point addresses cannot be modified by the Watch table force function.

Table 10-190 STATUS parameter error code value

Error code (W#16#...)	Description
0	No errors
0x8090	Pulse generator with the specified hardware ID is in use.
0x8091	Frequency out-of-range. The desired frequency exceeds the maximum frequency of the pulse output selected.
0x80A1	PTO identifier (hardware ID) does not address a valid PTO.
0x80D0	Pulse generator with the specified hardware ID is not activated. Activate the pulse generator in the CPU properties under "Pulse generators (PTO/PWM)".
0x80D1	Pulse generator with the specified hardware ID has no PTO selection. Select PTO in Hardware Configuration.

10.8.3 Operation of the pulse outputs

① Cycle time

② Pulse width

Pulse width can be expressed as hundredths of the cycle time (0 to 100), as thousandths (0 to 1000), as ten thousandths (0 to 10000), or as S7 analog format. The pulse width can vary from 0 (no pulse, always off) to full scale (no pulse, always on).

Since the PWM output can be varied from 0 to full scale, it provides a digital output that in many ways is the same as an analog output. For example, the PWM output can be used to control the speed of a motor from stop to full speed, or it can be used to control position of a valve from closed to fully opened.

You configure frequency in the hardware configuration (Page 421). You control pulse width from the user program.

Four pulse generators are available for controlling high-speed pulse output functions: PWM and Pulse train output (PTO). PTO is used by the motion control instructions. You can assign each pulse generator to either PWM or PTO, but not both at the same time.

You can use onboard CPU outputs, or you can use the optional signal board outputs. The output point numbers are shown in the following table (assuming the default output configuration). If you have changed the output point numbering, then the output point numbers will be those you assigned. Note that PWM requires only one output, while PTO can optionally use two outputs per channel. If an output is not required for a pulse function, it is available for other uses. Refer to the table below for I/O assignment.

The table below shows the default I/O assignments; however, the four pulse generators can be configured to any CPU built-in or SB digital output. Different output points support different voltages and speeds, so take that into account when assigning PWM/PTO locations.

NOTE

Pulse-train outputs cannot be used by other instructions in the user program.

When you configure the outputs of the CPU or signal board as pulse generators (for use with the PWM or motion control PTO instructions), the corresponding outputs addresses are removed from the Q memory and cannot be used for other purposes in your user program. If your user program writes a value to an output used as a pulse generator, the CPU does not write that value to the physical output.

NOTE

PTO direction outputs can be freed for use elsewhere in your program.

Each PTO requires the assignment of two outputs: one as a pulse output and one as a direction output. You can use just the pulse output and not the direction output. You can then free the direction output for other purposes in your user program.

Table 10-191 Default output assignments for the pulse generators[3]

Description	Pulse	Direction
PTO1		
Built-in I/O	Q0.0	Q0.1
SB I/O	Q4.0	Q4.1
PWM1		
Built-in outputs	Q0.0	-
SB outputs	Q4.0	-
PTO2		
Built-in I/O	Q0.2	Q0.3
SB I/O	Q4.2	Q4.3
PWM2		
Built-in outputs	Q0.2	-
SB outputs	Q4.2	-
PTO3		
Built-in I/O	Q0.4[1]	Q0.5[1]
SB I/O	Q4.0	Q4.1
PWM3		
Built-in outputs	Q0.4[1]	-
SB outputs	Q4.1	-
PTO4		
Built-in I/O	Q0.6[2]	Q0.7[2]
SB I/O	Q4.2	Q4.3
PWM4		
Built-in outputs	Q0.6[2]	-
SB outputs	Q4.3	-

[1] The CPU 1211C does not have outputs Q0.4, Q0.5, Q0.6, or Q0.7. Therefore, these outputs cannot be used in the CPU 1211C.

[2] The CPU 1212C does not have outputs Q0.6 or Q0.7. Therefore, these outputs cannot be used in the CPU 1212C.

[3] This table applies to the CPU 1211C, CPU 1212C, CPU 1214C, CPU 1215C, and CPU 1217C PTO/PWM functions.

10.8.4 Configuring a pulse channel for PWM or PTO

To prepare for PWM or PTO operation, first configure a pulse channel in the device configuration by selecting the CPU, then Pulse Generator (PTO/PWM), and choose PWM1/PTO1 through PWM4/PTO4. Enable the pulse generator (check box). If a pulse generator is enabled, a unique default name is assigned to this particular pulse generator. You can change this name by editing it in the "Name:" edit box, but it must be a unique name. Names of enabled pulse generators will become tags in the "constant" tag table and will be available for use as one of the following:

- PWM parameter of the CTRL_PWM instruction
- PTO parameter of the CTRL_PTO instruction

You can also write a comment about this specific pulse generator in the "Comment:" edit box.

Table 10-192 CPU output: Maximum frequency (PTO) and minimum cycle time (PWM)

CPU	CPU output channel	PTO maximum frequency	PWM minimum cycle time
1211C	Qa.0 to Qa.3	100 kHz	10 µs
1212C	Qa.0 to Qa.3	100 kHz	10 µs
	Qa.4, Qa.5	20 kHz	50 µs
1214C and 1215C	Qa.0 to Qa.3	100kHz	10 µs
	Qa.4 to Qb.1	20 kHz	50 µs
1217C	DQa.0 to DQa.3 (.0+, .0- to .3+, .3-)	1 MHz	1 µs
	DQa.4 to DQb.1	100 kHz	10 µs

Table 10-193 SB signal board output: Maximum frequency (PTO) and minimum cycle time (PWM)

SB signal board	SB output channel	PTO maximum frequency	PWM minimum cycle time
SB 1222, 200 kHz	DQe.0 to DQe.3	200kHz	5 µs
SB 1223, 200 kHz	DQe.0, DQe.1	200kHz	5 µs
SB 1223	DQe.0, DQe.1	20 kHz	50 µs

NOTE

The minimum cycle time of each of the CPU and Signal Board outputs is given in the tables above. However, the TIA Portal does not alert you when you configure a PWM pulse generator with a cycle time that falls below the minimum cycle time of the hardware. Problems can result with your application, so always ensure that the cycle time lies within the hardware limits.

NOTE

When you set the Pulse duration of a PWM signal, the actual Pulse duration time (time that the pulse is high) must be greater than or equal to 1 millisecond if the Time base is "Milliseconds". If the Time base is "Microseconds", the actual Pulse duration time must be greater than or equal to 1 microsecond. The output turns off if the Pulse duration time is less than 1 "Time base".

For example, a Cycle time of 10 microseconds and a Pulse duration of 5 hundredths produces a Pulse duration time of 0.5 microseconds. Because this is less than 1 microsecond, the PWM signal is off.

Parameter assignment

The Parameter assignment section allows the user to configure the parameters of the output pulse. The following options are available, depending on whether PWM or PTO is selected:

- Signal type: Configure the pulse output as PWM or PTO. For PTO selections, refer to SIMATIC STEP 7 S7-1200 Motion Control (https://support.industry.siemens.com/cs/us/en/view/109773400) for further information:
  - PWM
  - PTO (pulse A and direction B)
  - PTO (pulse up A and pulse down B)
  - PTO (A/B phase-shifted)
  - PTO (A/B phase-shifted - fourfold)
- Time base (only applies to PWM): Select which units of time to use:
  - Milliseconds
  - Microseconds
- Pulse duration format (only applies to PWM): Assign the resolution of the pulse duration (width):
  - Hundredths (0 to 100)
  - Thousandths (0 to 1000)
  - Ten-thousandths (0 to 10000)
  - S7 analog format (0 to 27648)
- Cycle time (only applies to PWM): Assign the time duration it takes to complete one pulse (pulse high time plus pulse low time equals cycle time). You can change the cycle time at runtime by selecting the check box "Allow runtime modification of the cycle time". Refer to the "I/O addresses" section below for further information. Range is 1 to 16,777,215 units of time.
- Initial pulse duration (only applies to PWM): Assign the pulse duration of the first pulse. You can change this value at runtime using the Q word address configured in I/O addresses. Range is based upon the Pulse duration format.
- Allow runtime modification of the cycle time (only applies to PWM): Selecting this option allows your program to modify the cycle time of the PWM signal while the program is running. Refer to the "I/O addresses" section below for further information.

NOTE

When setting the pulse duration of a PWM signal, be sure to consider the switching delay of the output channel as specified in Appendix A. The actual pulse duration measured at the output may be greater than the selected pulse duration. The increase of the pulse duration is more pronounced for small pulse duration and higher frequencies. Be sure to verify that the pulse duration measured at the output matches your requirements.

Determining the Pulse duration value

"Pulse duration" is derived by multiplying the "Initial pulse duration" by the "Cycle time". When you select a "Time base", "Pulse duration format", "Cycle time", and "Initial pulse duration", you must keep in mind that the overall "Pulse duration" cannot be a fractional value. If your resulting "Pulse duration" is a fractional value, you should adjust your "Initial pulse duration" or change your "Time base" to generate an integer value.

Here are two examples:

- Example 1: If you select the following values:
  - Time base = Milliseconds (ms)
  - Pulse duration format = Hundredths (0 to 100)
  - Cycle time = 3 ms
  - Initial pulse duration = 75

  The resulting "Pulse duration" = .75 x 3 ms = 2.25 ms

  This "Pulse duration" value is fractional and causes an error when you operate the CTRL_PWM instruction. The "Pulse duration" value must be an integer value.
- Example 2: If you select the following values:
  - Time base = Microseconds (µs)
  - Pulse duration format = Hundredths (0 to 100)
  - Cycle time = 3000 µs
  - Initial pulse duration = 75

  The resulting "Pulse duration" = .75 x 3000 µs = 2250 µs

  This "Pulse duration" value is an integer value, and the CTRL_PWM instruction functions properly with this value.

Hardware outputs

In the hardware outputs section, select the output channel from the dropdown menu. Depending on the configuration, there may be one or two outputs to select. If you do assign an output channel to a pulse generator, the output channel cannot be used by another pulse generator, HSC, or the process image register.

NOTE

Pulse generator outputs cannot be used by other instructions in the user program

When you configure the outputs of the CPU or signal board as pulse generators (for use with the PWM, PTO, or motion control instructions), the corresponding outputs addresses are removed from the Q memory and cannot be used for other purposes in your program. If your program writes a value to an output used as a pulse generator, the CPU does not write that value to the physical output.

I/O addresses

The PWM has two bytes of Q memory designated for "Pulse duration". While the PWM is running, you can modify the value in the assigned Q memory and change the Pulse duration.

In the I/O Address section, enter the Q word address where you want to store the Pulse duration value.

The default addresses for the PWM Pulse duration values are as follows:

- PWM1: QW1000
- PWM2: QW1002
- PWM3: QW1004
- PWM4: QW1006

For the PWM, the value at this location controls the duration of the pulse and is initialized to the "Initial pulse duration:" value (assigned above) each time the CPU transitions from STOP to RUN mode. You change this Q-word value during runtime to cause a change in the pulse duration. The range of this value is dependent on the Pulse duration format configured under Parameter assignment.

You can also allocate an additional four bytes of Q memory for the "Cycle time" of the PWM signal. Refer to "Operation of the pulse outputs" (Page 419) for a diagram of the PWM signal. When you select the "Allow runtime modification of the cycle time" check box, the first two bytes hold the Pulse duration value and the last four bytes hold the Cycle time value.

While the PWM is running, you can modify the value of the double word at the end of the Q memory that is allocated to that PWM. This changes the Cycle time of the PWM signal. For example, you enable this option so that the CPU allocates six bytes for PWM1, and you decide to use QB1008 to QB1013. Once you download the program and start the PWM, you can modify the Pulse duration using QW1008 and the Cycle time using QD1010.

Each time the CPU transitions from STOP to RUN mode, the CPU initializes the Cycle time value in Q memory to the "Cycle time" value assigned above in the "Parameter assignment" section. The units and range of values for the Cycle time value in Q memory are the same as the configuration in the "Parameter assignment" section.

When you select the "Allow runtime modification of the cycle time" check box, the TIA Portal automatically selects a new address for the output address. The new output address cannot be the same as the default address for that pulse generator. The TIA Portal uses the next available block of six consecutive bytes. If the search does not find an available block of Q memory before it reaches the end of Q memory, the search starts over at address "0" of Q memory and continues searching for an available block.

A pulse generator configured for PTO does not use the Q-word address.

10.9 Recipes and Data logs

10.9.1 Recipes

10.9.1.1 Recipe overview

Recipe data storage

- A recipe data block that you create in your project must be stored in CPU **load** memory. Internal CPU memory or an external memory "Program" card can be used.
- Another DB that you must create is the active recipe data block. This DB must be in **work** memory, where one active recipe record is read or written with your program logic.

Recipe data management

The recipe DB uses an array of product recipe records. Each element of the recipe array represents a different recipe flavor that is based on a common set of components.

- You create a PLC data type or struct that defines all the components in one recipe record. This data type template is reused for all recipe records. Product recipes vary according to the start values that are assigned to the recipe components.
- One of the recipes can be transferred at any time from the recipe DB (all recipes in load memory) to the active recipe DB (one recipe in work memory) using the READ_DBL instruction. After a recipe record is moved to work memory, then your program logic can read the component values and begin a production run. This transfer minimizes the amount of CPU work memory that is required for recipe data.
- If the active recipe component values are adjusted by an HMI device during a production run, you can write the modified values back to the recipe DB, using the WRIT_DBL instruction.

Recipe export (from recipe DB to CSV file)

The complete set of recipe records can be generated as a CSV file using the RecipeExport instruction. Unused recipe records are also exported.

Recipe import (from CSV file to recipe DB)

Once a recipe export operation is completed, then you can use the generated CSV file as a data structure template.

1. Use the file browser page in the CPU web server to download an existing recipe CSV file from the CPU to a PC
2. Modify the recipe CSV with an ASCII text editor. You can modify the start values assigned to components, but not the data types or data structure

3. Upload the modified CSV file from PC back to the CPU. However, the old CSV file in CPU load memory (with the same name) must be deleted or renamed before the CPU Web server allows the upload operation.
4. After the modified CSV file is uploaded to the CPU, then you can use the RecipeImport instruction to transfer the new start values from the modified CSV file (in CPU load memory) to the recipe DB (in CPU load memory).

10.9.1.2 Recipe example

Example recipes

The table below shows how to prepare recipe information for use in a recipe DB. The example recipe DB stores five records, three of which are used. The fourth and fifth records are free for later expansions. Each table row represents one record that stores the recipe name, component data types, and component values.

productname	water	barley	wheat	hops	yeast	waterTmp	mashTmp	mashTime	QTest
Pils	10	9	3	280	39	40	30	100	0
Lager	10	9	3	150	33	50	30	120	0
BlackBeer	10	9	3	410	47	60	30	90	1
Not_used	0	0	0	0	0	0	0	0	0
Not_used	0	0	0	0	0	0	0	0	0

Creating a recipe data block

NOTE
Rules for recipe data blocks

- The recipe DB must contain a single dimension array of either a PLC data type or a struct. The recipe example shows how to create a recipe DB with a PLC data type.
- In the example, the data type of the component ingredients are all the UINT data type. The component data types may also be a mix of any data type except for structs. In a recipe DB array element, a struct in a PLC data type or a struct in a struct is not allowed.

First, create a new PLC data type

Add a new PLC data type whose name is the recipe type. In the following image, "Beer_Recipe" is the new complex PLC data type that stores a sequence of simple data types. The "Beer_Recipe" PLC data type is a data template that is reused in each recipe DB record and also in the active recipe DB. Enter the component names and data types that are common to all the example recipes. The individual component values are added later in the recipe DB.

Beer_Recipe

	Name	Data type	Default value
1	productname	String[20]	'Beer_Recipe'
2	water	UInt	0
3	barley	UInt	0
4	wheat	UInt	0
5	hops	UInt	0
6	yeast	UInt	0
7	waterTmp	UInt	0
8	mashTmp	UInt	0
9	mashTime	UInt	0
10	QTest	UInt	0

Second, create a recipe data block

- Create your recipe DB as a global data block with the DB property "Only store in load memory" enabled.
- The name of a recipe data block is used as file name of the corresponding CSV file. The DB name characters you assign must follow the Windows file system naming restrictions. Characters \ / : * ? " < > | and the space character are not allowed.
- The recipe array assignment is "Products" as Array [1.. 5] of "Beer_Recipe". The array size 5 is the maximum number of recipe flavors that are possible.
- The values for recipe components are added as DB start values.

In the following image, the "BlackBeer" recipe is expanded to show all the components of a recipe record.

Recipe_DB

	Name	Data type	Offset	Start value
1	Static			
2	Products	Array [1 .. 5] of "Beer_Recipe"	...	
3	Products[1]	"Beer_Recipe"	...	
4	Products[2]	"Beer_Recipe"	...	
5	Products[3]	"Beer_Recipe"	...	
6	productname	String[20]	...	'BlackBeer'
7	water	UInt	...	10
8	barley	UInt	...	9
9	wheat	UInt	...	3
10	hops	UInt	...	410
11	yeast	UInt	...	47
12	waterTmp	UInt	...	60
13	mashTmp	UInt	...	30
14	mashTime	UInt	...	90
15	QTest	UInt	...	1
16	Products[4]	"Beer_Recipe"	...	
17	Products[5]	"Beer_Recipe"	...	

Recipe export (from recipe DB to CSV file)

"RecipeExport (Page 429)" execution transfers recipe DB data to a CSV file, as shown in the following text file.

```
Recipe_DB.csv
index,productname,water,barley,wheat,hops,yeast,waterTmp,
mashTmp,mashTime,QTest
1,”Pils”,10,9,3,280,39,40,30,100,0
2,”Lager”,10,9,3,150,33,50,30,120,0
3,”BlackBeer”,10,9,3,410,47,60,30,90,1
4 ”Not_used”,0,0,0,0,0,0,0,0,0
5 ”Not_used”,0,0,0,0,0,0,0,0,0
```

Recipe import (from CSV file to recipe DB)

1. Use the file browser page (Page 794) in the Web server to download an existing recipe CSV file from CPU load memory to a PC
2. Modify the recipe CSV with an ASCII text editor. You can modify the start values assigned to components, but not the data types or data structure
3. Upload the modified CSV file from the PC back to the CPU. You must, however, delete or rename the old CSV file in CPU load memory (of the same name) before the Web server allows the upload operation.
4. After you upload the modified CSV file to the CPU, then you can use the RecipeImport instruction to transfer the new start values from the modified CSV file (in CPU load memory) to the recipe DB (in CPU load memory).

CSV files must exactly match the corresponding recipe DB structure

- The values in the CSV file can be changed, but changing the structure is not allowed. The RecipeImport instruction requires that the exact number of records and components matches the destination recipe DB structure. Otherwise, RecipeImport execution fails. For example, if 10 recipes are defined in the recipe DB but only 6 are in use, then line 7 to 10 in the CSV file are also transferred to the DB. You must coordinate whether this data is valid or not. For example, you can assign a variable “Not_used” for the product name in unused recipe records.
- If you add data records to the text file and import the modified file, make sure the recipe DB array limit you assign has enough elements for all the recipe records.
- An index number is automatically generated during export to the CSV file. If you create additional data records, add consecutive index numbers accordingly.
- RecipeImport execution checks the CSV file data for correct structure and whether the values fit in the data types assigned in the associated recipe DB. For example, a Bool data type cannot store an integer value and the RecipeImport execution fails.

Display CSV recipe data in Excel

You can open the CSV file in Excel for easy reading and editing. If the commas are not recognized as decimal separators, use the Excel import function to output the data in structured form.

	A	B	C	D	E	F	G	H	I	J	K
1	index	product	water	barley	wheat	hops	yeast	waterTmp	mashTmp	mashTime	QTest
2	1	"Pils"	10	9	3	280	39	40	30	100	0
3	2	"Lager"	10	9	3	150	33	50	30	120	0
4	3	"BlackBeer"	10	9	3	410	47	60	30	90	1
5	4	"Not_used"	0	0	0	0	0	0	0	0	0
6	5	"Not_used"	0	0	0	0	0	0	0	0	0

NOTE

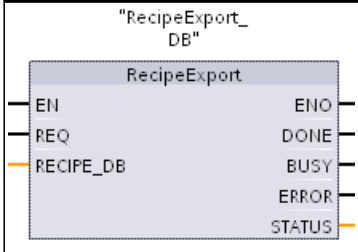
Commas in the name field of the PLC data type element

Do not place commas in the name field of the PLC data type element(s) used in a recipe. If you place commas in the name field, Excel inserts extra columns in the displayed .csv file. These extra columns can introduce errors when you edit the recipe record file start values.

10.9.1.3 Program instructions that transfer recipe data

RecipeExport (Recipe export)

Table 10-194 RecipeExport instruction

LAD/FBD	SCL	Description
	**"RecipeExport_DB"(req:=_bool_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, Recipe_DB:=_variant_inout_);**	The "RecipeExport" instruction exports all recipe records from a recipe data block to the CSV file format. The CSV file contains product names, component names, and start values. The CSV file is stored in internal load memory or external load memory, if an optional external "program" memory card is installed. The export operation is triggered by the "REQ" parameter. The BUSY parameter is set to "1" during export processing. After the execution of RecipeExport stops, BUSY is reset to "0" and the completion of the operation is indicated with "1" at the DONE parameter. If an error occurs during execution, then parameters ERROR and STATUS indicate the result.

A recipe DB must be created before a recipe export is possible. The name of a recipe data block is used as the file name of the new CSV file. If a CSV file with an identical name already exists, then it is overwritten during the export operation.

You can use the File Browser page (Page 794) of the CPU's built-in Web server to access the recipe CSV file. The file is put in the recipe folder in the root directory of CPU load memory.

Table 10-195 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Control parameter REQUEST: Activates the export on a positive edge.
RECIPE_DB	In/Out	Variant	Pointer to the recipe data block. Refer to the "Recipe DB example (Page 426)" for details. The DB name characters must follow the Windows file system naming restrictions. Characters \ / : * ? " < > | and the space character are not allowed.
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error. (Default value: False)
BUSY	OUT	Bool	RecipeExport execution • 0: No operation in progress • 1: Operation on progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE. • 0: No warning or error • 1: An error has occurred. The STATUS parameter provides information on the type of error.
STATUS	OUT	Word	Execution condition code

Table 10-196 Values of ERROR and STATUS

ERROR	STATUS (W#16#....)	Description
0	0000	No error
0	7000	Call with no REQ edge: BUSY = 0, DONE = 0
0	7001	First call with REQ edge (working): BUSY = 1, DONE = 0
0	7002	N^{th} call (working): BUSY = 1, DONE = 0
1	8070	All instance memory is in use.
1	8090	File name contains invalid characters
1	8091	The data structure referenced with RECIPE_DB cannot be processed.
1	8092	Data structure specified in RECIPE_DB exceeds 5000 bytes
1	80B3	Not enough space in on MC or in internal load memory
1	80B4	MC is write protected
1	80B6	Recipe DB attribute "Only store in load memory" is not enabled.
1	80C0	CSV file is temporarily locked
1	80C1	DB is temporarily locked

RecipeImport (Recipe import)

Table 10-197 RecipeImport instruction

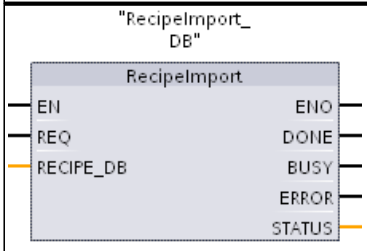
LAD/FBD	SCL	Description
	**"RecipeImport_DB"(req:=_bool_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, Recipe_DB:=_variant_inout_);**	The "RecipeImport" instruction imports recipe data from a CSV file, in CPU load memory, to a recipe data block referenced by the RECIPE_DB parameter. Start values in the recipe data block are overwritten by the import process. The import operation is triggered by the "REQ" parameter. The BUSY parameter is set to "1" during import processing. After the execution of RecipeImport stops, BUSY is reset to "0" and the completion of the operation is indicated with "1" at the DONE parameter. If an error occurs during execution, then parameters ERROR and STATUS indicate the result.

Table 10-198 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Control parameter REQUEST: Activates the import on a positive edge.
RECIPE_DB	In/Out	Variant	Pointer to the recipe data block. Refer to "Recipe DB example (Page 426)" for details. The DB name characters must follow the Windows file system naming restrictions. Characters \ / : * ? " < > | and the space character are not allowed.
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error. (Default value: False)
BUSY	OUT	Bool	• 0 - No operation in progress • 1 - Operation on progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code (Default value: 0)

A recipe DB that contains a structure which is consistent with the CSV file data structure must exist, before a recipe import operation is possible.

CSV file rules:

- The CSV file must be located in the root directory "Recipes" folder of internal load memory or external load memory, if an optional external "program" memory card is installed.
- The name of the CSV file must match the name of the data block at the RECIPE_DB parameter.
- The first line (header) of the CSV file contains the name of the recipe components. The first line is ignored during import. The names of the recipe components in the CSV file and the data block are not reconciled during the import process.

- In each case the first value in each line of the CSV file is the index number of the recipe. The individual recipes are imported in the order of the index. For this, the index in the CSV file has to be in ascending order and may contain no gaps (if this is not the case, the error message 80B0 is output at the STATUS parameter).
- The CSV file may not contain more recipe data records than provided for in the recipe data block. The maximum number of data records is indicated by the array limits in the data block.

Table 10-199 Values of ERROR and STATUS

ERROR	STATUS (W#16#....)	Description
0	0000	No error
0	7000	Call with no REQ edge: BUSY = 0, DONE = 0
0	7001	First call with REQ edge (working): BUSY = 1, DONE = 0
0	7002	N^{th} call (working): BUSY = 1, DONE = 0
1	8070	All instance memory is in use.
1	8090	The file name contains invalid characters.
1	8092	No matching CSV file found for the import. Possible cause: The name of the CSV file does not match the name of the recipe DB.
1	80C0	CSV file is temporarily locked.
1	80C1	Data block is temporarily locked.
1	80B0	Numbering in the index of the CSV file is not continuous, not ascending or exceeds the maximum number (array limit) in the data block.
1	80B1	Structure of the recipe data block and the CSV file do not match: The CSV file contains too many fields.
1	80B2	Structure of the recipe data block and the CSV file do not match: The CSV file contains too few fields.
1	80B6	Recipe DB attribute "Only store in load memory" is not enabled.
1	80D0 +n	Structure of the recipe data block and the CSV file do not match: Data type in field n does not match (n<=46).
1	80FF	Structure of the recipe data block and the CSV file do not match: Data type in field n does not match (n>46).

10.9.1.4 Recipe example program

Prerequisites for the recipe example program

The prerequisites for the recipe example program are as follows:

- A recipe DB that stores all recipe records. The recipe DB is stored in load memory.
- An active recipe DB that stores a copy of one recipe in work memory.

Refer to the "Recipe DB example (Page 426)" for details about the recipe DB and the corresponding CSV file.

Create the active recipe DB

On the "Add new block" window:

- Select the "Data block" button on the "Add new block" window
- On the "Type" drop-down menu, select the "Beer_recipe" PLC data type that you created previously.

Start values are not required. The DB data values are set when one recipe is transferred from the recipe DB to the active recipe DB. In the example, the active recipe DB is the destination for READ_DBL data and provides source data for WRITE_DBL. The following image shows the Active_Recipe DB.

Active_Recipe

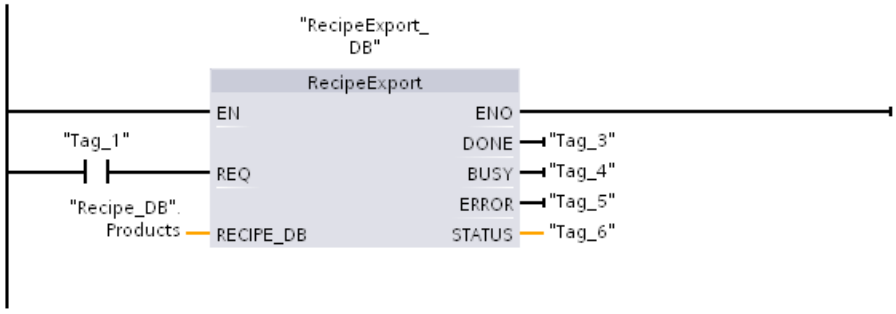
	Name	Data type	Start value
1	Static		
2	productname	String[20]	'Beer_Recipe'
3	water	UInt	0
4	barley	UInt	0
5	wheat	UInt	0
6	hops	UInt	0
7	yeast	UInt	0
8	waterTmp	UInt	0
9	mashTmp	UInt	0
10	mashTime	UInt	0
11	QTest	UInt	0

Instance DBs

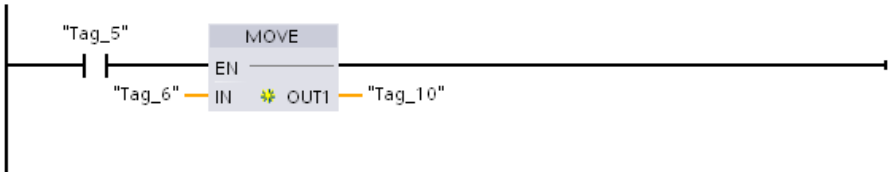
The instance DBs used by instructions RecipeExport ("RecipeExport_DB") and RecipeImport ("RecipeImport_DB") are created automatically when you place the instructions in your program. The instance DBs are used to control instruction execution and are not referenced in the program logic.

Example recipe program

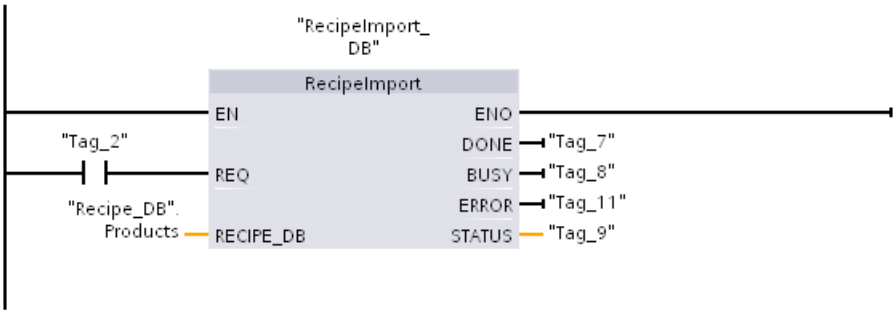
Network 1 A rising edge on REQ starts the export process. A CSV file is generated from the recipe DB data and placed in the CPU memory recipes folder.



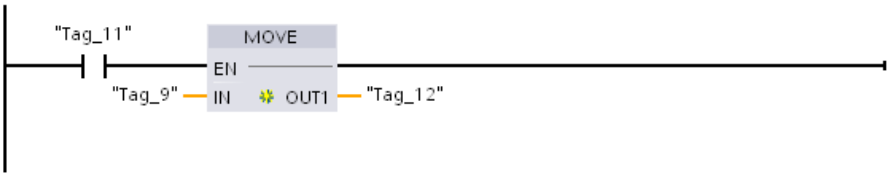
Network 2 Capture the STATUS output from RecipeExport execution, because it is only valid for one scan.



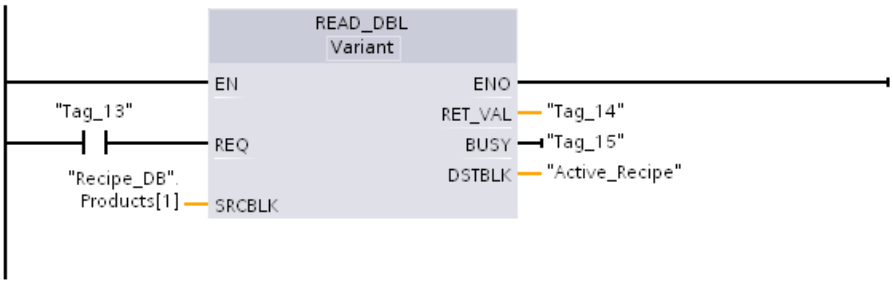
Network 3 A rising edge on REQ starts the import process. The existing recipe DB is loaded with all recipe data read from the corresponding CSV file that is located in the CPU memory recipes folder.



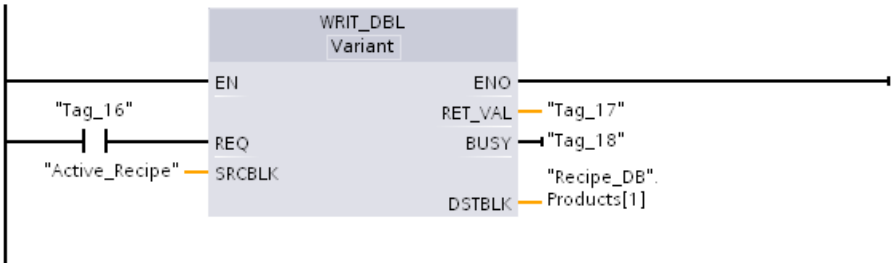
Network 4 Capture the STATUS output from RecipeImport execution, because it is only valid for one scan.



Network 5 READ_DBL copies the start values from one recipe "Recipe_DB". Products[1] (in CPU load memory) to the Active_Recipe DB current values (in CPU work memory). After READ_DBL execution, your program logic can access the recipe component values by addressing locations in the Active_Recipe DB. For example, the symbolic addresses ("Active_Recipe".productname) and ("Active_Recipe.water) provide your program logic with the current recipe name and quantity of water.



Network 6 During run time, An HMI device could modify a component value stored in the Active_Recipe DB. Improved recipe data can be stored by executing WRIT_DBL. In the example, all Recipe_DB start values for the single recipe "Recipe_DB". Products[1] are overwritten by the current values from the "Active_Recipe" DB.



10.9.2 Data logs

Your control program can use the data log instructions to store run-time data values in persistent log files. The CPU stores data log files in flash memory (CPU or memory card) in standard CSV (Comma Separated Value) format. The CPU organizes the data records as a circular log file of a pre-determined size.

You use the data log instructions in your program to create, open, write a record to, and close the log files. You decide which program values to log by creating a data buffer that defines a single log record. The CPU uses your data buffer as temporary storage for a new log record. Your control program moves new current values into the buffer during runtime. When the program has updated all of the current data values, it can then execute the DataLogWrite instruction to transfer data from the buffer to a data log record.

You can work with data logs from the Web Server (Page 753).

10.9.2.1 Data log record structure

The DATA and HEADER parameters of the DataLogCreate instruction assign the data type and the column header description of all data elements in a log record.

DATA parameter for the DataLogCreate instruction

The DATA parameter points to memory used as a temporary buffer for a new log record and must be assigned to an M or DB location.

You can assign an entire DB (derived from a PLC data type that you assign when the DB is created) or part of a DB (the specified DB element can be any data type, data type structure, PLC data type, or data array).

The DataLogCreate instruction limits structure data types to a single nesting level. An array-of-strings is not considered a single nesting level in this context. Currently the DataLogCreate instruction does not return an error. The instruction only processes the first string in the array-of-strings. The total number of data elements declared should correspond to the number of columns specified in the header parameter. The maximum number of data elements you can assign is 253 (with a timestamp) or 255 (without a timestamp). This restriction keeps your record inside the 256 column limit of an Excel sheet.

The DATA parameter can assign either retentive or non-retentive data elements in a "Standard" (compatible with S7-300/400) or "Optimized" DB type.

In order to write a Data log record you must first load the temporary DATA record with new process values and then execute the DataLogWrite instruction that saves new record values in the Datalog file.

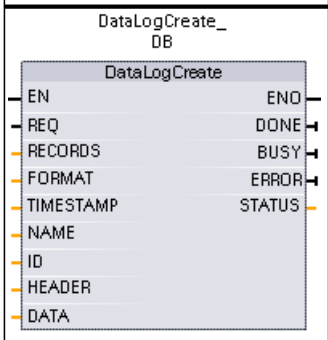
HEADER parameter for the DataLogCreate instruction

The HEADER parameter points to column header names for the top row of the data matrix encoded in the CSV file. HEADER data must be located in DB or M memory and the characters must follow standard CSV format rules with commas separating each column name. The data type may be a string, byte array, or character array. Character/byte arrays allow increased size, where strings are limited to a maximum of 255 bytes. The HEADER parameter is optional. If the HEADER is not assigned, then no header row is created in the Data log file.

10.9.2.2 Program instructions that control data logs

DataLogCreate (Create data log)

Table 10-200 DataLogCreate instruction

LAD/FBD	SCL	Description
	**"DataLogCreate_DB"(** **req:=_bool_in_,** **records:=_udint_in_,** **format:=_uint_in_,** **timestamp:=_uint_in_,** **done=>_bool_out_,** **busy=>_bool_out_,** **error=>_bool_out_,** **status=>_word_out_,** **name:=_string_inout_,** **ID:=_dword_inout_,** **header:=_variant_inout_,** **data:=_variant_inout_);**	Creates and initializes a data log file. The CPU creates the file in the \DataLogs folder, using the name in the NAME parameter, and implicitly opens the file for write operations. You can use the Data log instructions in your program to store runtime process data in the flash memory of the CPU or on the memory card. STEP 7 automatically creates the associated instance DB when you insert the instruction.

[1] In the SCL example, "DataLogCreate_DB" is the name of the instance DB.

Table 10-201 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	A low to high (positive edge) signal starts the operation. (Default value: False)
RECORDS	IN	UDint	The maximum number of data records the circular data log can contain before overwriting the oldest entry: The header record is not included. Sufficient available PLC load memory must exist in order to successfully create the data log. (Default value - 1)
FORMAT	IN	UInt	Data log format: • 0 - Internal format (not supported) • 1 - Comma separated values "csv-eng" (Default value)

Parameter and type		Data type	Description
TIMESTAMP	IN	UInt	Data time stamp format: Column headers for date and time fields are optional. The time stamp can use either the system time (Coordinated Universal Time - UTC) or the local time. • 0 - No time stamp • 1 - system time mm/dd/yyyy,hh:mm:ss • 2 - local time mm/dd/yyyy,hh:mm:ss • 3 - system time mm/dd/yyyy,hh:mm:ss • 4 - local time yyyy-mm-dd,hh:mm:ss • 5 - system time yyyy-mm-dd,hh:mm:ss
NAME	IN	Variant	Data log name: You provide the name. This variant only supports a String data type and must be located in DB, or local memory. (Default value: ' ') The string reference is the name of the data log file. Use characters from the ASCII character set, with the exception of the characters \ / : * ? " < > | and the space character.
ID	In/Out	DWord	Data log numeric identifier: You store this generated value for use with other Data log instructions. The ID parameter is only used as an output with the DataLogCreate instruction. (Default value: 0) Symbolic name access for this parameter is not allowed.
HEADER	In/Out	Variant	Pointer to data log column header names for the top row of the data matrix encoded in the CSV file. (Default value: null). HEADER data must be located in DB or M memory. The characters must follow standard CSV format rules with commas separating each column name. The data type may be a string, byte array, or character array. Character/byte arrays allow increased size, where strings are limited to a maximum of 255 bytes. The HEADER parameter is optional. If the HEADER is not parameterized, then no header row is created in the Data log file.
DATA	In/Out	Variant	Pointer to the record data structure, user defined type (UDT), or array. Record data must be located in DB or M memory. The DATA parameter specifies the individual data elements (columns) of a data log record and their data type. The DataLogCreate instruction limits structure data types to a single nesting level. An array-of-strings is not considered a single nesting level in this context. Currently the DataLogCreate instruction does not return an error. The instruction only processes the first string in the array-of-strings. The number of data elements declared should correspond to the number of columns specified in the header parameter. The maximum number of data elements you can assign is 253 (with a timestamp) or 255 (without a timestamp). This restriction keeps your record inside the 256 column limit of an Excel sheet.
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error. (Default value: False)

Parameter and type		Data type	Description
BUSY	OUT	Bool	• 0 - No operation in progress • 1 - Operation on progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code (Default value: 0)

The CPU creates a data log file with a pre-determined fixed sized based on the RECORDS and DATA parameters and organizes the data records as a circular log file. The DataLogCreate instruction allocates persistent CPU memory for the entire data log when the instruction returns DONE = TRUE. The required memory in the CPU is greater than the size of the file due to file system management and related values. The persistent memory for the data log remains allocated until the CPU deallocates the memory in one of the following ways:

- The user program calls the DataLogDelete instruction
- A Web server user deletes the data log from the Web server
- A SIMATIC Automation Tool user deletes the data log from the SIMATIC Automation Tool

Deleting the data log file by other means, such as using a card reader, does not deallocate the CPU persistent memory for the data log.

The DataLogWrite instruction appends new records to the data log file until it stores the maximum number of records that is specified by the RECORDS parameter. The next record written will overwrite the oldest record. Another DataLogWrite operation will overwrite the next oldest data record and so on.

Memory resource usage:

- The data logs consume only load memory.
- The size of all data logs combined is limited by the available resources of load memory. Only eight data logs can be open at one time. You can manage your data logs from the File Browser (Page 794) standard Web page. See the description of this standard Web page for guidelines on how many data logs to maintain at a time.
- The maximum possible number for the RECORDS parameter is the limit for an UDint number (4,294,967,295). The actual limit for the RECORD parameter depends on the size of a single record, the size of other data logs, and the available resources of load memory. In addition, Excel limits the number of rows allowed in an Excel sheet.

NOTE

Data log creation execution must be complete before starting a data log write operation

- DataLogCreate and DataLogNewFile log file creation operations extend over many program scan cycles. The actual time required for the log file creation depends on the record structure and number of records. Your program logic must monitor and catch the DONE bit's transition to the TRUE state that signals the completion of a log file creation. If the user program executes a DataLogWrite instruction before a data log creation operation is complete, then the write operation will fail to write a new data log record as expected.
- In certain situations when a very fast program scan is running, data log creation can take an extended time. If the long creation time is too slow, you should ensure that the checkbox for the Enable minimum cycle time for cyclic OBs is active, and the minimum cycle time is set to one ms or greater. Refer to Configuring the cycle time and communication load (Page 81) for more information.

NOTE

The DataLogNewFile instruction copies an existing data log's record structure

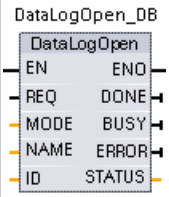
If you want to prevent overwriting any data records, then you can use the DataLogNewFile instruction to create a new data log based on the current data log, after the current data log has stored the maximum number of records. New data records are stored in the new data log file. The old data log file and record data remain stored in flash memory.

Table 10-202 Values of ERROR and STATUS

ERROR	STATUS (W#16#....)	Description
0	0000	No error
0	7000	Call with no REQ edge: BUSY = 0, DONE = 0
0	7001	First call with REQ edge (working): BUSY = 1, DONE = 0
0	7002	N^{th} call (working): BUSY = 1, DONE = 0
1	8070	All internal instance memory is in use.
1	807F	Internal error
1	8090	Invalid file name
1	8091	Name parameter is not a String reference.
1	8093	A data log already exists with that name. Use a different name, make sure the existing data log's .csv file is not open, and then use the File Browser (Page 794) page of the Web Server to delete the existing data log.
1	8097	Requested file length exceeds file system maximum.
1	80B2	Out of resource IDs Note: Delete some existing data logs or decrease the number of columns in the data record structure to avoid this error.
1	80B3	Insufficient load memory available.
1	80B4	MC (memory card) is write-protected.
1	80C0	Archive file is locked
1	80C1	Too many open files: No more than eight opened data log files are allowed.
1	8253	Invalid record count
1	8353	Invalid format selection
1	8453	Invalid timestamp selection
1	8B24	Invalid HEADER area assignment: For example, pointing to local memory
1	8B51	Invalid HEADER parameter data type
1	8B52	Too many HEADER parameter data elements
1	8C24	Invalid DATA area assignment: For example, pointing to local memory
1	8C51	Invalid DATA parameter data type
1	8C52	Too many DATA parameter data elements

DataLogOpen (Open data log)

Table 10-203 DataLogOpen instruction

LAD / FBD	SCL	Description
	**"DataLogOpen_DB"(req:=_bool_in_, mode:=_uint_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, name:=_string_inout_, ID:=_dword_inout_);**	Opens a pre-existing data log file. You must open a data log before you can write (Page 441) new records to the log. You can open and close data logs individually. A maximum of eight data logs can be open at the same time. STEP 7 automatically creates the associated instance DB when you insert the instruction.

[2] In the SCL example, "DataLogOpen_DB" is the name of the instance DB.

Table 10-204 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	A low to high (positive edge) signal starts the operation. (Default value: False)
MODE	IN	UInt	Operation mode: • 0 - Append to existing data (Default value) • 1 - Clear all existing records
NAME	IN	Variant	Name of an existing data log: This variant only supports a String data type and can only be located in local, DB, or M memory. (Default value: ' ')
ID	In/Out	DWord	Numeric identifier of a data log. (Default value: 0) **Note:** Symbolic name access for this parameter is not allowed.
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error. (Default value: False)
BUSY	OUT	Bool	• 0 - No operation in progress • 1 - Operation in progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code (Default value: 0)

You can provide either the NAME or an ID (ID parameter as an input) of a pre-existing data log. If you provide both parameters and a valid ID does correspond to the NAME data log, then the ID is used, and the NAME ignored.

The NAME must be the name of a data log created by the DataLogCreate instruction. If only the NAME is provided and the NAME specifies a valid data log, then the corresponding ID will be returned (ID parameter as an output).

NOTE

General usage of data log files

- Data log files are automatically opened after the DataLogCreate and DataLogNewFile operations.
- Data log files are automatically closed after a PLC RUN to STOP transition or a PLC power cycle.
- A Data log file must be open before a new DataLogWrite operation is possible.
- A maximum of eight data log files may be open at one time. More than eight data log files can exist, but some of them must be closed so no more than eight are open.

Table 10-205 Values of ERROR and STATUS

ERROR	STATUS (W#16#)	Description
0	0000	No error
0	0002	Warning: Data log file already open by this application program
0	7000	Call with no REQ edge: BUSY = 0, DONE = 0
0	7001	First call with REQ edge (working): BUSY = 1, DONE = 0
0	7002	N^{th} call (working): BUSY = 1, DONE = 0
1	8070	All internal instance memory is in use.
1	8090	Data log definition is inconsistent with existing data log file.
1	8091	Name parameter is not a String reference.
1	8092	Data log does not exist.
1	80C0	Data log file is locked.
1	80C1	Too many open files: No more than eight opened data log files are allowed.

NOTE

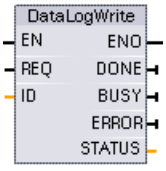
Load memory overuse

Each open or close of a data log file causes multiple writes to the load memory. Frequent opening and closing of data log files might cause the load memory to degrade prematurely.

It is not necessary to close a data log between write operations.

DataLogWrite (Write data log)

Table 10-206 DataLogWrite instruction

LAD / FBD	SCL	Description
	**"DataLogWrite_DB"(req:=_bool_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, ID:=_dword_inout_);**	Writes a data record into the specified data log. The pre-existing target data log must be open (Page 440) before you can write to it with a DataLogWrite instruction. STEP 7 automatically creates the associated instance DB when you insert the instruction.

[2] In the SCL example, "DataLogWrite_DB" is the name of the instance DB.

Table 10-207 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	A low to high (positive edge) signal starts the operation. (Default value: False)
ID	In/Out	DWord	Numeric data log identifier. Only used as an input for the DataLogWrite instruction. (Default value: 0) **Note:** Symbolic name access for this parameter is not allowed.
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error.
BUSY	OUT	Bool	• 0 - No operation in progress • 1 - Operation on progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code (Default value: 0)

The DATA parameter of a DataLogCreate instruction defines the memory address and data structure of the record buffer. The control program must load the record buffer with current runtime process values and then execute the DataLogWrite instruction to move new record data from the buffer to the data log.

The ID parameter identifies a data log and data record configuration. The DataLogCreate instruction generates the ID number.

If there are empty records in the circular data log file, then the DataLogWrite instruction writes the next available empty record. If all records are full, then the DataLogWrite instruction overwrites the oldest record.

Data log creation operations must be complete, before starting a data log write operation. DataLogCreate and DataLogNewFile log file creation operations extend over many program scan cycles. The actual time required for the log file creation depends on the record structure and number of records. Your program logic must monitor and catch the DONE bit's transition to the TRUE state that signals the completion of a log file creation. If a DataLogWrite instruction executes before a data log creation operation is complete, then the write operation does not write a new data log record.

NOTE

Effect of data logs on internal load memory

Each data log write consumes at a minimum 2 KB of memory. If your program writes small amounts of data frequently, it is consuming at least 2 KB of memory on each write. A better implementation would be to accumulate the small data items in a data block (DB), and to write the data block to the data log at less frequent intervals.

If your program writes many data log entries at a high frequency, consider using a replaceable SIMATIC memory card.

NOTICE

Potential for data log data loss during a CPU power failure

If there is a power failure during an incomplete DataLogWrite operation, then the data record being transferred to the data log could be lost.

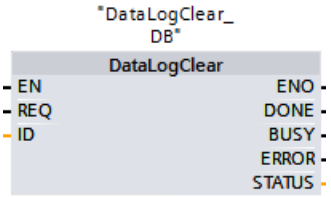
Table 10-208 Values of ERROR and STATUS

ERROR	STATUS (W#16#)	Description
0	0000	No error
0	0001	Indicates that the data log is full: Each data log is created with a specified maximum number of records. The last record of the maximum number has been written. The next write operation will overwrite the oldest record.
0	7000	Call with no REQ edge: BUSY = 0, DONE = 0
0	7001	First call with REQ edge (working): BUSY = 1, DONE = 0
0	7002	N^{th} call (working): BUSY = 1, DONE = 0
1	8070	All internal instance memory is in use.
1	8092	Data log does not exist.
1	80B0	Data log file is not open (for explicit open mode only).

DataLogClear (Empty data log)

Description

Table 10-209 DataLogClear instruction

LAD / FBD	SCL	Description
	**"DataLogClear_DB"(REQ:=_bool_in_, DONE=>_bool_out_, BUSY=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, ID:=_dword_inout_);**	The "DataLogClear" instruction deletes all data records in an existing data log. The instruction does not delete the optional header of the CSV file (see the description of the HEADER parameter of the instruction "DataLogCreate (Page 436)"). You use the ID parameter to select the data log whose data records are to be deleted.

"DataLogClear_DB" is the name of the instance DB.

Requirement

Before you can delete data records, the data log must be open. Use the DataLogOpen (Page 440) instruction to open a data log.

Parameters

The following table shows the parameters of the "DataLogClear" instruction:

Parameter	Declaration	Data type	Memory area	Description
REQ	Input	BOOL	I, Q, M, L, D, T, C or constant (T and C are only available in LAD and FBD with S7-1500)	Execution of the instruction upon a rising edge.
ID	InOut	DWORD	I, Q, M, D, L	Numeric data log identifier
DONE	Output	BOOL	I, Q, M, D, L	Instruction was executed successfully.
BUSY	Output	BOOL	I, Q, M, D, L	Execution of the instruction not yet complete.
ERROR	Output	BOOL	I, Q, M, D, L	• 0: No error. • 1: An error occurred during execution of the instruction. Detailed information is output at the STATUS parameter.
STATUS	Output	WORD	I, Q, M, D, L	Status parameter The parameter is only set for the duration of one call. To display the status, you should therefore copy the STATUS parameter to a free data area.

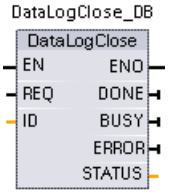
You can find additional information on valid data types under "Data types (Page 95)".

Parameter STATUS

Error code* (W#16#...)	Explanation
0000	No error.
7000	No job processing active.
7001	Start of job processing. Parameter BUSY = 1, DONE = 0
7002	Intermediate call (REQ irrelevant): Instruction already active; BUSY has the value "1".
8080	The data log file selected with the ID parameter cannot be processed with the "DataLogClear" instruction.
8092	Data log does not exist.
80A2	Write error signaled back by the file system.
80B0	Data log is not open.
80B4	The memory card is write-protected.
* The error codes can be displayed as integer or hexadecimal values in the program editor. For information on switching the display formats, refer to "See also".	

DataLogClose (Close data log)

Table 10-210 DataLogClose instruction

LAD / FBD	SCL	Description
	**"DataLogClose_DB"(req:=_bool_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, ID:=_dword_inout_);**	Closes an open data log file. DataLogWrite operations to a closed data log result in an error. No write operations are allowed to this data log until another DataLogOpen operation is performed. A transition to STOP mode will close all open data log files. STEP 7 automatically creates the associated instance DB when you insert the instruction.

[2] In the SCL example, "DataLogClose_DB" is the name of the instance DB.

Table 10-211 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	A low to high (positive edge) signal starts the operation. (Default value: False)
ID	In/Out	DWord	Numeric identifier of a data log. Only used as an input for the DataLogClose instruction. (Default value: 0) **Note:** Symbolic name access for this parameter is not allowed.
DONE	OUT	Bool	The DONE bit is TRUE for one scan after the last request was completed with no error.
BUSY	OUT	Bool	• 0 - No operation in progress • 1- Operation in progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code (Default value: 0)

Table 10-212 Values of ERROR and STATUS

ERROR	STATUS (W#16#)	Description
0	0000	No error
0	0001	Data log not open
0	7000	Call with no REQ edge: BUSY = 0, DONE = 0
0	7001	First call with REQ edge (working): BUSY = 1, DONE = 0
0	7002	N^{th} call (working): BUSY = 1, DONE = 0
1	8092	Data log does not exist.

NOTE

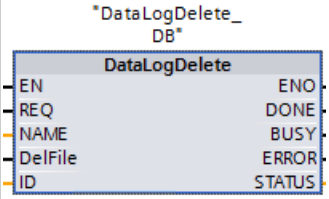
Load memory overuse

Each open or close of a data log file causes multiple writes to the load memory. Frequent opening and closing of data log files might cause the load memory to degrade prematurely.

It is not necessary to close a data log between write operations.

DataLogDelete (Delete data log)

Table 10-213 DataLogDelete instruction

LAD / FBD	SCL	Description
	**"DataLogDelete_DB"(REQ:=_bool_in_, NAME:=_variant_in_, DelFile:=_bool_in_, DONE=>_bool_out_, BUSY=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, ID:=_dword_inout_);**	You use the "DataLogDelete" instruction to delete a data log file. The data log and the data records it contains can only be deleted if it was created with the "DataLogCreate" or "DataLogNewFile" instruction.

"DataLogDelete_DB" is the name of the instance DB.

Parameters

The following table shows the parameters of the "DataLogDelete" instruction:

Parameter	Declaration	Data type	Memory area	Description
REQ	Input	BOOL	I, Q, M, L, D, T, C or constant (T and C are only available in LAD and FBD with S7-1500)	Execution of the instruction upon a rising edge.
NAME	Input	VARIANT	L, D	File name of the data log
DELFILE	Input	BOOL	I, Q, M, D, L or constant	• 0: Data log is retained. • 1: Data log is deleted.
ID	InOut	DWORD	I, Q, M, D, L	Numeric data log identifier
DONE	Output	BOOL	I, Q, M, D, L	Instruction executed successfully.
BUSY	Output	BOOL	I, Q, M, D, L	Deletion of the data log is not yet complete.
ERROR	Output	BOOL	I, Q, M, D, L	• 0: No error. • 1: An error occurred during execution of the instruction. Detailed information is output at the STATUS parameter.
STATUS	Output	WORD	I, Q, M, D, L	Status parameter The parameter is only set for the duration of one call. To display the status, you should therefore copy the STATUS parameter to a free data area.

You can find additional information on valid data types under "Data types (Page 95)".

Retained data logs

When you retain a data log, the CPU deactivates the data log and the user program can no longer access it. The file representing the data log remains on the SIMATIC memory card or, if no card is present, in the internal load memory (Page 451). The file is still accessible through the Web server or the SIMATIC Automation Tool. From the Web server, use the File Browser (Page 794) and the Data Logs (Page 789) standard Web pages (Page 764) to access the file.

Only retain a deleted data log when using a SIMATIC memory card. Deleted data logs, retained in the CPU's internal memory, are not included in load memory calculations.

Parameters NAME and ID

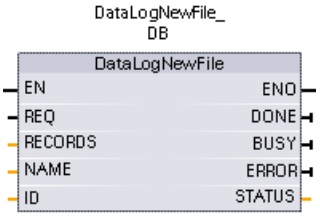
Select the data log to be deleted using the NAME and ID parameters. The ID parameter is evaluated first. If there is a data log with the relevant ID, the NAME parameter will not be evaluated. If the value "0" is used at the ID parameter, a value with the data type STRING must be used at the NAME parameter.

Parameter RET_VAL

Error code* (W#16#...)	Explanation
0	No error.
7000	No job processing active.
7001	Start of job processing. Parameter BUSY = 1, DONE = 0
7002	Intermediate call (REQ irrelevant): Instruction already active; BUSY has the value "1".
8091	A data type other than STRING is being used at the NAME parameter.
8092	Data log does not exist.
80A2	Write error signaled back by the file system.
80B4	The memory card is write-protected.
* The error codes can be displayed as integer or hexadecimal values in the program editor. For information on switching the display formats, refer to "See also".	

DataLogNewFile (Data log in new file)

Table 10-214 DataLogNewFile instruction

LAD / FBD	SCL	Description
	**"DataLogNewFile_DB"(req:=_bool_in_, records=:_udint_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, name=:_DataLog_out_, ID:=_dword_inout_);**	Allows your program to create a new data log file based upon an existing data log file. STEP 7 automatically creates the associated instance DB when you insert the instruction.

[2] In the SCL example, "DataLogNewFile_DB" is the name of the instance DB.

Table 10-215 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	A low to high (positive edge) signal starts the operation. (Default value: False)
RECORDS	IN	UDInt	The maximum number of data records the circular data log can contain before overwriting the oldest entry. (Default value: 1) The header record is not included. Sufficient available CPU load memory must exist in order to successfully create the data log.
NAME	IN	Variant	Data log name: You provide the name. This variant only supports a String data type and can only be located in local, DB, or M memory. (Default value: ' ') The string reference is also used as the name of the data log file. The name characters must follow the Windows file system naming restrictions. Characters \ / : * ? " < > | and the space character are not allowed.)
ID	In/Out	DWord	Numeric data log identifier(Default value: 0): • At execution, the ID input identifies a valid data log. The new data log configuration is copied from this data log. • After execution, the ID parameter becomes an output that returns the ID of the newly created data log file. **Note:** Symbolic name access for this parameter is not allowed.
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error.
BUSY	OUT	Bool	• 0 - No operation in progress • 1 - Operation in progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code (Default value: 0)

You can execute the DataLogNewFile instruction when a data log becomes full or is deemed completed and you do not want to lose any data that is stored in the data log. A new empty data log file can be created based on the structure of the full Data log file. The header record will be duplicated from the original data log with the original data log properties (DATA record buffer, data format, and timestamp settings). The original Data log file is implicitly closed and the new Data log file is implicitly opened.

DataLogWrite parameter trigger: Your program must monitor the ERROR and STATUS parameters of each DataLogWrite operation. When the final record is written and a data log is full, the DataLogWrite ERROR bit = 1 and the DataLogWrite STATUS word = 1. These ERROR and STATUS values are valid for one scan only, so your monitoring logic must use ERROR = 1 as a time gate to capture the STATUS value and then test for STATUS = 1 (the data log is full).

DataLogNewFile operation: When your program logic gets the data log is full signal, this state is used to activate a DataLogNewFile operation. You must execute DataLogNewFile with the ID of an existing (usually full) and open data log, but a new unique NAME parameter. After the DataLogNewFile operation is done, a new data log ID value is returned (as an output parameter) that corresponds to the new data log name. The new data log file is implicitly opened and is ready to store new records. New DataLogWrite operations that are directed to the new data log file, must use the ID value returned by the DataLogNewFile operation.

Data log creation operations must be complete, before starting a data log write operation. DataLogCreate and DataLogNewFile log file creation operations extend over many program scan cycles. The actual time required for the log file creation depends on the record structure and number of records. Your program logic must monitor and catch the DONE bit's transition to the TRUE state that signals the completion of a log file creation. If a DataLogWrite instruction is executed before a data log creation operation is complete, then the write operation will fail to write a new data log record as expected.

Table 10-216 Values of ERROR and STATUS

ERROR	STATUS (W#16#)	Description
0	0000	No error
0	7000	Call with no REQ edge: BUSY = 0, DONE = 0
0	7001	First call with REQ edge (working): BUSY = 1, DONE = 0
0	7002	N^{th} call (working): BUSY = 1, DONE = 0
1	8070	All internal instance memory is in use.
1	8090	Invalid file name
1	8091	Name parameter is not a String reference.
1	8092	Data log does not exist.
1	8093	Data log already exists.
1	8097	Requested file length exceeds file system maximum.
1	80B2	Out of resource IDs Note: Delete some existing data logs to create resources for a new data log.
1	80B3	Insufficient load memory available.
1	80B4	MC is write-protected.
1	80C1	Too many open files.

10.9.2.3 Working with data logs

The data log files are stored as comma separated value format (*.csv) in persistent flash memory. You can view the data logs by using the PLC Web server feature or by removing the PLC memory card and inserting it in a standard PC card reader.

Viewing data logs with the Web server

If the PLC and PC are connected to a common network, then you can use the Web server to access data logs. The PLC can be in run mode or stop mode when you operate the PLC Web server. If the PLC is in run mode, then your control program continues to execute while the PLC Web server is transferring log data through the network.

Web server access:

1. Enable the Web server in the Device Configuration for the target CPU (Page 755).
2. Connect your PC to the PLC through the PROFINET network (Page 764).
3. Access the CPU through the built-in Web server (Page 768).
4. Work with data log files with the "File Browser" (Page 794) or "Data Logs" (Page 789) standard Web page.
5. Open the .csv file with a spreadsheet application like Microsoft Excel.

NOTE

Data log management

Keep no more than 1000 data logs in a file system. Exceeding this number can prevent the Web server from having enough CPU resources to display the data logs.

If you find that the File Browser Web page is not able to display the data logs, then you must place the CPU in STOP mode in order to display and delete data logs.

Manage your data logs to ensure that you only keep the number that you need to maintain, and do not exceed 1000 data logs.

Viewing data logs on a SIMATIC memory card

If the S7-1200 CPU has a "Program" type S7-1200 memory card inserted, then you can remove the memory card and insert the card into a standard SD (Secure Digital) card slot on a PC or PG. The PLC is in stop mode when the memory card is removed and your control program is not executed.

Use the Windows file explorer and navigate to the \DataLog directory on the memory card. All your *.csv data log files are located in this directory.

Make a copy of the data log files and put the copies on a local drive of your PC. Then, you can use Excel to open a local copy of a *.csv file and not the original file that is stored on the memory card.

NOTE

Editing data logs on the memory card

You can copy data logs from a memory card using a PC card reader. Do not change them or delete them using a PC card reader.

To delete, download, or display data logs use one of the following methods:

- Web server
- SIMATIC Automation Tool
- DataLogDelete instruction (Page 446)

If you open the file system of the memory card in the File explorer, you run the risk of accidentally deleting or changing a data log or other system files, potentially damaging files or making the memory card unusable.

NOTICE

Recommended frequency for write operations when using data logs

When using data logs on memory cards, a high frequency of write operations can affect the S7-1200 system negatively.

To ensure the overall performance and robustness of your system, limit write operations to every 200 ms or longer.

Exceeding this limit can shorten the lifespan of the memory card or internal flash.

10.9.2.4 Limit to the size of data log files

Data log files share PLC load memory space with the program, program data, configuration data, user-defined Web pages, and PLC system data. A large program using internal load memory requires a large amount of load memory. There might be insufficient free space for data log files. In this case, you can use a "Program card" (Page 112) to increase the size of load memory. S7-1200 CPUs can use either internal or external load memory, but not both at once.

Maximum size rule for Data log files

The maximum size of one data log file cannot exceed the free load memory size or 500 megabytes, whichever is smaller. The size of 500 megabytes in this case refers to the decimal definition of megabyte, such that the maximum data log file size is 500,000,000 bytes or 500 x 1000^2 bytes.

Table 10-217 Load memory size

Data area	CPU 1211C	CPU 1212C	CPU 1214C	CPU 1215C, CPU 1217C	Data storage
Internal load memory flash memory	1 MB	2 MB	4 MB	4 MB	User program and program data, configuration data, Data logs, user-defined Web pages, and PLC system data
External load memory Optional "Program card" flash memory	4 MB, 12 MB, 24 MB, 256 MB, 2 GB, or 32 GB depending on the SD card size				

Determining load memory free space

The amount of load memory free space varies during normal operations as the operating system uses and releases memory. Use the following steps to view the load memory memory size.

1. Establish an online connection between STEP 7 and the target S7-1200 PLC.
2. Download the program that controls your data log operations.
3. Create any optional user-defined Web pages that you need. The standard Web pages that access data logs are stored in PLC firmware and do not use load memory.
4. Use the Online and diagnostic tools (Page 1047) or the Web server Diagnostics page (Page 773)to view total load memory size and free space.

Calculating the size of a data log file (all data records)

When the data log file is created the CPU allocates the maximum memory size. In addition to the size required for all the data records, you must include storage space for a data log header (if used), time stamp header (if used), record index header, and the minimum block size for memory allocation.

Use the following formula to determine the size of your data log files and ensure you do not violate the maximum size rule.

Data log data bytes = ((data bytes in one record + time stamp bytes + 12 bytes) * number of records)

Header

Data log header bytes = header character bytes + 2 bytes

Header character bytes

- No data header and no timestamps = 7 bytes
- No data header and timestamps (has a timestamp header) = 21 bytes
- Data headers and no timestamps = number of character bytes in all column head text including separator commas
- Data headers and timestamps (has a timestamp header) = number of character bytes in all column head text including separator commas +21 bytes

Data

Data log data bytes = ((data bytes in one record + time stamp bytes + 12 bytes) * number of records)

Data bytes in one data record

The DataLogCreate DATA parameter points to a structure that assigns the number of data fields and the data type of each data field for one data log record.

Multiply the number of occurrences for a given data type by the number of bytes required. Repeat the process for each data type in a record and sum all the data bytes to get the total of all data elements in one record.

Size of individual data elements

Log data is stored as character bytes in the CSV (comma separated values) file format. The following table shows the number of bytes that are required to store each data element.

Data type	Number of bytes (includes data plus one comma byte)
Bool	2
Byte	5
Word	7
DWord	12
Char	4
String	**Example 1**: MyString String[10] The maximum string size is assigned as 10 characters. Text characters + automatic padding with blank characters = 10 bytes Opening and closing double quote + comma characters = 3 bytes 10 + 3 = 13 total bytes **Example 2**: Mystring2 String If no size is assigned with square brackets, then 254 bytes is allocated by default. Text characters + automatic padding with blank characters = 254 bytes Opening and closing double quote + comma characters = 3 bytes 254 + 3 = 257 total bytes
USInt	5
UInt	7
UDInt	12
SInt	5
Int	7
DInt	12
Real	16

LReal	25
Time	15
DTL	24

Number of records in a data log file

The RECORDS parameter of the DataLogCreate instruction sets the maximum number of records in a data log file.

Time stamp bytes in one data record

- No time stamp = 0 bytes
- Time stamp = 20 bytes

10.9.2.5 Data log example program

This data log example program does not show all the program logic necessary to get sample values from a dynamic process, but does show the key operations of the data log instructions. The structure and number of log files that you use depends on your process control requirements.

NOTE

General usage of data log files

- Data log files are automatically opened after the DataLogCreate and DataLogNew file operations.
- Data log files automatically close after a PLC RUN to STOP transition or a PLC power cycle.
- A data log file must be open before a DataLogWrite operation is possible.
- A maximum of eight data log files can be open at one time. More than eight data log files can exist, but no more than eight can be open at the same time.

Example data log program

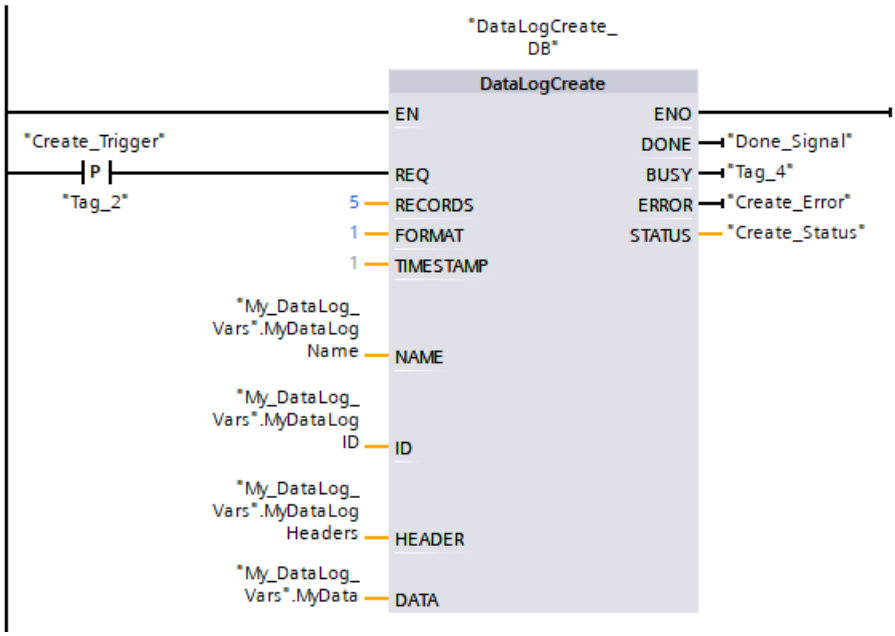
This example uses a data block for data log names, header text, and the MyData structure. The three MyData variables temporarily store new sample values. When executed, the DataLogWrite instruction transfers process sample values at these DB locations to a data log file.

My_DataLog_Vars

	Name	Data type	Start value
1	Static		
2	MyNewDataLogName	String	'DataLog002'
3	MyDataLogName	String	'DataLog001'
4	MyDataLogID	DWord	0
5	MyDataLogHeaders	String	'Count,Temperature,Pressure'
6	MyData	Struct	
7	MyCount	Int	0
8	MyTemperature	Real	0.0
9	MyPressure	Real	0.0

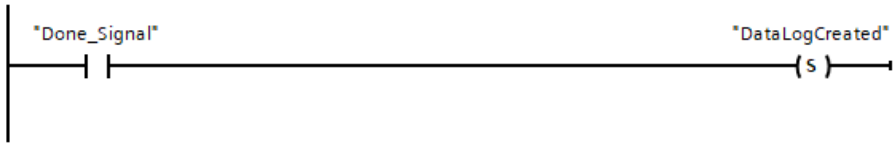
Figure

Network 1 Start the data log creation process with REQ rising edge "Create_Trigger".



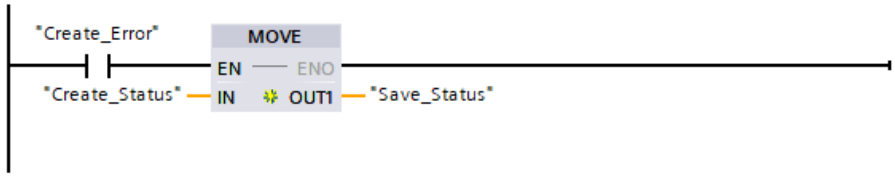
Figure

Network 2 Capture the DONE output from DataLogCreate because it is only valid for one scan.

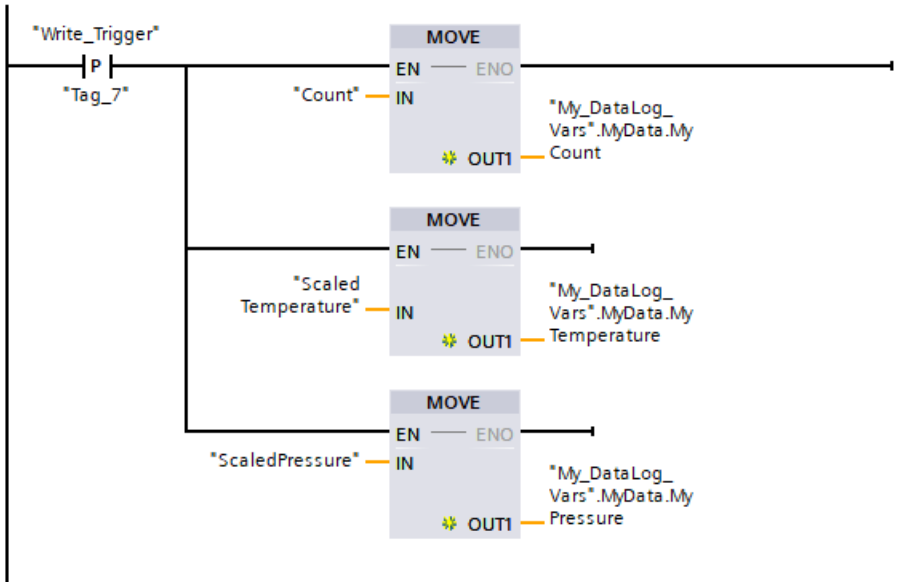


Figure

Network 3 If an error exists, save the status output.

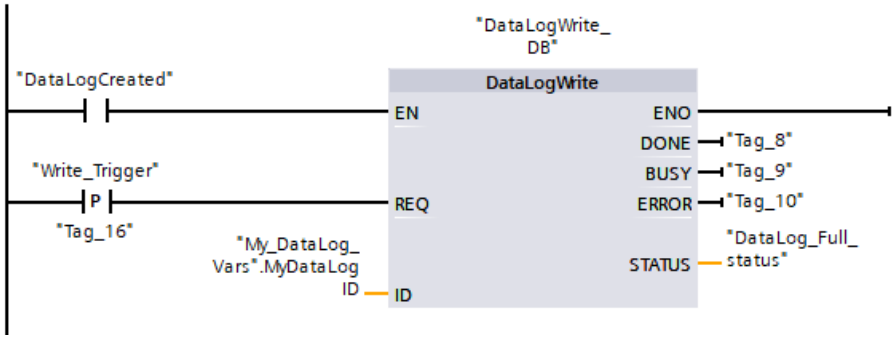


Network 4 A positive edge "Write_Trigger" signal triggers when to store new process values in the MyData structure.



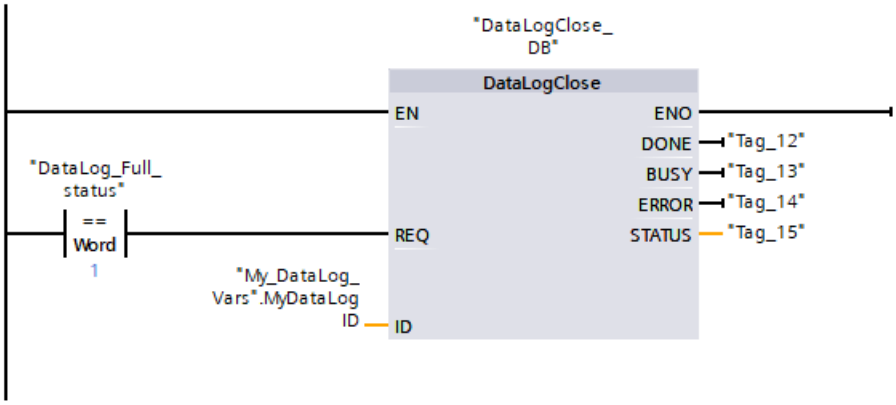
Figure

Network 5 The EN input state is based upon when the DataLogCreate operation is complete. A create operation extends over many scan cycles and must be complete before executing a write operation. The positive edge signal on the REQ input is the event that triggers a write operation.



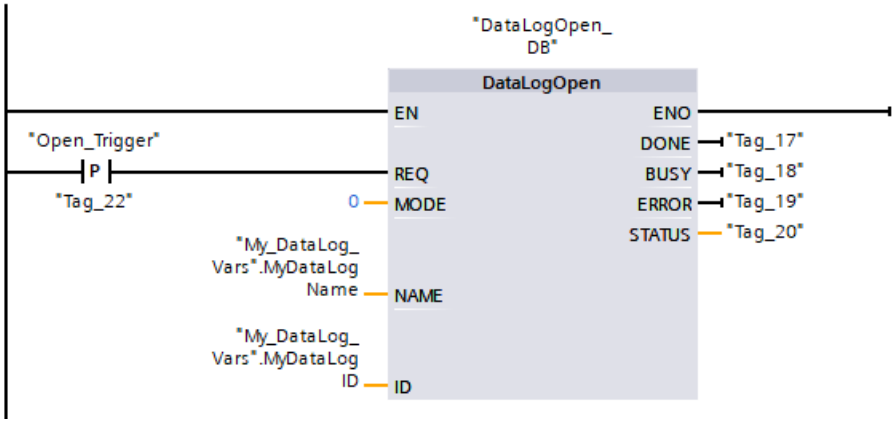
Figure

Network 6 Close the data log after executing the DataLogWrite operation that writes the last record. The DataLogWrite STATUS output = 1 signals the log file full status.



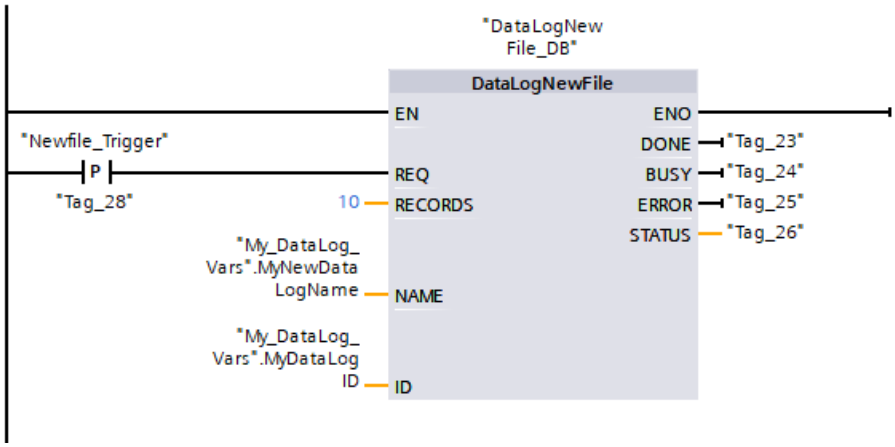
Figure

Network 7 A positive signal edge DataLogOpen REQ input simulates the operator pressing a button on an HMI that opens a data log file. If you open a data log file that has all records filled with process data, then the next DataLogWrite operation overwrites the oldest record. You might want to preserve the old data log and create a new data log, as shown in network 7.



Figure

Network 8 The ID parameter is an IN/OUT type. First, you supply the ID value of the existing data log structure you want to copy. After the DataLogNewFile operation is complete, a new and unique ID value for the new data log is written back to the ID reference location. The required DONE bit = TRUE capture is not shown. Refer to networks 1, 2, and 4 for an example of DONE bit logic.



Data log files viewed with the S7-1200 CPU Web Server

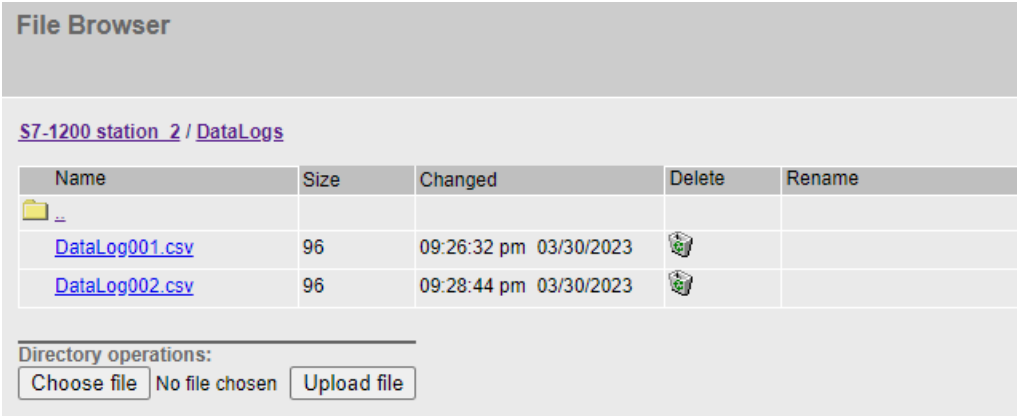


Table 10-218 Downloaded .csv file examples viewed with Excel

Records 1 and 2 written in a data log with a 5 record maximum

	A	B	C	D	E	F
1	Record	Date	UTC Time	Count	Temperature	Pressure
2	1	3/14/2022	18:31:19	1	9.86E+01	3.52E+01
3	2	3/14/2022	18:36:34	2	1.00E+02	3.73E+01
4						
5						
6						
7						

Figure

Records 1-5 written in a data log file with a 5 record maximum

	A	B	C	D	E	F
1	Record	Date	UTC Time	Count	Temperature	Pressure
2	1	3/14/2022	18:31:19	1	9.86E+01	3.52E+01
3	2	3/14/2022	18:36:34	2	1.00E+02	3.73E+01
4	3	3/14/2022	18:38:15	3	9.99E+02	3.68E+01
5	4	3/14/2022	18:38:51	4	9.95E+01	3.64E+01
6	5	3/14/2022	18:40:08	5	9.92E+01	3.74E+01
7						

Figure

Records 2-6 written in a data log file with a 5 record maximum

After one additional record is written to the full file, the 6th write operation overwrites the oldest record (1) with record 6. Another write operation will overwrite record 2 with record 7, and so on.

	A	B	C	D	E	F
1	Record	Date	UTC Time	Count	Temperature	Pressure
2	6	3/14/2022	18:42:45	6	9.86E+01	3.58E+01
3	2	3/14/2022	18:36:34	2	1.00E+02	3.73E+01
4	3	3/14/2022	18:38:15	3	9.99E+02	3.68E+01
5	4	3/14/2022	18:38:51	4	9.95E+01	3.64E+01
6	5	3/14/2022	18:40:08	5	9.92E+01	3.74E+01
7						

Figure

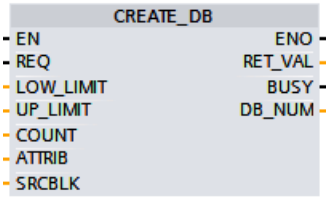
NOTE

Data logs no longer use an //END marker to mark the end of a data log file that is not full. Prior to V4.1 of the S7-1200 CPU, data logs that were not full included an //END marker.

10.10 Data block control

10.10.1 CREATE_DB (Create data block)

Table 10-219 CREATE_DB instruction

LAD / FBD	SCL	Description
	**ret_val := CREATE_DB(REQ:=_bool_in_, LOW_LIMIT:=_uint_in_, UP_LIMIT:=_uint_in_, COUNT:=_udint_in_, ATTRIB:=_byte_in_, BUSY=>_bool_out_, DB_NUM=>_uint_out_);**	Use the instruction "CREATE_DB" to create a new data block in the load and/or work memory. The instruction "CREATE_DB" does not change the checksum of the user program. A data block that you create only in work memory has the following properties: • After a memory reset or POWER OFF / POWER ON this block no longer exists. • When loading or when there is a STOP-RUN transition, its content remains unchanged.

Number of the data block

The data block created is assigned a number from the range defined at the LOW_LIMIT (low limit) and UP_LIMIT (high limit) parameters. "CREATE_DB" assigns the smallest possible number from the specified range to the DB. You cannot assign the numbers of the DBs already contained in the user program.

To create a DB with a specific number, enter the same number for the high and low limit of the range to be specified. If a DB with the same number already exists in the work memory and/or load memory, or if the DB exists as a copied version, the instruction will be terminated and an error message will be generated at the RET_VAL parameter.

Start values of the data block

The SRCBLK parameter is used to define start values for the DB that is to be created. The SRCBLK parameter is a pointer to a DB or a DB area from which you apply the start values. The DB addressed at the SRCBLK parameter must have been generated with standard access ("Optimized block access" attribute disabled).

- If the area specified at the SRCBLK parameter is larger than the DB generated, the values up to the length of the DB generated will be applied as start values.
- If the area specified at the SRCBLK parameter is smaller than the DB generated, the remaining values will be filled with "0".

To ensure data consistency, you must not change this data area while "CREATE_DB" is being executed (which means as long as the BUSY parameter has the value TRUE).

Functional description

The "CREATE_DB" instruction works asynchronously. Processing takes place across several calls. You start the job by calling "CREATE_DB" with REQ = 1.

The output parameters RET_VAL and BUSY indicate the status of the job.

See also: DELETE_DB (Delete data block) (Page 466)

Parameters

The following table shows the parameters of the "CREATE_DB" instruction:

Parameter	Declaration	Data type	Memory area	Description
REQ	Input	BOOL	I, Q, M, D, L or constant	Level-triggered control parameter "request to activate" REQ = 1: Request to generate the data block
LOW_LIMIT	Input	UINT	I, Q, M, D, L or constant	Low limit of the range for the assignment of a DB number. The smallest possible number is 60000.
UP_LIMIT	Input	UINT	I, Q, M, D, L or constant	High limit of the area used by "CREATE_DB" to assign a number to your DB (largest possible DB number: 60999)
COUNT	Input	UDINT	I, Q, M, D, L or constant	The count value specifies the number of bytes which you want to reserve for the DB generated. The number of bytes must be an even number. The maximum length is 65534 bytes.
ATTRIB	Input	BYTE	I, Q, M, D, L or constant	You use the first 4 bits of the byte at parameter ATTRIB to define the properties of the data block *:
				• Bit 0 = 0: Attribute "Only store in load memory" is not set. • Bit 0 = 1: Attribute "Only store in load memory" is set. With this setting, the DB takes up no space in the work memory and is not included in the program. The DB cannot be accessed with bit commands. When bit 0 = 1, the selection for bit 2 is irrelevant. To ensure compatibility with STEP 7 V5.x, bits 0 and 3 must be considered together (see below).
				• Bit 1 = 0: Attribute "Data block write-protected in the device" is not set. • Bit 1 = 1: Attribute "Data block write-protected in the device" is set.
				• Bit 2 = 0: DB is retentive (only for DBs generated in the load and in the work memory). The DB is regarded as retentive if at least one value has been set as retentive. • Bit 2 = 1: DB is not retentive Retentivity is not supported with DBs that are only stored in load memory or only in the work memory. If you call the "CREATE_DB" instruction with one of the two combinations "retentive and only load memory" or "retentive and only work memory" the DB to be generated will not be marked as retentive.
				• Bit 3 = 0: Creation of the DB either in the load memory or in the work memory (selection using bit 0, see above) • Bit 3 = 1: Creation of the DB both in the load memory and in the work memory (bit 0 irrelevant) To ensure compatibility with STEP 7 V5.x, bits 0 and 3 must be used in combination. When bit 3 = 1, bit 0 is irrelevant.

Bit 0	Bit 3	DB generation
0	0	In work memory only
1	0	In load memory only
Irrelev-ant	1	Work and load memory

				• Bit 4 = 0 - No start values specified (input values at the SRCBLK parameter will be ignored). • Bit 4 = 1 - Specify start values (values correspond to the DB addressed by the SRCBLK parameter).

Parameter	Declaration	Data type	Memory area	Description
SRCBLK	Input	VARIANT	D	Pointer to the data block whose values will be used to initialize the data block to be generated.
RET_VAL	Return	INT	I, Q, M, D, L	Error information
BUSY	Output	BOOL	I, Q, M, D, L	BUSY = 1: The process is not yet complete.
DB_NUM	Output	DB_DYN (UINT)	I, Q, M, D, L	Number of the DB created.
* The properties selected here correspond to the attributes in the properties of a data block.				

You can find additional information on valid data types under "Data types (Page 95)".

Parameter RET_VAL

Error code* (W#16#...)	Description
0000	No error
0081	The destination area is greater than the source area. The source area is written completely to the destination area. The remaining bytes of the destination area remain unchanged.
7000	First call with REQ = 0: No data transfer active; BUSY has the value "0".
7001	First call with REQ = 1: Data transfer triggered; BUSY has the value "1".
7002	Intermediate call (REQ irrelevant): Data transfer already active; BUSY has the value "1".
8081	The source area is larger than the destination area. The complete destination area is written. The remaining bytes of the source area are ignored.
8092	The "Create data block" function is currently unavailable because • The "Compress user memory" function is currently active. • The maximum number of blocks on your CPU has already been reached.
8093	No data block or a data block that is not in the work memory is specified for the SRCBLK parameter.
8094	An invalid value was specified at parameter ATTRIB.
80A1	DB number error: • The number is "0" • The number exceeds the CPU-specific high limit for DB numbers • Low limit > high limit
80A2	DB length error: • The length is "0" • The length is an odd number • The length is greater than permitted by the CPU
80A3	The data block at the SRCBLK parameter was not created with standard access.
80B1	There is no DB number free.
80B2	Not enough work memory.
80B4	The memory card is write-protected.
80BB	Not enough load memory.

Error code* (W#16#...)	Description
80C3	The maximum number of simultaneously active "CREATE_DB" instructions has already been reached.
General error information	See also: Common error codes for the Extended instructions (Page 473)
* You can display the error code as either integer or hexadecimal values in the program editor.	

10.10.2 READ_DBL and WRIT_DBL (Read/write a data block in load memory) instructions

Table 10-220 READ_DBL and WRIT_DBL instructions

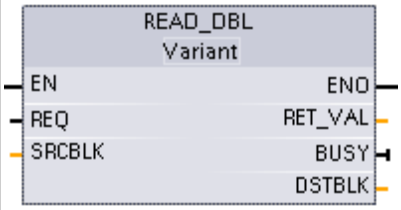
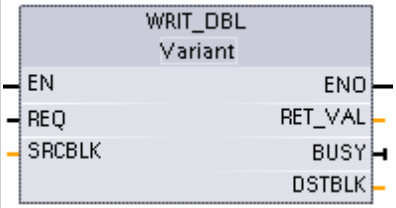
LAD / FBD	SCL	Description
	**READ_DBL(** **req:=_bool_in_,** **srcblk:=_variant_in_,** **busy=>_bool_out_,** **dstblk=>_variant_out_);**	Copies DB start values or part of the values, from load memory to a target DB in the work memory. The content of load memory is not changed during the copy process.
	**WRIT_DBL(** **req:=_bool_in_,** **srcblk:=_variant_in_,** **busy=>_bool_out_,** **dstblk=>_variant_out_);**	Copies DB current values or part of the values from work memory to a target DB in load memory. The content of work memory is not changed during the copy process.

Table 10-221 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	BOOL	A high signal starts the operation, if BUSY = 0.
SRCBLK	IN	VARIANT	READ_DBL: Pointer to the source data block in load memory WRIT_DBL: Pointer to the source data block in work memory
RET_VAL	OUT	INT	Execution condition code
BUSY	OUT	BOOL	BUSY = 1 signals that the reading/writing process is not complete.
DSTBLK	OUT	VARIANT	READ_DBL: Pointer to the destination data block in work memory WRIT_DBL: Pointer to the destination data block in load memory

Typically, a DB is stored in both load memory (flash) and work memory (RAM). The start values (initial values) are always stored in load memory, and the current values are always stored in work memory. READ_DBL can be used to copy a set of start values from load memory to the current values of a DB in work memory that is referenced by your program. You can use WRIT_DBL to update the start values stored in internal load memory or memory card from current values in work memory.

NOTE

Effect of WRIT_DBL and READ_DBL instruction on flash memory

The WRIT_DBL instruction performs write operations in flash memory (internal load memory or memory card). To avoid reducing the lifetime of the flash memory, use the WRIT_DBL instruction for infrequent updates such as recording changes to a production process. For similar reasons, avoid frequent calls to READ_DBL for read operations.

You must create the data blocks for READ_DBL and WRIT_DBL prior to calling these instructions in the STEP 7 program. If you created the source DB as a "standard" type then the destination DB must also be the "standard" type. If you created the source data block as an "optimized" type then the destination data block must also be the "optimized" type.

If the DBs are standard, then you can specify either a tag name or a P# value. The P# value allows you to specify and copy any number of elements of the specified size (Byte, Word, or DWord). Thus, you can copy part or all of a DB. If the DBs are optimized, you can only specify a tag name; you cannot use the P# operator. If you specify a tag name for either standard or optimized DBs (or for other work-memory types), then the instruction copies the data that this tag name references. This could be a user-defined type, an array, or a basic element. You can only use type Struct with these instructions if the DB is standard, not optimized. You must use a user-defined type (UDT) if it is a structure in optimized memory. Only a user-defined type ensures that the "data types" are exactly the same for both the source and destination structures.

NOTE

Using a structure (data type Struct) in an "optimized" DB

When using a Struct data type with "optimized" DBs, you must first create a user-defined data type (UDT) for the Struct. You then configure both the source and destination DBs with the UDT. The UDT ensures that the data types within the Struct remain consistent for both DBs.

For "standard" DBs, you use the Struct without creating a UDT.

READ_DBL and WRIT_DBL execute asynchronously to the cyclic program scan. The processing extends over multiple READ_DBL and WRIT_DBL calls. You start the DB transfer job by calling with REQ = 1 and then monitor the BUSY and RET_VAL outputs to determine when the data transfer is complete and correct.

NOTE

Effect of WRIT_DBL and READ_DBL instruction on communication load

When the WRIT_DBL or READ_DBL instruction is continually active, it can consume communication resources to the point that STEP 7 loses communication with the CPU. For this reason, use a positive edge input (Page 202) for the REQ parameter rather than a normally open or closed input (Page 197) that would remain on (signal level high) for multiple scans.

To ensure data consistency, do not modify the destination area during the processing of READ_DBL or the source area during the processing of WRIT_DBL (that is, as long as the BUSY parameter is TRUE).

SRCBLK and DSTBLK parameter restrictions:

- A data block must have been previously created before it can be referenced.
- The length of a VARIANT pointer of type BOOL must be divisible by 8.
- The length of a VARIANT pointer of type STRING must be the same in the source and destination pointers.

Recipes and machine setup information

You can use the READ_DBL and WRIT_DBL instructions to manage recipes or machine setup information. This essentially becomes another method of achieving retentive data for values that do not change often, although you would want to limit the number of writes to prevent wearing out the flash prematurely. This effectively allows you to increase the amount of retentive memory beyond that supported for the normal power-down retentive data, at least for values that do not change often. You could save recipe information or machine-setup information from work memory to load memory using the WRIT_DBL instruction, and you could retrieve such information from load memory into work memory using the READ_DBL instruction.

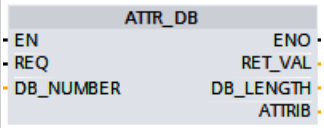
Table 10-222 Condition codes

RET_VAL (W#16#...)	Description
0000	No error
0081	Warning: that the source area is smaller than the destination area. The source data is copied completely with the extra bytes in the destination area unchanged.
7000	Call with REQ = 0: BUSY = 0
7001	First call with REQ = 1 (working): BUSY = 1
7002	N^{th} call (working): BUSY = 1
8051	Data block type error
8081	The source area is larger than the destination area. The destination area is completely filled and the remaining bytes of the source are ignored.
8251	Source data block type error
82B1	Missing source data block
82C0	The source DB is being edited by another statement or a communication function.
8551	Destination data block type error
85B1	Missing destination data block
85C0	The destination DB is being edited by another statement or a communication function.
80C3	More than 50 READ_DBL or 50 WRIT_DBL statements are currently queued for execution.

See also Recipes (Page 425)

10.10.3 ATTR_DB (Read data block attribute)

Table 10-223 ATTR_DB instruction

LAD / FBD	SCL	Description
	**ret_val := ATTR_DB(REQ:=_bool_in_, DB_NUMBER:=_uint_in_, DB_LENGTH=>_udint_out_, ATTRIB=>_byte_out_);**	You use the instruction "ATTR_DB" to obtain information about a data block (DB) located in the work memory of the CPU. The instruction determines the attributes set at the ATTRIB parameter for the DB selected. The length cannot be read out for data blocks with optimized access and data blocks that are only in load memory. In these cases, the DB_LENGH parameter has the value "0". Do not apply ATTR_DB to data blocks with optimized access and activated memory reserve.

LAD / FBD	SCL	Description
		Do not read out the data blocks for motion control with the "ATTR_DB" instruction. The error code 80B2 is output for this.

Parameters

The following table shows the parameters of the "ATTR_DB" instruction:

Parameter	Declaration	Data type	Memory area	Description
REQ	Input	BOOL	I, Q, M, D, L or constant	REQ = 1: Request to read block attributes
DB_NUMBER	Input	DB_ANY	I, Q, M, D, L or constant	Number of the DB to be tested
RET_VAL	Output	INT	I, Q, M, D, L	Error information
DB_LENGTH	Output	UDINT	I, Q, M, D, L	• Number of data bytes that the selected DB contains. • "0" for data blocks with optimized access and data blocks that are only in load memory.
ATTRIB	Output	BYTE	I, Q, M, D, L	DB properties:
				• Bit 0*= 0: Attribute "Only store in load memory" is not set. • Bit 0*= 1: Attribute "Only store in load memory" is set.
				• Bit 1 = 0: Attribute "Data block write-protected in the device" is not set. • Bit 1 = 1: Attribute "Data block write-protected in the device" is set.
				If bit 0 = 1, then bit 2 is irrelevant and gets the value 1. • Bit 2 = 0: Retentive - The DB is regarded as retentive if at least one value has been set as retentive. • Bit 2 = 1: Not retentive - The complete DB is not retentive.
				• Bit 3*= 0: The DB is either in the load memory (bit 0 = 1) or in the work memory (bit 0 = 0). • Bit 3*= 1: The DB is generated in both the load and the work memory
* The relationship between bit 0 and bit 3 is explained in the parameters of the instruction "CREATE_DB (Create data block) (Page 459)".				

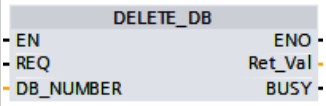
You can find additional information on valid data types under "Data types (Page 95)".

Parameter RET_VAL

Error code* (W#16#...)	Explanation
0000	No error occurred.
80A1	Error in input parameter DB_NUMBER: the actual parameter selected • Is "0" • Is greater than the maximum permitted DB number for the CPU used.
80B1	The DB with the specified number does not exist on the CPU.
80B2	Data blocks of motion control technology objects cannot be read with the "ATTR_DB" instruction.
General error information	See also: Common error codes for the Extended instructions (Page 473)
* You can display the error code as either integer or hexadecimal values in the program editor.	

10.10.4 DELETE_DB (Delete data block)

Table 10-224 DELETE_DB instruction

LAD / FBD	SCL	Description
	**ret_val := DELETE_DB(REQ := _bool_in_, DB_NUMBER := _uint_in_, BUSY => _bool_out_);**	You use the instruction "DELETE_DB" to delete a data block (DB) that the user program created by calling the instruction "CREATE_DB (Page 459)". If the data block was not created with "CREATE_DB", DELETE_DB returns the error code W#16#80B5 at the RET_VAL parameter. The DELETE_DB call does not delete the selected data block immediately, but rather at the cycle control point after execution of the cycle OB.

Functional description

The "DELETE_DB" instruction works asynchronously, that is, its execution extends over multiple calls. You start the interrupt transfer by calling the instruction with REQ = 1.

Output parameter BUSY and bytes 2 and 3 of output parameter RET_VAL show the status of the job.

The deletion of the data block is complete when output parameter BUSY has the value FALSE.

Parameters

The following table shows the parameters of the "DELETE_DB" instruction:

Parameter	Declaration	Data type	Memory area	Description
REQ	Input	BOOL	I, Q, M, D, L or constant	REQ =1: Request to delete the DB with the number in parameter DB_NUMBER
DB_NUMBER	Input	UINT	I, Q, M, D, L or constant	Number of the DB to be deleted
RET_VAL	Output	INT	I, Q, M, D, L	Error information (see "RET_VAL parameter")
BUSY	Output	BOOL	I, Q, M, D, L	BUSY= 1: The process is not yet complete.

You can find additional information on valid data types under "Data types (Page 95)".

Parameter RET_VAL

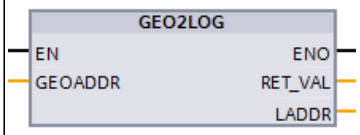
Error code* (W#16#...)	Explanation
0000	No error occurred.
7000	First call with REQ = 0: No data transfer active; BUSY has the value "0".
7001	First call with REQ = 1: Data transfer triggered; BUSY has the value "1".
7002	Intermediate call (REQ irrelevant): Data transfer already active; BUSY has the value "1".
80A1	Error in input parameter DB_NUMBER: • The value at the parameter is "0". • The value at the parameter is greater than the maximum permitted DB number for the CPU used.
80B1	The DB with the specified number does not exist on the CPU.
80B4	The DB cannot be deleted because the memory card of the CPU is write-protected.
80B5	The DB was not created using "CREATE_DB".
80BB	Not enough load memory.
80C3	The "Delete a DB" function cannot be executed at this time due to a temporary resource bottleneck.
General error information	See also: Common error codes for the Extended instructions (Page 473)
* You can display the error code as either integer or hexadecimal values in the program editor.	

10.11 Address handling

10.11.1 GEO2LOG (Determine the hardware identifier from the slot)

You use the GEO2LOG instruction to determine the hardware identifier based upon slot information.

Table 10-225 GEO2LOG instruction

LAD / FBD	SCL	Description
	**ret_val := GEO2LOG(GEOADDR:=_variant_in_out_, laddr:=_word_out_);**	You use the GEO2LOG instruction to determine the hardware identifier based upon slot information.

The GEO2LOG instruction determines the hardware identifier based upon slot information that you define using the GEOADDR system data type:

Depending on the type of hardware you define at the parameter HWTYPE, the following information is evaluated from the other GEOADDR parameters:

- With HWTYPE = 1 (PROFINET IO system):
  - Only IOSYSTEM is evaluated. The other parameters of GEOADDR are not taken into consideration.
  - The hardware identifier of the PROFINET IO system is output.
- With HWTYPE = 2 (PROFINET IO device):
  - IOSYSTEM and STATION are evaluated. The other parameters of GEOADDR are not taken into consideration.
  - The hardware identifier of the PROFINET IO device is output.
- With HWTYPE = 3 (rack):
  - Only IOSYSTEM and STATION are evaluated. The other parameters of GEOADDR are not taken into consideration.
  - The hardware identifier of the rack is output.
- With HWTYPE = 4 (module):
  - IOSYSTEM, STATION, and SLOT are evaluated. The SUBSLOT parameter of GEOADDR is not taken into consideration.
  - The hardware identifier of the module is output.
- With HWTYPE = 5 (submodule):
  - All parameters of GEOADDR are evaluated.
  - The hardware identifier of the submodule is output.

The AREA parameter of the GEOADDR system data type is not evaluated.

Table 10-226 Data types for the parameters

Parameter and type		Data type	Description
GEOADDR	IN/OUT or IN ?	Variant	Pointer to the structure of the GEOADDR system data type. The GEOADDR system data type contains the slot information from which the hardware ID is determined. Refer to the "GEOADDR system data type (Page 472)" for further information.
RET_VAL	OUT or RETURN ?	Int	Output of error information.
LADDR	OUT	HW_ANY	Hardware identifier of the assembly or the module. The number is automatically assigned and is stored in the properties in the hardware configuration.

For further information on valid data types, refer to "Overview of the valid data types" in the STEP 7 online help.

Table 10-227 Condition codes

RET_VAL* (W#16#...)	Explanation
0	No error occurred.
8091	Invalid value for in GEOADDR for HWTYPE.
8094	Invalid value for in GEOADDR for IOSYSTEM.
8095	Invalid value for in GEOADDR for STATION.
8096	Invalid value for in GEOADDR for SLOT.
8097	Invalid value for in GEOADDR for SUBSLOT.
* The error codes can be displayed as integer or hexadecimal values in the program editor.	

10.11.2 LOG2GEO (Determine the slot from the hardware identifier)

You use the LOG2GEO instruction to determine the geographical address (module slot) from the logical address belonging to a hardware identifier.

Table 10-228 LOG2GEO instruction

LAD / FBD	SCL	Description
	ret_val := LOG2GEO(laddr:=_word_in_, GEOADDR:=_variant_in_out_);	You use the LOG2GEO instruction to determine the module slot belonging to a hardware identifier.

The LOG2GEO instruction determines the geographic address of a logical address based upon the hardware identifier:

- Use the LADDR parameter to select the logical address based upon the hardware identifier.
- The GEOADDR contains the geographic address of the logical address given at the LADDR input.

NOTE

In the cases where the HW type does not support a component, a subslot number for a module 0 is returned.

An error is provided if the LADDR input does not address a HW object.

Table 10-229 Data types for the parameters

Parameter and type		Data type	Description
LADDR	IN	HW_ANY	Hardware identifier of the IO system or the module. The number is assigned automatically and is stored in the properties of the CPU or the interface of the hardware configuration.
RET_VAL	OUT	Int	Error code of the instruction
GEOADDR	IN_OUT	Variant	Pointer to the GEOADDR system data type. The GEOADDR system data type contains the slot information. Refer to the "GEOADDR system data type (Page 472)" for further information.

For further information on valid data types, refer to "Overview of the valid data types" in the STEP 7 online help.

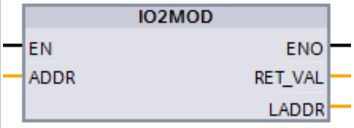
Table 10-230 Condition codes

RET_VAL (W#16#...)	Description
0000	No error
8090	The address specified at the LADDR parameter is invalid.
* The error codes can be displayed as integer or hexadecimal values in the program editor.	

10.11.3 IO2MOD (Determine the hardware identifier from an I/O address)

You use the IO2MOD instruction to determine the hardware identifier of the module from an I/O address of a (sub)module.

Table 10-231 IO2MOD instruction

LAD / FBD	SCL	Description
	**ret_val := IO2MOD(ADDR:=_word_in_, LADDR:=_word_out_);**	You use the IO2MOD instruction to determine the module slot belonging to a hardware identifier.

The IO2MOD instruction determines the hardware identifier of the module from an IO address (I, Q, PI, PQ) of a (sub)module.

Enter the IO address at the ADDR parameter. If a series of IO addresses is used at this parameter, only the first address is evaluated to determine the hardware identifier. If the first address is correctly specified, the length for the address specification at the ADDR is of no significance. If an address area is used that encompasses several modules or non-used addresses, the hardware identifier of the first module can also be determined.

If no IO address of a (sub)module is specified at the ADDR parameter, the error code "8090" is output at the RET_VAL parameter.

NOTE

Input of IO address in SCL

You cannot program using the IO access ID "%QWx:P" in SCL. In this case, use the symbolic tag name or the absolute address in the process image.

Table 10-232 Data types for the parameters

Parameter	Declaration	Data type	Memory area	Description
ADDR	IN or IN/OUT ?	Variant	I, Q, M, D, L	IO address (I, Q, PI, PQ) within a (sub)module. Make sure that slice access is not used for the parameter ADDR. If this is the case, incorrect values are output at the LADDR parameter.
RET_VAL	OUT or RETURN ?	Int	I, Q, M, D, L	Error code of the instruction.
LADDR	OUT	HW_IO	I, Q, M, D, L	Determined hardware identifier (logical address) of the IO (sub)module.

For further information on valid data types, refer to "Overview of the valid data types" in the STEP 7 online help.

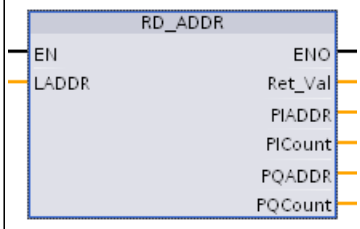
Table 10-233 Condition codes

RET_VAL* (W#16#...)	Explanation
0	No error occurred.
8090	IO address specified at ADDR parameter is not used by any hardware component.
* The error codes can be displayed as integer or hexadecimal values in the program editor.	

10.11.4 RD_ADDR (Determine the IO addresses from the hardware identifier)

You use the RD_ADDR instruction to get the I/O addresses of a submodule.

Table 10-234 RD_ADDR instruction

LAD / FBD	SCL	Description
	**ret_val := RD_ADDR(laddr:=_word_in_, PIADDR=>_udint_out_, PICount=>_uint_out_, PQADDR=>_udint_out_, PQCount=>_uint_out_,);**	You use the RD_ADDR instruction to get the I/O addresses of a submodule.

The RD_ADDR instruction determines the length and the start address of the inputs or outputs based on the hardware identifier of a submodule:

- Use the LADDR parameter to select the input or output module based upon the hardware identifier.
- The following output parameters are used depending on whether it is an input module or output module:
  - In the case of an input module, the determined values are output at the PIADDR and PICOUNT parameters.
  - In the case of an output module, the determined values are output at the PQADDR and PQCOUNT parameters.
- The PIADDR and PQADDR parameters each contain the start address of the I/O addresses of the module.
- The PICOUNT and PQCOUNT parameters each contain the number of bytes of the inputs or outputs (1 byte for 8 inputs/outputs, 2 bytes for 16 inputs/outputs).

Table 10-235 Data types for the parameters

Parameter and type		Data type	Description
LADDR	IN	HW_IO	Hardware identifier of the (sub)module
RET_VAL	OUT	Int	Error code of the instruction
PIADDR	OUT	UDInt	Start address of the input module
PICOUNT	OUT	UInt	Number of bytes of the inputs
PQADDR	OUT	UDInt	Start address of the output module
PQCOUNT	OUT	UInt	Number of bytes of the outputs

For further information on valid data types, refer to "Overview of the valid data types" in the STEP 7 online help.

Table 10-236 Condition codes

RET_VAL (W#16#...)	Description
0000	No error
8090	Hardware identifier of the module at the LADDR parameter is invalid.
* The error codes can be displayed as integer or hexadecimal values in the program editor.	

10.11.5 GEOADDR system data type

Geographical address

The system data type GEOADDR contains the geographical address of a module (or the slot information).

- Geographical address for PROFINET IO:
  For PROFINET IO, the geographical address is composed of the ID of the PROFINET IO system, the device number, the slot number, and the submodule (if a sub-module is used).
- Geographical address for PROFIBUS DP:
  For PROFIBUS DP, the geographical address consists of the ID of the DP master system, the station number, and the slot number.

The slot information of the modules can be found in the hardware configuration of each module.

Structure of the GEOADDR system data type

The structure GEOADDR is automatically created if you enter "GEOADDR" as the data type in a data block.

Parameter name	Data type	Description
GEOADDR	STRUCT	
HWTYPE	UINT	Hardware type: • 1: IO system (PROFINET/PROFIBUS) • 2: IO device/DP slave • 3: Rack • 4: Module • 5: Submodule If a hardware type is not supported by the instruction, a HWTYPE "0" is output.
AREA	UINT	Area ID: • 0 = CPU • 1 = PROFINET IO • 2 = PROFIBUS DP • 3 = AS-i
IOSYSTEM	UINT	PROFINET IO system (0=central unit in the rack)

Parameter name		Data type	Description
	STATION	UINT	• Number of the rack if area identifier AREA = 0 (central module). • Station number if area identifier AREA > 0.
	SLOT	UINT	Slot number
	SUBSLOT	UINT	Number of the submodule. This parameter has the value "0" if no submodule is available or can be plugged.

10.12 Common error codes for the Extended instructions

Table 10-237 Common condition codes for the extended instructions

Condition code (W#16#....)[1]	Description
8x22[2]	Area too small for input
8x23	Area too small for output
8x24	Illegal input area
8x25	Illegal output area
8x28	Illegal input bit assignment
8x29	Illegal output bit assignment
8x30	Output area is a read-only DB.
8x3A	DB does not exist.

[1] If one of these errors occurs when a code block is executed, then the CPU remains in RUN (default) or can be configured to go to STOP. Optionally, you can use the GetError or GetErorID instructions within that code block to handle the error locally (CPU remains in RUN), and create a programmed reaction to the error.

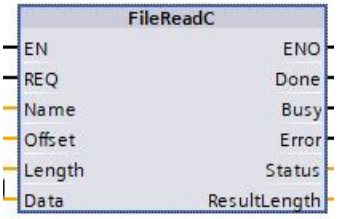
[2] The "x" represents the parameter number with the error. Parameter numbers start with 1.

10.13 File handling

10.13.1 FileReadC: Read file from the memory card

You can use the "FileReadC" instruction to read data from a file located on the memory card and write it to a destination area on the CPU. You specify the file by entering its name and complete path.

Table 10-238 FileReadC instruction

LAD / FBD	SCL	Description
	**"FileReadC_SFB_DB_2"(REQ:=_bool_in_ Name:=_string_in_ Offset:=_udint_in_, Length:=_udint_in_, Done=>_bool_out_, Busy=>_bool_out_, Error=>_bool_out_, Status=>_word_out_, ResultLength=>_udint_out_, Data:=_variant_inout_);**	You can use the "FileReadC" instruction to read data from a file located on the memory card and write it to a destination area on the CPU.

Enable reading from the file using the REQ control parameter. The output parameters Done, Busy, Error and Status indicate the status of the job.

The following rules apply for the file name and path specification:

- The file name must not be longer than 55 characters.
- The following characters are permitted for the folder and file name: "0" to "9", "a" to "z", "A" to "Z", "-", "_"
- The file name must not contain more than one dot ("."); the dot separates the name from the file extension. The file name must contain at least one character. A file extension is not necessary.
- The path name must not start with "/", "\" or ".".
- The path name must not contain any ".."
- The path name must not contain a subfolder under the UserFiles folder.

Examples of valid paths and file names: "UserFiles/Lift16_DataBase.txt", "UserFiles/2017-04-13_ErrorLog.bin"

You can read up to 16 MB (16,777,216 bytes) by executing "FileReadC"; the data is read segment by segment. The segment size is device-specific; an S7-1500-CPU, for example, uses 32 KB (32,768 byte) blocks. If the number of data items to be read is greater than the segment size, you will need to call the instruction multiple times in your program. For consistency reasons, you should therefore not access the data read until after you call the instruction for the last time.

The parameters "Offset" and "Length" specify the length of the items of data to be read. The resource occupied is released again once the read process is complete.

The "FileReadC" instruction works asynchronously. Processing takes place across several calls. You start processing with a rising edge at the parameter "REQ".

The parameters "Busy" and "Done" indicate the status of the job.

If an error occurs during execution, this is signaled by the parameters "Error" and "Status".

Table 10-239 Data types for the parameters

Parameters and type		Data type	Description
REQ	Input	BOOL	Control parameter Request Enables reading a file from the memory card with a rising edge.
Name	Input	STRING	Name of the file to be read incl. complete path
Offset	Input	UDINT	Byte offset after which the file is to be read
Length	Input	UDINT	Length of the area to be read in bytes Length = 0 means that the maximum possible number of data items per call is read (for an S7-1200-CPU, 8 KB or the size of the "Data" parameter)
Done	Output	BOOL	1: The instruction has been executed successfully. The information read has been transferred to the "Data" parameter.
Busy	Output	BOOL	Status parameter • 0: Execution of the instruction completed or not yet started. • 1: Execution of the instruction not yet complete.
Error	Output	BOOL	Status parameter • 0: No error. • 1: An error occurred during execution of the instruction. Detailed information is output via the "Status" parameter.

Parameters and type		Data type	Description
Status	Output	WORD	Error code
ResultLength	Output	UDINT	Length of data read in bytes
Data	InOut	VARIANT	Destination area for data read Permitted data types: BYTE and Array of BYTE

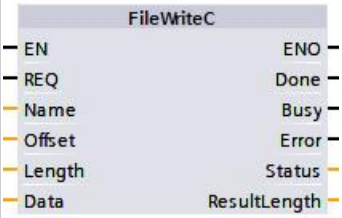
Table 10-240 Condition codes

Error code* (W#16#...)	Explanation
0	No error
7000	No job processing active
7001	Start of job processing. Parameter Busy = 1, Done = 0.
7002	Intermediate call (REQ irrelevant): Instruction already active; Busy has the value "1".
0081	Warning: Offset + Length is greater than the length of the file. Data is read from "Offset" to the end of the file. "Data" contains fewer data items than requested; "ResultLength" is shorter than "Length"; data past "ResultLength" in "Data" remains unchanged.
8091	Path does not exist or is invalid.
8092	The "Name" parameter is not of the data type "STRING", is too long or contains invalid characters.
8093	The "Offset" parameter points past the end of the file to be read.
8094	The "Length" parameter is larger than the maximum permitted value. For an S7-1500 or S7-1200 CPU, for example, the maximum value permitted is 16 MB, i.e. 16,777,216 bytes.
80A1	Read error; the destination area specified by the "Data" parameter may be partly overwritten.
80B1	The destination area specified by the "Data" parameter is shorter than the length required at the "Length" parameter.
80C0	The file cannot be accessed (write-protected or blocked by another process).
80C3	The maximum number of simultaneously active FileReadC instructions has already been reached.
8A30	The target range is write-protected, for example a write-protected DB.
8A3A	The "Data" points to an impermissible area, for example to the load memory or the local data.
8A51	Invalid data type of the "Data" parameter.
8A52	The tag at the Data parameter is insufficient. A part of the source area data may have been written.
* The error codes in the program editor are displayed as integer or hexadecimal values. For information on switching the display formats, refer to "See also".	

10.13.2 FileWriteC: Write file on the memory card

You can use the "FileWriteC" instruction to write data located in a source area on the CPU to a file located in the "UserFiles" folder on the memory card.

Table 10-241 FileWriteC instruction

LAD / FBD	SCL	Description
	**"FileWriteC_SFB_DB_1"(REQ:=_bool_in_, Name:=_string_in_, Offset:=_udint_in_, Length:=_udint_in_, Done=>_bool_out_, Busy=>_bool_out_, Error=>_bool_out_, Status=>_word_out_, ResultLength=>_udint_out_, Data:=_variant_inout_);**	Use the "FileWriteC" instruction to write data located in a source area on the CPU to a file located in the "UserFiles" folder on the memory card. You specify this file by entering its name and complete path. If the file does not exist, it is created by the CPU in the "UserFiles" folder. If the "UserFiles" folder does not exist either, it is also created by the CPU; subfolders are not created – in this case, W#16#8091 is output at the "Status" parameter.

Enable writing to the file using the "REQ" control parameter. The output parameters "Done", "Busy", "Error" and "Status" indicate the status of the job.

The following rules apply for the file name and path specification:

- The file name must not be longer than 55 characters.
- The following characters are permitted for the folder and file name: "0" to "9", "a" to "z", "A" to "Z", "-", "_"
- The file name must not contain more than one dot ("."); the dot separates the name from the file extension. The file name must contain at least one character. A file extension is not necessary.
- The path name must not start with "/", "\" or ".".
- The path name must not contain any ".."
- The path name must not contain a subfolder under the UserFiles folder.

Examples of valid paths and file names: "UserFiles/Lift16_DataBase.txt", "UserFiles/2017-04-13_ErrorLog.bin"

You can write up to 16 MB (16,777,216 bytes) by executing "FileWriteC"; the data is written segment by segment. The segment size is device-specific; an S7-1200-CPU, for example, uses 8 KB (8192 byte) blocks. If the number of data items to be written is greater than the segment size, you will need to call the instruction multiple times in your program. For consistency reasons, you should therefore not access the data written until after you call the instruction for the last time. If the available file is too short, it is extended to the required size.

The parameters "Offset" and "Length" specify the location in the file to which the data is to be written. The resource occupied is released again once the write process is complete.

The "FileWriteC" instruction only starts the write operation if the following condition is fulfilled: "Offset" + "Length" <= 16 MB.

The "FileWriteC" instruction works asynchronously. Processing takes place across several calls. You start processing with a rising edge at the parameter "REQ".

The parameters "Busy" and "Done" indicate the status of the job.

If an error occurs during execution, this is signaled by the parameters "Error" and "Status".

Table 10-242 Data types for the parameters

Parameters and type		Data type	Description
REQ	Input	BOOL	Control parameter Request Enables writing a file on the memory card with a rising edge.
Name	Input	STRING	Name of the file to be written incl. complete path
Offset	Input	UDINT	Byte offset from which the file is to be written
Length	Input	UDINT	Length of the area to be written in bytes "Length" = 0 means that the entire source area specified with the "Data" parameter is written.
Done	Output	BOOL	1: The instruction has been executed successfully.
Busy	Output	BOOL	Status parameter • 0: Execution of the instruction completed or not yet started. • 1: Execution of the instruction not yet complete.
Error	Output	BOOL	Status parameter • 0: No error. • 1: An error occurred during execution of the instruction. Detailed information is output via the "Status" parameter.
Status	Output	WORD	Error code
ResultLength	Output	UDINT	Length of data written in bytes
Data	InOut	VARIANT	Source area Permitted data types: BYTE and Array of BYTE

Table 10-243 Condition codes

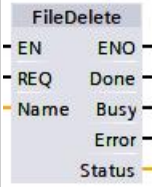
Error code* (W#16#...)	Explanation
0	No error
7000	No job processing active
7001	Start of job processing. Parameter Busy = 1, Done = 0.
7002	Intermediate call (REQ irrelevant): Instruction already active; Busy has the value "1".
8091	Path does not exist or is invalid.
8092	The "Name" parameter is not of the data type "STRING", is too long or contains invalid characters.
8093	• The "Offset" parameter points past the end of the file to be written. • The creation of the file is rejected because "Offset" is greater than zero.
8094	• "Length" is greater than the maximum permitted value. For an S7-1500 CPU, for example, the maximum value permitted is 16 MB, i.e. 16,777,216 bytes. • "Length" + "Offset" is greater than the maximum permitted value.
80A1	Write error; the data in the file on the memory card may be partly overwritten.
80B1	The source area specified by the "Data" parameter is shorter than the length required at the "Length" parameter.
80B3	There is not enough space on the memory card or in the internal load memory.
80B4	The memory card or file is write-protected.
80C0	The file cannot be accessed.
80C3	The maximum number of simultaneously active FileWriteC instructions has already been reached.
8A24	The "Data" points to an impermissible area, for example to the load memory or the local data.

Error code* (W#16#...)	Explanation
8A51	Invalid data type of the "Data" parameter.
8A52	The tag at the Data parameter is insufficient. A part of the source area data may have been written.
* The error codes in the program editor are displayed as integer or hexadecimal values. For information on switching the display formats, refer to "See also".	

10.13.3 FileDelete: Delete file on the memory card

You use the "FileDelete" instruction to delete an existing file from the memory card.

Table 10-244 FileDelete instruction

LAD / FBD	SCL	Description
	**"FileDelete_DB_1"(REQ:=_bool_in_, Name:=_string_in_, Done=>_bool_out_, Busy=>_bool_out_, Error=>_bool_out_, Status=>_word_out_)**	You use the "FileDelete" instruction to delete an existing file from the memory card.

The file must not be open. Wildcards in the "Name" parameter are not supported, meaning that names such as "UserFiles/*.txt" and "UserFiles/?.txt" are not permissible.
The "FileDelete" instruction is only permitted in the "Recipes" and "UserFiles" folders. Folders within these folders are possible, e.g. "UserFiles/Test/file1.txt".

NOTE
Deleting data logs
Deleting a file in the "DataLog" folder with the "FileDelete" instruction is not permissible. You must use the "DataLogDelete" instruction to delete data logs.

"FileDelete" is an asynchronous instruction. Processing can extend over multiple calls. You start processing with a rising edge at the parameter "REQ".
The parameters "Busy" and "Done" indicate the status of the job.

If an error occurs during execution, this is signaled by the parameters "Error" and "Status".

Table 10-245 Data types for the parameters

Parameters and type		Data type	Description
REQ	Input	BOOL	Control parameter Request Processing is started on a rising edge at REQ.
Name	Input	STRING	Path and name of the file to be deleted
Done	Output	BOOL	Status parameter • 1: The instruction has been executed successfully.
Busy	Output	BOOL	Status parameter • 0: The instruction is currently not being executed. • 1: The instruction is currently being executed.
Error	Output	BOOL	Status parameter • 0: No error • 1: An error occurred during execution of the instruction. For detailed information, see the "Status" parameter.
Status	Output	WORD	Error code

Table 10-246 Condition codes

Error code* (W#16#...)	Explanation
0000	Instruction finished successfully
7000	No job processing active
7001	Start of job processing: Busy = 1, Done = 0.
7002	Intermediate call (REQ irrelevant): Instruction already active; Busy has the value "1"
8090	File locked, e.g. file is open
8091	Path does not exist or is invalid.
8092	File does not exist in the path
80A2	Write error
80A3	The file is too large (>= 2147483648 bytes) and cannot be deleted using "FileDelete".
80B4	The memory card is write-protected
80C3	The maximum number of simultaneously active FileDelete instructions has already been reached
* The error codes in the program editor are displayed as integer or hexadecimal values.	

Technology instructions 11

11.1 Counting (High-speed counters)

The basic counter instructions, described in "Counter operations" (Page 211), are limited to counting events that occur at a rate slower than the scan cycle of the S7-1200 CPU. The High-speed counter (HSC) function provides the ability to count pulses occurring at a higher rate than the PLC scan cycle. In addition, you can configure the HSC to measure the frequency and period of the occurring pulses, or be setup such that motion control can use the HSC to read a motor encoder signal.

To use the HSC function, the HSC must first be enabled and configured using the CPU's Properties tab in the Device Configuration screen. To get started configuring the HSC, refer to "Configuring a high-speed counter" (Page 494).

After you download the hardware configuration, the HSC can count pulses or measure frequency without the need for any instructions to be called. When the HSC is in Count or Period mode, the count value is automatically captured and updated in the process image (I memory) each scan cycle. If the HSC is in Frequency mode, the process image value is the frequency in Hz.

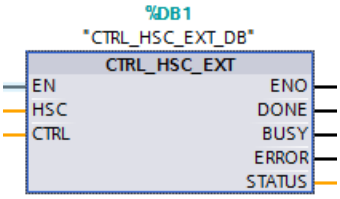
In addition to counting and measuring, the HSC can generate hardware interrupt events, operate dependent on the state of physical input points, and produce an output pulse according to a specified counter event. Technology instruction CTRL_HSC_EXT allows the user program to control the HSC programmatically. CTRL_HSC_EXT updates HSC parameters and returns the most up-to-date values when executed. You can use the CTRL_HSC_EXT instruction while the HSC is in Count, Period, or Frequency mode.

NOTE

The CTRL_HSC_EXT instruction replaces the legacy CTRL_HSC instruction for projects targeting V4.2 CPUs and later. All of the functionality of the CTRL_HSC instruction, plus several additional features, is available with the CTRL_HSC_EXT instruction. The legacy CTRL_HSC instruction is only available for compatibility with older S7-1200 projects and should not be used in new projects.

11.1.1 CTRL_HSC_EXT (Control high-speed counter, extended)

Table 11-1 CTRL_HSC_EXT instruction

LAD / FBD	SCL	Description
	**"CTRL_HSC_1_DB" (hsc:=_hw_hsc_in_, done:=_done_out_, busy:=_busy_ out_, error:=_error_out_, status:=_status_out_, ctrl:=_variant_in_);**	Each CTRL_HSC_EXT (Control high-speed counter, extended) instruction uses a system-defined data structure stored in a user-defined Global DB to store counter data. You assign the HSC_Count, HSC_Period, or HSC_Frequency data types as an input parameter to the CTRL_HSC_EXT instruction.

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "CTRL_HSC_1_DB" is the name of the instance DB.

Table 11-2 Data types for the parameters

Parameter	Declaration	Data type	Description
HSC	IN	HW_HSC	HSC identifier
CTRL	IN_OUT	Variant	SFB input and return data. Note: Refer to "CTRL_HSC_EXT instruction System Data Types (SDT) (Page 485)" for further information.
DONE	OUT	Bool	1= Indicates SFB is finished. Always 1 because SFB is synchronous
BUSY	OUT	Bool	Always 0, function is never busy
ERROR	OUT	Bool	1 = Indicates an error
STATUS	OUT	Word	Execution condition code Note: Refer to the "Execution condition codes" table below for further information.

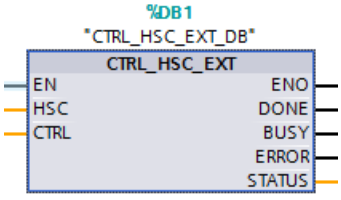
Table 11-3 Execution condition codes

STATUS (W#16#)	Description
0	No error
80A1	HSC identifier does not address an HSC
80B1	Illegal value in NewDirection
80B4	Illegal value in NewPeriod
80B5	Illegal value in NewOpModeBehavior
80B6	Illegal value in NewLimitBehavior
80D0	SFB 124 not available

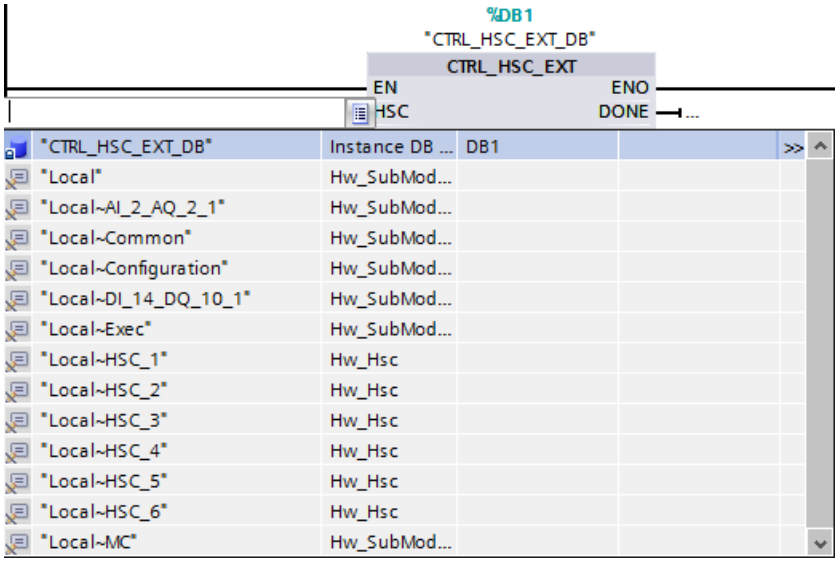
11.1.1.1 CTRL_HSC_EXT example

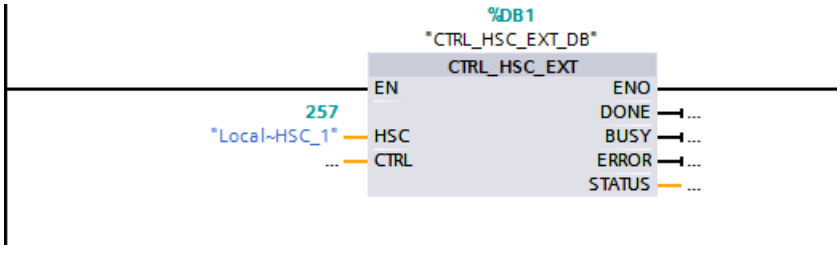
To use the CTRL_HSC_EXT instruction, follow the steps below:

1. Place the CTRL_HSC_EXT instruction in the ladder network, which also creates the following instance data block: "CTRL_HSC_EXT_DB":



2. Attach the HSC's hardware identifier, found in the HSC's properties, to the "HSC" pin of the ladder instruction. You can also select one of the six "Hw_Hsc" objects from the dropdown menu of this input pin. The default tag name for HSC1 is "Local~HSC_1":



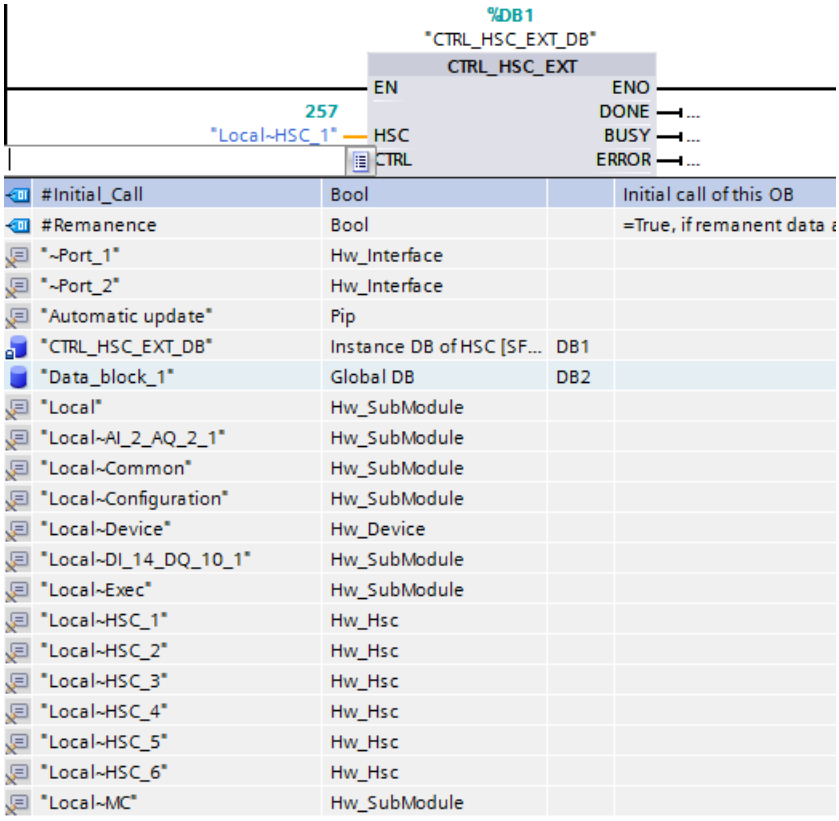


3. Create a global data block named "Data_block_1" (You can also use an existing global data block.):
   - Within "Data_block_1", locate an empty row and add a variable named "MyHSC".
   - In the "Data type" column, add one of the following System Data Types (SDT). Select the SDT that corresponds to the HSC's configured type of counting. More HSC SDT information can be found later in this section. The dropdown list does not contain these types so ensure that you enter the SDT name exactly as shown: HSC_Count, HSC_Period, or HSC_Frequency
   - After you enter the data type, you can expand the "MyHSC" variable to see all the fields contained in the data structure. Here, you can find the data type of each of the fields and change the default starting values:

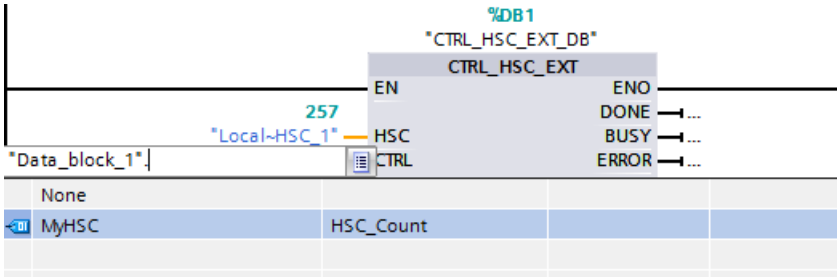
Data_block_1

	Name	Data type	Start value
1	Static		
2	MyHSC	HSC_Count	
3	CurrentCount	DInt	0
4	CapturedCount	DInt	0
5	SyncActive	Bool	false
6	DirChange	Bool	false
7	CmpResult_1	Bool	false
8	CmpResult_2	Bool	false
9	OverflowNeg	Bool	false
10	OverflowPos	Bool	false
11	EnHSC	Bool	false
12	EnCapture	Bool	false
13	EnSync	Bool	false
14	EnDir	Bool	false
15	EnCV	Bool	false
16	EnSV	Bool	false
17	EnReference1	Bool	false
18	EnReference2	Bool	false
19	EnUpperLmt	Bool	false
20	EnLowerLmt	Bool	false
21	EnOpMode	Bool	false
22	EnLmtBehavior	Bool	false
23	EnSyncBehavior	Bool	false
24	NewDirection	Int	0
25	NewOpModeBeha...	Int	0
26	NewLimitBehavior	Int	0
27	NewSyncBehavior	Int	0
28	NewCurrentCount	DInt	0
29	NewStartValue	DInt	0
30	NewReference1	DInt	0
31	NewReference2	DInt	0
32	NewUpperLimit	DInt	0
33	New_Lower_Limit	DInt	0

4. Assign the variable "'Data_block_1'. MyHSC" to the CTRL input pin of the CTRL_HSC_EXT instruction:
   – Select "Data_Block_1".



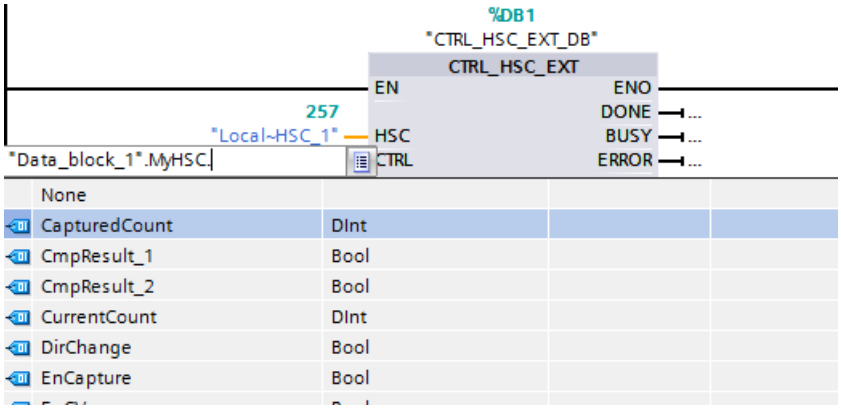
   – Select "MyHSC".



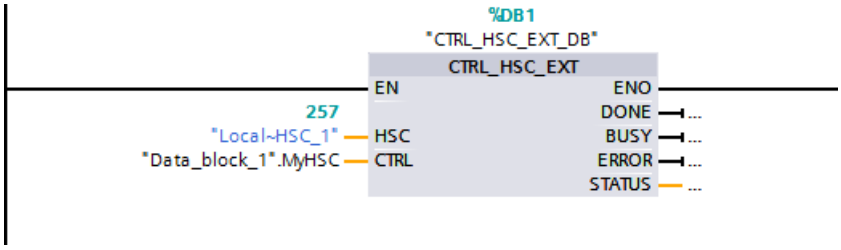
   – Delete the period (".") following: "'Data_Block_1'.MyHSC". Then, either click outside the box or press the ESC key once and then press the Enter key.

NOTE

After deleting the period (".") following: "'Data_Block_1'.MyHSC", do not press only the Enter key. This action places the period (".") back into the box.



– The completed CTRL input is shown below.



After you configure the HSC in the PLC, you can execute the CTRL_HSC_EXT instruction. If an error occurs, ENO is set to "0" and the STATUS output indicates the condition code.

11.1.1.2 CTRL_HSC_EXT Instruction System Data Types (SDT)

The following System Data Types (SDTs) are only used with the CTRL_HSC_EXT instruction's CTRL pin. To use them, create a user data block and add an object with the data type of the SDT that corresponds to the HSC's configured mode (type of counting). STEP 7 does not show these data types in the dropdown menu. Type the name of the SDT exactly as shown.

Inputs of the HSC's SDT are denoted by the prefix "En" or "New". Inputs prefixed with "En" either enables an HSC function or updates the corresponding parameter. The prefix "New" identifies the update value. In order for the new value to take effect, the corresponding "En" bit must be true, and the "New" value must be valid. When the CTRL_HSC_EXT instruction is executed, the program applies input changes and updates the outputs with the appropriate SDT reference attached.

SDT: HSC_Count

The "HSC_Count" data type corresponds to an HSC configured for "Count" mode. The Count mode provides the following capabilities:

- Access the current pulse count
- Latch the current pulse count on an input event
- Reset the current pulse count to the starting value on an input event
- Access status bits, indicating certain HSC events have occurred
- Disable the HSC using a software or hardware input
- Change the counting direction using a software or hardware input
- Change the current pulse count
- Change the starting value (used when CPU transitions to RUN state or when Sync function is triggered)

- Changing two independent reference (or preset) values used for comparison
- Change the upper and lower counting limits
- Change how the HSC operates when the pulse count reaches those limits
- Generate a hardware interrupt event when the current pulse count reaches a reference (preset) value
- Generate a hardware interrupt event when the Synchronization (reset) input activates
- Generate a hardware interrupt event when the counting direction changes based upon an external input
- Generate a single output pulse on a specified counting event

When an event occurs and the CTRL_HSC_EXT instruction executes, the instruction sets a status bit. On the following CTRL_HSC_EXT instruction execution, the instruction clears the status bit, unless the event occurs again before the instruction executes.

Table 11-4 HSC_Count structure

Structure element	Declaration	Data type	Description
CurrentCount	OUT	Dint	Returns the HSC's current count value
CapturedCount	OUT	Dint	Returns the counter value captured on the specified input event
SyncActive	OUT	Bool	Status bit: Sync input was activated
DirChange	OUT	Bool	Status bit: Counting direction has changed
CmpResult1	OUT	Bool	Status bit: CurrentCount equals Reference1 event occured
CmpResult2	OUT	Bool	Status bit: CurrentCount equals Reference2 event occured
OverflowNeg	OUT	Bool	Status bit: CurrentCount reached the LowerLimit
OverflowPos	OUT	Bool	Status bit: CurrentCount reached the UpperLimit
EnHSC	IN	Bool	Enables the HSC to count pulses when true; disables counting when false
EnCapture	IN	Bool	Enables the Capture input when true, Capture input has no effect when false
EnSync	IN	Bool	Enables the Sync input when true; Sync input has no effect when false
EnDir	IN	Bool	Enables the NewDirection value to take effect
EnCV	IN	Bool	Enables the NewCurrentCount value to take effect
EnSV	IN	Bool	Enables the NewStartValue value to take effect
EnReference1	IN	Bool	Enables the NewReference1 value to take effect
EnReference2	IN	Bool	Enables the NewReference2 value to take effect
EnUpperLmt	IN	Bool	Enables the NewUpperLimit value to take effect
EnLowerLmt	IN	Bool	Enables the New_Lower_Limit value to take effect
EnOpMode	IN	Bool	Enables the NewOpModeBehavior value to take effect
EnLmtBehavior	IN	Bool	Enables the NewLimitBehavior value to take effect
EnSyncBehavior	IN	Bool	This value is not used.
NewDirection	IN	Int	Counting direction: 1 = count up; -1 = count down; all other values are reserved.
NewOpModeBehavior	IN	Int	HSC's operation on overflow: 1 = HSC stops counting (HSC must be disabled and re-enabled to continue counting); 2 = HSC continues to operate; all other values are reserved.

Structure element	Declaration	Data type	Description
NewLimitBehavior	IN	Int	Result of the CurrentCount value on overflow: 1 = set CurrentCount to opposite limit; 2 = set CurrentCount to StartValue; all other values are reserved.
NewSyncBehavior	IN	Int	This value is not used.
NewCurrentCount	IN	Dint	CurrentCount Value
NewStartValue	IN	Dint	StartValue: Initial value of the HSC
NewReference1	IN	Dint	Reference1 Value
NewReference2	IN	Dint	Reference2 Value
NewUpperLimit	IN	Dint	Upper counting limit value
New_Lower_Limit	IN	Dint	Lower counting limit value

SDT: HSC_Period

The "HSC_Period" data type corresponds to an HSC configured for "Period" mode. The CTRL_HSC_EXT instruction provides program access to the number of input pulses over a specified measurement interval. This instruction allows for the time period between input pulses to be calculated with a fine nanosecond resolution.

Table 11-5 HSC_Period structure

Structure element	Declaration	Data type	Description
ElapsedTime	OUT	UDInt	See description below.
EdgeCount	OUT	UDInt	See description below.
EnHSC	IN	Bool	Enables the HSC for Period measurement when true; disables Period measurement when false.
EnPeriod	IN	Bool	Enables NewPeriod value to take effect.
NewPeriod	IN	Int	Specifies the measurement interval time in milliseconds. The only allowed values are 10, 100 or 1000 ms.

ElapsedTime returns the time, in nanoseconds, between the last counting events of sequential measurement intervals. If no counting events occurred during a measurement interval, ElapsedTime returns the cumulative time since the last counting event. ElapsedTime has a range from "0" to 4,294,967,280 nanoseconds (0x0000 0000 to 0xFFFF FFF0). The return value 4,294,967,295 (0xFFFF FFFF) indicates that period overflow has occurred. Overflow indicates that the time between pulse edges is greater than 4.295 seconds and the period cannot be calculated using this instruction. The values from 0xFFFF FFF1 to 0xFFFF FFFE are reserved.

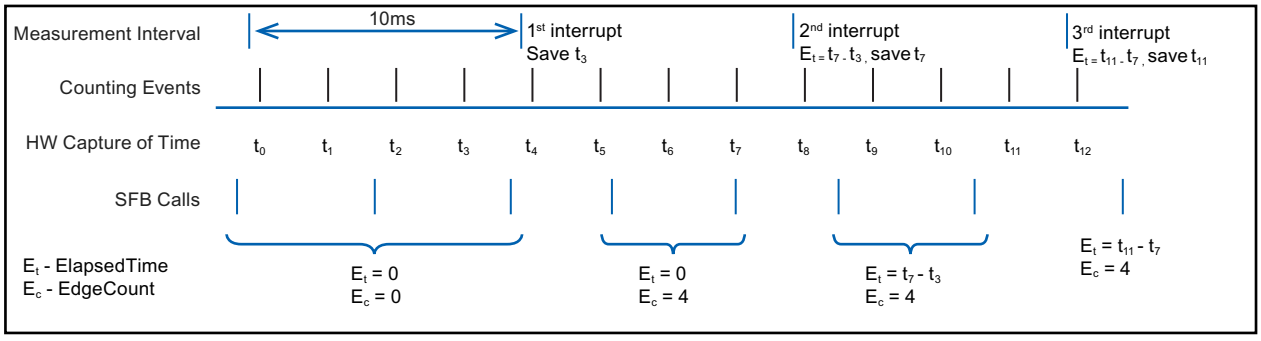
EdgeCount returns the number of counting events received during the measurement interval. The period can only be calculated when the value of EdgeCount is greater than zero. If ElapsedTime is either "0" (no input pulses received) or 0xFFFF FFFF (Period overflow), then EdgeCount is not valid.

When EdgeCount is valid, use the following formula to calculate the period in nanoseconds:
Period = ElapsedTime/EdgeCount

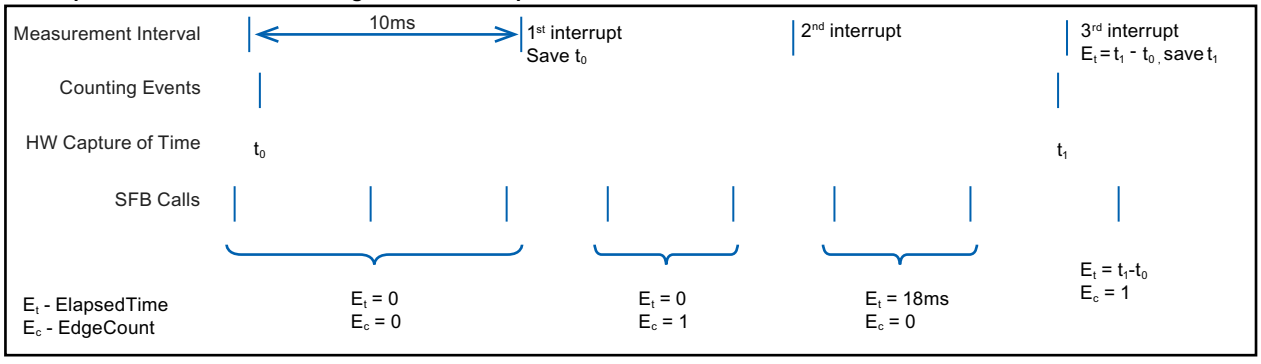
The calculated time period value is an average of the time periods of all of the pulses that occur during the measurement interval. If the period of an incoming pulse is greater than the measurement interval (10, 100, or 1000 ms), then the period calculation requires multiple measurement intervals.

The following examples show how the instruction makes period measurements:

Example 1: Multiple Counting Events in a Measurement Interval



Example 2: Zero and One Counting Events in Multiple Measurement Intervals



Rules:
1. If $E1_t = 0$, the period is invalid
2. Else, Period = E_t / E_c

SDT: HSC_Frequency

The "HSC_Frequency" data type corresponds to an HSC configured for "Frequency" mode. The instruction CTRL_HSC_EXT provides program access to the frequency of input pulses, measured over a specified time period.

Using the CTRL_HSC_EXT instruction in Frequency mode provides the following capabilities:

Table 11-6 HSC_Frequency structure

Structure element	Declaration	Data type	Description
Frequency	OUT	DInt	Returns a frequency in Hz, measured over the measurement interval time. When the HSC counts down, the instruction returns a negative frequency.
EnHSC	IN	Bool	Enables the HSC for Frequency measurement when true; disables Frequency measurement when false.
EnPeriod	IN	Bool	Enables NewPeriod value to take effect.
NewPeriod	IN	Int	Specifies the measurement interval time in milliseconds. The only allowed values are 10, 100, or 1000 ms.

The CTRL_HSC_EXT instruction measures the Frequency using the same measurement technique as Period mode to find the ElapsedTime and EdgeCount. The instruction calculates the frequency as a signed integer value in Hz using the formula: Frequency = EdgeCount/ElapsedTime

If you require a floating-point value for frequency, you can use the above formula for frequency when the HSC is in Period mode. Note that in Period mode, ElapsedTime is returned in nanoseconds and can require scaling of the value.

11.1.2 Operating the high-speed counter

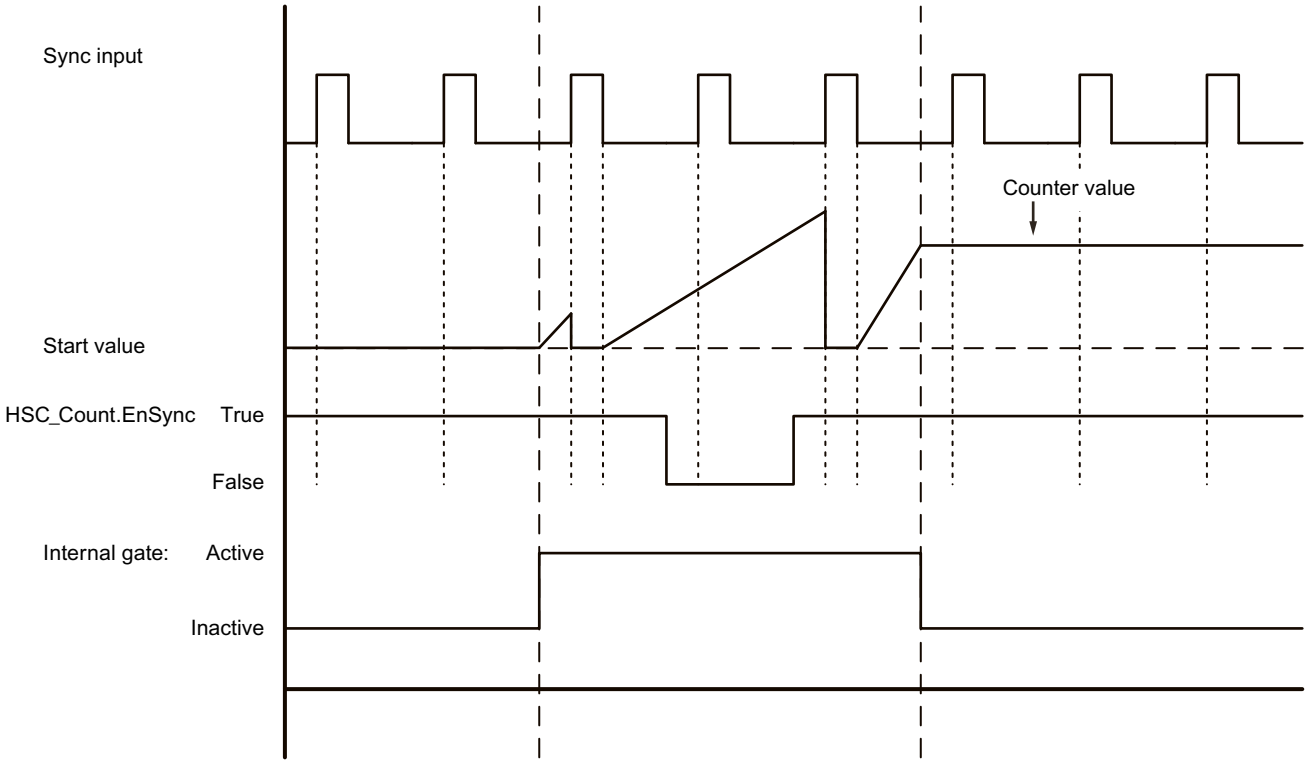
11.1.2.1 Synchronization function

You use the Sync (synchronization) function to set the counter to the start value with an external input signal. You can modify the start value by executing the CTRL_HSC_EXT instruction. This allows the user to synchronize the current count value to a desired value on occurrence of an external input signal.

Synchronization always takes place at the occurrence of the input signal and is effective regardless of the status of the internal gate. You must set the "HSC_Count.EnSync" bit to true in order to enable the Sync function.

The CTRL_HSC_EXT instruction sets the HSC_Count.SyncActive status bit to true after completion of synchronization. The CTRL_HSC_EXT instruction sets the HSC_Count.SyncActive status bit to false if synchronization has not occurred since the last instruction execution.

The figure below shows an example of synchronization when the input signal is configured for an active high level:



NOTE

The configured input filters delay the control signal of the digital input.

This input function is only available to be used when the HSC is configured for Count mode.

Refer to Input functions (Page 500) for information on how to configure the Synchronization function.

11.1.2.2 Gate function

Many applications require counting processes to be started or stopped in accordance with other events. In such cases, counting is started and stopped using the internal gate function. Each HSC channel has two gates: a software gate and a hardware gate. The state of these gates determines the state of the internal gate. See the table below.
The internal gate is open if the software gate is open and the hardware gate is open or has not been configured. If the internal gate is open, counting is started. If the internal gate is closed, all other count pulses are ignored and counting is stopped.

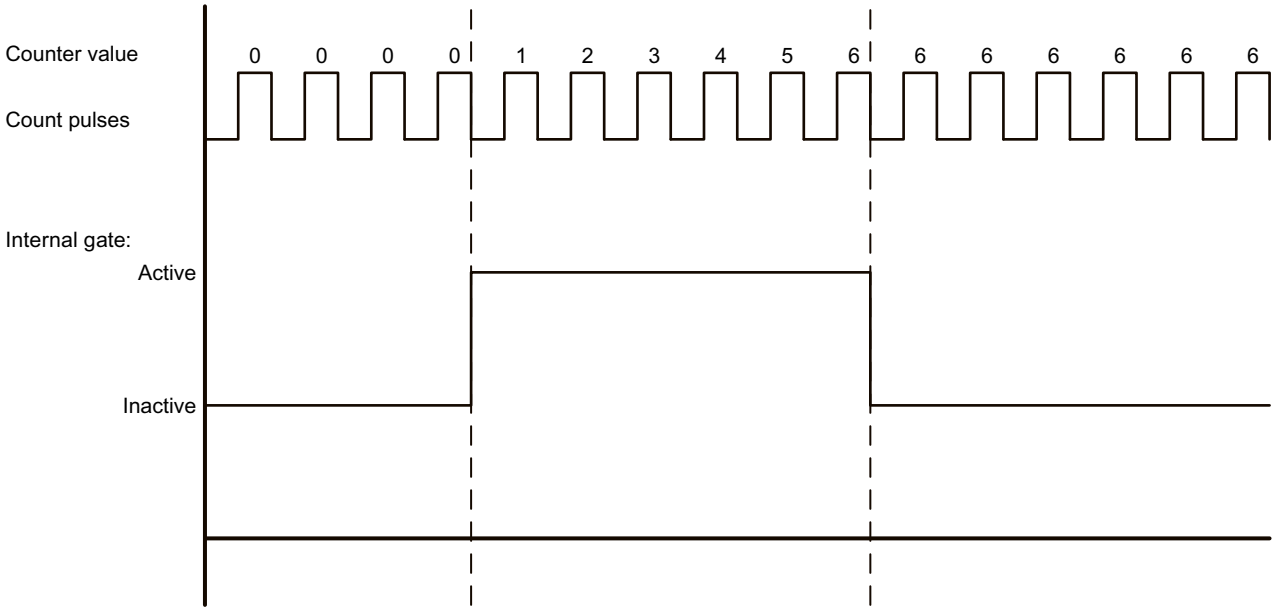
Table 11-7 Gate function states

Hardware gate	Software gate	Internal gate
Open/not configured	Open	Open
Open/not configured	Closed	Closed
Closed	Open	Closed
Closed	Closed	Closed

The term "open" is defined to be the active state of the gate. Similarly, the term "closed" is defined to be the inactive state of the gate.

You control the software gate with the "HSC_Count.EnHSC" enable bit in the SDT attached to the CTRL_HSC_EXT instruction. To open the software gate, set the "HSC_Count.EnHSC" bit true; to close the software gate, set the "HSC_Count.EnHSC" bit false. Execute the CTRL_HSC_EXT instruction to update the software gate's state.
The hardware gate is optional, and you can enable or disable it in the HSC properties section. To control a counting process with only the hardware gate, the software gate must remain open. If you do not configure a hardware gate, the hardware gate is considered to be always open and the internal gate state is the same as the software gate state.

The figure below shows an example of the hardware gate opening and closing with a digital input. The digital input is configured for an active high level:



NOTE

The configured input filters delay the control signal of the digital input.

The hardware gate function is only available to be used when the HSC is configured for Count mode. In Period and Frequency modes, the internal gate state is the same as the software gate state.

In Period mode, the software gate is controlled by "HSC_Period.EnHSC".

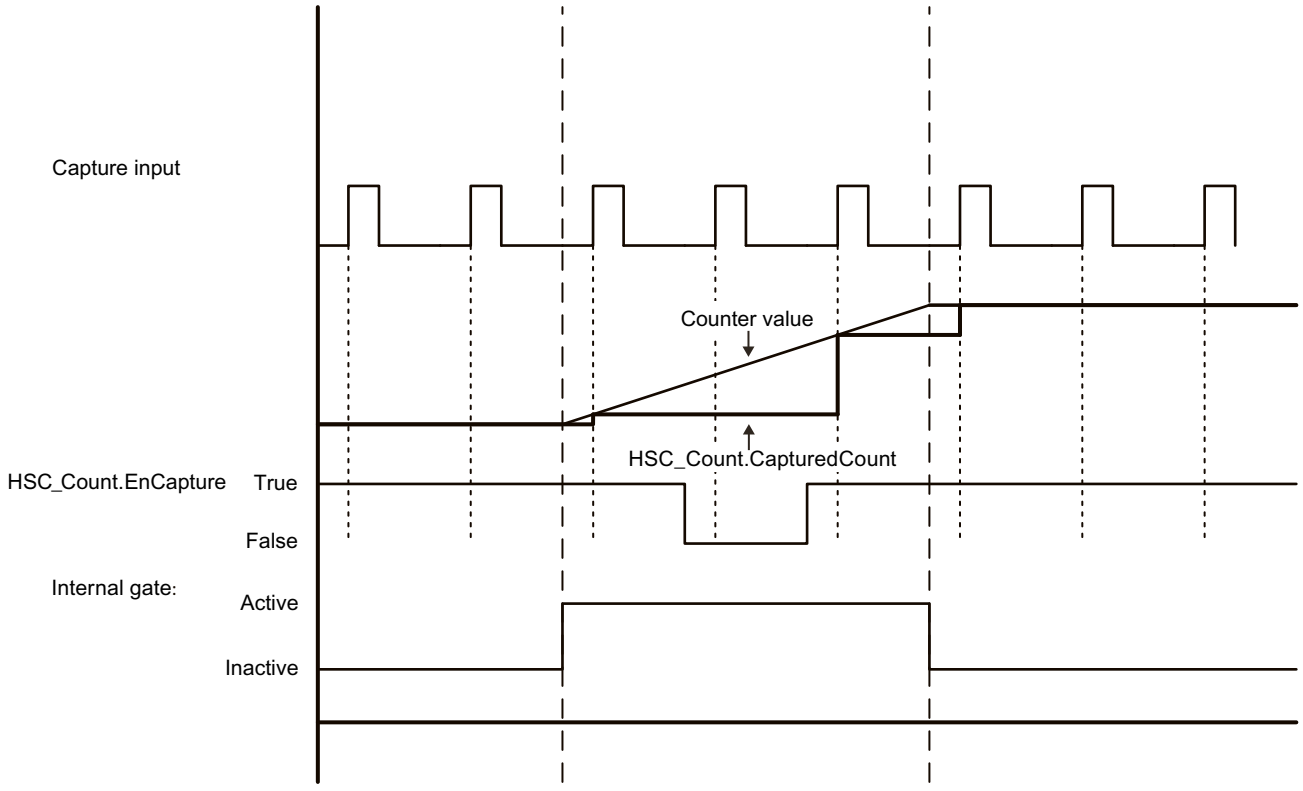
In Frequency mode, the software gate is controlled by "HSC_Frequency.EnHSC".

Refer to Input functions (Page 500) for information on how to configure the Gate function.

11.1.2.3 Capture function

You use the Capture function to save the current counter value with an external reference signal. When configured and enabled by the "HSC_Count.EnCapture" bit, the Capture function causes the current count to be captured on the occurrence of an external input edge. The Capture function is effective regardless of the status of the internal gate. The program saves the unchanged counter value when the gate is closed. After executing the CTRL_HSC_EXT instruction, the program stores the captured value in "HSC_Count.CapturedCount".

The figure below shows an example of the Capture function configured to capture on a rising edge. The Capture input does not trigger a capture of the current count when the "HSC_Count.EnCapture" bit is set false through the CTRL_HSC_EXT instruction.



NOTE

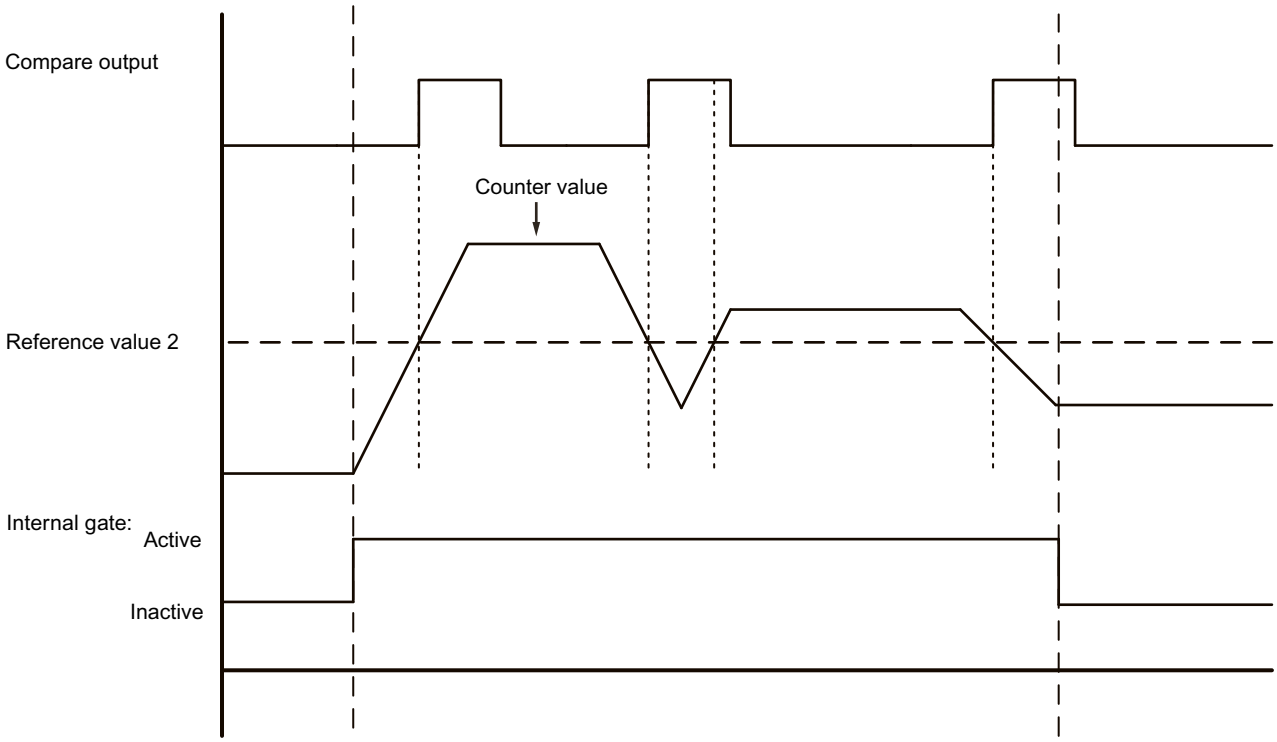
The configured input filters delay the control signal of the digital input.

This input function can only be used when the HSC is configured for Count mode.

Refer to Input functions (Page 500) for information on how to configure the Capture function.

11.1.2.4 Compare function

When enabled, the Compare output function generates a single, configurable pulse that occurs every time the configured event occurs. The events include count equal to one of the reference values or the counter overflows. If a pulse is in progress and the event occurs again, a pulse is not produced for that event.



NOTE

This output function can only be used when the HSC is configured for Count mode.

Refer to Output function (Page 501) for information on how to configure the Compare function.

11.1.2.5 Application

A typical application uses the HSC to monitor feedback from an incremental shaft encoder. The shaft encoder provides a specified number of counts per revolution that you can use as the clock generator input to the HSC. There is also a reset pulse that occurs once per revolution that you can use as the sync input to the HSC.

To start, the user program should load the initial reference value into the HSC and set the outputs to their initial states. The outputs remain in this state for the time period that the current count is less than the reference value. The HSC provides an interrupt when the current count is equal to the reference value, when the sync event (reset) occurs, and also when there is a direction change.

As each counter value equals the reference value, an interrupt event occurs. Within the interrupt OB, the user program should load the next reference value into the HSC and set the outputs to their next state.

When the sync input is triggered, the current count value is set to the start value, and an interrupt event occurs. Within this interrupt OB, the user program should load the initial reference value into the HSC and set the outputs to their initial state. At this point the HSC has returned to its initial state and the cycle repeats with the HSC continuing to count.

Since the interrupts occur at a much slower rate than the counting rate of the HSC, you can implement precise control of high-speed operations with relatively minor impact to the scan cycle of the CPU. The method of interrupt attachment allows each load of a new preset to be performed in a separate interrupt routine for easy state control. Alternatively, you can process all interrupt events in a single interrupt routine.

The Gate function (Page 490), triggered either by the user program or an external input signal, can disable counting of the encoder pulses. You can ignore any movement of the shaft by deactivating the gate. This means that while the encoder continues to send pulses to the HSC, the count value is held at the last value before the gate goes inactive. When the gate goes active, counting resumes from the last value before the gate went inactive.

When enabled, the Capture function (Page 491) causes the current count to be captured on the occurrence of an external input. A process (for example, a calibration routine) can use this function to determine how many pulses occur between events.

When enabled, the Compare function (Page 493) generates a single, configurable pulse that occurs every time the current count reaches one of the reference values or overflows (exceeds the counting limits). You can use this pulse as a signal to start another process whenever a certain HSC event occurs.

Either the user program or an external input signal controls the counting direction.

To obtain the speed of the rotating shaft, you can configure the HSC for Frequency mode (Page 488). This function provides a signed integer value in units of Hz. Because the reset signal occurs once per revolution, measuring the frequency of the reset signal provides a quick indication of the shaft's speed, in revolutions per second.

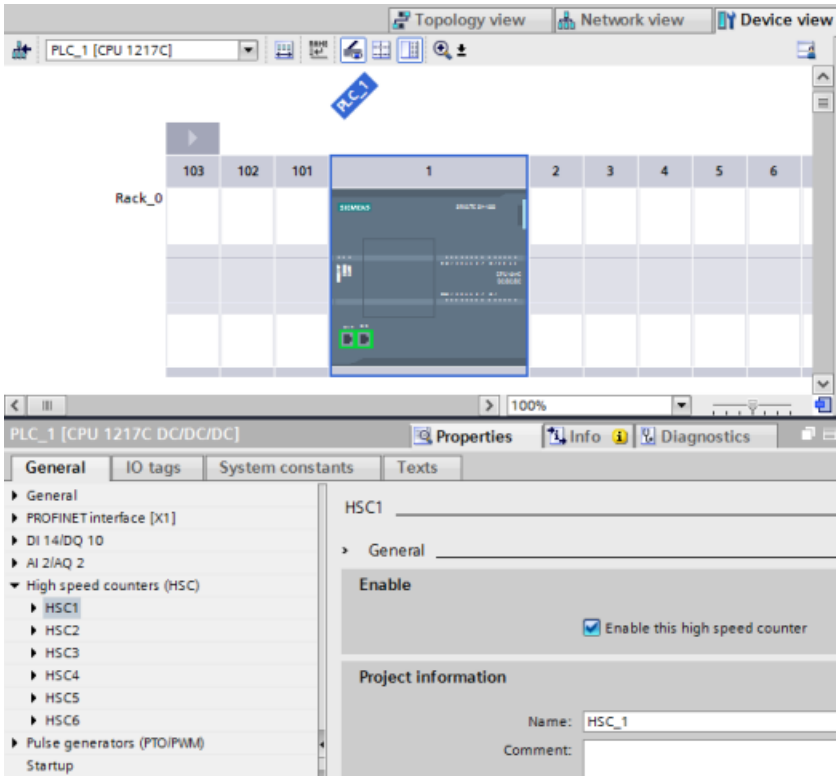
If you desire a floating point value of the frequency, configure the HSC for Period mode (Page 487). You can use the ElapsedTime and EdgeCount values returned in Period mode to calculate the frequency.

11.1.3 Configuring a high-speed counter

To set up the high-speed counter (HSC), follow these steps:

1. Select Device Configuration from the Project navigator.
2. Select the CPU to configure.
3. Click the Properties tab for the CPU, located in the Inspector window.
4. Select the HSC you want to enable from the list of high-speed counters shown under the General tab.

You may configure up to six high-speed counters (HSC1 through HSC6). Enable an HSC by selecting the "Enable this high speed counter" option. If enabled, STEP 7 assigns a unique default name to this HSC. You can change this name by editing it in the "Name:" edit field; however, it must be a unique name. Names of enabled HSCs become tags with the Data type "HW_Hsc" in the "System constant" tag table and are available for use as the "HSC" parameter of the CTRL_HSC_EXT instructions. Refer to "Configuring the operation of the CPU (Page 136)" for further information:



After enabling the HSC, STEP 7 sets single phase counting as the default configuration. Once you set the digital input filter for the HSC clock generator input, the program can be downloaded to the PLC, and the CPU is ready to count. To change the HSC's configuration, proceed to the next section, "Type of Counting".

The following table provides an overview of what inputs and outputs are available for each configuration:

Table 11-8 Counting modes for HSC

Type	Input 1	Input 2	Input 3	Input 4	Input 5	Output 1	Function
Single-phase with internal direction control	Clock	-	-	-	-	-	Count, Frequency, or Period
			Sync	Gate	Capture	Compare	Count
Single-phase with external direction control	Clock	Direction	-	-	-	-	Count, Frequency, or Period
			Sync	Gate	Capture	Compare	Count

[1] For an encoder: Phase Z, Home

Type	Input 1	Input 2	Input 3	Input 4	Input 5	Output 1	Function
Two-phase	Clock up	Clock down	-	-	-	-	Count, Frequency, or Period
			Sync	Gate	Capture	Compare	Count
A/B counter	Phase A	Phase B	-	-	-	-	Count, Frequency, or Period
			Sync[1]	Gate	Capture	Compare	Count
A/B counter fourfold	Phase A	Phase B	-	-	-	-	Count, Frequency, or Period
			Sync[1]	Gate	Capture	Compare	Count

[1] For an encoder: Phase Z, Home

11.1.3.1 Type of Counting

There are four types of counting or modes. When you change the mode, the available configuration options for that HSC also change:

- Count: Counts the number of pulses and increments or decrements the count value, depending on the state of the direction control. External I/O can reset the count, disable counting, initiate a capture of the current count, and produce a single pulse on a specified event. The output values are the current count value and the count value at the moment a capture event occurs.
- Period: Counts the number of input pulses over a specified time period. Returns the pulse count and time duration in nanoseconds (ns). Values are captured and calculated at the end of the time period specified by Frequency measuring period. Period mode is available for the CTRL_HSC_EXT instruction but not the CTRL_HSC instruction.
- Frequency: Measures the input pulses and time duration and calculates the frequency of the pulses. The program returns the frequency as a signed double integer in units of Hz. The value is negative if the counting direction is down. Values are captured and calculated at the end of the time period specified by the Frequency measuring period.
- Motion control: Used by the motion control technology object and not available to the HSC instructions. Refer to "Motion control (Page 507)" for further information.

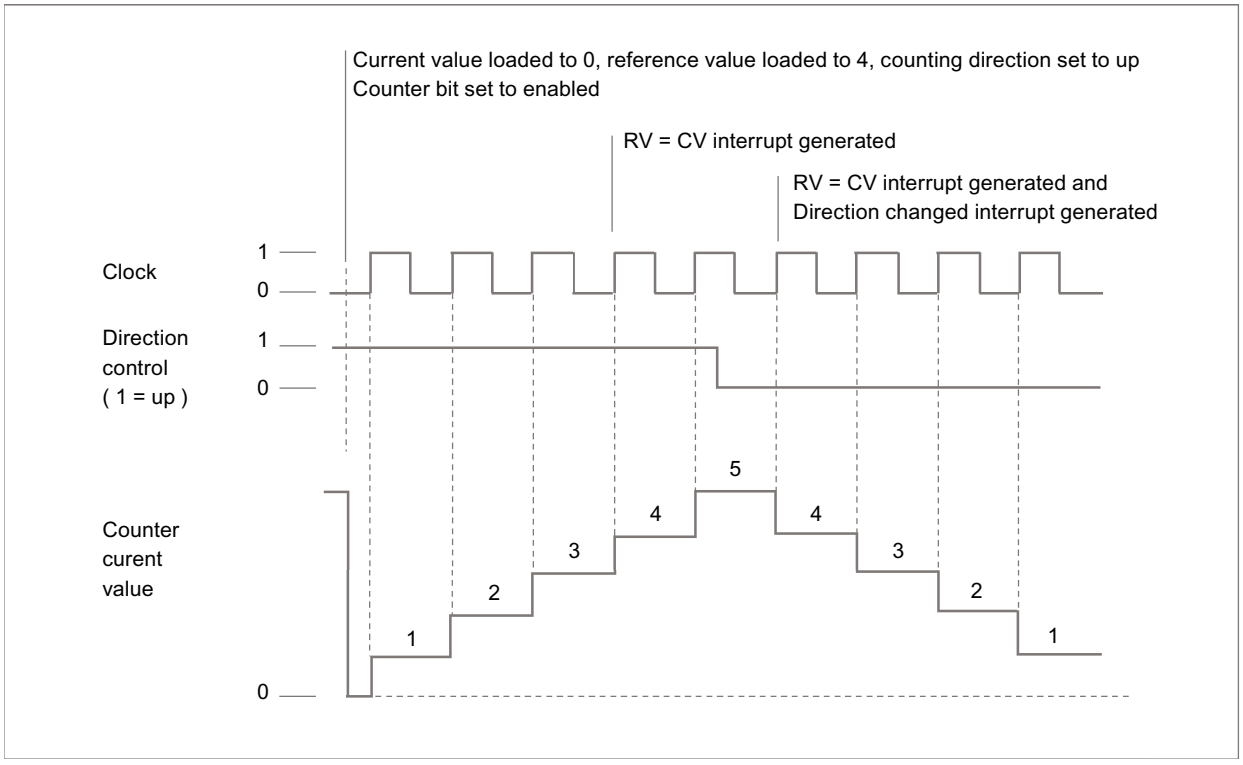
11.1.3.2 Operating phase

Select the desired operating phase of the HSC. The four figures below show when the counter value changes, when the current value (CV) equals the reference value (RV) event occurs, and when the direction change event occurs.

Single phase

Single-phase (not available with motion control) counts pulses:

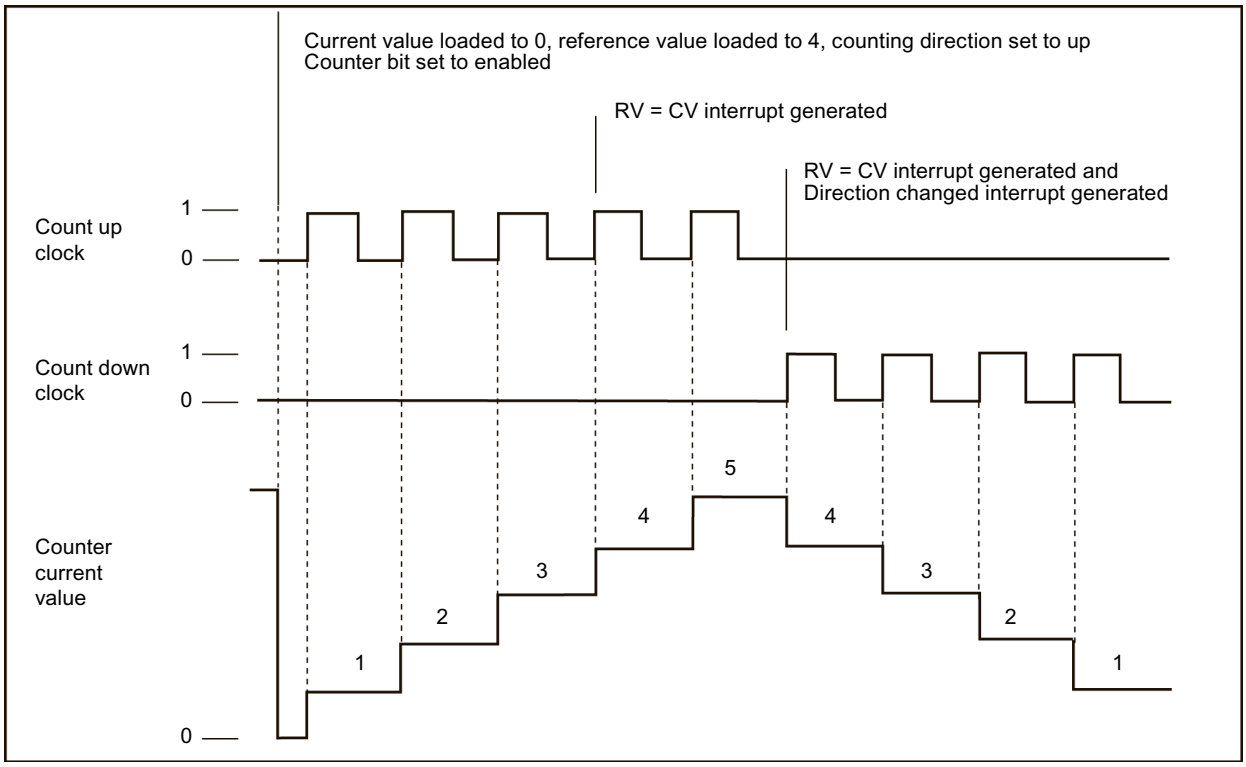
- User program (internal direction control):
  - 1 is up
  - -1 is down
- Hardware input (external direction control):
  - High level is up.
  - Low level is down.



Two phase

Two phase counts:

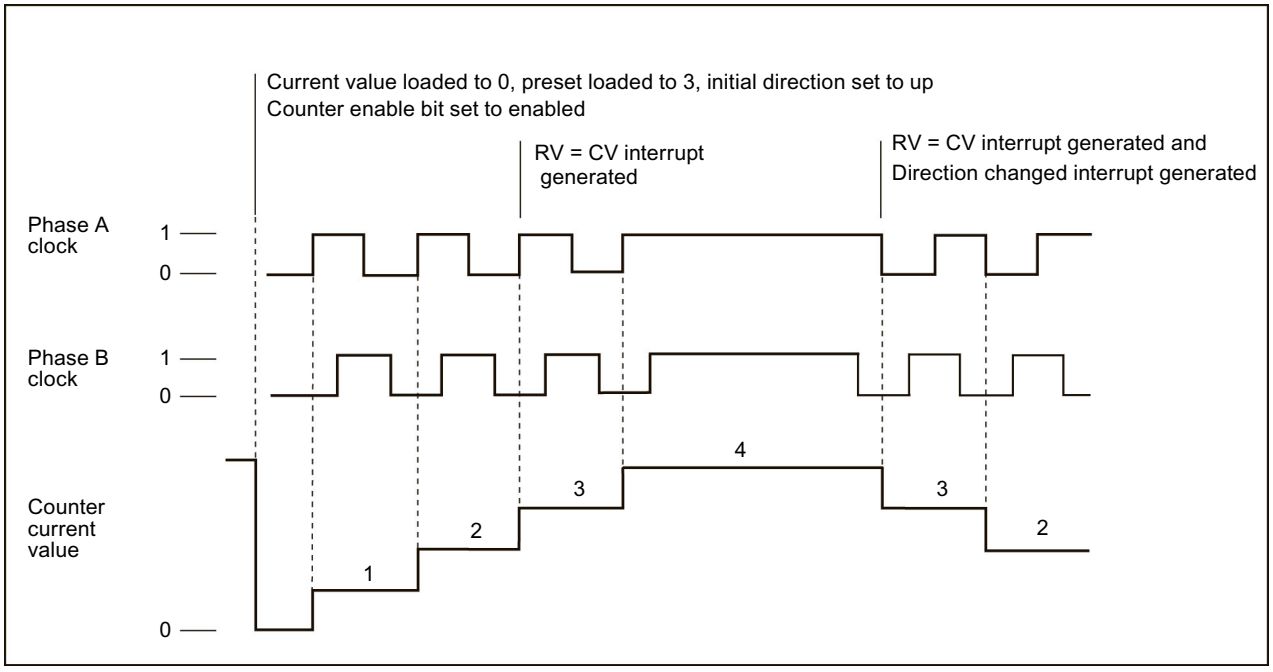
- Up on the clock up input
- Down on the clock down input



A/B counter

A/B phase quadrature counts:

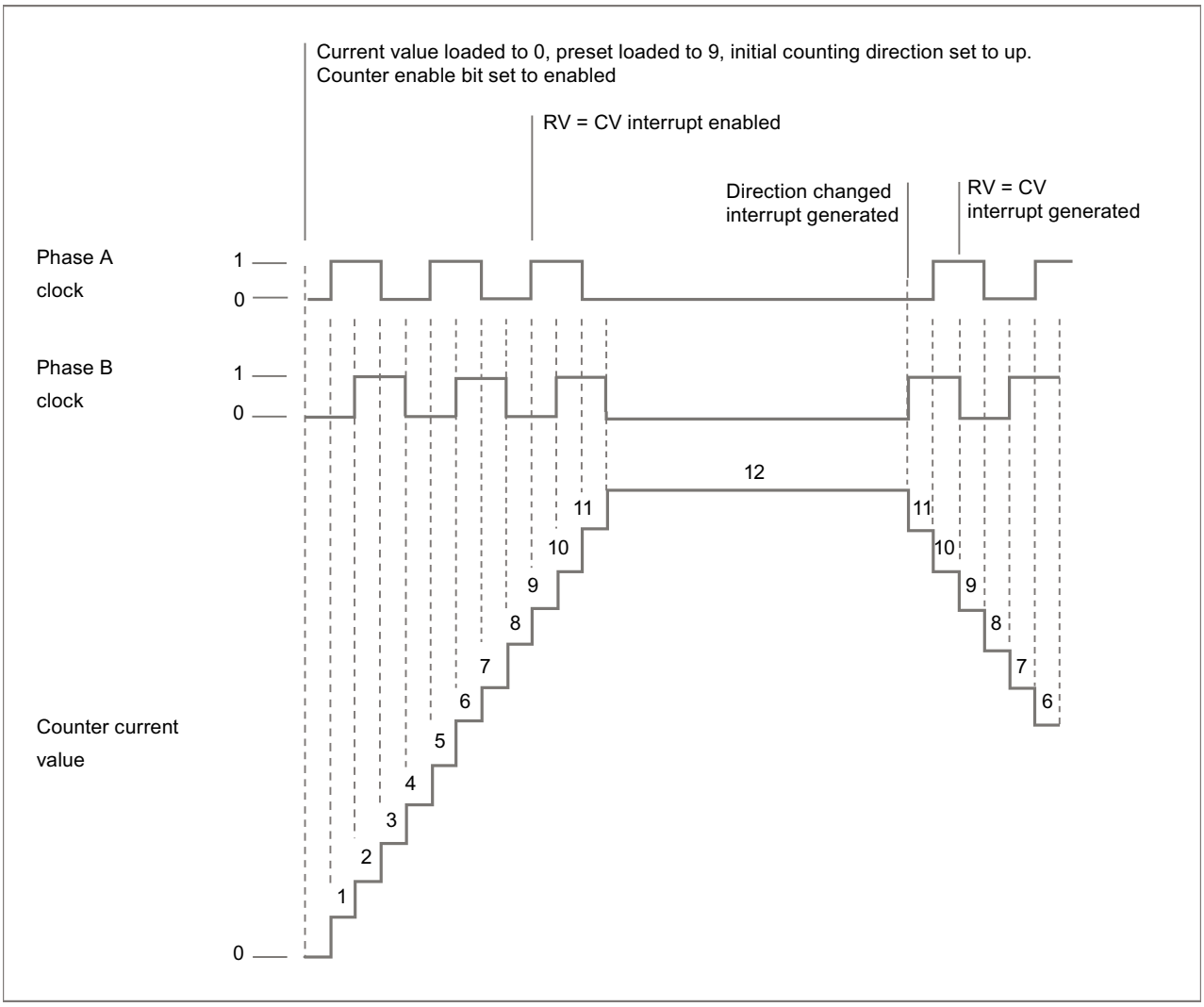
- Up on the rising edge of the clock A input when the clock B input is low
- Down on the falling edge of the clock A input when the clock B input is low



A/B counter fourfold

A/B phase quadrature fourfold counts:

- Up on the rising edge of the clock A input when the clock B input is low
- Up on the falling edge of the clock A input when the clock B input is high
- Up on the rising edge of the clock B input when the clock A input is high
- Up on the falling edge of the clock B input when the clock A input is low
- Down on the rising edge of the clock B input when the clock A input is low
- Down on the falling edge of the clock B input when the clock A input is high
- Down on the rising edge of the clock A input when the clock B input is high
- Down on the falling edge of the clock A input when the clock B input is low



11.1.3.3 Initial values

Each time the CPU goes to RUN, it loads initial values. The initial values are only used in count mode:

- Initial counter value: The program sets the current count value to the initial counter value when the CPU goes from STOP to RUN mode or when the program triggers the sync input.
- Initial reference value: When the current count reaches the reference value, if the respective functions are set up, the program generates an interrupt and/or an output pulse.
- Initial reference value 2: When the current count reaches the reference value 2, if the function is set up, the program generates an output pulse.
- Initial upper limit value: Maximum counting value. The default is the largest possible value of +2,147,483,647 pulses.
- Initial lower limit value: Minimum counting value. The default is the smallest possible value of -2,147,483,648 pulses.

The values above and the behavior of the counter when it reaches a limit are only available in Count mode. You can adjust the values and the behavior with the CTRL_HSC_EXT instruction using the HSC_Count SDT.

11.1.3.4 Input functions

The Clock and direction inputs determine count events and direction, based upon the operating phase. You can only use the Sync, Capture, and Gate inputs in Count mode and can individually enable and configure the inputs for different types of triggers.

Synchronization input

The Sync (synchronization) input sets the current count value to the starting (or initial counter) value. You typically use the Sync input to reset the counter to "0". You can trigger the Sync when the input pin is in one of the following states:

- High
- Low
- Goes from low to high
- Goes from high to low
- Goes from high to low or from low to high

Capture input

The Capture input sets the captured count value to the count value saved at the moment you triggered the Capture input. You can trigger the capture when the input pin is in one of the following states:

- Goes from low to high
- Goes from high to low
- Goes from high to low or from low to high

Gate input

The Gate input stops HSC counting. You can trigger the Gate when the input pin is in one of the following states:

- High
- Low

11.1.3.5 Output function

The compare output function is the only output for the HSC and is only available in Count mode.

Compare output

You can configure the Compare output to generate a single pulse on the occurrence of one of the following events:

- Counter equals reference value (count direction is up)
- Counter equals reference value (count direction is down)
- Counter equals reference value (count direction is up or down)
- Counter equals reference value 2 (count direction is up)
- Counter equals reference value 2 (count direction is down)
- Counter equals reference value 2 (count direction is up or down)
- Positive overflow
- Negative overflow

You can configure the output pulse with a cycle time ranging from 1 to 500 ms; the default cycle time is 10 ms. You can set the pulse width, or duty cycle, anywhere from 1 to 100%; the default pulse width is 50%.

If multiple compare output events occur within the specified cycle time, the output pulses from those events are lost due to the fact that the current pulse has not completed its cycle yet. Once the pulse has finished (the configured cycle time has passed), the pulse generator is available to produce a new pulse.

11.1.3.6 Interrupt events

Under the Event configuration section, you can select a hardware interrupt OB from the dropdown menu (or you can create a new OB) and attach it to an HSC event. The priority of the interrupt is in a range from 2 to 26, where 2 is the lowest priority and 26 is the highest priority. Depending on the HSC's configuration, the following events are available:

- Counter value equals reference value event: A counter value equals reference value event occurs when the HSC's count value reaches the reference value. You can set the reference value during configuration under the Initial reference value section, or by updating "NewReference1" using the CTRL_HSC_EXT instruction. Refer to the "Operating phase (Page 497)" section for further information.
- Synchronization event: A Sync (synchronization) occurs whenever you enable and trigger the Sync input.
- Change of direction event: A change of direction event occurs when the counting direction changes. Refer to the "Operating phase (Page 497)" section for further information.

11.1.3.7 Hardware input pin assignment

For each HSC input that you enable, select the desired input point, located either on the CPU or optional signal board (communication and signal modules do not support HSC inputs). When you select a point, STEP 7 displays the maximum frequency value next to the selection. The digital input filter settings may need to be adjusted so that all valid signal frequencies can pass through the filter. To set up the HSC input filters, refer to "Configuring digital input filter times (Page 139)".

NOTE

CPU and SB input channels (V4 or later firmware) have configurable input filter times

Earlier firmware versions had fixed HSC input channels and fixed filter times that you could not change.

With V4 or later versions, you can assign input channels and filter times. The default input filter setting is 6.4 ms, which limits the maximum counting rate to 78 Hz. You can change the filter settings to count higher or lower frequencies depending on the design of your system.

WARNING

Risks with changes to filter time setting for digital input channels

If the filter time for a digital input channel is changed from a previous setting, a new "0" level input value might need to be presented for up to a 20.0 ms accumulated duration before the filter becomes fully responsive to new inputs. During this time, short "0" pulse events of duration less than 20.0 ms may not be detected or counted.

To ensure that a new filter time goes immediately into effect, power cycle the CPU.

The changing of filter times can result in unexpected machine or process operation, which can cause death or serious injury to personnel, and/or damage to equipment.

Use the following table and ensure that the CPU and SB input channels that you connect can support the maximum pulse rates in your process signals:

Table 11-9 CPU input: maximum frequency

CPU	CPU Input channel	Operating phase: Single phase or Two phase	Operating phase: A/B counter or A/B Counter fourfold
1211C	Ia.0 to Ia.5	100 kHz	80 kHz
1212C	Ia.0 to Ia.5	100 kHz	80 kHz
	Ia.6, Ia.7	30 kHz	20 kHz
1214C and 1215C	Ia.0 to Ia.5	100kHz	80kHz
	Ia.6 to Ib.5	30 kHz	20 kHz
1217C	Ia.0 to Ia.5	100 kHz	80 kHz
	Ia.6 to Ib.1	30 kHz	20 kHz
	Ib.2 to Ib.5 (.2+, .2- to .5+, .5-)	1 MHz	1 MHz

Table 11-10 SB signal board input: maximum frequency (optional board)

SB signal board	SB input channel	Operating phase: Single phase or Two phase	Operating phase: A/B counter or A/B Counter fourfold
SB 1221, 200 kHz	Ie.0 to Ie.3	200kHz	160 kHz
SB 1223, 200 kHz	Ie.0, Ie.1	200kHz	160 kHz
SB 1223	Ie.0, Ie.1	30 kHz	20 kHz

When assigning an input point to an HSC function, you can assign the same input point to multiple HSC functions. For example, assigning I0.3 to the Sync input of HSC1 and the Sync input of HSC2 to synchronize the count of both HSCs at the same time is a valid configuration; however, it generates a compiler warning.

When possible, avoid assigning multiple input functions of the same HSC to the same input point. For example, assigning I0.3 to the Sync input and the Gate input of HSC 1 to synchronize the count and disable counting at the same time is also a valid configuration. You can make this configuration, but it could produce unintended results.

WARNING

Risks with assigning multiple functions to a single digital input channel

Assigning multiple input functions of the same HSC to a common input point can produce unpredictable results. When a trigger occurs on a point with multiple functions assigned to that trigger, the order in which the functions are executed by the PLC cannot be known. This is known as a race condition and is often an undesirable situation.

To avoid a race condition, do not assign more than two input functions, of the same HSC, to the same input pin. If an HSC has two input functions assigned to the same pin, set the triggers such that they can never occur at the same time. Remember that a falling edge occurs at the same instance that a low level begins and that a rising edge occurs at the same instance that a high level begins.

This race condition can result in unexpected machine or process operation, which can cause death or serious injury to personnel, and/or damage to equipment.

NOTE

You assign the digital input and output points used by high-speed counter (HSC) devices during CPU device configuration. When you assign input and output points to HSC devices, you cannot modify the values of these points using the force function in a watch table. The HSC has full control of these input and output points.

11.1.3.8 Hardware output pin assignment

If you enable the Compare output, select an available output point. Once you configure an output point for use by an HSC (or other technology objects such as a pulse generator), that output point is owned exclusively by that object. No other component can use the output point, and the output point cannot be forced to a value. If you configure a single output channel for multiple HSCs or for use in an HSC and a pulse output, the program generates a compile error.

11.1.3.9 HSC input memory addresses

Each HSC uses a double word section of I-memory that stores the current count. If you configure the HSC for frequency, then the frequency is stored in that input memory location. The available input address range is I0.0 to I1023.7 (maximum start address is I1020.0). The HSC cannot use an input address that overlaps with an input address mapped to another component. For further information on the process image, refer to "Execution of the user program (Page 61)".
The following table shows the default addresses assigned for each HSC:

Table 11-11 HSC default addresses

High-speed counter (HSC)	Current value data type	Default current value address
HSC1	DInt	ID 1000
HSC2	DInt	ID 1004
HSC3	DInt	ID 1008
HSC4	DInt	ID 1012
HSC5	DInt	ID 1016
HSC6	DInt	ID 1020

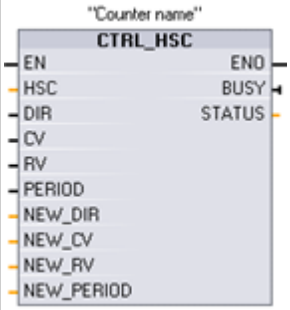
11.1.3.10 Hardware identifier

Each HSC has a unique hardware identifier, which is used by the HSC_CTRL and HSC_CTRL_EXT instructions. You can find the PLC tag for the hardware identifier under "System Constants". An HSC with the name "HSC_1" has the tag "Local~HSC_1" and data type "Hw_Hsc". This tag is also shown in the dropdown menu when selecting the HSC input of the CTRL_HSC_EXT instructions.

11.1.4 Legacy CTRL_HSC (Control high-speed counter) instruction

11.1.4.1 CTRL_HSC (Control high-speed counter)

Table 11-12 CTRL_HSC instruction (For general purpose counting)

LAD / FBD	SCL	Description
	**"CTRL_HSC_1_DB" (hsc:=W#16#0, dir:=False, cv:=False, rv:=False, period:=False, new_dir:=0, new_cv:=L#0, new_rv:=L#0, new_period:=0, busy=>_bool_out_, status=>_word_out_);**	Each CTRL_HSC (Control high-speed counter) instruction uses a structure stored in a DB to maintain counter data. You assign the DB when the CTRL_HSC instruction is placed in the editor.

[1] When you insert the instruction, STEP 7 displays the "Call Options" dialog for creating the associated DB.

[2] In the SCL example, "CTRL_HSC_1_DB" is the name of the instance DB.

Table 11-13 Data types for the parameters

Parameter	Declaration	Data type	Description
HSC	IN	HW_HSC	HSC identifier
DIR[1, 2]	IN	Bool	1 = Request new direction
CV[1]	IN	Bool	1 = Request to set new counter value
RV[1]	IN	Bool	1= Request to set new reference value
PERIOD[1]	IN	Bool	1 = Request to set new period value (only for frequency measurement mode)
NEW_DIR	IN	Int	New direction: 1= forward, -1= backward
NEW_CV	IN	DInt	New counter value
NEW_RV	IN	DInt	New reference value
NEW_PERIOD	IN	Int	New period value is in milliseconds (only for frequency measurement mode). The only allowed values are 10, 100, or 1000 milliseconds: 1000 = 1 second 100 = 0.1 second 10 = 0.01 second
BUSY[3]	OUT	Bool	Function is busy
STATUS	OUT	Word	Execution condition code

1 If an update of a parameter value is not requested, then the corresponding input values are ignored.

2 The DIR parameter is only valid if the configured counting direction is set to "User program (internal direction control)". You determine how to use this parameter in the HSC device configuration.

3 For an HSC on the CPU or on the SB, the BUSY parameter always has a value of 0.

You configure the parameters for each HSC in the device configuration for the CPU for counting/frequency function, reset options, interrupt event configuration, hardware I/O, and count value address.

Some of the parameters for the HSC can be modified by your user program to provide program control of the counting process:

- Set the counting direction to a NEW_DIR value
- Set the current count value to a NEW_CV value
- Set the reference value to a NEW_RV value
- Set the period value (for frequency measurement mode) to a NEW_PERIOD value

If the following Boolean flag values are set to 1 when the CTRL_HSC instruction is executed, the corresponding NEW_xxx value is loaded to the counter. Multiple requests (more than one flag is set at the same time) are processed in a single execution of the CTRL_HSC instruction.

- DIR = 1 is a request to load a NEW_DIR value, 0 = no change
- CV = 1 is a request to load a NEW_CV value, 0 = no change
- RV = 1 is a request to load a NEW_RV value, 0 = no change
- PERIOD = 1 is a request to load a NEW_PERIOD value, 0 = no change

If an error occurs, ENO is set to "0" and the STATUS output indicates a condition code:

Table 11-14 Execution condition codes

STATUS (W#16#)	Description
0	No error
80A1	HSC identifier does not address a HSC
80B1	Illegal value in NEW_DIR
80B2	Illegal value in NEW_CV
80B3	Illegal value in NEW_RV
80B4	Illegal value in NEW_PERIOD
80C0	Multiple access to the high-speed counter This error can occur if the type of counting (Page 496) is set to "Period" or "Motion control". These types are invalid for the CTRL_HSC instruction and are only supported by the CTRL_HSC_EXT instruction.
80D0	High-speed counter (HSC) not enabled in CPU hardware configuration

11.1.4.2 Using CTRL_HSC

The CTRL_HSC instruction is typically placed in a hardware interrupt OB that is executed when the counter hardware interrupt event is triggered. For example, if a CV=RV event triggers the counter interrupt, then a hardware interrupt OB code block executes the CTRL_HSC instruction and can change the reference value by loading a NEW_RV value.

The current count value is not available in the CTRL_HSC parameters. The process image address that stores the current count value is assigned during the hardware configuration of the high-speed counter. You may use program logic to directly read the count value. The value returned to your program will be a correct count for the instant in which the counter was read. The counter will continue to count high-speed events. Therefore, the actual count value could change before your program completes a process using an old count value.

11.1.4.3 HSC current count value

The CPU stores the current value of each HSC in an input (I) address. The following table shows the default addresses assigned to the current value for each HSC. You can change the I address for the current value by modifying the properties of the CPU in the Device Configuration.

High-speed counters use a DInt value to store the current count value. A DInt count value has a range of -2147483648 to +2147483647. You can configure the range limits. Refer to "Initial values (Page 500)" for further information.

The counter rolls over from the maximum positive value to the maximum negative value when counting up, and from the maximum negative value to the maximum positive value when counting down. Frequency is returned in units of Hertz (for example, 123.4 Hz is returned as 123).

Table 11-15 HSC default addresses

HSC	Current value data type	Default current value address
HSC1	DInt	ID1000
HSC2	DInt	ID1004
HSC3	DInt	ID1008
HSC4	DInt	ID1012
HSC5	DInt	ID1016
HSC6	DInt	ID1020

11.2 Motion control

11.2.1 Motion control overview

The TIA Portal, together with the motion control functionality of the S7-1200 CPU, supports you in controlling stepper motors and servo motors:

- You configure the positioning axis and command table technology objects in the TIA Portal. The S7-1200 CPU uses these technology objects to control the outputs that control the drives.
- In the user program, you control the axis by means of motion control instructions and initiate motion commands to your drive.

11.2.2 Hardware components for motion control

The basic hardware configuration for a motion control application with the S7-1200 CPU consists of the following items.

S7-1200 CPU

The S7-1200 CPU combines the functionality of a programmable logic controller with motion control functionality for operation of drives. The motion control functionality takes over the control and monitoring of the drives.

Signal board

You add further inputs and outputs to the CPU with the signal boards. You can use the digital outputs as pulse generator outputs for controlling drives as required. In CPUs with relay outputs, the pulse signal cannot be output on the onboard outputs because the relays do not support the necessary switching frequencies. To be able to work with the Pulse Train Output (PTO) on these CPUs, you must use a signal board with digital outputs.

You can use the analog outputs for controlling connected analog drives as required.

PROFINET

Use the PROFINET interface to establish the online connection between the CPU S7-1200 and the programming device. In addition to the online functions of the CPU, additional commissioning and diagnostic functions are available for motion control.

PROFINET continues to support the PROFIdrive profile for connecting PROFIdrive capable drives and encoders.

Drives and encoders

Drives permit the movement of the axis. Encoders provide the actual position for the closed loop position control of the axis.

The table below shows the connection possibilities for drives and encoders:

Drive connection	Closed/open loop control of axis	Encoder connection
Pulse Train Output (PTO) (Stepper motors and servo motors with pulse interface)	Position-controlled	-
Analog output (AQ)	Position-controlled	• Encoder on high-speed counter (HSC) • Encoder on technology module (TM) • Encoder on PROFINET
PROFINET	Position-controlled	• Encoder on the drive • Encoder on high-speed counter (HSC) • Encoder on technology module (TM) • Encoder on PROFINET

11.2.3 Motion control instructions

11.2.3.1 MC instruction overview

The motion control instructions use an associated technology data block and the dedicated pulse train outputs (PTO) of the CPU to control the motion on an axis.

NOTE

Motion control instructions belong to different library versions.

Instructions in motion control V1.0 to V3.0 actively control the output of the instruction. When an error occurs within the block, the Enable out (ENO) output is turned to the OFF state. An error is indicated by the ERROR, ErrorID, and ErrorInfo outputs on the block. Using the ENO ouput, it is possible to evaluate the status of the instruction and execute subsequent instructions after it in a serial manner.

With instructions in motion control V4.0 and V5.0, the ENO output stays true as long as the instruction executes regardless of its error state. This could cause a program that used V3.0 or earlier motion control that depends on the ENO status to function incorrectly. To remedy this situation, use the DONE and ERROR outputs to evaluate the status of the instruction rather than the ENO output when using motion control V4.0 or later.

References

The STEP 7 Information System provides documentation for each motion control (MC) instruction. You can find help on programming and differences between past and present versions of the motion control instructions.

Refer to SIMATIC STEP 7 S7-1200 Motion Control (https://support.industry.siemens.com/cs/us/en/view/109773400) for information on the following topics:

- Configuring a pulse generator
- Open loop motion control
- Configuring the axis
- Commissioning
- Closed loop motion control
- Configuring the axis
- ServoOBs
- Speed controlled operation
- Telegram 4 support
- Simulation axis
- Data adaptation
- Axis control using the TM Pulse module
- Configuring the TO_CommandTable_PTO
- Operation of motion control for S7-1200
- CPU outputs used for motion control
- Hardware and software limit switches for motion control
- Homing
- Jerk limit
- Monitoring active commands

- Monitoring MC instructions with a "Done" output parameter
- Monitoring the MC_Velocity
- Monitoring the MC_MoveJog
- ErrorIDs and ErrorInfos for motion control
- Phasing

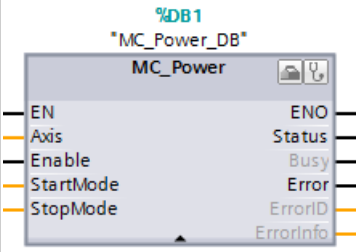
11.2.3.2 MC_Power (Release/block axis)

The MC_Power instruction enables and disables a motion control axis.

NOTE

If the axis is switched off due to an error, it will be enabled again automatically after the error has been eliminated and acknowledged. This requires that the Enable input parameter has retained the value TRUE during this process.

Table 11-16 MC_Power instruction

LAD / FBD	SCL	Description
	**"MC_Power_DB"(Axis:=_multi_fb_in_, Enable:=_bool_in_, StartMode:=_int_in_, StopMode:=_int_in_, Status=>_bool_out_, Busy=>_bool_out_, Error=>_bool_out_, ErrorID=>_word_out_, ErrorInfo=>_word_out_);**	The MC_Power motion control instruction enables or disables an axis. Before you can enable or disable the axis, ensure the following conditions: • The technology object has been configured correctly. • There is no pending enable-inhibiting error. The execution of MC_Power cannot be aborted by a motion control task. Disabling the axis (input parameter Enable = FALSE) aborts all motion control tasks for the associated technology object.

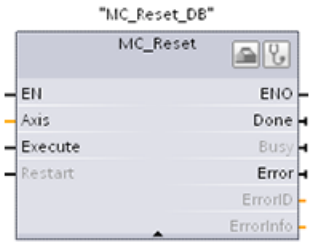
[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_Power_DB" is the name of the instance DB.

11.2.3.3 MC_Reset (Confirm error)

The MC_Reset instruction resets all motion control errors. All motion control errors that can be acknowledged are acknowledged.

Table 11-17 MC_Reset instruction

LAD / FBD	SCL	Description
	**"MC_Reset_DB"(Axis:=_multi_fb_in_, Execute:=_bool_in_, Restart:=_bool_in_, Done=>_bool_out_, Busy=>_bool_out_, Error=>_bool_out_, ErrorID=>_word_out_, ErrorInfo=>_word_out_);**	Use the MC_Reset instruction to acknowledge "Operating error with axis stop" and "Configuration error". The errors that require acknowledgement can be found in the "List of ErrorIDs and ErrorInfos" under "Remedy". Before using the MC_Reset instruction, you must have eliminated the cause of a pending configuration error requiring acknowledgement (for example, by changing an invalid acceleration value in "Axis" technology object to a valid value). As of V3.0 and later, the Restart command allows the axis configuration to be downloaded to the work memory in the RUN operating mode.

[1] STEP 7 automatically creates the DB when you insert the instruction.

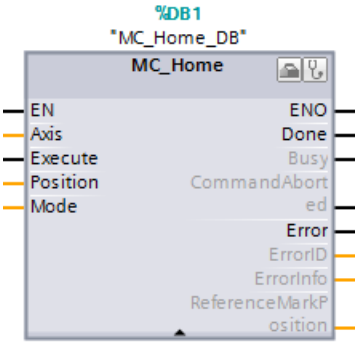
[2] In the SCL example, "MC_Reset_DB" is the name of the instance DB.

The MC_Reset task cannot be aborted by any other motion control task. The new MC_Reset task does not abort any other active motion control tasks.

11.2.3.4 MC_Home (Home axis)

The MC_Home instruction establishes the relationship between the axis control program and the axis mechanical positioning system.

Table 11-18 MC_Home instruction

LAD / FBD	SCL	Description
	**"MC_Home_DB"(Axis:=_multi_fb_in_, Execute:=_bool_in_, Position:=_real_in_, Mode:=_int_in_, Done=>_bool_out_, Busy=>_bool_out_, CommandAborted=>_bool_out_, Error=>_bool_out_, ErrorID=>_word_out_, ErrorInfo=>_word_out_, ReferenceMarkPosition=>_real_out_);**	Use the MC_Home instruction to match the axis coordinates to the real, physical drive position. Homing is required for absolute positioning of the axis: In order to use the MC_Home instruction, the axis must first be enabled.

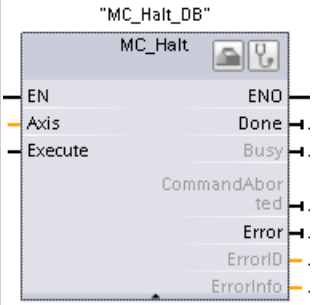
[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_Home_DB" is the name of the instance DB.

11.2.3.5 MC_Halt (Pause axis)

The MC_Halt instruction cancels all motion processes and causes the axis motion to stop. The stop position is not defined.

Table 11-19 MC_Halt instruction

LAD / FBD	SCL	Description
	**"MC_Halt_DB"(Axis:=_multi_fb_in_, Execute:=_bool_in_, Done=>_bool_out_, Busy=>_bool_out_, CommandAborted=>_bool_out_, Error=>_bool_out_, ErrorID=>_word_out_, ErrorInfo=>_word_out_);**	Use the MC_Halt instruction to stop all motion and to bring the axis to a stand-still. The stand-still position is not defined. In order to use the MC_Halt instruction, the axis must first be enabled.

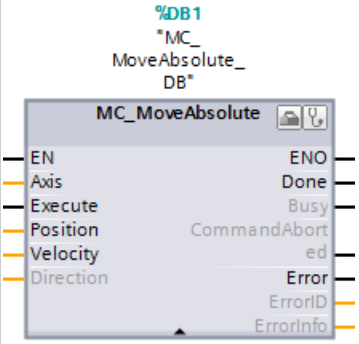
[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_Halt_DB" is the name of the instance DB.

11.2.3.6 MC_MoveAbsolute (Position axis absolutely)

The MC_MoveAbsolute instruction starts motion to an absolute position. The job ends when the target position is reached.

Table 11-20 MC_MoveAbsolute instruction

LAD / FBD	SCL	Description
	**"MC_MoveAbsolute_DB"(Axis:=_multi_fb_in_, Execute:=_bool_in_, Position:=_real_in_, Velocity:=_real_in_, Direction:=_int_in_, Done=>_bool_out_, Busy=>_bool_out_, CommandAborted=>_bool_out_, Error=>_bool_out_, ErrorID=>_word_out_, ErrorInfo=>_word_out_);**	Use the MC_MoveAbsolute instruction to start a positioning motion of the axis to an absolute position. In order to use the MC_MoveAbsolute instruction, the axis must first be enabled and also must be homed.

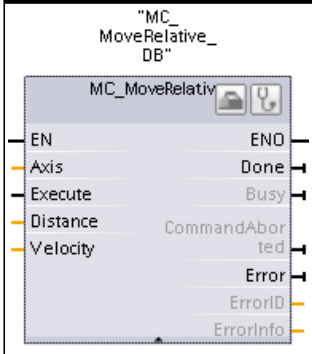
[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_MoveAbsolute_DB" is the name of the instance DB.

11.2.3.7 MC_MoveRelative (Position axis relatively)

The MC_MoveRelative instruction starts a positioning motion relative to the start position.

Table 11-21 MC_MoveRelative instruction

LAD / FBD	SCL	Description
	**"MC_MoveRelative_DB"(** **Axis:=_multi_fb_in_,** **Execute:=_bool_in_,** **Distance:=_real_in_,** **Velocity:=_real_in_,** **Done=>_bool_out_,** **Busy=>_bool_out_,** **CommandAborted=>_bool_out_,** **Error=>_bool_out_,** **ErrorID=>_word_out_,** **ErrorInfo=>_word_out_);**	Use the MC_MoveRelative instruction to start a positioning motion relative to the start position. In order to use the MC_MoveRelative instruction, the axis must first be enabled.

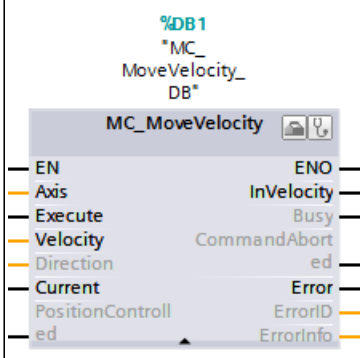
[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_MoveRelative_DB " is the name of the instance DB.

11.2.3.8 MC_MoveVelocity (Move axis at predefined velocity)

The MC_MoveVelocity instruction causes the axis to travel with the specified speed.

Table 11-22 MC_MoveVelocity instruction

LAD / FBD	SCL	Description
	**"MC_MoveVelocity_DB"(** **Axis:=_multi_fb_in_,** **Execute:=_bool_in_,** **Velocity:=_real_in_,** **Direction:=_int_in_,** **Current:=_bool_in_,** **PositionControlled:=_bool_in_,** **InVelocity=>_bool_out_,** **Busy=>_bool_out_,** **CommandAborted=>_bool_out_,** **Error=>_bool_out_,** **ErrorID=>_word_out_,** **ErrorInfo=>_word_out_);**	Use the MC_MoveVelocity instruction to move the axis constantly at the specified velocity. In order to use the MC_MoveVelocity instruction, the axis must first be enabled.

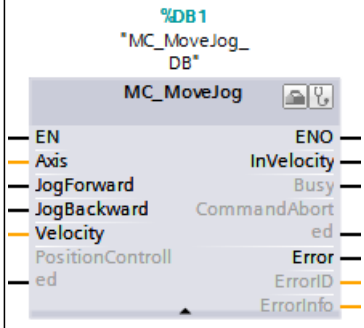
[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_MoveVelocity_DB " is the name of the instance DB.

11.2.3.9 MC_MoveJog (Move axis in jog mode)

The MC_MoveJog instruction executes jog mode for testing and startup purposes.

Table 11-23 MC_MoveJog instruction

LAD / FBD	SCL	Description
	**"MC_MoveJog_DB"(** **Axis:=_multi_fb_in_,** **JogForward:=_bool_in_,** **JogBackward:=_bool_in_,** **Velocity:=_real_in_,** **PositionControlled:=_bool_in_,** **InVelocity=>_bool_out_,** **Busy=>_bool_out_,** **CommandAborted=>_bool_out_,** **Error=>_bool_out_,** **ErrorID=>_word_out_,** **ErrorInfo=>_word_out_);**	Use the MC_MoveJog instruction to move the axis constantly at the specified velocity in jog mode. This instruction is typically used for testing and commissioning purposes. In order to use the MC_MoveJog instruction, the axis must first be enabled.

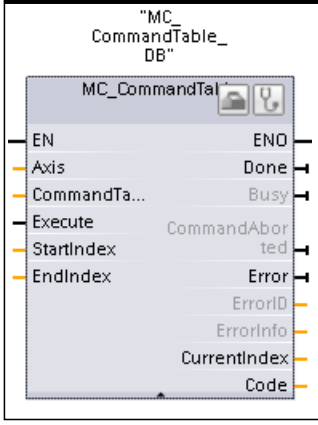
[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_MoveJog_DB " is the name of the instance DB.

11.2.3.10 MC_CommandTable (Run axis command as movement sequence)

The MC_CommandTable instruction runs axis commands as a movement sequence.

Table 11-24 MC_CommandTable instruction

LAD / FBD	SCL	Description
	**"MC_CommandTable_DB"(** **Axis:=_multi_fb_in_,** **CommandTable:=_multi_fb_in_,** **Execute:=_bool_in_,** **StartStep:=_uint_in_,** **EndStep:=_uint_in_,** **Done=>_bool_out_,** **Busy=>_bool_out_,** **CommandAborted=>_bool_out_,** **Error=>_bool_out_,** **ErrorID=>_word_out_,** **ErrorInfo=>_word_out_,** **CurrentStep=>_uint_out_,** **StepCode=>_word_out_);**	Executes a series of individual motions for a motor control axis that can combine into a movement sequence. Individual motions are configured in a technology object command table for pulse train output (TO_CommandTable_PTO).

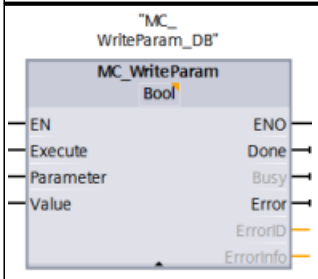
[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_CommandTable_DB " is the name of the instance DB.

11.2.3.11 MC_WriteParam (write parameters of a technology object)

You use the MC_WriteParam instruction to write a select number of parameters to change the functionality of the axis from the user program.

Table 11-25 MC_WriteParam instruction

LAD / FBD	SCL	Description
	**"MC_WriteParam_DB"(Parameter:=_variant_in_, Value:=_variant_in_, Execute:=_bool_in_, Done:=_bool_out_, Error:=_real_out_, ErrorID:=_word_out_, ErrorInfo:=_word_out_);**	You use the MC_WriteParam instruction to write to public parameters (for example, acceleration and user DB values).

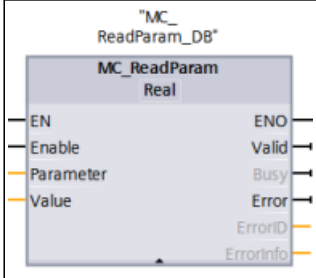
[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_WriteParam_DB" is the name of the instance DB.

11.2.3.12 MC_ReadParam instruction (read parameters of a technology object)

You use the MC_ReadParam instruction to read a select number of parameters that indicate the current position, velocity, and so forth of the axis defined in the Axis input.

Table 11-26 MC_ReadParam instruction

LAD / FBD	SCL	Description
	**"MC_ReadParam_DB"(Enable:=_bool_in_, Parameter:=_variant_in_, Value:=_variant_in_out_, Valid:=_bool_out_, Busy:=_bool_out_, Error:=_real_out_, ErrorID:=_word_out_, ErrorInfo:=_word_out_);**	You use the MC_ReadParam instruction to read single status values, independent of the cycle control point.

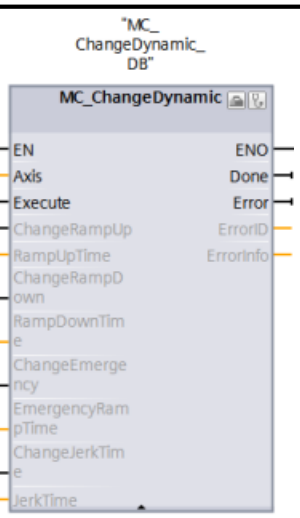
[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_ReadParam_DB " is the name of the instance DB.

11.2.3.13 MC_ChangeDynamic (Change dynamic settings for the axis)

You use the MC_ChangeDynamic instruction to change the dynamic settings of a motion control axis.

Table 11-27 MC_ChangeDynamic instruction

LAD / FBD	SCL	Description
	**"MC_ChangeDynamic_DB"(Axis:=_param_fb_in_, Execute:=_bool_in_, ChangeRampUp:=_bool_in_, RampUpTime:=_real_in_, ChangeRampDown:=_bool_in_, RampDownTime:=_real_in_, ChangeEmergency:=_bool_in_, EmergencyRampTime:=_real_in_, ChangeJerkTime:=_bool_in_, JerkTime:=_real_in_, Done=>_bool_out_, Error=>_bool_out_, ErrorID=>_word_out_, ErrorInfo=>_word_out_);**	Changes the dynamic settings of a motion control axis: • Change the ramp-up time (acceleration) value • Change the ramp-down time (deceleration) value • Change the emergency stop ramp-down time (emergency stop deceleration) value • Change the smoothing time (jerk) value

[1] STEP 7 automatically creates the DB when you insert the instruction.

[2] In the SCL example, "MC_ChangeDynamic_DB " is the name of the instance DB.

11.3 PID control

11.3.1 PID functionality

STEP 7 and the S7-1200 CPU provide proportional-integral-derivative (PID) control. With PID control you can control processes such as the following:

- Technical processes with continuous input- and output variables.
- Control of motor-actuated devices, such as valves that require discrete signals for open- and close actuation.
- Universal PID control that handles specific requirements of temperature control.

References

The STEP 7 Information System provides documentation for each PID instruction. You can find help on programming and differences between past and present versions of the PID instructions.

Refer to the SIMATIC S7-1200, S7-1500 PID Control Function Manual (https://support.industry.siemens.com/cs/de/en/view/108210036) for further information on S7-1200 PID control. In this manual, you can find detailed information on the following topics:

- Principles for control
- Configuring a software controller

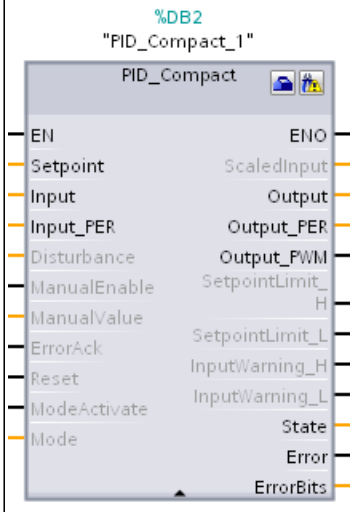
- Using PID_Compact:
  - Process value limits
  - ErrorBit parameters
  - Warning parameters
- Using PID_3Step:
  - ErrorBit parameters
  - Warning parameters
- Using PID_Temp:
  - ErrorBit parameters
  - Warning parameters
- Configuring the PID_Compact, PID_3Step, and PID_Temp controllers
- Commissioning the PID_Compact, PID_3Step, and PID_Temp controllers

11.3.2 PID instructions

11.3.2.1 PID_Compact instruction

The PID_Compact instruction provides a universal PID controller with integrated self-tuning for automatic and manual mode.

Table 11-28 PID_Compact instruction

LAD / FBD	SCL	Description
	**"PID_Compact_1"(Setpoint:=_real_in_, Input:=_real_in_, Input_PER:=_word_in_, Disturbance:=_real_in_, ManualEnable:=_bool_in_, ManualValue:=_real_in_, ErrorAck:=_bool_in_, Reset:=_bool_in_, ModeActivate:=_bool_in_, Mode:=_int_in_, ScaledInput=>_real_out_, Output=>_real_out_, Output_PER=>_word_out_, Output_PWM=>_bool_out_, SetpointLimit_H=>_bool_out_, SetpointLimit_L=>_bool_out_, InputWarning_H=>_bool_out_, InputWarning_L=>_bool_out_, State=>_int_out_, Error=>_bool_out_, ErrorBits=>_dword_out_);**	PID_Compact provides a PID controller with self-tuning for automatic and manual mode. PID_Compact is a PID T1 controller with anti-windup and weighting of the P- and D- component.

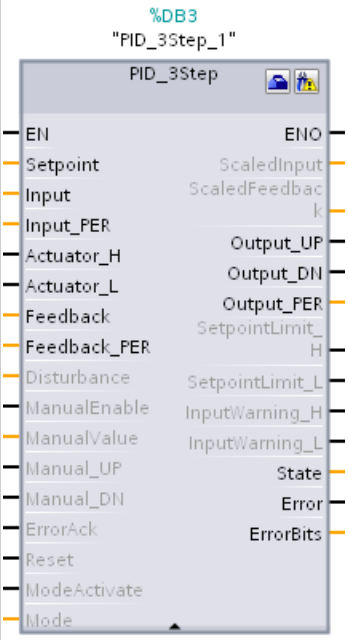
[1] STEP 7 automatically creates the technology object and instance DB when you insert the instruction. The instance DB contains the parameters of the technology object.

[2] In the SCL example, "PID_Compact_1" is the name of the instance DB.

11.3.2.2 PID_3Step instruction

The PID_3Step instruction configures a PID controller with self-tuning capabilities that has been optimized for motor-controlled valves and actuators.

Table 11-29 PID_3Step instruction

LAD / FBD	SCL	Description
	**"PID_3Step_1"(** **SetpoInt:=_real_in_,** **Input:=_real_in_,** **ManualValue:=_real_in_,** **Feedback:=_real_in_,** **InputPer:=_word_in_,** **FeedbackPer:=_word_in_,** **Disturbance:=_real_in_,** **ManualEnable:=_bool_in_,** **ManualUP:=_bool_in_,** **ManualDN:=_bool_in_,** **ActuatorH:=_bool_in_,** **ActuatorL:=_bool_in_,** **ErrorAck:=_bool_in_,** **Reset:=_bool_in_,** **ModeActivate:=_bool_in_,** **Mode:=_int_in_,** **ScaledInput=>_real_out_,** **ScaledFeedback=>_real_out_,** **ErrorBits=>_dword_out_,** **OutputPer=>_word_out_,** **State=>_int_out_,** **OutputUP=>_bool_out_,** **OutputDN=>_bool_out_,** **SetpoIntLimitH=>_bool_out_,** **SetpoIntLimitL=>_bool_out_,** **InputWarningH=>_bool_out_,** **InputWarningL=>_bool_out_,** **Error=>_bool_out_,** **ErrorBits=>_dword_out_);**	PID_3Step configures a PID controller with self-tuning capabilities that has been optimized for motor-controlled valves and actuators. It provides two Boolean outputs. PID_3Step is a PID T1controller with anti-windup and weighting of the P- and D-components.

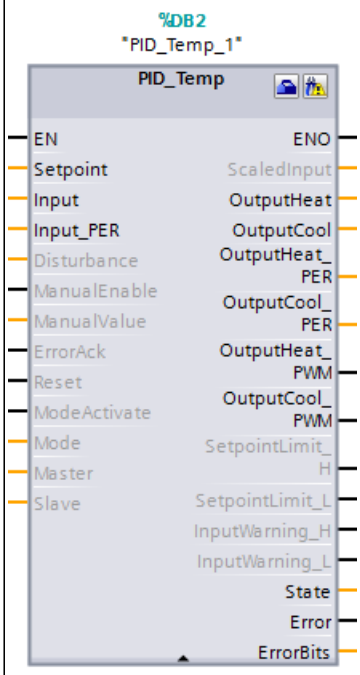
[1] STEP 7 automatically creates the technology object and instance DB when you insert the instruction. The instance DB contains the parameters of the technology object.

[2] In the SCL example, "PID_3Step_1" is the name of the instance DB.

11.3.2.3 PID_Temp instruction

The PID_Temp instruction provides a universal PID controller for temperature control.

Table 11-30 PID_Temp instruction

LAD / FBD	SCL	Description
	**"PID_Temp_1"(** **Setpoint:=_real_in_,** **Input:=_real_in_,** **Input_PER:=_int_in_,** **Disturbance:=_real_in_,** **ManualEnable:=_bool_in_,** **ManualValue:=_real_in_,** **ErrorAck:=_bool_in_,** **Reset:=_bool_in_,** **ModeActivate:=_bool_in_,** **Mode:=_int_in_,** **Master:=_dword_in** **Save:=_dword_in** **ScaledInput=>_real_out_,** **OutputHeat=>_real_out_,** **OutputCool=>_real_out_,** **OutputHeat_PER=>_int_out_,** **OutputCool_PER=>_int_out_,** **OutputHeat_PWM=>_bool_out_,** **OutputCool_PWM=>_bool_out_,** **SetpointLimit_H=>_bool_out_,** **SetpointLimit_L=>_bool_out_,** **InputWarning_H=>_bool_out_,** **InputWarning_L=>_bool_out_,** **State=>_int_out_,** **Error=>_bool_out_,** **ErrorBits=>_dword_out_);**	PID_Temp provides these capabilities: • Heating and cooling of the process with different actuators • Integrated autotuning to handle temperature processes • Cascading to process more than one temperature that depends on the same actuator

[1] STEP 7 automatically creates the technology object and instance DB when you insert the instruction. The instance DB contains the parameters of the technology object.

[2] In the SCL example, "PID_Temp_1" is the name of the instance DB.

Communication 12

12.1 Overview

The S7-1200 offers several types of communication between CPUs and programming devices, HMIs, and other CPUs.

PROFINET

PROFINET is used for exchanging data through the user program with other communications partners through Ethernet:

- In the S7-1200, PROFINET supports 16 IO devices with a maximum of 256 submodules
- S7 communication
- User Datagram Protocol (UDP) protocol
- ISO on TCP (RFC 1006)
- Transport Control Protocol (TCP)

PROFINET IO controller

As an IO controller using PROFINET IO, the CPU communicates with up to 16 PN devices on the local PN network or through a PN/PN coupler (link). Refer to PROFIBUS and PROFINET International, PI (www.us.profinet.com) for more information.

PROFIBUS

PROFIBUS is used for exchanging data through the user program with other communications partners through the PROFIBUS network:

- In the S7-1200, PROFIBUS allows 3 independent PROFIBUS DP Masters, supporting 32 slaves per DP master, with a maximum of 512 modules per DP master.
- With CM 1242-5, the CPU operates as a PROFIBUS DP slave.
- With CM 1243-5, the CPU operates as a PROFIBUS DP master class1.
- PROFIBUS DP Slaves, PROFIBUS DP Masters, and AS-i and PROFINET are separate communications networks that do not limit each other.

AS-i

The S7-1200 CM 1243-2 AS-i Master allows the attachment of an AS-i network to an S7-1200 CPU.

CPU-to-CPU S7 communication

You can create a communication connection to a partner station and use the GET and PUT instructions to communicate with S7 CPUs.

TeleService communication

In TeleService, an engineering station on which STEP 7 is installed communicates via the cellular network and the Internet with a SIMATIC S7-1200 station with a CP 1243-7 LTE. The connection runs via a telecontrol server that serves as an intermediary and is connected to the Internet.

IO-Link

The S7-1200 SM 1278 4xIO-Link Master enables IO-Link devices to connect to an S7-1200 CPU.

Network security

WARNING

Avoiding security risks from physical network attacks

If an attacker can physically access your networks, the attacker can possibly read and write data.

For example, I/O exchange through PROFIBUS, PROFINET, AS-i, or other I/O bus, GET/PUT, T-Block, and communication modules (CMs) have no security features. You must protect these forms of communication by limiting physical access. If an attacker can physically access your networks using these forms of communication, the attacker can possibly read and write data.

If you fail to protect these forms of communication, death or severe personal injury can result.

For security information and recommendations, see the "Operational Guidelines" white paper on the Siemens Industrial Cybersecurity Web site (https://www.siemens.com/global/en/products/services/cert/news/operational-guidelines-for-industrial-security.html).

12.2 Secure vs. legacy communication

S7-1200 CPUs implement secure communication between PLCs and the TIA Portal, SIMATIC Automation Tool, and HMIs. This implementation uses the industry standard TLS 1.3 (Transport Layer Security) protocol. The S7-1200 CPU has provided secure communication enhancements since V4.0. To maintain compatibility with older devices and clients, legacy communication still exists. You have the choice whether to use secure or legacy communication. Siemens strongly recommends secure communication for clients and devices that support it.

Advantages of secure communication

Use secure communication to achieve the following objectives:

- Confidentiality: The data is secret and cannot by read by eavesdroppers.
- Integrity: The message that reaches the recipient is the same message, unchanged, that the sender sent. The message has not been altered on the way.
- End point authentication: The end point communication partner is exactly who it claims to be and the party who is to be reached. The identity of the partner is verified.

Today, networked industrial machinery and control systems with sensitive data are at high risk and consequently pose high security requirements for data exchange.

Protection through firewall, VPN connection, or a security module, was common in the past and remains common. In addition to physical security, however, using secure communications to transfer data to external communication partners in encrypted form is becoming necessary.

The CPU uses X.509 certificates (Page 529) to provide secure communication between the CPU and clients. Clients such as STEP 7 and the SIMATIC Automation Tool might require that you trust the certificate that is in the CPU. Be aware of the certificate you download to a CPU so that you can trust it when prompted.

Considerations when using secure communication

Be aware of the following concerns regarding secure communication:

- Communication speeds can be slower with secure communication compared to legacy communication.
- Secure PG/PC and HMI communication (Page 155) requires TIA Portal and V4.x S7-1200 CPUs.

The secure communication capabilities depend on several factors:

- Actual firmware version of the physical CPU
- Configured firmware version (Page 39) of the CPU in the STEP 7 project

The following table illustrates supported communication for a S7-1200 CPU with V4.x firmware:

Device configuration of the CPU in the STEP 7 project	Client versions			
	TIA Portal >= V17 / SIMATIC Automation Tool >= V4.0 SP3	**TIA Portal < V17 / SIMATIC Automation Tool < V4.0 SP3**	**HMI >= V17[1]**	**HMI < V17**
Firmware version configured in the STEP 7 project: V4.x Configuration setting: "Only permit secure PG/PC and HMI communication" selected	Secure	No connection	Secure	No connection
Firmware version configured in the STEP 7 project: V4.x Configuration setting: "Only permit secure PG/PC and HMI communication" deselected	Secure by default, legacy configurable	Legacy	Secure	Legacy
Firmware version configured in the STEP 7 project: V4.x	Legacy			
No project	Secure or legacy	Legacy	Not applicable	

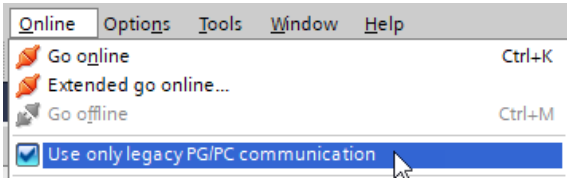
[1] Not applicable for HMIs with S7 communication

You must configure the firmware version of the CPU in the STEP 7 project to be V4.x to use TLS 1.3. The CPU uses TLS 1.2 if the configured firmware version in the project is prior to V4.5.

Configuring secure or legacy communication

You configure the security features of your CPU in the device configuration (Page 121) of the CPU in the TIA Portal under Protection & Security. The TIA Portal dialogs provide access to the TIA Portal Information System to guide you through the configuration process. To simplify configuration, TIA Portal and higher provides a Security Wizard (Page 144) to guide you through your security choices.

TIA Portal defaults to secure PG/PC and HMI communication; however, for commissioning reasons you can force the TIA Portal to use legacy PG/PC communications by selecting "Use only legacy PG/PC communication" from the Online menu.



Additional information

You can find additional details about the implementation of secure communication in the TIA Portal Information System. In particular, additional information about certificates is in the following TIA Portal Information System topics:

- Confidentiality through encryption
- Managing certificates with STEP 7
- Examples for the management of certificates
- Authenticity and integrity through signatures

12.3 Communication protocols and ports used by Ethernet communication

This is an overview of the supported protocols and ports used for communication over PN/IE interfaces. The specified ports are the standard port numbers that the S7-1200 PLC uses. Many communication protocols and implementations enable you to use other port numbers. The following tables show different layers, protocols, and ports used in the S7-1200 PLC.

Table 12-1 Transport layer ports and protocols by S7-1200

Port(s)	Direction	Protocol	Applica-tion	Description	Default setting/notes
25	Outbound	TCP	SMTP	SMTP is used for sending e-mails.	Default: Deactivated. Can be enabled via TMAIL_C instruction in the STEP 7 program.
80	Inbound	TCP	HTTP	HTTP is used for communication with the CPU-internal webserver.	Default: Deactivated. Can be enabled in the CPU properties. Requirement: Web server in the CPU properties is enabled.
102	Inbound/ Outbound	TCP	ISO-on-TCP	ISO-on-TCP (according to RFC 1006). The S7 protocol users ISO-on-TCP according to RFC 1006 for PG/HMI communication with TIA Portal.	Default: Activated. This function cannot be deactivated.
123	Outbound	UDP	NTP	NTP is used for synchronization of the CPU system time with the time of an NTP server.	Default: Deactivated. Can be enabled in the CPU properties.
161	Inbound	UDP	SNMP	SNMP is used for reading and setting network management data (SNMP managed Objects) by the SNMP Manager.	Default: Deactivated. Can be enabled via data record in the user program, CPU properties, and as write-protected in the CPU properties.
443	Inbound	TCP	HTTPS	HTTPS is used for secure communication with the CPU-internal web server over TLS.	Default: Deactivated. Can be enabled in the CPU properties. Requirement: Web server in the CPU properties is enabled.
465, 587	Outbound	TCP	SMTPS	SMTPS is used for sending e-mails over secure connections.	Default: Deactivated. Can be enabled via TMAIL_C instruction in the STEP 7 program.

Port(s)	Direction	Protocol	Application	Description	Default setting/notes
502	Inbound/ Outbound	TCP	Modbus	Modbus/TCP is used by MB_CLIENT/MB_SERVER instructions in the user program.	Default: Deactivated. Can be activated via Modbus instructions in the STEP 7 program.
4840	Inbound	TCP	OPC UA	Communication standard ranging from the enterprise level to the field level.	Default: Deactivated. Server and client function can be enabled in the CPU properties. Client access can be configured in the STEP 7 program.
6514, 514	Outbound	TCP (6514) UDP (514)	Syslog Client	The Syslog client of the CPU is used for transferring syslog messages to a server.	Default: Deactivated. Can be enabled in the CPU properties. You can configure the forwarding of syslog messages to a syslog server in the CPU properties. The collection of system logging events within a CPU cannot be disabled. Port 6514 is the default value for Syslog servers in STEP 7. Port 514 is the standard port for UDP Syslog servers, but it is not the default value even if you select UDP in the STEP 7 project configuration.
34964	Inbound/ Outbound	UDP	PROFINET Context Manager	The PROFINET Context Manager provides an endpoint mapper in order to establish an application relation (PROFINET AR).	Default: Enabled (UDP port open). This function cannot be deactivated.

Table 12-2 Port ranges that could be used by open user communication (OUC) and other protocols. Exact communication parameters are defined by the user as a part of the S7-1200 user program

Port Range	Direction	Protocol	Application	Description
1-1999	Varies	TCP/UDP	OUC	Port range can be used to limited extent, excluding already used ports.
2000-5000	Varies	TCP/UDP	OUC	Recommended port range for OUC
5001-49151	Varies	TCP/UDP	OUC	Port range can be used to limited extent, excluding already used ports.
49152-65535	Outbound	TCP/UDP	Varies	Dynamic port area used for active connection end point if the application does not determine the local port number.

Table 12-3 Protocols used by S7-1200 in the Data Link and Network Layer (Layer 2, 3) of the OSI model.

Protocol	Direction	Ethertype	Description
PROFINET DCP	Inbound/Outbound	0x8892	DCP is used by PROFINET to discover PROFINET devices and provide basic settings. DCP uses the special multicast MAC addresses: 01-0E-CF-00-00-00 and 01-0E-CF-00-00-01.
LLDP	Outbound	0x88CC	LLDP is used by PROFINET to discover and manage neighbor relationships between PROFINET devices. LLDP uses the special multicast MAC address: 01-80-C2-00-00-0E.

Protocol	Direction	Ethertype	Description
PROFINET IO	Inbound/Outbound	0x8892	The PROFINET IO frames are used to transmit IO data cyclically between PROFINET IO controller and IO devices via Ethernet.
ICMP	Inbound	0x0800	Internet Control Message Protocol is used for diagnostic or control purposes.
MRP	Inbound/Outbound	0x88E3	Media Redundancy Protocol enables control of redundant transmission paths in a ring topology. MRP uses the special multicast MAC addresses: 01:15:4E:00:00:01 and 01:15:4E:00:00:02

12.4 Asynchronous communication connections

Overview of communication services

The CPU supports the following communication services:

Communication service	Functionality	Using PROFIBUS DP		Using Ethernet
		CM 1243-5 DP master module	CM 1242-5 DP slave module	
PG communication	Commissioning, testing, diagnostics	Yes	No	Yes
HMI communication	Operator control and monitoring	Yes	No	Yes
S7 communication	Data exchange using configured connections	Yes	No	Yes
Routing of PG functions	For example, testing and diagnostics beyond network boundaries	No	No	No
PROFIBUS DP	Data exchange between master and slave	Yes	Yes	No
PROFINET IO	Data exchange between I/O controllers and I/O devices	No	No	Yes
Web server	Diagnostics	No	No	Yes
SNMP [1] (Simple Network Management Protocol)	Standard protocol for network diagnostics and parameterization	No	No	Yes
S7 routing	Using routing tables, communication partners can communicate with each device even though the devices are on different S7 subnets.	No	No	Yes
Open communication over TCP/IP	Data exchange over Industrial Ethernet with TCP/IP protocol (with loadable FBs)	No	No	Yes

[1] The CPU supports SNMP V1 without TRAPs.

[2] OPC UA is only supported using the CPU's integrated Ethernet port.

Communication service	Functionality	Using PROFIBUS DP		Using Ethernet
		CM 1243-5 DP master module	CM 1242-5 DP slave module	
Open communication over ISO on TCP	Data exchange over Industrial Ethernet with ISO on TCP protocol (with loadable FBs)	No	No	Yes
Open communication over UDP	Data exchange over Industrial Ethernet with UDP protocol (with loadable FBs)	No	No	Yes
OPC UA Server	Data exchange over Industrial Ethernet with OPC UA clients	No	No	Yes[2]

[1] The CPU supports SNMP V1 without TRAPs.

[2] OPC UA is only supported using the CPU's integrated Ethernet port.

Available connections

The CPU supports the following number of maximum simultaneous, asynchronous communication connections for PROFINET and PROFIBUS. The maximum number of connection resources allocated to each category are fixed; you cannot change these values. However, you can configure the "Free available connections" to increase the number of any category as required by your application.

Some connection types have a fixed number of reserved resources (sometimes called guaranteed). This means that the CPU is guaranteed to support up to the number of reserved resources for the connection type. For example, at least 12 HMI connections can be made to the CPU simultaneously. Additional connections beyond the number of reserved resources can be made for a connection type, but those connections resources must come from the "dynamic" resources pool.

The dynamic resources (sometimes called Free) are a collection of resources that can be used for any connection type. These resources are used by connections that do not have any reserved resources (such as OPC UA) or by connections that have used up all of their reserved resources.

S7-1200 CPUs have 34 dynamic resources.

Connection resources

	Station resources			Module resources
	Reserved		Dynamic	PLC_1 [CPU 1215C DC/DC/...
Maximum number of resources:	34		34	68
	Maximum	Configured	Configured	Configured
PG communication:	4	-	-	-
HMI communication:	12	0	0	0
S7 communication:	8	0	0	0
Open user communication:	8	0	0	0
Web communication:	2	-	-	-
OPC UA client/server communicat...	0	-	-	-
Other communication:	-	-	0	0
Total resources used:	0		0	0
Available resources:	34		34	68

NOTE

The total number of S7-1200 communication connections does not increase when you add CM/CP modules.

NOTE

OPC UA connections

OPC UA connections consume resources from the dynamic resources. Ensure that you have enough available connections for your application.

Based upon the allocated connection resources, the following number of connections per device are available:

Type	Reserved	Maximum[1]
Programming terminal (PG) communication	4	4
Human Machine Interface (HMI) communication	12	18
S7 communication	8	14
Open User communication	8	14
Web communication	2	30
OPC UA Client/Server communication	0	10
Other communication	0	-

[1] Since the dynamic connections are shared, it is not possible to max out all connections simultaneously.

For an example, the CPU has four available PG connection resources. Depending on the current PG functions in use, the PG might actually use one, two, three, or four of its available connection resources. You can always use one PG.

Another example is the number of HMIs, as shown in the figure below. HMIs have 12 available connection resources. Depending on what HMI type or model that you have and the HMI functions that you use, each HMI might actually use one, two, or three of its available connection resources. Given the number of available connection resources being used, it might be possible to use more than four HMIs at one time. However, you are always guaranteed at least four HMIs. An HMI can use its available connection resources (one each for a total of three) for the following functions:

- Reading
- Writing
- Alarming plus diagnostics

This is only an example. The actual number of connections used can vary by HMI type and version.

Example	HMI 1	HMI 2	HMI 3	HMI 4	HMI 5	Total connection resources available
Connection resources used	2	2	2	3	3	12

NOTE

Web server connections: The CPU provides connections for multiple web browsers. The number of browsers that the CPU can simultaneously support depends upon how many connections a given web browser requests/utilizes and the number of dynamic connection resources available in the CPU.

NOTE

The Open User Communications, S7 connection, HMI, programming device, OPC UA, and Web server communication connections may utilize multiple connection resources based upon the features currently being used.

12.5 Supported certificates

Secure communication services require certificates with certain security parameters.

You can create or select these certificates from the following areas in the TIA Portal "General" tab of the CPU "Properties" window:

- "Web server > Security": Use for the generation and assignment of Web server certificates, which can be either hardware generated or software downloaded.
- "Protection & Security > Connection mechanisms": Use for the generation or assignment of PLC communication or Secure PG/PC and HMI communication certificates.
- "Protection & Security > Certificate manager": Use for the generation or assignment of all types of certificates. The default setting for the creation of certificates is TLS certificates for Secure Open User Communication (Secure OUC).
- "OPC UA > Server > Security": Use for the generation or assignment of OPC UA server certificates.

For more information on generating and assigning certificates, refer to the STEP 7 Information System.

Recommended certificate parameters for all security-enabled communication services:

Certificate Parameters		Communication services			
Encryption method	**Encryption parameter**	**Web server** (Page 767)	**Secure PG/PC and HMI communication** (Page 155)	**Secure OUC** (Page 546)	**OPC UA** (Page 725)
EC	prime256v1	Supported	Supported	Supported	Unsupported
EC	secp384r1	Supported	Supported	Supported	Unsupported
RSA	2048	Supported	Supported	Supported	Supported

You can use certificate parameter RSA 4096 with a significantly increased minimum scan cycle (Page 81) that allocates at least 60% of the scan cycle load to communication.

NOTE

Although you can select unsupported certificate parameters from the "Certificate manager," only use the recommended certificate parameters listed in the table above.

Using an unlisted certificate parameter might cause communication problems or cause the communication service to be inoperable.

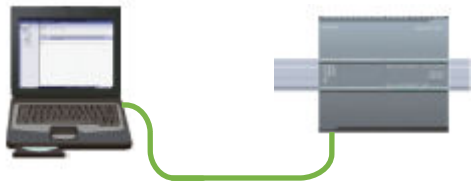
12.6 PROFINET

The CPU can communicate with the following devices:

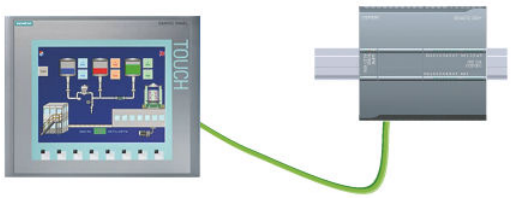
- Other CPUs
- Programming devices
- HMI devices
- Non-Siemens devices using standard TCP communications protocols

Example connections are as follows:

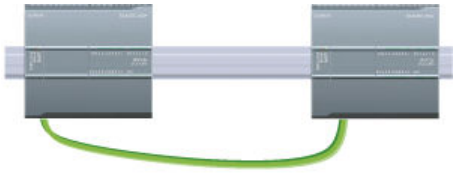
Programming device connected to the CPU



HMI connected to the CPU



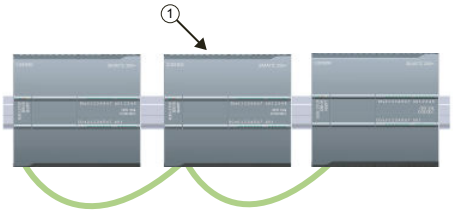
A CPU connected to another CPU



Ethernet switching

The CPU 1211C, 1212C, and 1214C have a single Ethernet port and do not include a integrated Ethernet Switch. A direct connection between a programming device or HMI and a CPU does not require an Ethernet switch. However, a network with more than two CPUs or HMI devices requires an Ethernet switch.

The CPU 1215C and the CPU 1217C have a built-in 2-port Ethernet switch. You can have a network with a CPU 1215C and two other S7-1200 CPUs.



① CPU 1215C

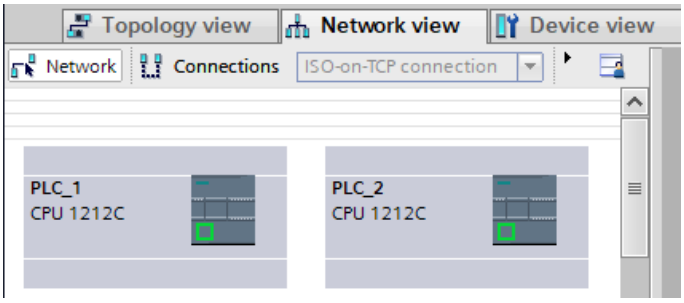
You can also use the rack-mounted CSM1277 4-port Ethernet switch for connecting multiple CPUs and HMI devices.

② CSM1277 Ethernet switch

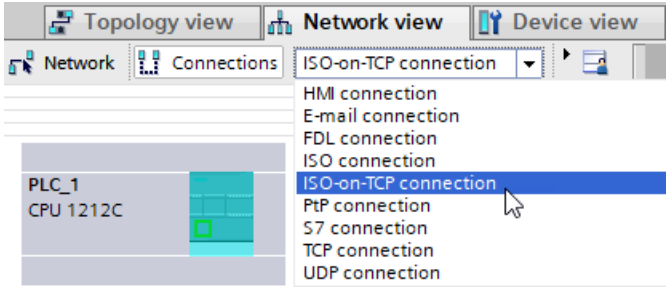
12.6.1 Creating a network connection

Use the "Network view" of Device configuration to create the network connections between the devices in your project.

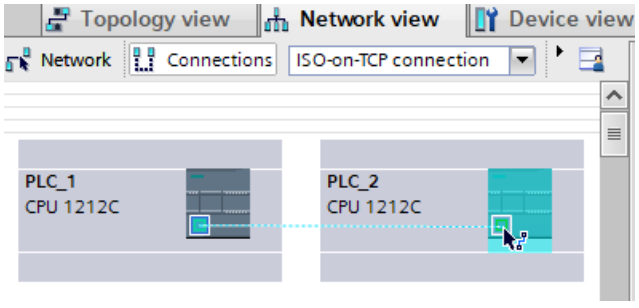
1. Select "Network view" to display the devices to be connected.



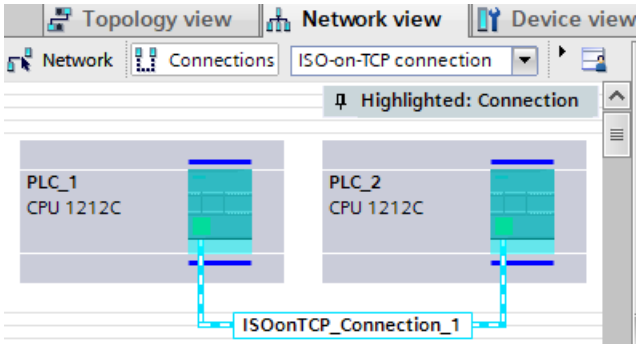
2. Select the "Connections" tab and choose your connection type from the dropdown menu.



3. Select the port on one device and drag the connection to the port on the second device.



4. Release the mouse button to create the network connection.



After creating the network connection, use the "Properties" tab of the inspector window to configure the parameters of the network.

12.6.2 Configuring the Local/Partner connection path

A Local / Partner (remote) connection defines a logical assignment of two communication partners to establish communication services. A connection defines the following:

- Communication partners involved (One active, one passive)
- Type of connection (for example, a PLC, HMI, or device connection)
- Connection path

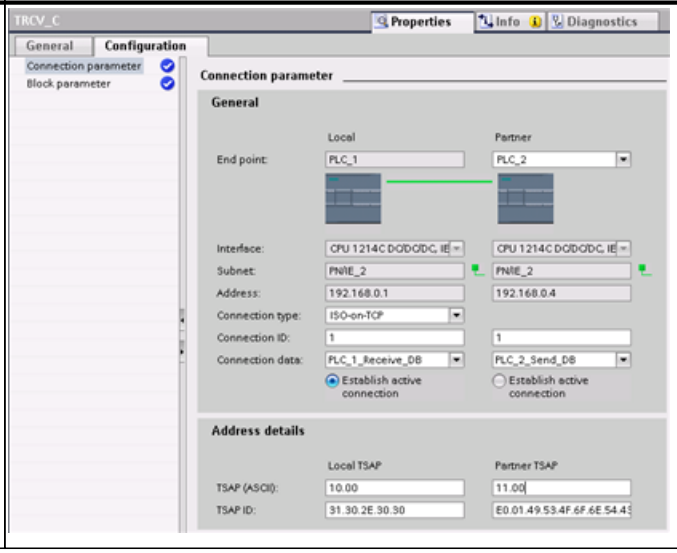
Communication partners execute the instructions to set up and establish the communication connection. You use parameters to specify the active and passive communication end point partners. After the connection is set up and established, it is automatically maintained and monitored by the CPU.

If the connection is terminated (for example, due to a line break), the active partner attempts to re-establish the configured connection. You do not have to execute the communication instruction again.

Connection paths

After inserting a TSEND_C, TRCV_C or TCON instruction into the user program, the inspector window displays the properties of the connection whenever you have selected any part of the instruction. Specify the communication parameters in the "Configuration" tab of the "Properties" for the communication instruction.

Table 12-4 Configuring the connection path (using the properties of the instruction)

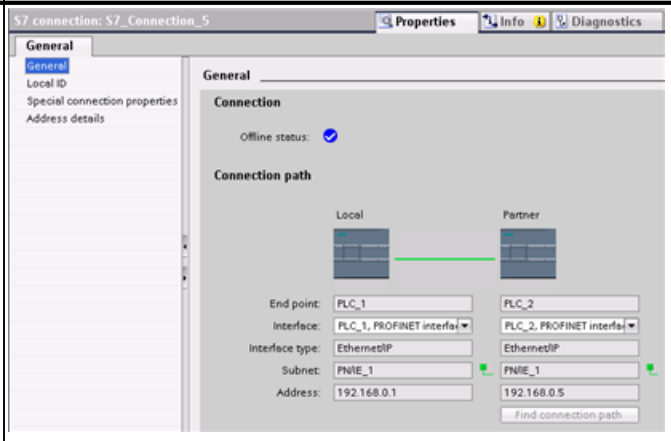
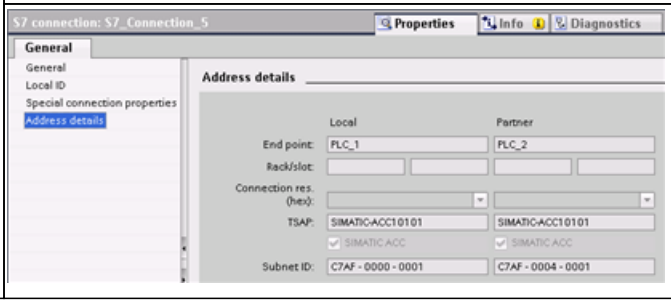
TCP, ISO-on-TCP, and UDP	Connection properties
For the TCP, ISO-on-TCP, and UDP Ethernet protocols, use the "Properties" of the instruction (TSEND_C, TRCV_C, or TCON) to configure the "Local/Partner" connections. The illustration shows the "Connection properties" of the "Configuration tab" for an ISO-on-TCP connection.	

NOTE

When you configure the connection properties for one CPU, STEP 7 allows you either to select a specific connection DB in the partner CPU (if one exists), or to create the connection DB for the partner CPU. The partner CPU must already have been created for the project and cannot be an "unspecified" CPU.

You must still insert a TSEND_C, TRCV_C or TCON instruction into the user program of the partner CPU. When you insert the instruction, select the connection DB that was created by the configuration.

Table 12-5 Configuring the connection path for S7 communication (Device configuration)

S7 communication (GET and PUT)	Connection properties
For S7 communication, use the "Devices & networks" editor of the network to configure the Local/Partner connections. You can click the "Highlighted: Connection" button to access the "Properties". The "General" tab provides several properties: • "General" (shown) • "Local ID" • "Special connection properties" • "Address details" (shown)	 

Refer to "Protocols" (Page 546) in the "PROFINET" section or to "Creating an S7 connection" (Page 709) in the "S7 communication" section for more information and a list of available communication instructions.

Table 12-6 Parameters for the multiple CPU connection

Parameter		Definition
Address		Assigned IP addresses
General	End point	Name assigned to the partner (receiving) CPU
	Interface	Name assigned to the interfaces
	Subnet	Name assigned to the subnets
	Interface type	*S7 communication only*: Type of interface
	Connection type	Type of Ethernet protocol
	Connection ID	ID number
	Connection data	Local and Partner CPU data storage location
	Establish active connection	Radio button to select Local or Partner CPU as the active connection
Address details	End point	*S7 communication only*: Name assigned to the partner (receiving) CPU
	Rack/slot	*S7 communication only*: Rack and slot location

[1] When configuring a connection with an S7-1200 CPU for ISO-on-TCP, use only ASCII characters in the TSAP extension for the passive communication partners.

Parameter		Definition
Address details	Connection resource	*S7 communication only*: Component of the TSAP used when configuring an S7 connection with an S7-300 or S7-400 CPU
	Port (decimal):	TCP and UPD: Partner CPU port in decimal format
	TSAP [1] and Subnet ID:	ISO on TCP (RFC 1006) and S7 communication: Local and partner CPU TSAPs in ASCII and hexadecimal formats

[1] When configuring a connection with an S7-1200 CPU for ISO-on-TCP, use only ASCII characters in the TSAP extension for the passive communication partners.

Transport Service Access Points (TSAPs)

Using TSAPs, ISO on TCP protocol and S7 communication allows multiple connections to a single IP address. TSAPs uniquely identify these communication end point connections to an IP address.

In the "Address Details" section of the Connection Parameters dialog, you define the TSAPs to be used. The TSAP of a connection in the CPU is entered in the "Local TSAP" field. The TSAP assigned for the connection in your partner CPU is entered under the "Partner TSAP" field.

Port Numbers

With TCP and UDP protocols, the connection parameter configuration of the Local (active) connection CPU must specify the remote IP address and port number of the Partner (passive) connection CPU.

In the "Address Details" section of the Connection Parameters dialog, you define the ports to be used. The port of a connection in the CPU is entered in the "Local Port" field. The port assigned for the connection in your partner CPU is entered under the "Partner Port" field.

12.6.3 Assigning Internet Protocol (IP) addresses

12.6.3.1 Assigning IP addresses to programming and network devices

If the network interface of your programming device connects to a local area network (LAN) with multiple subnets, both the programming device and the CPU must be on the same subnet. You assign the subnet as a combination of the IP address and subnet mask for the device. See your local network administrator for help.

The Network ID of a Class C IP address is the first three octets of the IP address. The network ID of 211.154.184.16, for example, is 211.154.184. This network ID uniquely identifies your IP network. The subnet mask normally has a value of 255.255.255.0. Because your computer is on a plant LAN, however, the subnet mask might have various values, for example, 255.255.254.0, to set up unique subnets. The subnet mask, when combined with the device IP address in a logical AND operation, defines the boundaries of an IP subnet.

NOTE

You must assign unique IP addresses to all devices on your subnet.

WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server or OPC UA users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

- Enable Access control (Page 147) under "Protection & Security > Access control".
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Enable the setting "Only allow secure PG/PC and HMI communication" under "Protection & Security > Connection mechanisms".
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC from a location outside your protected network.
- Enable access to the Web server only with the HTTPS protocol.
- Perform error-checking and range-checking on your variables in your program logic because Web server or OPC UA users can change PLC variables to invalid values.
- For the OPC UA server: In your STEP 7 Device configuration, navigate to "Properties > OPC UA > Server > Security" and deselect "No security" in "Security policies available on the server for the secure channel".

Disruption of process operations can result in death, severe personal injury, and/or property damage.

NOTE

A secondary network adapter card is useful when you do not want your CPU on your company LAN. During initial testing or commissioning tests, this arrangement is particularly useful.

Assigning or checking the IP address of your programming device

To assign or check your programming device's IP address, follow these steps:

1. Open the Control Panel.
2. Navigate to the "Network and Sharing Center".
3. Click the network interface connected to your CPU.
4. Click "Properties" to open the properties dialog.
5. In the properties dialog, select the checkbox for "Internet Protocol Version 4 (TCP/IPv4)".
6. Click the "Properties" button.

7. Select "Obtain an IP address automatically" or to enter a static IP address select "Use the following IP address".
   If you selected "Use the following IP address", set the IP address and subnet mask:
   – Set the IP address to use the same Network ID and same subnet as the CPU. For example, if the CPU IP address is **192.168.0**.1, you could set the IP address to **192.168.0**.200.
   – Select a subnet mask of 255.255.255.0.
   – Leave the default gateway blank.

Consult your network administrator to help you set up a network configuration to allow you to connect to the S7-1200 G2 CPU.

12.6.3.2 Checking the IP address and MAC address of your network interface

You can check the MAC and IP addresses of your network interface in STEP 7 with the following menu selections:

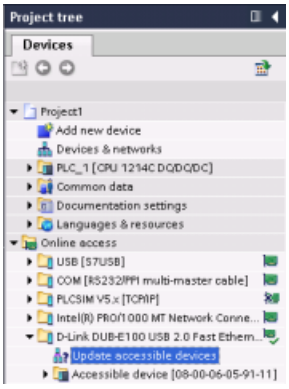
1. In the "Project tree", expand "Online access".
2. Right-click the required network interface and select "Properties".
3. In the dialog, expand "Configurations", and select "Industrial Ethernet".

The dialog displays the MAC and IP addresses of the network interface.

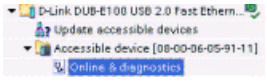
12.6.3.3 Assigning an IP address to a CPU online

You can assign an IP address to a network device online. This is particularly useful in an initial device configuration.

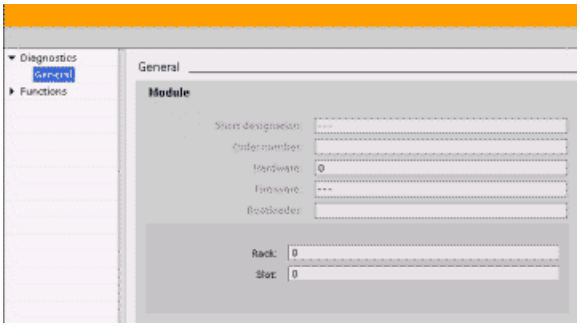
1. In the "Project tree," verify that the CPU does not have a configured IP address. Expand "Online access" > <Adapter card for the network in which the device is located and double-click "Update accessible devices".
If STEP 7 displays a MAC address instead of an IP address, then no IP address has been assigned.



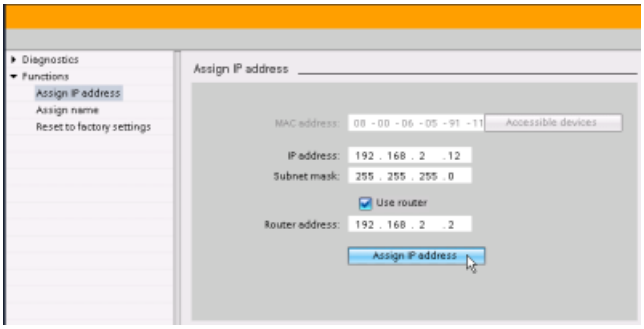
2. Under the required accessible device, double-click "Online & diagnostics".



3. In the "Online & diagnostics" dialog, select "Functions" > "Assign IP address".

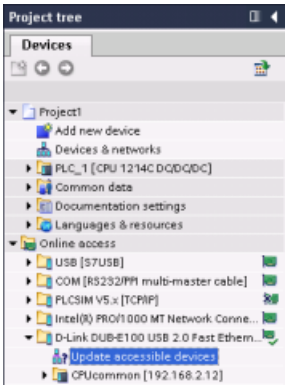


4. In the "IP address" field, enter your new IP address, and click the "Assign IP address" button.



5. In the "Project tree," verify that STEP 7 has assigned your new IP address to the CPU.

Double-click "Update accessible devices" to display the IP address that you configured.



12.6.3.4 Configuring an IP address for a CPU in your project

Configuring the PROFINET interface

To configure parameters for the PROFINET interface, select the green PROFINET interface on the CPU. The "Properties" tab in the inspector window displays the PROFINET port.

Configuring the IP address

Ethernet (MAC) address: In a PROFINET network, each device is assigned a Media Access Control address (MAC address) by the manufacturer for identification. A MAC address consists of six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), in transmission order, (for example, 01-23-45-67-89-AB or 01:23:45:67:89:AB).

IP address: Each device must also have an Internet Protocol (IP) address. This address allows the device to deliver data on a more complex, routed network.

Each IP address is divided into four 8-bit segments and is expressed in a dotted, decimal format (for example, 211.154.184.16). The first part of the IP address is used for the Network

ID (What network are you on?), and the second part of the address is for the Host ID (unique for each device on the network). An IP address of 192.168.x.y is a standard designation recognized as part of a private network that is not routed on the Internet.

Subnet mask: A subnet is a logical grouping of connected network devices. Nodes on a subnet tend to be located in close physical proximity to each other on a Local Area Network (LAN). A mask (known as the subnet mask or network mask) defines the boundaries of an IP subnet.

A subnet mask of 255.255.255.0 is generally suitable for a small local network. This means that all IP addresses on this network should have the same first three octets, and the various devices on this network are identified by the last octet (8-bit field). An example of this is to assign a subnet mask of 255.255.255.0 and an IP addresses of 192.168.2.0 through 192.168.2.255 to the devices on a small local network.

The only connection between different subnets is via a router. If subnets are used, an IP router must be employed.

IP router: Routers are the link between LANs. Using a router, a computer in a LAN can send messages to any other networks, which might have other LANs behind them. If the destination of the data is not within the LAN, the router forwards the data to another network or group of networks where it can be delivered to its destination.

Routers rely on IP addresses to deliver and receive data packets.

IP addresses properties: In the Properties window, select the "Ethernet addresses" configuration entry. STEP 7 displays the Ethernet address configuration dialog, which associates the software project with the IP address of the CPU that will receive that project.

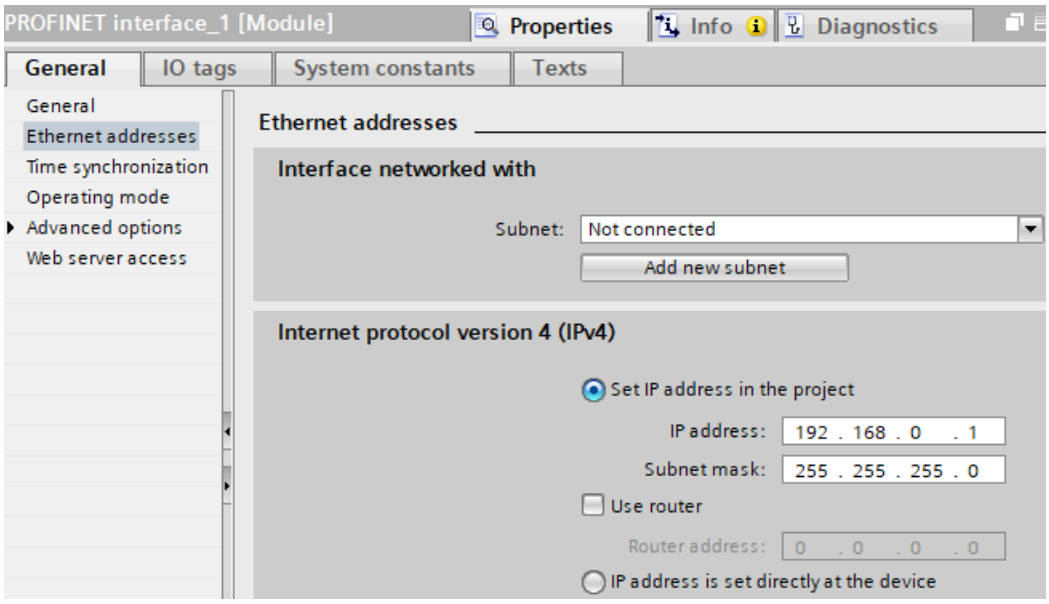


Table 12-7 Parameters for the IP address

Parameter		Description
Subnet	Name of the Subnet to which the device is connected. Click the "Add new subnet" button to create a new subnet. "Not connected" is the default. Two connection types are possible: • The "Not connected" default provides a local connection. • A subnet is required when your network has two or more devices.	
IP protocol	IP address	Assigned IP address for the CPU
	Subnet mask	Assigned subnet mask
	Use IP router	Click the checkbox to indicate the use of an IP router
	Router address	Assigned IP address for the router, if applicable

NOTE

All IP addresses are configured when you download the project. If the CPU does not have a pre-configured IP address, you must associate the project with the MAC address of the target device. If your CPU is connected to a router on a network, you must also enter the IP address of the router.

The "IP address is set directly at the device" radio button allows you to change the IP address online or by using the "T_CONFIG (Page 629)" instruction after the program is downloaded.

WARNING

Downloading a hardware configuration with "IP address is set directly at the device"

After downloading a hardware configuration with the "IP address is set directly at the device" option enabled, it is not possible to transition the CPU operating mode from RUN to STOP or from STOP to RUN until you set an IP address. User equipment continues to run under these conditions and can result in unexpected equipment and process operations.

Ensure that your CPU IP address(es) are set before using the CPU in an actual automation environment. This can be done by using your STEP 7 programming package, the SIMATIC Automation Tool, or an attached HMI device in conjunction with the T_CONFIG instruction.

Unexpected equipment and process operations can cause death, severe personal injury, or property damage if proper precautions are not taken.

WARNING

Condition in which PROFINET network might stop

When changing the IP address of a CPU online or from the user program, it is possible to create a condition in which the PROFINET network might stop. If the IP address of a CPU is changed to an IP address outside the subnet, the PROFINET network will lose communication, and all data exchange will stop. User equipment might be configured to keep running under these conditions. Loss of PROFINET communication can result in unexpected machine or process operations.

If an IP address must be changed manually, ensure that the new IP address lies within the subnet.

Unexpected machine or process operations can cause death, severe personal injury, or property damage if proper precautions are not taken.

Configuring the PROFINET port

By default, the CPU configures port(s) of the PROFINET interface for autonegotiation. For autonegotiation to function properly, you must configure both stations to autonegotiate. If one station has a fixed configuration (for example, full-duplex at 100 Mbps) and the other station is set to autonegotiate, then autonegotiation fails, resulting in half-duplex operation.

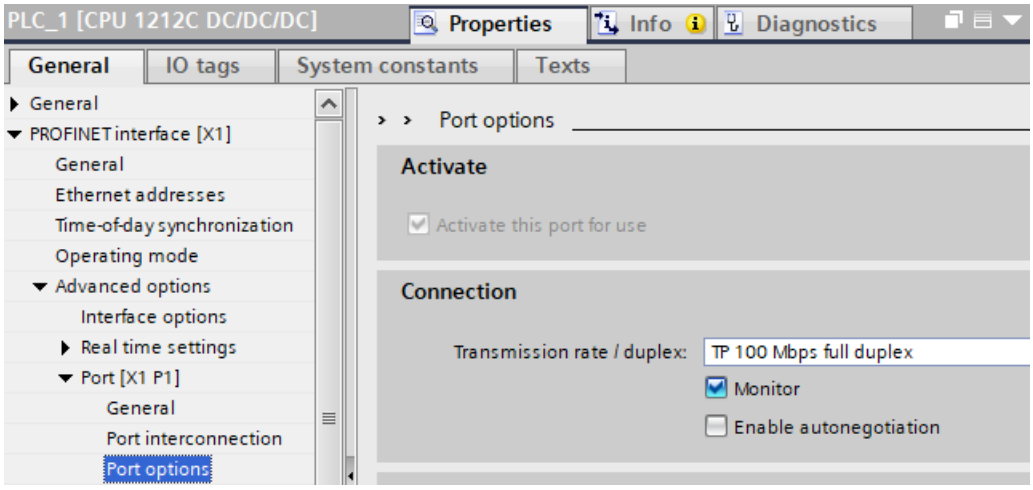
To overcome this limitation of autonegotiation, the S7-1200 provides an option to disable autonegotiation. When you disable autonegotiation, the S7-1200 is automatically configured for full-duplex operation at 100 Mbps.

You can set the transmission rate and duplex to a fixed value for each port:

1. Select Advanced options and the port you need to configure. Then, select Port options.
2. In the Connection, Transmission rate / duplex field, select one of the following:
   - Automatic: The CPU and the peer device determine the port's transmission rate and duplex by autonegotiation.
   - TP 100 Mbps full-duplex: If you disable autonegotiation, the port operates at 100 Mbps full-duplex. If you enable autonegotiation, the port can operate at 100 Mbps full-duplex or another transmission rate / duplex that is autonegotiated between the CPU and the peer device. This places a message in the diagnostics buffer if "Monitor" is selected (see below).
3. Monitor: When you select this check box, a message is placed in the diagnostics buffer if any of the following occur at the port:
   - A link cannot be established at the port
   - An established link fails
   - You select "TP 100 Mbps full-duplex" as the Transmission rate / duplex, and the CPU establishes a link using autonegotiation with the negotiated transmission rate not equal to 100 Mbps or the negotiated duplex equal to half-duplex.
4. Enable autonegotiation: Once you set the Transmission rate / duplex field to full-duplex at 100 Mbps, you can then disable autonegotiation. Deselect the "Enable autonegotiation" check box to disable autonegotiation.

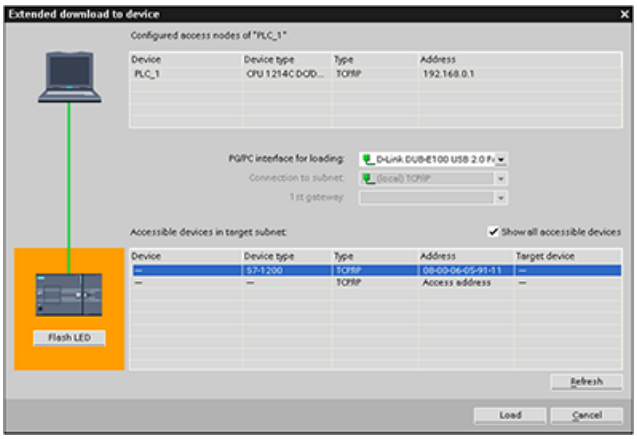
NOTE

If you disable autonegotiation, the CPU and the peer device do not negotiate the port's transmission rate and duplex.



12.6.4 Testing the PROFINET network

After completing the configuration, download the project (Page 189) to the CPU. All IP addresses are configured when you download the project.



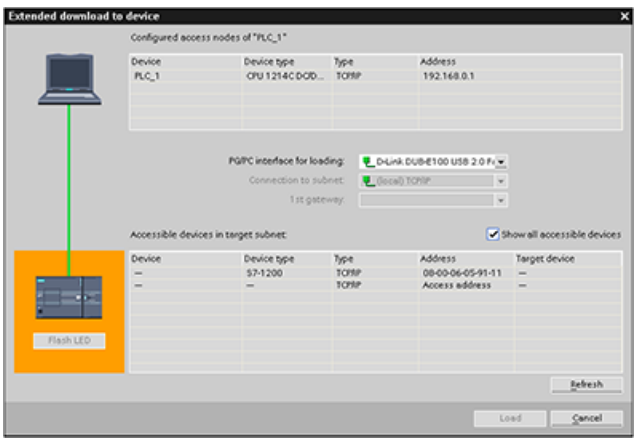
Assigning an IP address to a device online

The S7-1200 CPU does not have a pre-configured IP address. You must manually assign an IP address for the CPU:

- To assign an IP address to a device online, refer to "Device configuration: Assigning an IP address to a CPU online" (Page 537) for this step-by-step procedure.
- To assign an IP address in your project, you must configure the IP address in the Device configuration, save the configuration, and download it to the PLC. Refer to "Device configuration: Configuring an IP address for a CPU in your project" (Page 538) for more information.

Using the "Extended download to device" dialog to test for connected network devices

The S7-1200 CPU "Download to device" function and its "Extended download to device" dialog can show all accessible network devices and whether or not unique IP addresses have been assigned to all devices. To display all accessible and available devices with their assigned MAC or IP addresses, check the "Show all accessible devices" checkbox.



If the required network device is not in this list, communications to that device have been interrupted for some reason. The device and network must be investigated for hardware and/or configuration errors.

12.6.5 Locating the Ethernet (MAC) address on the CPU

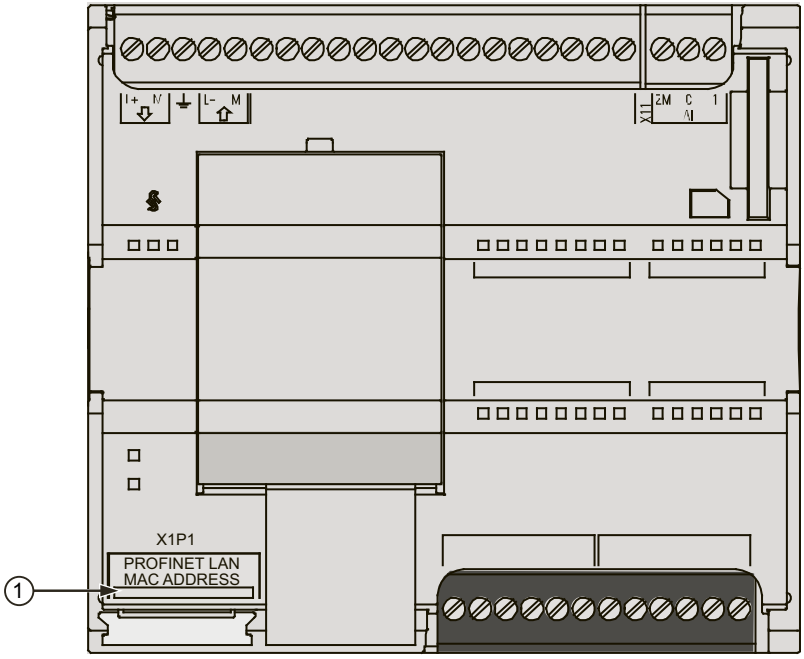
In PROFINET networking, a Media Access Control address (MAC address) is an identifier assigned to the network interface by the manufacturer for identification. A MAC address usually encodes the manufacturer's registered identification number.

The standard (IEEE 802.3) format for printing MAC addresses in human-friendly form is six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), in transmission order, (for example, 01-23-45-67-89-ab or 01:23:45:67:89:ab).

NOTE

Each CPU is loaded at the factory with a permanent, unique MAC address. You cannot change the MAC address of a CPU.

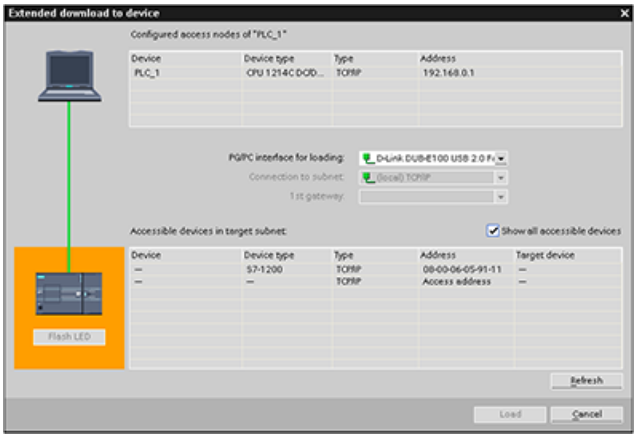
The MAC address is printed on the front, lower-left corner of the CPU. Note that you have to lift the lower door to see the MAC address information.



① MAC address

Figure

Initially, the CPU has no IP address, only a factory-installed MAC address. PROFINET communications requires that all devices be assigned a unique IP address.



Use the CPU "Download to device" function and the "Extended download to device" dialog to show all accessible network devices and ensure that unique IP addresses have been assigned to all devices. This dialog displays all accessible and available devices with their assigned MAC or IP addresses. MAC addresses are all-important in identifying devices that are missing the required unique IP address.

12.6.6 Configuring Network Time Protocol (NTP) synchronization

The Network Time Protocol (NTP) is widely used to synchronize the clocks of computer systems to Internet time servers. In NTP mode, the CPU sends time-of-day queries at regular intervals (in the client mode) to the NTP server in the subnet (LAN). Based on the replies from the server, the most reliable and most accurate time is calculated and the time of day on the station is synchronized.

WARNING

Risk of network attacks through Network Time Protocol (NTP) synchronization

If an attacker can access your networks through Network Time Protocol (NTP) synchronization, the attacker can possibly disrupt control of your process by shifting the CPU system time.

The S7-1200 CPU disables the NTP client feature by default. When you enable the NTP feature, then only the IP addresses that you configure can act as NTP servers. You must configure the NTP feature to allow CPU system time corrections from remote servers.

The S7-1200 CPU supports "time of day" interrupts and clock instructions that depend upon accurate CPU system time. If you configure NTP and accept time synchronization from a server, you must ensure that the server is a trusted source. Failure to do so can cause a security breach that allows an unknown user to disrupt control of your process by shifting the CPU system time.

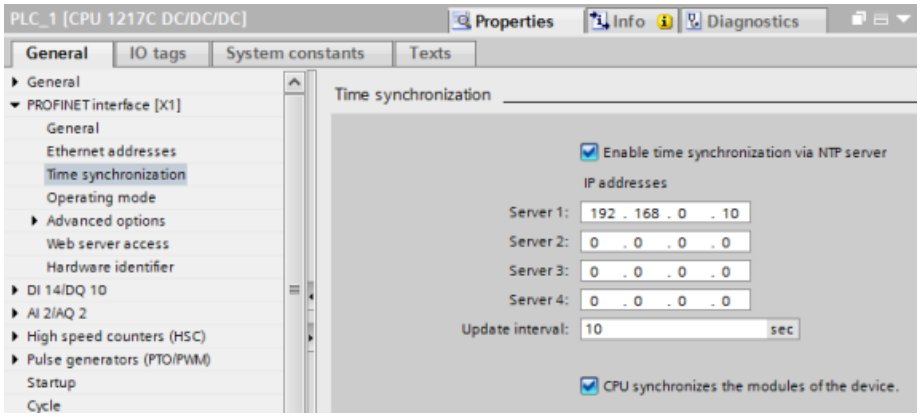
Disruptions to process control can possibly cause death, severe injury, or property damage.

For security information and recommendations, see the "Operational Guidelines" white paper on the Siemens Industrial Cybersecurity Web site (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

The advantage of this mode is that it allows the time to be synchronized across subnets. You configure the IP addresses of up to four NTP servers. The update interval defines the interval between the time queries (in seconds). The value of the interval ranges between 10 seconds and one day.

In NTP mode, the servers generally transfer UTC (Universal Time Coordinated), which corresponds to GMT (Greenwich Mean Time).

In the Properties window of the CPU's device configuration, select the "Time synchronization" configuration entry. STEP 7 displays the Time synchronization configuration dialog:



NOTE

The CPU receives all the IP addresses when you download the project.

Table 12-8 Parameters for time synchronization

Parameter	Definition
Enable time synchronization via NTP server	Select the checkbox to enable time synchronization via NTP server.
Server 1	Assigned IP Address for network time server 1
Server 2	Assigned IP Address for network time server 2
Server 3	Assigned IP Address for network time server 3
Server 4	Assigned IP Address for network time server 4
Time synchronization update interval	Interval value (sec)
CPU synchronizes the modules of the device.	Select the checkbox to synchronize the CP clock with the CPU clock.

12.6.7 PROFINET device start-up time, naming, and address assignment

PROFINET IO can extend the start-up time for your system (configurable time-out). More devices and slow devices impact the amount of time it takes to switch to RUN.

You can have a maximum of 16 PROFINET IO devices on your PROFINET network.

Each station (or IO device) starts up independently on start-up, and this affects the overall CPU start-up time. If you set the configurable time-out too low, there may not be a sufficient overall CPU start-up time for all stations to complete start-up. If this situation occurs, false station errors will result.

The default configurable time-out is 60,000 ms (1 minute). You can configure this in CPU Properties > Startup > Configuration time.

PROFINET device naming and addressing in STEP 7

All PROFINET devices **must** have a Device Name and an IP Address. Use STEP 7 to define the Device Names and to configure the IP addresses. Device names are downloaded to the IO devices using PROFINET DCP (Discovery and Configuration Protocol).

PROFINET address assignment at system start-up

The controller broadcasts the names of the devices to the network, and the devices respond with their MAC addresses. The controller then assigns an IP address to the device using PROFINET DCP protocol:

- If the MAC address has a configured IP address, then the station performs start-up.
- If the MAC address does not have a configured IP address, STEP 7 assigns the address that is configured in the project, and the station then performs start-up.
- If there is a problem with this process, a station error occurs and no start-up takes place. This situation causes the configurable time-out value to be exceeded.

12.6.8 Open user communication

12.6.8.1 Protocols

The integrated PROFINET port of the CPU supports multiple communications standards over an Ethernet network:

- Transport Control Protocol (TCP) (Page 547)
- ISO on TCP (Page 547)
- User Datagram Protocol (UDP) (Page 623)

Table 12-9 Protocols and communication instructions for each

Protocol	Usage examples	Entering data in the receive area	Communication instructions	Addressing type
TCP	CPU-to-CPU communication Transport of frames	Ad hoc mode	Only TRCV_C and TRCV	Assigns port numbers to the Local (active) and Partner (passive) devices
		Data reception with specified length	TSEND_C, TRCV_C, TCON, TDISCON, TSEND, and TRCV	
ISO on TCP	CPU-to-CPU communication Message fragmentation and reassembly	Ad hoc mode	Only TRCV_C and TRCV	Assigns TSAPs to the Local (active) and Partner (passive) devices
		Protocol-controlled	TSEND_C, TRCV_C, TCON, TDISCON, TSEND, and TRCV	

Protocol	Usage examples	Entering data in the receive area	Communication instructions	Addressing type
UDP	CPU-to-CPU communication User program communications	User Datagram Protocol	TUSEND and TURCV	Assigns port numbers to the Local (active) and Partner (passive) devices, but is not a dedicated connection
S7 communication	CPU-to-CPU communication Read/write data from/to a CPU	Data transmission and reception with specified length	GET and PUT	Assigns TSAPs to the Local (active) and Partner (passive) devices
PROFINET IO	CPU-to-PROFINET IO device communication	Data transmission and reception with specified length	Built-in	Built-in

12.6.8.2 TCP and ISO on TCP

Transport Control Protocol (TCP) is a standard protocol described by RFC 793: Transmission Control Protocol. The primary purpose of TCP is to provide reliable connection service between pairs of processes. This protocol has the following features:

- An efficient communications protocol since it is closely tied to the hardware
- Suitable for medium-sized to large data amounts (up to 8192 bytes)
- Provides considerably more facilities for applications, notably error recovery, flow control, and reliability
- A connection-oriented protocol
- Can be used very flexibly with third-party systems which exclusively support TCP
- Routing-capable
- Only static data lengths are applicable.
- Messages are acknowledged.
- Applications are addressed using port numbers.
- Most of the user application protocols, such as TELNET and FTP, use TCP.
- Programming effort is required for data management due to the SEND / RECEIVE programming interface.

International Standards Organization (ISO) on Transport Control Protocol (TCP) (RFC 1006) (ISO on TCP) is a mechanism that enables ISO applications to be ported to the TCP/IP network. This protocol has the following features:

- An efficient communications protocol closely tied to the hardware
- Suitable for medium-sized to large data amounts (up to 8192 bytes)
- In contrast to TCP, the messages feature an end-of-data identification and are message-oriented.
- Routing-capable; can be used in WAN
- Dynamic data lengths are possible.
- Programming effort is required for data management due to the SEND / RECEIVE programming interface.

Using Transport Service Access Points (TSAPs), TCP protocol allows multiple connections to a single IP address (up to 64K connections). With RFC 1006, TSAPs uniquely identify these communication end point connections to an IP address.

12.6.8.3 Ad hoc mode

Typically, TCP and ISO-on-TCP receive data packets of a specified length, ranging from 1 to 8192 bytes. However, the TRCV_C and TRCV communication instructions also provide an "ad hoc" communications mode that can receive data packets of a variable length from 1 to 1460 bytes.

NOTE

If you store the data in an "optimized" DB (symbolic only), you can receive data only in arrays of Byte, Char, USInt, and SInt data types.

To configure the TRCV_C or TRCV instruction for ad hoc mode, set the ADHOC instruction input parameter.

If you do not call the TRCV_C or TRCV instruction in ad hoc mode frequently, you could receive more than one packet in one call. For example: If you were to receive five 100-byte packets with one call, TCP would deliver these five packets as one 500-byte packet, while ISO-on-TCP would restructure the packets into five 100-byte packets.

12.6.8.4 Communication services and used port numbers

The CPU supports the protocols listed in the table below. For each protocol, the CPU assigns the address parameters, the respective communications layer as well as the communications role, and the communications direction.

This information makes it possible to match the security measures for protection of the automation system to the used protocols. Only the Ethernet or PROFINET networks have security measures.

The table below shows the different layers and protocols that the CPU uses:

Protocol	Port number	(2) Link layer (4) Transport layer	Function	Description
PROFINET protocols				
DCP (Discovery and Configuration Protocol)	Not relevant	(2) Ethernet II and IEEE 802.1Q and Ethertype 0x8892 (PROFINET)	Accessible devices PROFINET Discovery and configuration	PROFINET uses DCP to discover devices and provide basic settings. DCP uses the special multicast MAC address: 01-0E-CF-xx-xx-xx where xx-xx-xx = Organizationally Unique Identifier
LLDP (Link Layer Discovery Protocol)	Not relevant	(2) Ethernet II and IEEE 802.1Q and Ethertype 0x88CC (PROFINET)	PROFINET Link Layer Discovery protocol	PROFINET uses LLDP to discover and manage neighbor relationships between PROFINET devices. LLDP uses the special multicast MAC address: 01-80-C2-00-00-0E

12.6.8.5 Connection IDs for the Open user communication instructions

When you insert the TSEND_C, TRCV_C or TCON PROFINET instructions into your user program, STEP 7 creates an instance DB to configure the communications channel (or connection) between the devices. Use the "Properties" (Page 532) of the instruction to configure the parameters for the connection. Among the parameters is the connection ID for that connection.

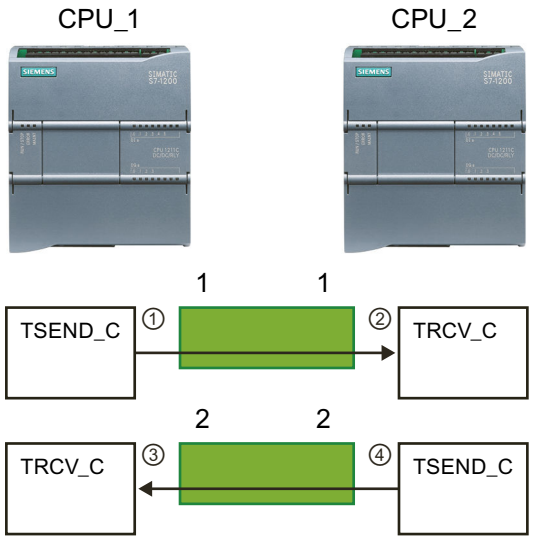
- The connection ID must be unique for the CPU. Each connection that you create must have a different DB and connection ID.
- Both the local CPU and the partner CPU can use the same connection ID number for the same connection, but the connection ID numbers are not required to match. The connection ID number is relevant only for the PROFINET instructions within the user program of the individual CPU.
- You can use any number for the connection ID of the CPU. However, configuring the connection IDs sequentially from "1" provides an easy method for tracking the number of connections in use for a specific CPU.

NOTE

Each TSEND_C, TRCV_C or TCON instruction in your user program creates a new connection. It is important to use the correct connection ID for each connection.

The following example shows the communication between two CPUs that utilize two separate connections for sending and receiving the data.

- The TSEND_C instruction in CPU_1 links to the TRCV_C in CPU_2 over the first connection ("connection ID 1" on both CPU_1 and CPU_2).
- The TRCV_C instruction in CPU_1 links to the TSEND_C in CPU_2 over the second connection ("connection ID 2" on both CPU_1 and CPU_2).



① TSEND_C on CPU_1 creates a connection and assigns a connection ID to that connection (connection ID 1 for CPU_1).

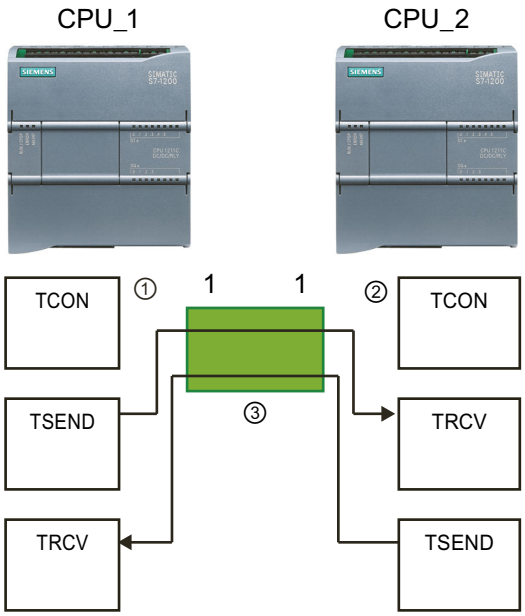
② TRCV_C on CPU_2 creates the connection for CPU_2 and assigns the connection ID (connection ID 1 for CPU_2).

③ TRCV_C on CPU_1 creates a second connection for CPU_1 and assigns a different connection ID for that connection (connection ID 2 for CPU_1).

④ TSEND_C on CPU_2 creates a second connection and assigns a different connection ID for that connection (connection ID 2 for CPU_2).

The following example shows the communication between two CPUs that utilize 1 connection for both sending and receiving the data.

- Each CPU uses a TCON instruction to configure the connection between the two CPUs.
- The TSEND instruction in CPU_1 links to the TRCV instruction in CPU_2 by using the connection ID ("connection ID 1") that was configured by the TCON instruction in CPU_1. The TRCV instruction in CPU_2 links to the TSEND instruction in CPU_1 by using the connection ID ("connection ID 1") that was configured by the TCON instruction in CPU_2.
- The TSEND instruction in CPU_2 links to the TRCV instruction in CPU_1 by using the connection ID ("connection ID 1") that was configured by the TCON instruction in CPU_2. The TRCV instruction in CPU_1 links to the TSEND instruction in CPU_2 by using the connection ID ("connection ID 1") that was configured by the TCON instruction in CPU_1.

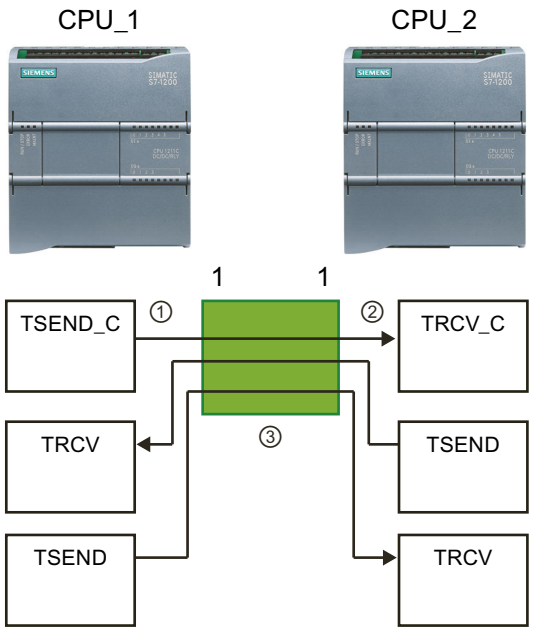


① TCON on CPU_1 creates a connection and assigns a connection ID for that connection on CPU_1 (ID=1).

② TCON on CPU_2 creates a connection and assigns a connection ID for that connection on CPU_2 (ID=1).

③ TSEND and TRCV on CPU_1 use the connection ID created by the TCON on CPU_1 (ID=1).
TSEND and TRCV on CPU_2 use the connection ID created by the TCON on CPU_2 (ID=1).

As shown in the following example, you can also use individual TSEND and TRCV instruction to communication over a connection created by a TSEND_C or TRCV_C instruction. The TSEND and TRCV instructions do not themselves create a new connection, so you must use the DB and connection ID that was created by a TSEND_C, TRCV_C or TCON instruction.



① TSEND_C on CPU_1 creates a connection and assigns a connection ID to that connection (ID=1).

② TRCV_C on CPU_2 creates a connection and assigns the connection ID to that connection on CPU_2 (ID=1).

③ TSEND and TRCV on CPU_1 use the connection ID created by the TSEND_C on CPU_1 (ID=1).
TSEND and TRCV on CPU_2 use the connection ID created by the TRCV_C on CPU_2 (ID=1).

12.6.8.6 Parameters for the PROFINET connection

The TSEND_C, TRCV_C and TCON instructions require connection-related parameters to connect to the partner device. The TCON_Param structure assigns these parameters for the TCP, ISO-on-TCP, and UDP protocols. Use the "Configuration" (Page 532) tab of the "Properties" of the instruction to specify these parameters. If the "Configuration" tab is not accessible, provide the TCON_Param structure in the instruction parameters.

Use the TCON_QDN and TCON_QDN_SEC structure to configure the communication connections for TCP and UDP via the fully qualified domain name. Use the TCON_QDN_SEC structure to configure the communication connections for TCP via the fully qualified domain name with secure communication.

TCON_Param

Table 12-10 Structure of the connection description (TCON_Param)

Byte	Parameter and data type		Description
0 to 1	block_length	UInt	Length: 64 bytes (fixed)
2 to 3	id	CONN_OUC (Word)	Reference to this connection: Range of values: 1 (default) to 4095. Specify the value of this parameter for the TSEND_C, TRCV_C or TCON instruction under ID.
4	connection_type	USInt	Connection type: • 17: TCP (default) • 18: ISO-on-TCP • 19: UDP
5	active_est	Bool	ID for the type of connection: • TCP and ISO-on-TCP: – FALSE: Passive connection – TRUE: Active connection (default) • UDP: FALSE
6	local_device_id	USInt	ID for the local PROFINET or Industrial Ethernet interface: 1 (default)
7	local_tsap_id_len	USInt	Length of parameter local_tsap_id used, in bytes; possible values: • TCP: 0 (active, default) or 2 (passive) • ISO-on-TCP: 2 to 16 • UDP: 2
8	rem_subnet_id_len	USInt	This parameter is not used.
9	rem_staddr_len	USInt	Length of address of partner end point, in bytes: • 0: unspecified (parameter rem_staddr is irrelevant) • 4 (default): Valid IP address in parameter rem_staddr (only for TCP and ISO-on-TCP)
10	rem_tsap_id_len	USInt	Length of parameter rem_tsap_id used, in bytes; possible values: • TCP: 0 (passive) or 2 (active, default) • ISO-on-TCP: 2 to 16 • UDP: 0
11	next_staddr_len	USInt	This parameter is not used.
12 to 27	local_tsap_id	Array [1..16] of Byte	Local address component of connection: • TCP and ISO-on-TCP: local port no. (possible values: 1 to 49151; recommended values: 2000...5000): – local_tsap_id[1] = high byte of port number in hexadecimal notation; – local_tsap_id[2] = low byte of port number in hexadecimal notation; – local_tsap_id[3-16] = irrelevant • ISO-on-TCP: local TSAP-ID: – local_tsap_id[1] = B#16#E0; – local_tsap_id[2] = rack and slot of local end points (bits 0 to 4: slot number, bits 5 to 7: rack number); – local_tsap_id[3-16] = TSAP extension, optional • UDP: This parameter is not used. Note: Make sure that every value of local_tsap_id is unique within the CPU.
28 to 33	rem_subnet_id	Array [1..6] of USInt	This parameter is not used.

Byte	Parameter and data type		Description
34 to 39	rem_staddr	Array [1..6] of USInt	TCP and ISO-on-TCP only: IP address of the partner end point. (Not relevant for passive connections.) For example, IP address 192.168.002.003 is stored in the following elements of the array: rem_staddr[1] = 192 rem_staddr[2] = 168 rem_staddr[3] = 002 rem_staddr[4] = 003 rem_staddr[5-6]= irrelevant
40 to 55	rem_tsap_id	Array [1..16] of Byte	Partner address component of connection • TCP: partner port number. Range: 1 to 49151; Recommended values: 2000 to 5000): – rem_tsap_id[1] = high byte of the port number in hexadecimal notation – rem_tsap_id[2] = low byte of the port number in hexadecimal notation; – rem_tsap_id[3-16] = irrelevant • ISO-on-TCP: partner TSAP-ID: – rem_tsap_id[1] = B#16#E0 – rem_tsap_id[2] = rack and slot of partner end point (bits 0 to 4: Slot number, bits 5 to 7: rack number) – rem_tsap_id[3-16] = TSAP extension, optional • UDP: This parameter is not used.
56 to 61	next_staddr	Array [1..6] of Byte	This parameter is not used.
62 to 63	spare	Word	Reserved: W#16#0000

TCON_IP_V4

Table 12-11 Structure of the connection description (TCON_IP_V4): For use with TCP

Byte	Parameter and data type		Description
0 to 1	InterfaceId	HW_ANY	HW-identifier of the IE-interface submodule
2 to 3	ID	CONN_OUC (Word)	Reference to this connection: Range of values: 1 (default) to 4095. Specify the value of this parameter for the TSEND_C, TRCV_C, or TCON instruction under ID.
4	ConnectionType	Byte	Connection type: • 11: TCP/IP (default) • 17: TCP/IP (This connection type is included for legacy reasons. It is recommended that you use "11: TCP/IP (default)".) • 19: UDP
5	ActiveEstablished	Bool	Active/passive connection establishment: • TRUE: Active connection (default) • FALSE: Passive connection
	V4 IP address		
6	ADDR[1]	Byte	Octet 1
7	ADDR[1]	Byte	Octet 2
8	ADDR[1]	Byte	Octet 3

Byte	Parameter and data type		Description
9	ADDR[1]	Byte	Octet 4
10 to 11	RemotePort	UInt	Remote UDP/TCP port number
12 to 13	LocalPort	UInt	Local UDP/TCP port number

TCON_IP_V4_SEC

Table 12-12 Structure of the connection description (TCON_IP_V4_SEC): For use with TCP

Byte	Parameter and data type		Description
0 to 15	ConnPara	TCON_IP_v4	SDT for the connection parameters Information about the interface_id: • If you leave the interface_id at the preset value of 0, the operating system of the CPU evaluates the remote IP address and the IP routes existing locally and then specifies an Industrial Ethernet interface of the CPU for establishing the secure OUC connection. In this case, the diagnostics data is always assigned to the first Industrial Ethernet interface of the CPU. • If you specify the hardware identifier of an Industrial Ethernet interface of the CPU or of a CP as interface_id, the secure OUC connection is established using the associated Industrial Ethernet interface.
16	ActivateSecure-Conn	Bool	Activation of Secure Communication for this connection If this parameter has the value FALSE (default), the subsequent security parameters are irrelevant, meaning that the connection is non-secure. You can set up a non-secure TCP or UDP connection in this case.
17	TLSServerReq-ClientCert	Bool	Only for the server side: Request for an X.509-V3 certificate from the TLS (Page 529) client. FALSE (default)
18 to 19	ExtTLSCapabilities	Word	• Bit 0: Only for the client side. A set bit means that the client validates the alternative name of the certificate subject (subjectAlternateName) in the X.509-V3 certificate of the server to check the identity of the server. The certificates are checked when the connection is established. 16#0 (default) • Bit 1 to 15: Reserved for future upgrades
20 to 23	TLSServerCertRef	UDInt	• Server side: ID of its own X.509-V3 certificate (Page 529) • Client side: ID of the X.509-V3 certificate (usually a CA certificate) that is used by the TLS client to validate the TLS server authentication. If this parameter is 0, the TLS client uses all the (CA) certificates currently loaded in the client certificate store to validate the server authentication. 0 (default)
24 to 27	TLSClientCertRef	UDInt	• Client side: ID of its own X.509-V3 certificate (Page 529) • Server side: ID of the X.509-V3 certificate (or a group of X.509-V3 certificates) that is used by the TLS server to validate the TLS client. If this parameter is 0, the TLS server uses all (CA) certificates currently loaded in the server certificate store to validate the client authentication. 0 (default)

The CONNECT connection parameter of the instance DBs for the TCON, TSEND_C, and TRCV_C instructions contains a reference to the data block used.

NOTE

You can make non-secure TCP or UDP connections over IPv4.

You can also use SDT TCON_IP_V4_SEC for a non-secure TCP or UDP connection over IPv4.

TCON_IP_RFC

Table 12-13 Structure of the connection description (TCON_IP_RFC): For use with ISO on TCP

Byte	Parameter and data type		Description
0 to 1	InterfaceId	HW_ANY	HW-identifier of the IE-interface submodule
2 to 3	ID	CONN_OUC (Word)	Reference to this connection: Range of values: 1 (default) to 4095. Specify the value of this parameter for the TSEND_C, TRCV_C, or TCON instruction under ID.
4	ConnectionType	Byte	Connection type: • 12: ISO-on-TCP (default) • 17: ISO-on-TCP (This connection type is included for legacy reasons. It is recommended that you use "12: ISO-on-TCP (default)".)
5	ActiveEstablished	Bool	Active/passive connection establishment: • TRUE: Active connection (default) • FALSE: Passive connection
6 to 7	Spare		Not used
	V4 IP address		
8	ADDR[1]	Byte	Octet 1
9	ADDR[1]	Byte	Octet 2
10	ADDR[1]	Byte	Octet 3
11	ADDR[1]	Byte	Octet 4
	Remote transport selector		
12 to 13	TSelLength	UInt	Length of TSelector
14 to 45	TSel	array [1..32] of Byte	Character array for TSAP name
	Local transport selector		
46 to 47	TSelLength	UInt	Length of TSelector
48 to 79	TSel	array [1..32] of Byte	Character array for TSAP name

TCON_QDN

Table 12-14 Structure of the connection description in accordance with TCON_QDN

Byte	Parameter and data type		Description
0 to 1	InterfaceId	HW_ANY	S7-1200-CPUs as of firmware V4.x: • InterfaceId of a plugged CP: – With CPs of S7-1200 – With CPs of ET 200SP
2 to 3	ID	CONN_O UC	Reference to this connection (value range: 1 to 4095). Specify the value of this parameter for the TCON instruction under ID.
4	ConnectionType	BYTE	Connection type: • 11: TCP (11 dec = 0x0B hex) • 19: UDP (19 dec = 0x13 hex)
5	ActiveEstablished	BOOL	Identifier for the type of connection establishment: • FALSE: Passive connection establishment • TRUE: Active connection establishment
6 to 261	RemoteQDN	Array of STRING [1..254]	Fully qualified domain name of the partner end point, which must finish with "." Please note that in a SIMATIC network, the name including the concluding dot must not exceed 254 characters.
262 to 263	RemotePort	UINT	Port address of the remote connection partner
264 to 265	LocalPort	UINT	Port address of the local connection partner

TCON_QDN_SEC

Table 12-15 Structure of the connection description in accordance with TCON_QDN_SEC

Byte	Parameter and data type		Description
0 to 271	ConnPara	TCON_QDN	Connection parameter
272	ActivateSecureConn	BOOL	Activation of secure communication for this connection. If this parameter has the value FALSE, the subsequent security parameters are irrelevant. You can set up a non-secure TCP or UDP connection in this case.
273	TLSServerReqClientCert	BOOL	Only for the server side: Request for an X.509-V3 certificate from the TLS client
274 to 275	ExtTLSCapabilities	WORD	• Bit 0: Only for the client side. A set bit means that the client validates the subjectAlternate- Name in the X.509-V3 certificate of the server to check the identity of the server. The certificates are checked when the connection is established. • Bit 1 to 15: reserved for future upgrades
276 to 279	TLSServerCertRef	UDINT	• Server side: ID of its own X.509-V3 certificate (Page 529) • Client side: ID of the X.509-V3 certificate (usually a CA certificate) that is used by the TLS client to validate the TLS server authentication. If this parameter is 0, the TLS client uses all (CA) certificates currently loaded in the client certificate store to validate the server authentication.

Byte	Parameter and data type		Description
280 to 283	TLSClientCertRef	UDINT	• Client side: ID of its own X.509-V3 certificate (Page 529) • Server side: ID of the X.509-V3 certificate (or a group of X.509-V3 certificates) that is used by the TLS server to validate TLS client authentication. If this parameter is 0, the TLS server uses all (CA) certificates currently loaded in the server certificate store to validate the client authentication.

12.6.8.7 Supported TLS versions

TLS is Transport Layer Security in the application layer of data communications. TLS increases security and privacy in communication between the S7-1200 CPU and other devices. The TLS version depends on the S7-1200 CPU firmware version and the version of the CPU in the Device Configuration of your STEP 7 project.

To find the CPU version in your STEP 7 project, follow these steps:

1. Click the CPU in the Device configuration.
2. View the General section of the Properties tab in the Inspector window.
3. Note the Firmware version in the Catalog information section.

To use the highest version of TLS, configure the CPU version in STEP 7 to be the actual firmware version of your CPU. The open user communication partner can then use the highest supported TLS version for maximum security.

TLS version support based on CPU and STEP 7 project firmware version

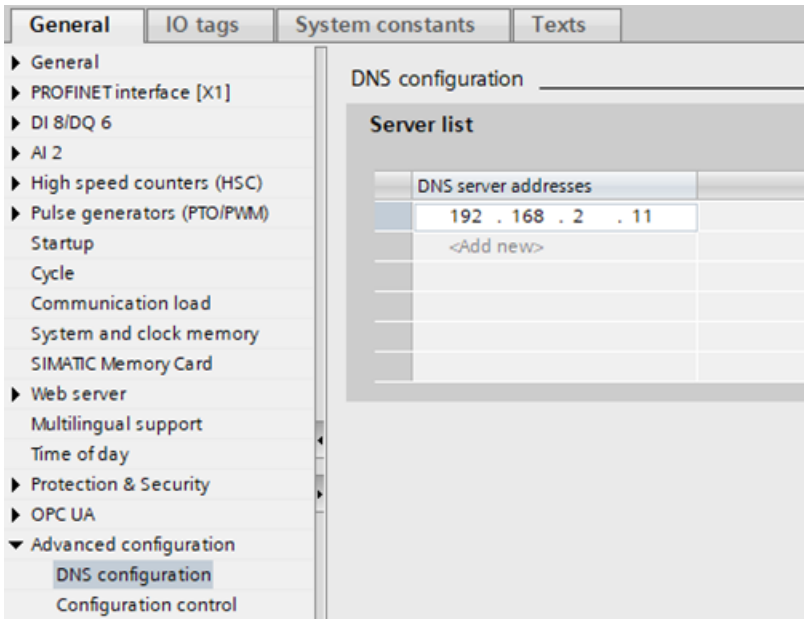
Firmware version configured in the STEP 7 project	Supported TLS version
V4.5 - V4.7	TLS 1.2, TLS 1.3
V4.3 - V4.4	TLS 1.2

12.6.8.8 Configuring DNS

To use DNS, you must have at least one DNS server in your network, and you must configure at least one DNS server for the S7-1200 CPU.

You configure a DNS server using the following steps:

1. From the Device view for your S7-1200 CPU, navigate to "Properties > General".
2. Click on "DNS configuration" to display the configuration page.

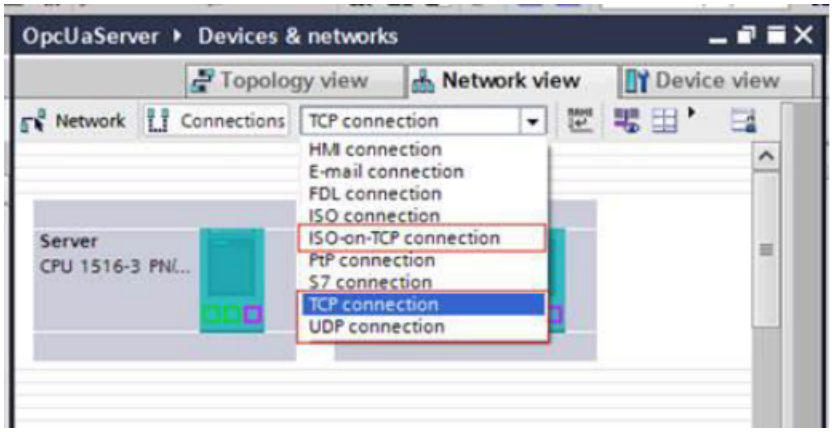


3. In the Server list table, the first row under the DNS server addresses, click on "<Add new>" and enter the IP address of your DNS server.

12.6.8.9 Configuring an OUC connection in the TIA Portal

In the TIA Portal, you can select the following Open User Communications connections (as shown below) for drawing to or from the S7-1200 or S7-1500 CPUs.

- Iso-on-TCP connection
- TCP connection
- UDP connection



When you draw a line between devices, a connection is configured to compile and download to the device. This connection configuration allows the S7-1200 firmware to establish a connection with the partner when the CPU goes to RUN. There is no need to run a TCON instruction with a configured connection. Also, there is no need for a T_DISCON instruction for a configured connection.

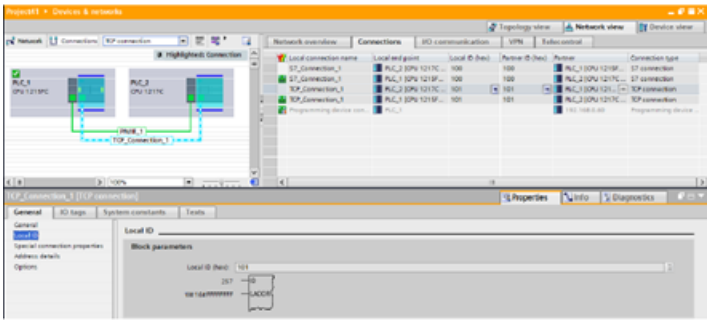
To draw a line for these connections, both network interfaces for the CPU (or CP) should be on the same subnet. The TIA portal does not limit you from drawing a connection to devices on different networks. However, the TIA Portal will generate an error when compiling or downloading to the device.

You can now draw an OUC connection between the S7-1200 or S7-1500 CPUs, download the configuration, and automatically establish the connection between the CPUs (if the connection was physically possible).

Configuration options for configured OUC connections

You configure the following properties of the connection as shown below:

- Connection ID
- Name of the Connection
- Which partner is the Active establishment
- Port details in the property menu of the Network view by selecting a connection end

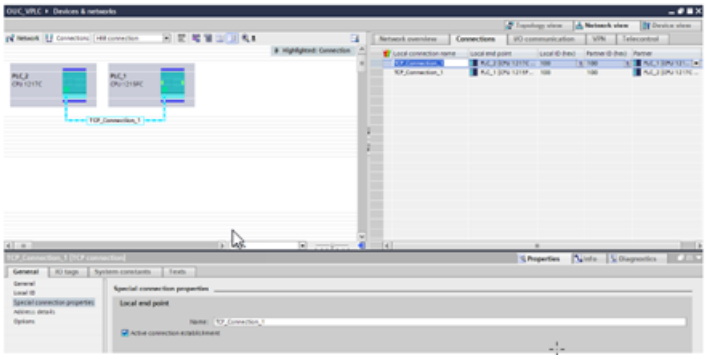


When you draw an OUC connection in the TIA Portal, a "Local ID" and "Partner ID" is assigned in the valid range for an OUC connection ID. You can change the value assigned in the connections table or in the Local ID. The value entered in each ID must be within the range defined by the TBlock instructions (See TSEND).

NOTE

Assigned range for the connection ID

The assigned range for the connection ID is in the same range as allocated for an S7 connection. If an S7 Connection ID is supplied to a TSEND, it would result in an error from the instruction. The error will be 16#80A1 as there will be no OUC connection established.



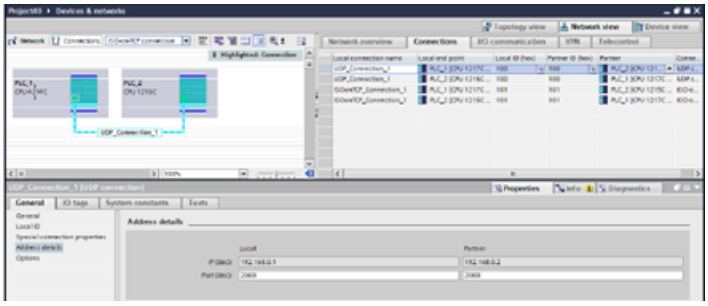
In the "Special connection properties" menu, the "active connection establishment" field defines the device which sends connection messages out upon downloading of the configuration to the CPUs. If the "active connection establishment" checkbox is not checked, the downloaded device waits for connection messages from its partner. TIA portal automatically updates the partner when the "Active connection establishment" checkbox is clicked. Only one side of the connection can be set as active.

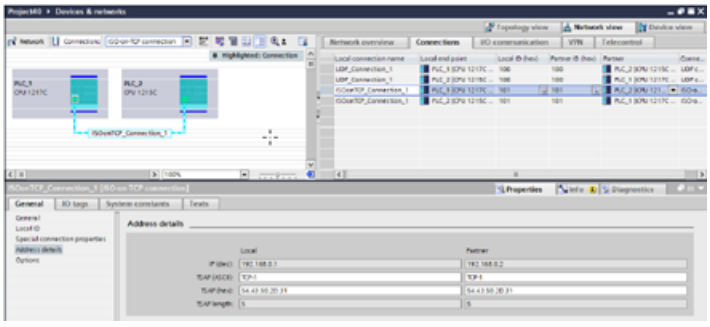
NOTE

UDP connections

For UDP connections, the "active connection establishment" is not present.

The "address details" property menu shows configuration of the addresses that will be used for the communication of the connection for TCP and Iso-on-TCP types. When using TUSEND and TURCV on a UDP connection, the address for communication is overridden by a parameter on the instructions. Additionally, for Iso-on-TCP connection types, the TSAPs can be modified in the "address details" property menu as shown in the 2nd screen below.





Operation of existing TBlock instructions with configured connections

Once a connection is established, a configured connection operates in the same manner as a programmed connection. Other OUC instructions operate in the same manner as if operated

on a programmed connection. Below is a description for OUC instructions and they operate with configured connections.

OUC instruction	Description with configured connection
TSEND_C (Page 562)	Must have a TCON_configured SDT passed to the Connect parameter. If a configured connection is used, then the ID field of the TCON_Configured should be set to the Configured Connection ID and the Connection Type field should be set to 254. When using a configured connection, the connection mechanism in the instruction should be skipped as the connection is already established.
TRCV_C (Page 562)	Must have a TCON_Configured SDT passed to the Connect parameter. If a configured connection is used, then the ID field of the TCON_Configured should be set to the Configured Connection ID and the Connection Type field should be set to 254. When using a configured connection, the connection mechanism in the instruction should be skipped as the connection is already established.
TMAIL_C (Page 604)	Does not work with a configured connection
TCON (Page 577)	Gives an error (0x8085) if the Connection ID for a configured connection is provided because the connection is already open
TDISCON (Page 577)	Gives an error (0x80A3)
TCONSettings (Page 586)	Gives an error (0x8085) TCONSettings cannot use configured connections. The TCONSettings write function returns an error. The TCONSettings read operation returns FALSE for the graceful shutdown (Page 586) option.
TSEND (Page 577)	Operates the same
TRCV (Page 577)	Operates the same
TUSEND (Page 623)	Operates the same
TURCV (Page 623)	Operates the same
T_RESET (Page 599)	Operates the same. A disconnect occurs on the connection and a reconnect occurs. The SendBytes and Received bytes will be reset to 0.
T_DIAG (Page 601)	Operates the same. The "Kind" field of the TDIAG_Status variant should indicate a configured connection.
T_CONFIG (Page 629)	Operates the same. (Not directly OUC protocol communication related.)
MB_CLIENT (Page 906)	Must have a TCON_Configured SDT passed to the Connect parameter. If a configured connection is used, then the ID field of the TCON_Configured should be set to the Configured Connection ID and the Connection Type field should be set to 254. When using a configured connection, the connection mechanism in the instruction should be skipped as the connection is already established.
MB_SERVER (Page 914)	Must have a TCON_Configured SDT passed to the Connect parameter. If a configured connection is used, then the ID field of the TCON_Configured should be set to the Configured Connection ID and the Connection Type field should be set to 254. When using a configured connection, the connection mechanism in the instruction should be skipped as the connection is already established.

12.6.8.10 TSEND_C and TRCV_C instructions

The S7-1200 supports two sets of TSEND_C and TRCV_C instructions:

- TSEND_C and TRCV_C instructions (Page 562): These TSEND_C and TRCV_C instructions provide all of the functionality of the legacy instructions, plus the ability to use connection parameters with structures according to TCON_IP_V4, TCON_IP_V4_SEC, TCON_IP_RFC, TCON_QDN, and TCON_QDN_SEC.
- Legacy TSEND_C and TRCV_C instructions (Page 571): These TSEND_C and TRCV_C instructions existed prior to version V4.1 of the S7-1200 and only work with connection parameters with structures according to TCON_Param.

STEP 7 provides different versions of the TSEND_C and TRCV_C instructions. For information on instruction versions, refer to Use Instruction versions (https://support.industry.siemens.com/cs/ww/en/view/109798671/113722878475) in the STEP 7 Information System.

TSEND_C and TRCV_C (Send and receive data using Ethernet)

The TSEND_C instruction combines the functions of the TCON, TDISCON and TSEND instructions. The TRCV_C instruction combines the functions of the TCON, TDISCON, and TRCV instructions. (Refer to "TCON, TDISCON, TSEND, AND TRCV (Page 578)" for more information on these instructions.)

The minimum size of data that you can transmit (TSEND_C) or receive (TRCV_C) is one byte; the maximum size is 8192 bytes. TSEND_C does not support the transmission of data from Boolean locations, and TRCV_C will not receive data into Boolean locations. For information on transferring data with these instructions, see the section on data consistency (Page 178).

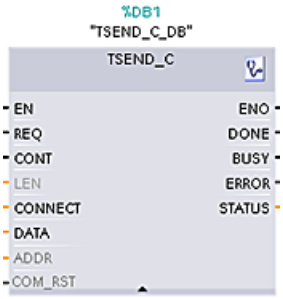
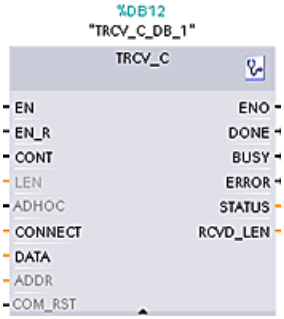
NOTE

Initializing the communication parameters

After you insert the TSEND_C or TRCV_C instruction (Page 549), use the "Properties" of the instruction (Page 532) to configure the communication parameters (Page 551). As you enter the parameters for the communication partners in the inspector window, STEP 7 enters the corresponding data in the DB for the instruction.

If you want to use a multi-instance DB, you must configure the DB on both CPUs.

Table 12-16 TSEND_C and TRCV_C instructions

LAD / FBD	SCL	Description
	**"TSEND_C_DB"(req:=_bool_in_, cont:=_bool_in_, len:=_uint_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, connect:=_struct_inout_, data:=_variant_inout_, com_rst:=_bool_inout_);**	TSEND_C establishes a TCP or ISO on TCP communication connection to a partner station, sends data, and can terminate the connection. After the connection is set up and established, it is automatically maintained and monitored by the CPU.
	**"TRCV_C_DB"(en_r:=_bool_in_, cont:=_bool_in_, len:=_uint_in_, adhoc:=_bool_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, rcvd_len=>_uint_out_, connect:=_struct_inout_, data:=_variant_inout_, com_rst:=_bool_inout_);**	TRCV_C establishes a TCP or ISO on TCP communication connection to a partner CPU, receives data, and can terminate the connection. After the connection is set up and established, it is automatically maintained and monitored by the CPU.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 12-17 TSEND_C and TRCV_C data types for the parameters

Parameter and type		Data type	Description
REQ (TSEND_C)	IN	Bool	Starts the send job on a rising edge
EN_R (TRCV_C)	IN	Bool	Receive enable
CONT	IN	Bool	Controls the communication connection: • 0: Disconnect the communication connection after data is sent. • 1: Establish and maintain the communication connection. When sending data (TSEND_C) (rising edge at the REQ parameter) or receiving data (TRCV_C) (rising edge at the EN_R parameter), the CONT parameter must have the value TRUE in order to establish or maintain a connection.
LEN	IN	UDInt	Optional parameter (hidden) Maximum number of bytes to be sent (TSEND_C) or received (TRCV_C) with the job. If you use purely symbolic values at the DATA parameter, the LEN parameter must have the value "0".
ADHOC (TRCV_C)	IN	Bool	Optional parameter (hidden) Ad hoc mode request for connection type TCP.

Parameter and type		Data type	Description
CONNECT	IN_OUT	Variant	Pointer to the connection description: • For TCP or UDP, use the structure TCON_IP_v4 or TCON_QDN. For a description, refer to: "Parameters for the PROFINET connection (Page 551)". • For TCP using secure communication, use the structure TCON_IP_V4_SEC or TCON_QDN_SEC. For a description, refer to: "Parameters for the PROFINET connection (Page 551)". • For ISO-on-TCP, use the structure TCON_IP_RFC. For a description, refer to: "Parameters for the PROFINET connection (Page 551)". • For ISO connections of the CP 1543-1 / CP 1545-1, use the structure TCON_ISOnative. For a description, refer to TIA Portal Online Help: "Structure of the connection description according to TCON_ISOnative". • For connections to SMS clients, use the TCON_PHONE system data type. For a description, refer to TIA Portal Online Help: "Connection parameters to TCON_Phone".
DATA	IN_OUT	Variant	Pointer to the send area containing: • Address and length of data to be sent (TSEND_C) • Address and maximum length of received data (TRCV_C)
ADDR	IN_OUT	Variant	Optional parameter (hidden) Pointer to the address of the recipient with the connection type UDP. The address information is mapped in the structure TADDR_Param ###.
COM_RST	IN_OUT	Bool	Optional parameter (hidden) Restarts the instruction: • 0: Irrelevant • 1: Completely restarts the instruction; the existing connection is either terminated or reset and established again in accordance with CONT. The COM_RST parameter is reset after evaluation by the TSEND_C or TRCV_C instruction and should not, therefore, be switched statically.
DONE	OUT	Bool	Status parameter with the following values: • 0: Send job not yet started or is still executing. • 1: Send job executed without errors. This state is only displayed for one cycle.
BUSY	OUT	Bool	Status parameter with the following values: • 0: Send job not yet started or already completed. • 1: Send job not yet completed. A new send job cannot be started.
ERROR	OUT	Bool	Status parameters with the following values: • 0: No error • 1: Error occurred during connection establishment, data transmission, or connection termination.
STATUS	OUT	Word	Status of instruction (see the ERROR and STATUS parameters description).
RCVD_LEN (TRCV_C)	OUT	Int	Amount of data actually received (in bytes).

NOTE

The TSEND_C instruction requires a low-to-high transition at the REQ input parameter to start a send job. The BUSY parameter is then set to 1 during processing. Completion of the send job is indicated by either the DONE or ERROR parameters being set to 1 for one scan. During this time, any low-to-high transition at the REQ input parameter is ignored.

NOTE

The default setting of the LEN parameter (LEN = 0) uses the DATA parameter to determine the length of the data being transmitted. It is recommended that the data transmitted by the TSEND_C instruction be the same size as the DATA parameter of the TRCV_C instruction.

If using the default setting of the LEN parameter and it is necessary to send the data in segments smaller than the DATA parameter size, the following applies. If the size of the data transmitted from TSEND_C does not equal the TRCV_C DATA parameter size, TRCV_C remains in a busy status (status code: 7006) until the overall size of the data transmitted from TSEND_C equals the TRCV_C DATA parameter size.

The TRCV_C DATA parameter buffer does not display the new data received until the data size equals the DATA parameter buffer size.

TSEND_C operations

The TSEND_C instruction is executed asynchronously and implements the following functions in sequence:

1. Setting up and establishing a communications connection:
   TSEND_C sets up a communication connection and establishes this connection if a rising edge is detected at the REQ parameter and no communication connection is in place yet. Once the connection has been set up and established, it is automatically maintained and monitored by the CPU. The connection description specified at the CONNECT parameter is used to set up the communications connection.
   An existing connection is terminated and the connection which has been set up is removed when the CPU goes into STOP mode. To set up and establish the connection again, you must execute TSEND_C again. For information on the number of possible communication connections, refer to the technical specifications for your CPU.
2. Sending data via an existing communications connection:
   The send job is executed when a rising edge is detected at the REQ parameter. As described above, the communications connection is established first. You specify the send area with the DATA parameter. This includes the address and the length of the data to be sent. Do not use a data area with the data type BOOL or Array of BOOL at the DATA parameter. With the LEN parameter, you specify the maximum number of bytes sent with a send job. If using a symbolic name at the DATA parameter, the LEN parameter should have the value "0".
   The data to be sent must not be edited until the send job is completed.
3. Terminating the communications connection:
   The communications connection is terminated after the data has been sent if the CONT parameter had the value "0" at the time of the rising edge at the REQ parameter. Otherwise, the communications connection will be maintained.

If the send job executes successfully, the DONE parameter is set to "1". The communications connection may be terminated before this (see the above description of the dependency on

the CONT parameter). Signal state "1" at the DONE parameter is not confirmation that the data sent has already been read by the communications partner.

TSEND_C is reset when the COM_RST parameter is set to "1". Data loss may occur if data is being transferred at this point.

The following scenarios are possible depending on the CONT parameter:

- CONT = "0":
  An existing communications connection is established.
- CONT = "1" and a communications connection was established:
  An existing communications connection is reset and established again.
- CONT = "1" and no communications connection was established.
  No communications connection is established.

The COM_RST parameter is reset following evaluation by the instruction T_SEND. To enable TSEND_C again after the execution (DONE = 1), call the instruction once with REQ = 0

TRCV_C operations

The TRCV_C instruction is executed asynchronously and implements the following functions in sequence:

1. Setting up and establishing a communications connection:
   TRCV_C sets up a communication connection and establishes this connection if the EN_R parameter = "1" and there is no communication connection. Once the connection has been set up and established, it is automatically maintained and monitored by the CPU.
   The connection description specified at the CONNECT parameter is used to set up the communications connection. The following connection types can be used:
   – TCON_Param structure for the TCP, ISO-on-TCP, and UDP protocols
   – TCP / UDP: Connection description via the structure TCON_IP_V4 at the parameter CONNECT
   – ISO-on-TCP: Connection description via the structure TCON_IP_RFC at the parameter CONNECT
   – TCP: Connection description using the structure TCON_IP_V4_SEC at the parameter CONNECT
   – TCP: Connection description using the structures TCON_QDN and TCON_QDN_SEC.
   An existing connection is terminated and the connection which has been set up is removed when the CPU goes into STOP mode. To set up and establish the connection again, you must execute TRCV_C again with EN_R = "1".
   If EN_R is set to "0" before the communications connection has been established, the connection will be established and remain in place even if CONT = "0". However, no data will be received (DONE will remain "0").
   For information on the number of possible communication connections, please refer to the technical specifications for your CPU.
2. Receiving data via an existing communications connection:
   Receipt of data is enabled when the EN_R parameter is set to the value "1". As described above, the communications connection is established first. The received data is entered in a receive area. You specify the length of the receive area either with the LEN parameter (if LEN <> 0) or with the length information of the DATA parameter (if LEN = 0), depending on the protocol variant being used. If you use purely symbolic values at the DATA parameter, the LEN parameter must have the value "0".

If EN_R is set to "0" before data is received for the first time, the communication connection will remain in place even if CONT = 0. However, no data will be received (DONE will remain "0").

3. Terminating the communications connection:
   The communications connection is terminated after data has been received if the CONT parameter had the value "0" when connection established was started. Otherwise, the communications connection will be maintained.

If the receive job executes successfully, the DONE parameter is set to "1". The communications connection may be terminated before this (see the above description of the dependency on the CONT parameter).

TRCV_C is reset when the COM_RST parameter is set. If data is being received when it executes again, this can lead to a loss of data. The following scenarios are possible depending on the CONT parameter:

- CONT = "0":
  An existing communications connection is established.
- CONT = "1" and a communications connection was established:
  An existing communications connection is reset and established again.
- CONT = "1" and no communications connection was established:
  No communications connection is established.

The COM_RST parameter is reset following evaluation by the instruction TRCV_".

TRCV_C handles the same receive modes as the TRCV instruction. The following table shows how data is entered in the receive area:

Protocol variant	Availability of data in the receive area	Connection_type parameter of the connection description	LEN parameter	RCVD_LEN parameter
TCP (Ad hoc mode)	The data is immediately available.	B#16#11	Selected with the TRCV_C instruction ADHOC input	1 to 1460
TCP (data receipt with specified length)	The data is available as soon as the data length specified at the LEN parameter has been fully received.	B#16#11	1 to 8192	Identical to the value at the LEN parameter
ISO on TCP (protocol-controlled data transfer)	The data is available as soon as the data length specified at the LEN parameter has been fully received.	B#16#12	1 to 8192	Identical to the value at the LEN parameter

NOTE

Ad hoc mode

The "ad hoc mode" is only available with the TCP protocol variant. To configure the TRCV_C instruction for ad hoc mode, set the ADHOC instruction input parameter. The length of the receive area is defined by the pointer at the DATA parameter. The data length actually received is output at the RCVD_LEN parameter. A maximum of 1460 bytes can be received.

NOTE

Importing of S7-300/400 STEP 7 projects containing "ad hoc mode" into the S7-1200

In S7-300/400 STEP 7 projects, "ad hoc mode" is selected by assigning "0" to the LEN parameter. In the S7-1200, you configure the TRCV_C instruction for ad hoc mode by setting the ADHOC instruction input parameter..

If you import an S7-300/400 STEP 7 project containing "ad hoc mode" into the S7-1200, you must change the LEN parameter to "65535".

NOTE

TCP (data receipt with specified length)

You use the value of the LEN parameter to specify the length for the data receipt. The data specified at the DATA parameter is available in the receive area as soon as the length specified at the LEN parameter has been completely received.

NOTE

ISO on TCP (protocol-controlled data transfer)

With the ISO on TCP protocol variant, data is transferred protocol-controlled. The receive area is defined by the LEN and DATA parameters.

BUSY, DONE, and ERROR parameters

NOTE

Due to the asynchronous processing of TSEND_C, you must keep the data in the sender area consistent until the DONE parameter or the ERROR parameter assumes the value TRUE.

For TSEND_C, a TRUE state at the parameter DONE means that the data was sent successfully. It does not mean that the connection partner CPU actually read the receive buffer.

Due to the asynchronous processing of TRCV_C, the data in the receiver area are only consistent when parameter DONE = 1.

Table 12-18 TSEND_C and TRCV_C instructions BUSY, DONE, and ERROR parameters

BUSY	DONE	ERROR	Description
1	0	0	The send job is being processed.
0	1	0	The send job was completed successfully.
0	0	1	The connection establishment or the send job was completed with an error. The cause of the error is specified in the STATUS parameter.
0	0	0	No new send job was assigned.

You can check the status of the execution with the BUSY, DONE, ERROR, and STATUS parameters. The BUSY parameter indicates the processing status. With the DONE parameter, you can check whether or not a send job executed successfully. The ERROR parameter is set when errors occurred during execution of TSEND_C or TRCV_C. The error information is output at the STATUS parameter.

Error and Status parameters

Table 12-19 TSEND_C and TRCV_C condition codes for ERROR and STATUS

ERROR	STATUS * (W#16#...)	Description
0	0000	Send (TSEND_C) or receive (TRCV_C) job executed without errors.
0	0001	Communication connection established.
0	0003	Communication connection closed.
0	7000	No active send job execution; no communications connection established.
0	7001	• Start send (TSEND_C) or receive (TRCV_C) job execution. • Establish connection. • Wait for connection partner.
0	7002	Job executing (REQ irrelevant)
0	7003	The instruction is terminating the communications connection.
0	7004	Communications connection established and monitored; no send (TSEND_C) or receive (TRCV_C) job execution active.
0	7005	TSEND_C: Data transfer is in progress.
0	7006	TRCV_C: The instruction is receiving the data.
1	8085	• The LEN parameter is larger than the highest permitted value. • The instruction changed the value at the LEN or DATA parameter after the first call.
1	8086	The ID parameter within the CONNECT parameter is outside the permitted range.
1	8087	Maximum number of connections reached; no additional connection possible.
1	8088	The value at the LEN parameter does not correspond to the receive area set at the DATA parameter.
1	8089	• The CONNECT parameter does not point to a data block. • The CONNECT parameter does not point to a connection description. • The manually-created connection description has an incorrect structure for the selected connection type.
1	8091	Maximum nesting depth exceeded.
1	809A	The CONNECT parameter points to a field that does not correspond to the length of the connection description.
1	809B	The InterfaceId in the connection description does not correspond to the CPU or CP.
1	80A1	• Connection or port being used. • Communication error: – The specified connection has not yet been established. – The specified connection is being terminated. Transfer through this connection is not possible. – The interface is being re-initialized.
1	80A2	Local or remote port is being used by the system. Refer to "TCON and TDISCON instructions" (Page 578), "ERROR and STATUS condition codes" for further information.
1	80A3	• Attempt being made to re-establish an existing connection. • Attempt being made to terminate a non-existent connection. • The nested T_DIAG instruction reports that the instruction closed the connection.
1	80A4	IP address of the remote endpoint of the connection is invalid, which means it corresponds to the IP address of the local partner.

ERROR	STATUS * (W#16#...)	Description
1	80A7	Communication error: You called the instruction with COM_RST = 1 before the send job was complete.
1	80AA	Another block is establishing a connection using the same connection ID. Repeat the job with a new rising edge at the REQ parameter.
1	80B3	• When using the protocol variant UDP, the ADDR parameter does not contain any data. • Error in the connection description • A different connection description is already using the local port.
1	80B4	You have violated one or both of the following conditions for passive connection establishment (ActiveEstablished = FALSE) when using the ISO-on-TCP protocol variant (ConnectionType = B#16#12): • local_tsap_id_len >= B#16#02 • local_tsap_id[1] = B#16#E0
1	80B5	Only passive connection establishment is permitted for connection type 13 = UDP.
1	80B6	Parameter assignment error in the ConnectionType parameter of the data block for connection description.
1	80B7	• For TCON_Param system data type: Error in one of the following parameters of the data block for connection description: block_length, local_tsap_id_len, rem_subnet_id_len, rem_staddr_len, rem_tsap_id_len, next_staddr_len. • For TCON_IP_V4, TCON_IP_RFC, TCON_IP_V4_SEC, TCON_QDN, and TCON_QDN_SEC system data types: The instruction set the IP address of the partner end point to 0.0.0.0.
1	80C3	• All connection resources are in use. • A block with this ID is already being processed in a different priority group.
1	80C4	Temporary communication error: • The instruction cannot establish the connection at this time. • The instruction cannot establish the connection because the firewalls on the connection path are not open for the required ports. • The interface is receiving new parameters, or the instruction is establishing the connection. • The "TDISCON (Page 578)" instruction is removing the configured connection. • A call with COM_RST = 1 is terminating the connection used. • Temporarily, no receive resources available at the connection partner. The connection partner is not ready to receive.
1	80C5	• Connection terminated by the communication partner. • The remote connection partner did not release the LSAP.
1	80C6	Network error: • The local device cannot reach the remote partner. • Physical interruption on PROFIBUS
1	8722	Error in the CONNECT parameter: Invalid source area (area not declared in data block).
1	873A	Error in the CONNECT parameter: Access to connection description is not possible (no access to data block).
1	877F	Error in the CONNECT parameter: Internal error
1	8822	TSEND_C: DATA parameter: Invalid source area, the area does not exist in the DB.
1	8824	TSEND_C: DATA parameter: Area error in the VARIANT pointer.
1	8832	TSEND_C: DATA parameter: The DB number is too high.

ERROR	STATUS * (W#16#...)	Description
1	883A	TSEND_C: CONNECT parameter: Access to specified connection data not possible (for example, because the DB does not exist).
1	887F	TSEND_C: DATA parameter: Internal error (for example, invalid VARIANT reference)
1	893A	TSEND_C: DATA parameter: Access to send area not possible (for example, because the DB does not exist).
1	8922	TRCV_C: DATA parameter: Invalid target area; the area does not exist in the DB.
1	8924	TRCV_C: DATA parameter: Area error in the VARIANT pointer.
1	8932	TRCV_C: DATA parameter: The DB number is too high.
1	893A	TRCV_C: CONNECT parameter: Access to specified connection data not possible (for example, because the DB does not exist).
1	897F	TRCV_C: DATA parameter: Internal error (for example, invalid VARIANT reference).
1	8A3A	TRCV_C: DATA parameter: No access to the data area (for example because the data block does not exist).
* The error codes can be displayed as integer or hexadecimal values in the program editor.		

NOTE

Error messages of the instructions TCON, TSEND, TRCV, and TDISCON

Internally, the TSEND_C instruction uses the TCON, TSEND, and TDISCON instructions; and the TRCV_C instruction uses the TCON, TRCV, and TDISCON instructions. Refer to "TCON, TDISCON, TSEND, AND TRCV (Page 578)" for more information on error messages of these instructions.

Connection Ethernet protocols

Every CPU has an integrated PROFINET port, which supports standard PROFINET communications. The TSEND_C and TRCV_C and TSEND and TRCV instructions all support the TCP and ISO on TCP Ethernet protocols.

Refer to "Device Configuration: Configuring the Local/Partner connection path (Page 532)" for more information.

12.6.8.11 Legacy TSEND_C and TRCV_C instructions

Prior to the release of STEP 7 V13 SP1 and the S7-1200 V4.1 CPUs, the TSEND_C and TRCV_C instructions could only work with connection parameters with structures according to "TCON_Param". The general concepts apply to both sets of instructions. Refer to the individual legacy TSEND_C and TRCV_C instructions for programming information.

STEP 7 provides different versions of the TSEND_C and TRCV_C instructions. For information on instruction versions, refer to Use Instruction versions (Page 577) in the STEP 7 Information System.

Legacy TSEND_C and TRCV_C (Send and receive data using Ethernet)

The legacy TSEND_C instruction combines the functions of the legacy TCON, TDISCON and TSEND instructions. The TRCV_C instruction combines the functions of the TCON, TDISCON, and TRCV instructions. (Refer to "Legacy TCON, TDISCON, TSEND, and TRCV (TCP communication) instructions (Page 592)" for more information on these instructions.)

The minimum size of data that you can transmit (TSEND_C) or receive (TRCV_C) is one byte; the maximum size is 8192 bytes. TSEND_C does not support the transmission of data from Boolean locations, and TRCV_C will not receive data into Boolean locations. For information on transferring data with these instructions, see the section on data consistency (Page 178).

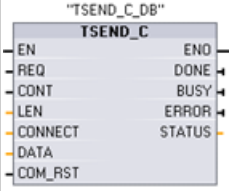
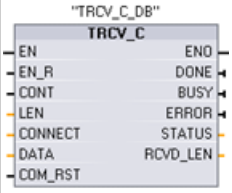
NOTE

Initializing the communication parameters

After you insert the TSEND_C or TRCV_C instruction, use the "Properties" of the instruction (Page 532) to configure the communication parameters (Page 551). As you enter the parameters for the communication partners in the inspector window, STEP 7 enters the corresponding data in the DB for the instruction.

If you want to use a multi-instance DB, you must configure the DB on both CPUs.

Table 12-20 TSEND_C and TRCV_C instructions

LAD / FBD	SCL	Description
	**"TSEND_C_DB"(req:=_bool_in_, cont:=_bool_in_, len:=_uint_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, connect:=_struct_inout_, data:=_variant_inout_, com_rst:=_bool_inout_);**	TSEND_C establishes a TCP or ISO on TCP communication connection to a partner station, sends data, and can terminate the connection. After the connection is set up and established, it is automatically maintained and monitored by the CPU.
	**"TRCV_C_DB"(en_r:=_bool_in_, cont:=_bool_in_, len:=_uint_in_, adhoc:=_bool_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, rcvd_len=>_uint_out_, connect:=_struct_inout_, data:=_variant_inout_, com_rst:=_bool_inout_);**	TRCV_C establishes a TCP or ISO on TCP communication connection to a partner CPU, receives data, and can terminate the connection. After the connection is set up and established, it is automatically maintained and monitored by the CPU.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 12-21 TSEND_C and TRCV_C data types for the parameters

Parameter and type		Data type	Description
REQ (TSEND_C)	IN	Bool	REQ = 1 starts the TSEND_C send job on a rising edge with the connection described in CONNECT parameter. (CONT = 1 is also required to establish and maintain the communication connection.
EN_R (TRCV_C)	IN	Bool	When EN_R = 1, TRCV_C is ready to receive. The receive job is processed. (CONT = 1 is also required to establish and maintain the communication connection.)
CONT	IN	Bool	Controls the communication connection: • 0: Disconnect the communication connection • 1: Establish and maintain the communication connection When sending data (TSEND_C) (rising edge at the REQ parameter), the CONT parameter must have the value TRUE in order to establish or maintain a connection. When receiving data (TRCV_C) (rising edge at the EN_R parameter), the CONT parameter must have the value TRUE in order to establish or maintain a connection.
LEN	IN	UInt	Maximum number of bytes to be sent (TSEND_C) or received (TRCV_C): • Default = 0: The DATA parameter determines the length of the data to be sent (TSEND_C) or received (TRCV_C). • Ad hoc mode = 65535: A variable length of data is set for reception (TRCV_C).
CONNECT	IN_OUT	TCON_Param	Pointer to the connection description (Page 551)
DATA	IN_OUT	Variant	• Contains address and length of data to be sent (TSEND_C) • Contains start address and maximum length of received data (TRCV_C).
COM_RST	IN_OUT	Bool	Allows restart of the instruction: • 0: Irrelevant • 1: Complete restart of the function block, existing connection will be terminated.
DONE	OUT	Bool	• 0: Job is not yet started or still running. • 1: Job completed without error.
BUSY	OUT	Bool	• 0: Job is completed. • 1: Job is not yet completed. A new job cannot be triggered.
ERROR	OUT	Bool	Status parameters with the following values: • 0: No error • 1: Error occurred during processing. STATUS provides detailed information on the type of error.
STATUS	OUT	Word	Status information including error information. (Refer to the "Error and Status Parameters" table below.)
RCVD_LEN (TRCV_C)	OUT	Int	Amount of data actually received, in bytes

NOTE

The TSEND_C instruction requires a low-to-high transition at the REQ input parameter to start a send job. The BUSY parameter is then set to 1 during processing. Completion of the send job is indicated by either the DONE or ERROR parameters being set to 1 for one scan. During this time, any low-to-high transition at the REQ input parameter is ignored.

NOTE

The default setting of the LEN parameter (LEN = 0) uses the DATA parameter to determine the length of the data being transmitted. It is recommended that the data transmitted by the TSEND_C instruction be the same size as the DATA parameter of the TRCV_C instruction.

If using the default setting of the LEN parameter and it is necessary to send the data in segments smaller than the DATA parameter size, the following applies. If the size of the data transmitted from TSEND_C does not equal the TRCV_C DATA parameter size, TRCV_C remains in a busy status (status code: 7006) until the overall size of the data transmitted from TSEND_C equals the TRCV_C DATA parameter size.

The TRCV_C DATA parameter buffer does not display the new data received until the data size equals the DATA parameter buffer size.

TSEND_C operations

The following functions describe the operation of the TSEND_C instruction:

- To establish a connection, execute TSEND_C with CONT = 1.
- After successful establishing of the connection, TSEND_C sets the DONE parameter for one cycle.
- To terminate the communication connection, execute TSEND_C with CONT = 0. The connection will be aborted immediately. This also affects the receiving station. The connection will be closed there and data inside the receive buffer could be lost.
- To send data over an established connection, execute TSEND_C with a rising edge on REQ. After a successful send operation, TSEND_C sets the DONE parameter for one cycle.
- To establish a connection and send data, execute TSEND_C with CONT =1 and REQ = 1. After a successful send operation, TSEND_C sets the DONE parameter for one cycle.

TRCV_C operations

The following functions describe the operation of the TRCV_C instruction:

- To establish a connection, execute TRCV_C with parameter CONT = 1.
- To receive data, execute TRCV_C with parameter EN_R = 1. TRCV_C receives the data continuously when parameters EN_R = 1 and CONT = 1.
- To terminate the connection, execute TRCV_C with parameter CONT = 0. The connection will be aborted immediately, and data could be lost.

TRCV_C handles the same receive modes as the TRCV instruction. The following table shows how data is entered in the receive area:

Table 12-22 Entering the data into the receive area

Protocol variant	Entering the data in the receive area	Parameter "connection_type"	Value of the LEN parameter	Value of the RCVD_LEN parameter (bytes)
TCP	Ad hoc mode	B#16#11	65535	1 to 1460
TCP	Data reception with specified length	B#16#11	0 (recommended) or 1 to 8192, except 65535	1 to 8192
ISO on TCP	Ad hoc mode	B#16#12	65535	1 to 1460
ISO on TCP	Protocol-controlled	B#16#12	0 (recommended) or 1 to 8192, except 65535	1 to 8192

NOTE

Ad hoc mode

The "ad hoc mode" exists with the TCP and ISO on TCP protocol variants. You set "ad hoc mode" by assigning "65535" to the LEN parameter. The receive area is identical to the area formed by DATA. The length of the received data will be output to the parameter RCVD_LEN.

If you store the data in an "optimized" DB (symbolic only), you can receive data only in arrays of Byte, Char, USInt, and SInt data types.

NOTE

Importing of S7-300/400 STEP 7 projects containing "ad hoc mode" into the S7-1200

In S7-300/400 STEP 7 projects, "ad hoc mode" is selected by assigning "0" to the LEN parameter. In the S7-1200, you set "ad hoc mode" by assigning "65535" to the LEN parameter.

If you import an S7-300/400 STEP 7 project containing "ad hoc mode" into the S7-1200, you must change the LEN parameter to "65535".

NOTE

Must keep the data in the sender area consistent until the DONE parameter or the ERROR parameter assumes the value TRUE

Due to the asynchronous processing of TSEND_C, you must keep the data in the sender area consistent until the DONE parameter or the ERROR parameter assumes the value TRUE.

For TSEND_C, a TRUE state at the parameter DONE means that the data was sent successfully. It does not mean that the connection partner CPU actually read the receive buffer.

Due to the asynchronous processing of TRCV_C, the data in the receiver area are only consistent when parameter DONE = 1.

Table 12-23 TSEND_C and TRCV_C instructions BUSY, DONE, and ERROR parameters

BUSY	DONE	ERROR	Description
TRUE	irrelevant	irrelevant	The job is being processed.
FALSE	TRUE	FALSE	The job is successfully completed.
FALSE	FALSE	TRUE	The job was ended with an error. The cause of the error can be found in the STATUS parameter.
FALSE	FALSE	FALSE	A new job was not assigned.

Error and Status parameters

Table 12-24 TSEND_C and TRCV_C condition codes for ERROR and STATUS

ERROR	STATUS	Description
0	0000	Job executed without error
0	7000	No job processing active
0	7001	Start job processing, establishing connection, waiting for connection partner
0	7002	Data being sent or received
0	7003	Connection being terminated
0	7004	Connection established and monitored, no job processing active
1	8085	LEN parameter is greater than the largest permitted value.
1	8086	The CONNECT parameter is outside the permitted range.
1	8087	Maximum number of connections reached; no additional connection possible.
1	8088	LEN parameter is not valid for the memory area specified in DATA.
1	8089	The CONNECT parameter does not point to a data block.
1	8091	Maximum nesting depth exceeded.
1	809A	The CONNECT parameter points to a field that does not match the length of the connection description.
1	809B	The local_device_id in the connection description does not match the CPU.
1	80A1	Communications error: • The specified connection was not yet established • The specified connection is currently being terminated; transmission over this connection is not possible • The interface is being reinitialized
1	80A3	Attempt being made to terminate a nonexistent connection
1	80A4	IP address of the remote partner connection is invalid. For example, the remote partner IP address is the same as the local partner IP address.
1	80A5	Connection ID (Page 549) is already in use.
1	80A7	Communications error: You called TDISCON before TSEND_C was complete.
1	80B2	The CONNECT parameter points to a data block that is set to "Only store in load memory."
1	80B3	Inconsistent parameters: • Error in the connection description • Local port (parameter local_tsap_id) is already present in another connection description. • ID in the connection description different from the ID specified as parameter

ERROR	STATUS	Description
1	80B4	When using the ISO on TCP (connection_type = B#16#12) to establish a passive connection, condition code 80B4 alerts you that the TSAP entered did not conform to one of the following address requirements: • For a local TSAP length of 2 and a TSAP ID value of either E0 or E1 (hexadecimal) for the first byte, the second byte must be either 00 or 01. • For a local TSAP length of 3 or greater and a TSAP ID value of either E0 or E1 (hexadecimal) for the first byte, the second byte must be either 00 or 01 and all other bytes must be valid ASCII characters. • For a local TSAP length of 3 or greater and the first byte of the TSAP ID does not have a value of either E0 or E1 (hexadecimal), then all bytes of the TSAP ID must be valid ASCII characters. Valid ASCII characters are byte values from 20 to 7E (hexadecimal).
1	80B7	Data type and/or length of the transmitted data does not fit in the area in the partner CPU in which it is to be written.
1	80C3	All connection resources are in use.
1	80C4	Temporary communications error: • The connection cannot be established at this time • The interface is receiving new parameters • The configured connection is currently being removed by a TDISCON.
1	8722	CONNECT parameter: Source area invalid: area does not exist in DB.
1	873A	CONNECT parameter: Access to connection description is not possible (for example, DB not available)
1	877F	CONNECT parameter: Internal error such as an invalid ANY reference
1	893A	Parameter contains the number of a DB that is not loaded.

Connection Ethernet protocols

Every CPU has an integrated PROFINET port, which supports standard PROFINET communications. The TSEND_C and TRCV_C and TSEND and TRCV instructions all support the TCP and ISO on TCP Ethernet protocols.

Refer to "Device Configuration: Configuring the Local/Partner connection path (Page 532)" for more information.

12.6.8.12 TCON, TDISCON, TSEND, and TRCV instructions

The S7-1200 supports two sets of TCON, TDISCON, TSEND, and TRCV instructions:

- TCON, TDISCON, TSEND, and TRCV instructions (Page 578): These TCON, TDISCON, TSEND, and TRCV instructions provide all of the functionality of the legacy instructions, plus the ability to use connection parameters with structures according to TCON_IP_V4, TCON_IP_V4_SEC, TCON_IP_RFC, TCON_QDN, and TCON_QDN_SEC.
- Legacy TCON, TDISCON, TSEND, and TRCV instructions (Page 592): These TCON, TDISCON, TSEND, and TRCV instructions existed prior to version V4.1 of the S7-1200 and only work with connection parameters with structures according to TCON_Param.

STEP 7 provides different versions of the TCON, TDISCON, TSEND, and TRCV instructions. For information on instruction versions, refer to Use Instruction versions (https://support.industry.siemens.com/cs/ww/en/view/109798671/113722878475) in the STEP 7 Information System.

TCON, TDISCON, TSEND, and TRCV (TCP communication) instructions

Ethernet communication using TCP and ISO on TCP protocols

NOTE

TSEND_C and TRCV_C instructions

To help simplify the programming of PROFINET/Ethernet communication, the TSEND_C instruction and the TRCV_C instruction combine the functionality of the TCON, TDISCON. TSEND and TRCV instructions:

- TSEND_C combines the TCON, TDISCON and TSEND instructions.
- TRCV_C combines the TCON, TDISCON and TRCV instructions.

The following instructions control the communication process:

- TCON establishes the TCP/IP connection between the client and server (CPU) PC.
- TSEND and TRCV send and receive data.
- TDISCON breaks the connection.

The minimum size of data that you can transmit (TSEND) or receive (TRCV) is one byte; the maximum size is 8192 bytes. TSEND does not support the transmission of data from Boolean locations, and TRCV will not receive data into Boolean locations. For information transferring data with these instructions, see the section on data consistency (Page 178).

TCON, TDISCON, TSEND, and TRCV operate asynchronously, which means that the job processing extends over multiple instruction executions. For example, you start a job for setting up and establishing a connection by executing an instruction TCON with parameter REQ = 1. Then you use additional TCON executions to monitor the job progress and test for job completion with parameter DONE.

The following table shows the relationships between BUSY, DONE, and ERROR. Use the table to determine the current job status:

Table 12-25 Interactions between the BUSY, DONE, and ERROR parameters

BUSY	DONE	ERROR	Description
1	0	0	The job is being processed.
0	1	0	The job successfully completed.
0	0	1	The job ended with an error. The cause of the error is output at the STATUS parameter.
0	0	0	No new job assigned.

TCON and TDISCON

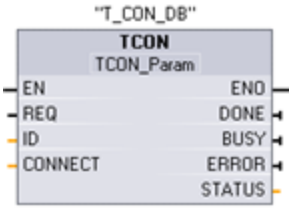
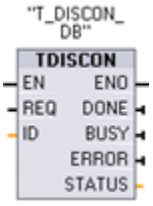
NOTE

Initializing the communication parameters

After you insert the TCON instruction, use the "Properties" of the instruction (Page 532) to configure the communication parameters (Page 551). As you enter the parameters for the communication partners in the inspector window, STEP 7 enters the corresponding data in the instance DB for the instruction.

If you want to use a multi-instance DB, you must configure the DB on both CPUs.

Table 12-26 TCON and TDISCON instructions

LAD / FBD		Description
	**"TCON_DB"(req:=_bool_in_, ID:=_undef_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, connect:=_struct_inout_);**	TCP and ISO on TCP: TCON initiates a communications connection from the CPU to a communication partner.
	**"TDISCON_DB"(req:=_bool_in_, ID:=_word_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_);**	TCP and ISO on TCP: TDISCON terminates a communications connection from the CPU to a communication partner.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 12-27 Data types for the parameters of TCON and TDISCON

Parameter	Declaration	Data type	Description
REQ	IN	Bool	Starts the job to establish the connection specified in the ID upon a rising edge.
ID	IN	CONN_OUC (Word)	Reference to the assigned connection. Range of values: W#16#0001 to W#16#0FFF
CONNECT (TCON)	IN_OUT	VARIANT	Pointer to the connection description: • For TCP or UDP, use the structure TCON_IP_v4 or TCON_QDN. For a description, refer to: "Parameters for the PROFINET connection (Page 551)". • For TCP using secure communication, use the structure TCON_IP_V4_SEC or TCON_QDN_SEC. For a description, refer to: "Parameters for the PROFINET (Page 551) connection (Page 551)". • For ISO-on-TCP, use the structure TCON_IP_RFC. For a description, refer to: "Parameters for the PROFINET connection (Page 551)". • For ISO connections of the CP 1543-1 / CP 1545-1, use the structure TCON_ISOnative. For a description, refer to: TIA Portal Online Help: "Structure of the connection description according to TCON_ISOnative". • For connections to SMS clients, use the TCON_PHONE system data type. For a description, refer to TIA Portal Online Help: "Connection parameters to TCON_Phone".
DONE	OUT	Bool	Status parameter with the following values: • 0: Job not yet started or still in progress. • 1: Job executed without errors.
BUSY	OUT	Bool	Status parameter with the following values: • 0: Job not yet started or already completed. • 1: Job not yet completed. A new job cannot be started.

Parameter	Declaration	Data type	Description
ERROR	OUT	Bool	Status parameter ERROR: • 0: No error • 1: Error occurred
STATUS	OUT	Word	Status of the instruction

Both communication partners execute the TCON instruction to set up and establish the communication connection. You use parameters to specify the active and passive communication end point partners. After the connection is set up and established, it is automatically maintained and monitored by the CPU.

If the connection is terminated due to a line break or due to the remote communications partner, for example, the active partner attempts to re-establish the configured connection. You do not have to execute TCON again.

An existing connection is terminated and the set-up connection is removed when the TDISCON instruction is executed or when the CPU has gone into STOP mode. To set up and re-establish the connection, you must execute TCON again.

Table 12-28 ERROR and STATUS condition codes for TCON and TDISCON

ERROR	STATUS * (W#16#...)	Explanation
0	0000	Connection successfully established.
0	7000	No job processing active
0	7001	Start job execution; establish connection (TCON) or terminate connection (TDISCON).
0	7002	The instruction is establishing a connection (REQ irrelevant); establish connection (TCON) or terminate connection (TDISCON).
1	8085	TCON: Connection ID is in use.
1	8086	TCON: The ID parameter is outside the valid range.
1	8087	TCON: Maximum number of connections reached; no additional connection possible
1	8089	TCON: The CONNECT parameter does not point to a connection description, or the connection description was created manually.
1	809A	TCON: The instruction does not support the structure at the CONNECT parameter, or the length is invalid.
1	809B	TCON: • The InterfaceId element in the connection description does not correspond to the CPU or the CP, or it is "0". • The InterfaceId element within the TCON_xxx structure does not reference a hardware identifier of a CPU or CM/CP interface.
1	80A1	TCON: For TCP/UDP: Connection or port is in use.
1	80A2	TCON: The system is using the local or remote port. Refer to "Common parameters for instructions" (Page 639), "Restricted TSAPs and port numbers for passive ISO and TCP communication" for further information.
1	80A3	TCON: A connection (TCON), created by the user program, is using the value at the ID parameter. The connection uses the identical ID and the same connection settings at the CONNECT parameter.
1	80A4	TCON: IP address of the remote endpoint of the connection is invalid, or it corresponds to the IP address of the local partner.
1	80A7	TCON: Communication error: You executed "TDISCON" before "TCON" had completed.
1	80B3	Inconsistent parameter assignment

ERROR	STATUS * (W#16#...)	Explanation
1	80B4	TCON: Only with TCON_IP_RFC: One of the following occurred: • The instruction did not assign the local T selector. • The first byte does not contain the value 0x0E. • The local T selector starts with "SIMATIC-".
1	80B5	TCON: The instruction permits only passive connection establishment for connection type 13 = UDP (Parameter ActiveEstablished of the structure TCON_xxx has the value TRUE).
1	80B6	TCON: Parameter assignment error in the ConnectionType parameter of the data block for connection description: • Only valid with TCON_IP_V4, TCON_IP_V4_SEC, TCON_QDN, TCON_QDN_SEC: 0x11, 0x0B and 0x13 • Only valid with TCON_IP_RFC: 0x0C and 0x12
1	80B7	TCON: With TCON_IP_V4, TCON_IP_V4_SEC, TCON_QDN, TCON_QDN_SEC: • TCP (active connection establishment): Remote port is "0". • TCP (passive connection establishment): Local port is "0". • UDP: Local port is "0". • The instruction set the IP address of the partner end point to 0.0.0.0. TCON: With TCON_IP_RFC: • The instruction assigned the local (local_tselector) or remote (remote_tselector) T selector with a length of more than 32 bytes. • For TSelLength of the T selector (local or remote), the instruction assigned a length greater than 32. • Error in the length of the IP address of the specific connection partner • The instruction set the IP address of the partner end point to 0.0.0.0.
1	80B8	TCON: ID parameter in the local connection description (structure at CONNECT parameter) and ID parameter of the instruction are different.
1	80C3	TCON: All connection resources are in use.
1	80C4	Temporary communication error: • The instruction cannot establish the connection at this time (TCON). • The instruction cannot establish the connection because the firewalls on the connection path are not open for the required ports (TCON). • The interface is receiving new parameters (TCON and TDISCON). • The "TDISCON" instruction is removing the configured connection (TCON).
1	80C5	TCON: The remote partner did one of the following: • Refused to establish the connection • Terminated the connection • Actively ended the connection
1	80C6	TCON: The instruction cannot reach the remote partner (network error).
1	80C7	TCON: Execution timeout
1	80C8	TCON: A connection (TCON), created by the user program, is using the value at the ID parameter. The connection uses the identical ID, but different connection settings at the CONNECT parameter.
1	80C9	TCON: Validation of the remote partner failed. The remote partner that wants to establish the connection does not match the defined partner of the structure at the CONNECT parameter.
1	80CE	TCON: The IP address of the local interface is 0.0.0.0.
1	80E0	TCON: The instruction received an unsuitable or poor message.

ERROR	STATUS * (W#16#...)	Explanation
1	80E1	TCON: Error during the handshake. Possible causes: • Abort by the user • Security not high enough • The instruction does not support renewed negotiation. • The instruction does not support SSL/TLS version. • Validation of the host name failed.
1	80E2	Certificate not supported / certificate invalid / no certificate Possible cause: For the module concerned, the CPU did not set the time-of-day or synchronize the module. Example: The default setting for the date of the module is 1/1/2012, and the CPU did not set the date during commissioning. The validity period of the certificate starts on 20 August 2016, and ends on 20 August 2024. In this case, the date of the module is outside the validity period of the certificate; the certificate is invalid for the module.
1	80E3	Certificate discarded.
1	80E4	No valid certification authority found.
1	80E5	Certificate expired.
1	80E6	Integrity errors in the Transport Layer Security Protocol
1	80E7	Not supported extension in X.509-V3 certificate
1	80E9	The instruction does not support a TLS server without a server certificate.
1	80EA	The instruction does not support DTLS (UDP) protocol.
1	80EB	A client cannot request a client certificate.
1	80EC	The server cannot perform validation based on the subjectAlternateName (only clients can do this).
1	80ED	TLSServerCertRef_m-ID invalid
* The error codes in the program editor can be displayed as integer or hexadecimal values.		

TSEND and TRCV

NOTE

When using PROFINET Open User communication, if you execute a TSEND instruction without a corresponding TRCV instruction executing on the remote device, then the TSEND instruction may reside indefinitely in a "Busy State", waiting for the TRCV instruction to receive the data. In this state, the TSEND instruction "Busy" output is set, and the "Status" output has a value of "0x7002". This condition may occur if you are transferring more than 4096 bytes of data. The issue is resolved at the next execution of the TRCV instruction.

Table 12-29 TSEND and TRCV instructions

LAD / FBD	SCL	Description
	"TSEND_DB"(req:=_bool_in_, ID:=_word_in_, len:=_udint_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, data:=_variant_inout_);	TCP and ISO on TCP: TSEND sends data through a communication connection from the CPU to a partner station.
	"TRCV_DB"(en_r:=_bool_in_, ID:=_word_in_, len:=_udint_in_, adhoc:=_bool_in_, ndr=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, rcvd_len=>_udint_out_, data:=_variant_inout_);	TCP and ISO on TCP: TRCV receives data through a communication connection from a partner station to the CPU.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 12-30 Data types for the parameters of TSEND and TRCV

Parameter and type		Data type	Description
REQ	IN	Bool	TSEND: Starts the send job on a rising edge. The data is transferred from the area specified by DATA and LEN.
EN_R	IN	Bool	TRCV: Enables the CPU to receive; with EN_R = 1, the TRCV is ready to receive. The receive job is processed.
ID	IN	CONN_OUC (Word)	Reference to the associated connection. ID must be identical to the associated parameter ID in the local connection description. Value range: W#16#0001 to W#16#0FFF
LEN	IN	UDInt	Maximum number of bytes to be sent (TSEND) or received (TRCV): • Default = 0: The DATA parameter determines the length of the data to be sent (TSEND) or received (TRCV). • Ad hoc mode = 65535: A variable length of data is set for reception (TRCV).
ADHOC	IN	Bool	TRCV: Optional parameter (hidden) Ad hoc mode request for connection type TCP.
DATA	IN_OUT	Variant	Pointer to send (TSEND) or receive (TRCV) data area; data area contains the address and length. The address refers to I memory, Q memory, M memory, or a DB.
DONE	OUT	Bool	TSEND: • 0: Job not yet started or still running. • 1: Job executed without error.
NDR	OUT	Bool	TRCV: • NDR = 0: Job not yet started or still running. • NDR = 1: Job successfully completed.

Parameter and type		Data type	Description
BUSY	OUT	Bool	• BUSY = 1: The job is not yet complete. A new job cannot be triggered. • BUSY = 0: Job is complete.
ERROR	OUT	Bool	ERROR = 1: Error occurred during processing. STATUS provides detailed information on the type of error
STATUS	OUT	Word	Status information including error information. (Refer to the Error and Status condition codes in the table below.)
RCVD_LEN	OUT	UDInt	TRCV: Amount of data actually received in bytes

NOTE

The TSEND instruction requires a low-to-high transition at the REQ input parameter to start a send job. The BUSY parameter is then set to 1 during processing. Completion of the send job is indicated by either the DONE or ERROR parameters being set to 1 for one scan. During this time, any low-to-high transition at the REQ input parameter is ignored.

TRCV Operations

The TRCV instruction writes the received data to a receive area that is specified by the following two variables:

- Pointer to the start of the area
- Length of the area or the value supplied at the LEN input if not 0

NOTE

The default setting of the LEN parameter (LEN = 0) uses the DATA parameter to determine the length of the data being transmitted. It is recommended that the data transmitted by the TSEND instruction be the same size as the DATA parameter of the TRCV instruction.

If using the default setting of the LEN parameter and it is necessary to send the data in segments smaller than the DATA parameter size, the following applies. It is recommended to keep the EN_R bit high until the corresponding TSEND transfers the appropriate amount of data to fill the TRCV DATA parameter. If the size of the data transmitted from TSEND does not equal the TRCV DATA parameter size, TRCV remains in a busy status (status code: 7002) while the EN_R bit is high until the overall size of the data transmitted from TSEND equals the TRCV DATA parameter size. If the EN_R bit of TRCV is pulsed, it needs to be pulsed the same number of times as TSEND is executed to receive the data.

The TRCV DATA parameter buffer does not display the new data received until the data size equals the DATA parameter buffer size.

As soon as all the job data has been received, TRCV transfers it to the receive area and sets NDR to 1.

Table 12-31 Entering the data into the receive area

Protocol variant	Entering the data in the receive area	Parameter "connection_type"	Value of the LEN parameter	Value of the RCVD_LEN parameter (bytes)
TCP	Ad hoc mode	B#16#11	Selected with the TRCV instruction ADHOC input	1 to 1460
TCP	Data reception with specified length	B#16#11	0 (recommended) or 1 to 8192, except 65535	1 to 8192
ISO on TCP	Ad hoc mode	B#16#12	65535	1 to 1460
ISO on TCP	protocol-controlled	B#16#12	0 (recommended) or 1 to 8192, except 65535	1 to 8192

NOTE

Ad hoc mode

The "ad hoc mode" exists with the TCP and ISO on TCP protocol variants. To configure the TRCV instruction for ad hoc mode, set the ADHOC instruction input parameter. The receive area is identical to the area formed by DATA. The length of the received data will be output to the parameter RCVD_LEN. Immediately after receiving a block of data, TRCV enters the data in the receive area and sets NDR to 1.

If you store the data in an "optimized" DB (symbolic only), you can receive data only in arrays of Byte, Char, USInt, and SInt data types.

NOTE

Importing of S7-300/400 STEP 7 projects containing "ad hoc mode" into the S7-1200

In S7-300/400 STEP 7 projects, "ad hoc mode" is selected by assigning "0" to the LEN parameter. In the S7-1200, you configure the TRCV instruction for ad hoc mode by setting the ADHOC instruction input parameter.

If you import an S7-300/400 STEP 7 project containing "ad hoc mode" into the S7-1200, you must change the LEN parameter to "65535".

Table 12-32 ERROR and STATUS condition codes for TSEND and TRCV

ERROR	STATUS	Description
0	0000	• Send job completed without error (TSEND) • New data accepted: The current length of the received data is shown in RCVD_LEN (TRCV).
0	7000	• No job processing active (TSEND) • Block not ready to receive (TRCV)
0	7001	• Start of job processing, data being sent: During this processing the operating system accesses the data in the DATA send area (TSEND). • Block is ready to receive, receive job was activated (TRCV).
0	7002	• Follow-on instruction execution (REQ irrelevant), job being processed: The operating system accesses the data in the DATA send area during this processing (TSEND). • Follow-on instruction execution, receive job being processed: Data is written to the receive area during this processing. For this reason, an error could result in inconsistent data in the receive area (TRCV).

ERROR	STATUS	Description
1	8085	• LEN parameter is greater than the largest permitted value (TSEND) and (TRCV). • LEN or DATA parameter changed since the first instruction execution (TRCV).
1	8086	The ID parameter is not in the permitted address range.
1	8088	The LEN parameter is larger than the memory area specified in DATA.
1	80A1	Communications error: • The specified connection has not yet established (TSEND and TRCV). • The specified connection is currently being terminated. Transmission or a receive job over this connection is not possible (TSEND and TRCV). • The interface is being reinitialized (TSEND). • The interface is receiving new parameters (TRCV).
1	80C3	Internal lack of connection (Page 549) resources: A block with this ID is already being processed in a different priority class.
1	80C4	Temporary communications error: • The connection to the communications partner cannot be established at this time. • The interface is receiving new parameter settings, or the connection is currently being established.

Connection Ethernet protocols

Every CPU has an integrated PROFINET port, which supports standard PROFINET communications. The TSEND_C, TRCV_C, TSEND and TRCV instructions all support the TCP and ISO on TCP Ethernet protocols.

Refer to "Device Configuration: Configuring the Local/Partner connection path (Page 532)" for more information.

12.6.8.13 TCONSettings

You can use the "TCONSettings" instruction to execute the following functions:

- Request a connection ID for a new OUC connection
- Request a connection ID for a new OUC connection and at the same time specify a property for this connection
- Read a property of a prepared or an existing OUC connection
- Write a property for a prepared or an existing OUC connection

You can read or write the following connection properties with the "TCONSettings" instruction:

- How a TCP connection is terminated

The "TCONSettings" instruction is an asynchronous instruction. Processing extends over multiple calls. You start processing with a rising edge at the "REQ" parameter.

The parameters "Busy" and "Done" indicate the status of the job.

If an error occurs during execution, this is signaled by the parameters "Error" and "Status".

Table 12-33 TCONSettings data types for the parameters

Parameters and type		Data type	Description
REQ	Input	Bool	Control parameter Request Activates the job on a positive edge.
MODE	Input	USInt	Use the "Mode" parameter to select the information you want to read from your CPU: • 0: Request a connection ID for a new OUC connection and, if necessary, write a property of the associated connection (if a valid value for a property is present in the OPTION parameter) • 1: Reading a property of the OUC connection referenced by ID • 2: Write a property of the OUC connection referenced by ID • 3 to 255: Reserved
DONE	Output	Bool	Status parameter with the following values: • 0: Job not yet started or still in progress. • 1: Job completed without error. This state is only displayed for one call.
BUSY	Output	Bool	Status parameter with the following values: • 0: Job not yet started or already completed. • 1: Job not yet completed. A new job with this instance cannot be started
ERROR	Output	Bool	Status parameter with the following values: • 0: No error occurred. • 1: Error occurred during processing. STATUS supplies detailed information on the type of error. This state is only displayed for one call.
STATUS	Output	Word	Return value or error information of the "TCONSettings" instruction.
ID	InOut	CONN_OUC	Reference to the connection: Note: For MODE=0, ID is an output parameter, for MODE=1 and MODE=2 ID is an input parameter.
OPTION	InOut	Variant	Pointer to the description of the connection property to be read or specified: • TCON_TCPTermination: How to terminate the TCP connection.

BUSY, DONE and ERROR parameters

You can check the status of the job with the BUSY, DONE, ERROR and STATUS parameters. The BUSY parameter indicates the processing status. With the DONE parameter, you can check whether or not a job executed successfully. The ERROR parameter is set if errors occur during the execution of "TCONSettings". The error information is output at the STATUS parameter.

The following table shows the relationship between the BUSY, DONE and ERROR parameters:

BUSY	DONE	ERROR	Description
1	0	0	The job is being processed.
0	1	0	The job was completed successfully.
0	0	1	The job ended with an error. The cause of the error is output at the STATUS parameter.
0	0	0	No new job was assigned.

Table 12-34 TCONSettings condition codes for Status

STATUS (W#16#...)	Explanation
0000	"TCONSettings" was completed without errors.
7000	No job processing active.
7001	Start of job execution
7002	Intermediate call (REQ irrelevant):
8086	ID is outside the permitted range.
8087	Maximum number of OUC connections reached; no additional connections possible.
8089	OPTION does not point to a valid data type or OPTION is empty.
8090	OPTION points to a connection property which must not be changed for the connection referenced by ID.
8091	Invalid value for MODE
8092	A value in the data block referenced by OPTION is not permitted.
8093	If MODE has the value 0, ID must also have the value 0.
809A	OPTION points to a data type that is not permitted for "TCONSettings".
80A3	ID points to a non-existent communication endpoint.
80B1	The OPTION parameter was changed before the execution of "TCONSettings" was completed. It is not permitted to change OPTION while "TCONSettings" are being executed.
80C3	The maximum number of simultaneously active jobs has already been reached.

Maximum number of simultaneously active jobs

The maximum number of simultaneously active jobs is identical to the maximum number of OUC connections of your CPU

Reserving a connection resource

Call TCONSettings with MODE=0. Assign the relevant parameters as follows:

- Enter the value NULL at the ID parameter.
- If you do not want to specify a property for the associated connection, leave the OPTION parameter empty.
  If you want to specify a property for the associated connection, assign a valid value to the OPTION parameter (Page 586).

After the DONE parameter of TCONSettings is TRUE, a connection ID for a new OUC connection is available at the ID parameter. If you specified a property in the OPTION parameter, the connection uses this property for the connection. The TCONSettings instruction uses an OUC connection resource for the ID and creates the corresponding diagnostic objects. The TCONSettings instruction has prepared the connection but external communication partners do not yet know about the connection.

You have not specified any details for the connection, neither the connection partner nor the protocol nor the interface nor the DB with the connection description.

NOTE

Establishing the connection

TCONSettings does not establish a connection.

Establishing the associated connection

If you want to establish the corresponding connection after the successful execution of "TCONSettings", follow these steps:

1. Save the connection ID provided by "TCONSettings".
2. Call the instruction "TCON" with exactly this ID.

The number of available OUC connections does not change, because the TCONSettings instruction already consumed the connection.

Release the connection ID and the corresponding connection resource

If you want to release the connection ID provided by "TCONSettings" and the corresponding connection resource again, call the "TDISCON" instruction with exactly this ID.

CPU changes to STOP mode

When the CPU changes to STOP mode, all connection IDs provided by "TCONSettings" and the corresponding connection resources are released.

Reading a property of a prepared or an existing connection

You call "TCONSettings" with MODE=1. You assign the relevant parameters as follows:

- At the ID parameter you specify the reference to the desired connection.
- At the OPTION parameter you specify which connection property you want to read.

After the DONE parameter has assumed the value TRUE, the current values of the desired property are available in the data area specified by OPTION.

Specifying a property of a prepared or an existing connection

You call "TCONSettings" with MODE=2. You assign the relevant parameters as follows:

- At the ID parameter you specify the reference to the connection to which you want to assign a property.
- At the OPTION parameter you indicate which connection property you want to specify.

After the DONE parameter has assumed the value TRUE, the connection has been assigned the desired property.

Connections created by OUC and Modbus instructions

The instructions of the OUC library ending with "_C" and the instructions of the MODBUS-TCP library establish connections by calling the instruction "TCON" internally. You can change such connections with "TCONSettings" in the same way as connections that you have created by explicitly calling "TCON".

Connection properties that can generally be read and specified

The following connection properties can be read and specified with the "TCONSettings" instruction:

- How a TCP connection is terminated.

Relation between the protocol or the interface and the actual readable or specifiable connection properties

Not every protocol or interface can read or specify all of the above connection properties. The following table shows which connection properties are possible for the individual protocols or interfaces.

Protocol / interface	Terminating a connection
Programmed connection:	Yes
Configured connection:	No [1]
TCP	Yes
UDP	No [3]
ISO on TCP	No
CPU interface	Yes
CP interface	No
Virtual CP interface	Yes
[1] You cannot call "TDISCON" for a configured connection. Therefore, there is no way to end the connection in an orderly manner. [2] UDP is connectionless at the protocol level, so no termination is necessary.	

Conflicts in the specification of connection properties

Each predefinable connection property is only permitted for specific protocols or interfaces. Therefore, there may be conflicts between your specification of a connection property and the desired protocol or interface. In this case "TCONSettings" returns the value W#16#8090 at the STATUS parameter.

How can you terminate a TCP connection?

You can terminate an existing TCP connection in the following two ways:

- With a TCP-Reset (default)
  The connection is closed after the frame has been sent with the RST bit set in the header. The associated resources are immediately deleted and enabled. Remaining data is neither sent nor transferred to the user program.
- With a TCP-Finish
  If you have set TCP-Finish as the way of terminating a connection and then call the instruction "TDISCON", the connection is closed from the user's point of view after the termination of "TDISCON" with DONE=TRUE, i.e. the connection ID is available again. In the lower layers in the TCP/IP stack of the module, however, the resources are still assigned for some time, as are the diagnostic objects belonging to the connection.

If you remove many connections using TCP-Finish and reserve (with "TCONSettings") or establish (with "TCON") connections before the timer for enabling the resources expires, this can result in a resource bottleneck.

Conditions for a TCP-Finish

The following conditions must be met in order for you to terminate a connection in an orderly manner using a TCP-Finish:

- The protocol used is TCP.
- The associated interface is located on the CPU.
- The reason for the termination of the connection is the call of the "TDISCON" instruction.

NOTE

Terminating a TCP connection during transition to STOP

During the transition to STOP, a TCP connection is always terminated with a TCP-Reset.

SDT for connection termination: TCON_TCPTermination

The SDT for the connection termination has the following structure:

Parameters	Data type	Start value	Description
GracefulShutdown	Bool	FALSE	• FALSE: Use a TCP-Reset to terminate the connection. • TRUE: Use a TCP-Finish to terminate the connection.

12.6.8.14 Legacy TCON, TDISCON, TSEND, and TRCV instructions

Prior to the release of STEP 7 V13 SP1 and the S7-1200 V4.1 CPUs, the TCON, TDISCON, TSEND, and TRCV instructions could only work with connection parameters with structures according to TCON_Param. The general concepts apply to both sets of instructions. Refer to the individual legacy TCON, TDISCON, TSEND, and TRCV instructions for programming information.

STEP 7 provides different versions of the TCON, TDISCON, TSEND, and TRCV instructions. For information on instruction versions, refer to Use Instruction versions (https://support.industry.siemens.com/cs/ww/en/view/109798671/113722878475) in the STEP 7 Information System.

Legacy TCON, TDISCON, TSEND, and TRCV (TCP communication) instructions

Ethernet communication using TCP and ISO on TCP protocols

NOTE

TSEND_C and TRCV_C instructions

To help simplify the programming of PROFINET/Ethernet communication, the TSEND_C instruction and the TRCV_C instruction combine the functionality of the TCON, TDISCON. TSEND and TRCV instructions:

- TSEND_C combines the TCON, TDISCON and TSEND instructions.
- TRCV_C combines the TCON, TDISCON and TRCV instructions.

The following instructions control the communication process:

- TCON establishes the TCP/IP connection between the client and server (CPU) PC.
- TSEND and TRCV send and receive data.
- TDISCON breaks the connection.

The minimum size of data that you can transmit (TSEND) or receive (TRCV) is one byte; the maximum size is 8192 bytes. TSEND does not support the transmission of data from Boolean locations, and TRCV will not receive data into Boolean locations. For information transferring data with these instructions, see the section on data consistency (Page 178).

TCON, TDISCON, TSEND, and TRCV operate asynchronously, which means that the job processing extends over multiple instruction executions. For example, you start a job for setting up and establishing a connection by executing an instruction TCON with parameter REQ = 1. Then you use additional TCON executions to monitor the job progress and test for job completion with parameter DONE.

The following table shows the relationships between BUSY, DONE, and ERROR. Use the table to determine the current job status:

Table 12-35 Interactions between the BUSY, DONE, and ERROR parameters

BUSY	DONE	ERROR	Description
TRUE	irrelevant	irrelevant	The job is being processed.
FALSE	TRUE	FALSE	The job successfully completed.
FALSE	FALSE	TRUE	The job was ended with an error. The cause of the error can be found in the STATUS parameter.
FALSE	FALSE	FALSE	A new job was not assigned.

TCON and TDISCON

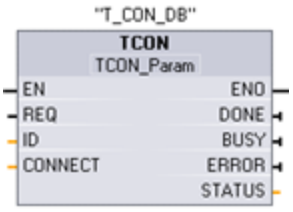
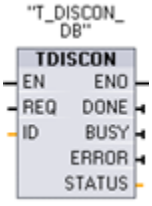
NOTE

Initializing the communication parameters

After you insert the TCON instruction, use the "Properties" of the instruction (Page 532) to configure the communication parameters (Page 551). As you enter the parameters for the communication partners in the inspector window, STEP 7 enters the corresponding data in the instance DB for the instruction.

If you want to use a multi-instance DB, you must configure the DB on both CPUs.

Table 12-36 TCON and TDISCON instructions

LAD / FBD		Description
	**"TCON_DB"(req:=_bool_in_, ID:=_undef_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, connect:=_struct_inout_);**	TCP and ISO on TCP: TCON initiates a communications connection from the CPU to a communication partner.
	**"TDISCON_DB"(req:=_bool_in_, ID:=_word_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_);**	TCP and ISO on TCP: TDISCON terminates a communications connection from the CPU to a communication partner.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 12-37 Data types for the parameters of TCON and TDISCON

Parameter and type		Data type	Description
REQ	IN	Bool	Control parameter REQ starts the job by establishing the connection specified by ID. The job starts at rising edge.
ID	IN	CONN_OUC (Word)	Reference to the connection to be established (TCON) or terminated (TDISCON) to the remote partner, or between the user program and the communication layer of the operating system. The ID must be identical to the associated parameter ID in the local connection description. Value range: W#16#0001 to W#16#0FFF
CONNECT (TCON)	IN_OUT	TCON_Param	Pointer to the connection description (Page 551)
DONE	OUT	Bool	• 0: Job is not yet started or still running. • 1: Job completed without error.
BUSY	OUT	Bool	• 0: Job is completed. • 1: Job is not yet completed. A new job cannot be triggered.
ERROR	OUT	Bool	Status parameters with the following values: • 0: No error • 1: Error occurred during processing. STATUS provides detailed information on the type of error.

Parameter and type		Data type	Description
STATUS	OUT	Word	Status information including error information. (Refer to the Error and Status condition codes in the table below.)

Both communication partners execute the TCON instruction to set up and establish the communication connection. You use parameters to specify the active and passive communication end point partners. After the connection is set up and established, it is automatically maintained and monitored by the CPU.

If the connection is terminated due to a line break or due to the remote communications partner, for example, the active partner attempts to re-establish the configured connection. You do not have to execute TCON again.

An existing connection is terminated and the set-up connection is removed when the TDISCON instruction is executed or when the CPU has gone into STOP mode. To set up and re-establish the connection, you must execute TCON again.

Table 12-38 ERROR and STATUS condition codes for TCON and TDISCON

ERROR	STATUS	Description
0	0000	Connection was established successfully.
0	7000	No job processing active
0	7001	Start job processing; establishing connection (TCON) or terminating connection (TDISCON)
0	7002	Follow-on call (REQ irrelevant); establishing connection (TCON) or terminating connection (TDISCON)
1	8086	The ID parameter is outside the permitted address range.
1	8087	TCON: Maximum number of connections reached; no additional connection possible.
1	809B	TCON: The local_device_id in the connection description does not match the CPU.
1	80A1	TCON: Connection or port is already occupied by user.
1	80A2	TCON: Local or remote port is occupied by the system.
1	80A3	Attempt being made to re-establish an existing connection (TCON) or terminate a non-existent connection (TDISCON).
1	80A4	TCON: IP address of the remote connection end point is invalid; it matches the local partner IP address.
1	80A5	TCON: Connection ID (Page 549) is already in use.
1	80A7	TCON: Communications error: You executed a TDISCON before the TCON completed. The TDISCON must first completely terminate the connection referenced by the ID.
1	80B2	TCON: The CONNECT parameter points to a data block that was generated with the attribute "Only store in load memory".
1	80B4	TCON: When using the ISO on TCP (connection_type = B#16#12) to establish a passive connection, condition code 80B4 alerts you that the TSAP entered did not conform to one of the following address requirements: • For a local TSAP length of 2 and a TSAP ID value of either E0 or E1 (hexadecimal) for the first byte, the second byte must be either 00 or 01. • For a local TSAP length of 3 or greater and a TSAP ID value of either E0 or E1 (hexadecimal) for the first byte, the second byte must be either 00 or 01 and all other bytes must be valid ASCII characters. • For a local TSAP length of 3 or greater and the first byte of the TSAP ID does not have a value of either E0 or E1 (hexadecimal), then all bytes of the TSAP ID must be valid ASCII characters. Valid ASCII characters are byte values from 20 to 7E (hexadecimal).

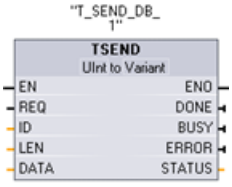
ERROR	STATUS	Description
1	80B5	TCON: Connection type "13 = UDP" permits only passive connection establishment.
1	80B6	TCON: Parameter assignment error in CONNECTION_TYPE parameter of the SDT TCON_Param.
1	80B7	TCON: Error in one of the following parameters of the data block for connection description: • block_length • local_tsap_id_len • rem_subnet_id_len • rem_staddr_len • rem_tsap_id_len • next_staddr_len Note: When operating TCON in TCP passive mode, the LOCAL_TSAP_ID_LEN must be "2" and the REM_TSAP_ID_LEN must be "0".
1	80B8	TCON: Parameter in the local connection description and Parameter ID are different.
1	80C3	TCON: All connection resources are in use.
1	80C4	Temporary communications error: • The connection cannot be established at this time (TCON). • The configured connection is currently being removed by TDISCON (TCON). • The connection is currently being established (TDISCON). • The interface is receiving new parameters (TCON and TDISCON).

TSEND and TRCV

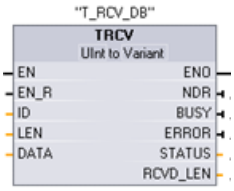
NOTE

When using PROFINET Open User communication, if you execute a TSEND instruction without a corresponding TRCV instruction executing on the remote device, then the TSEND instruction may reside indefinitely in a "Busy State", waiting for the TRCV instruction to receive the data. In this state, the TSEND instruction "Busy" output is set, and the "Status" output has a value of "0x7002". This condition may occur if you are transferring more than 4096 bytes of data. The issue is resolved at the next execution of the TRCV instruction.

Table 12-39 TSEND and TRCV instructions

LAD / FBD	SCL	Description
	**"TSEND_DB"(** **req:=_bool_in_,** **ID:=_word_in_,** **len:=_udint_in_,** **done=>_bool_out_,** **busy=>_bool_out_,** **error=>_bool_out_,** **status=>_word_out_,** **data:=_variant_inout_);**	TCP and ISO on TCP: TSEND sends data through a communication connection from the CPU to a partner station.

[1] STEP 7 automatically creates the DB when you insert the instruction.

LAD / FBD	SCL	Description
	**"TRCV_DB"(en_r:=_bool_in_, ID:=_word_in_, len:=_udint_in_, ndr=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, rcvd_len=>_udint_out_, data:=_variant_inout_);**	TCP and ISO on TCP: TRCV receives data through a communication connection from a partner station to the CPU.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 12-40 Data types for the parameters of TSEND and TRCV

Parameter and type		Data type	Description
REQ	IN	Bool	TSEND: Starts the send job on a rising edge. The data is transferred from the area specified by DATA and LEN.
EN_R	IN	Bool	TRCV: Enables the CPU to receive; with EN_R = 1, the TRCV is ready to receive. The receive job is processed.
ID	IN	CONN_OUC (Word)	Reference to the associated connection. ID must be identical to the associated parameter ID in the local connection description. Value range: W#16#0001 to W#16#0FFF
LEN	IN	UInt	Maximum number of bytes to be sent (TSEND) or received (TRCV): • Default = 0: The DATA parameter determines the length of the data to be sent (TSEND) or received (TRCV). • Ad hoc mode = 65535: A variable length of data is set for reception (TRCV).
DATA	IN_OUT	Variant	Pointer to send (TSEND) or receive (TRCV) data area; data area contains the address and length. The address refers to I memory, Q memory, M memory, or a DB.
DONE	OUT	Bool	TSEND: • 0: Job not yet started or still running. • 1: Job executed without error.
NDR	OUT	Bool	TRCV: • NDR = 0: Job not yet started or still running. • NDR = 1: Job successfully completed.
BUSY	OUT	Bool	• BUSY = 1: The job is not yet complete. A new job cannot be triggered. • BUSY = 0: Job is complete.
ERROR	OUT	Bool	ERROR = 1: Error occurred during processing. STATUS provides detailed information on the type of error
STATUS	OUT	Word	Status information including error information. (Refer to the Error and Status condition codes in the table below.)
RCVD_LEN	OUT	Int	TRCV: Amount of data actually received in bytes

NOTE

The TSEND instruction requires a low-to-high transition at the REQ input parameter to start a send job. The BUSY parameter is then set to 1 during processing. Completion of the send job is indicated by either the DONE or ERROR parameters being set to 1 for one scan. During this time, any low-to-high transition at the REQ input parameter is ignored.

TRCV Operations

The TRCV instruction writes the received data to a receive area that is specified by the following two variables:

- Pointer to the start of the area
- Length of the area or the value supplied at the LEN input if not 0

NOTE

The default setting of the LEN parameter (LEN = 0) uses the DATA parameter to determine the length of the data being transmitted. It is recommended that the data transmitted by the TSEND instruction be the same size as the DATA parameter of the TRCV instruction.

If using the default setting of the LEN parameter and it is necessary to send the data in segments smaller than the DATA parameter size, the following applies. It is recommended to keep the EN_R bit high until the corresponding TSEND transfers the appropriate amount of data to fill the TRCV DATA parameter. If the size of the data transmitted from TSEND does not equal the TRCV DATA parameter size, TRCV remains in a busy status (status code: 7002) while the EN_R bit is high until the overall size of the data transmitted from TSEND equals the TRCV DATA parameter size. If the EN_R bit of TRCV is pulsed, it needs to be pulsed the same number of times as TSEND is executed to receive the data.

The TRCV DATA parameter buffer does not display the new data received until the data size equals the DATA parameter buffer size.

As soon as all the job data has been received, TRCV transfers it to the receive area and sets NDR to 1.

Table 12-41 Entering the data into the receive area

Protocol variant	Entering the data in the receive area	Parameter "connection_type"	Value of the LEN parameter	Value of the RCVD_LEN parameter (bytes)
TCP	Ad hoc mode	B#16#11	65535	1 to 1460
TCP	Data reception with specified length	B#16#11	0 (recommended) or 1 to 8192, except 65535	1 to 8192
ISO on TCP	Ad hoc mode	B#16#12	65535	1 to 1460
ISO on TCP	protocol-controlled	B#16#12	0 (recommended) or 1 to 8192, except 65535	1 to 8192

NOTE

Ad hoc mode

The "ad hoc mode" exists with the TCP and ISO on TCP protocol variants. You set "ad hoc mode" by assigning "65535" to the LEN parameter. The receive area is identical to the area formed by DATA. The length of the received data will be output to the parameter RCVD_LEN. Immediately after receiving a block of data, TRCV enters the data in the receive area and sets NDR to 1.

If you store the data in an "optimized" DB (symbolic only), you can receive data only in arrays of Byte, Char, USInt, and SInt data types.

NOTE

Importing of S7-300/400 STEP 7 projects containing "ad hoc mode" into the S7-1200

In S7-300/400 STEP 7 projects, "ad hoc mode" is selected by assigning "0" to the LEN parameter. In the S7-1200, you set "ad hoc mode" by assigning "65535" to the LEN parameter.

If you import an S7-300/400 STEP 7 project containing "ad hoc mode" into the S7-1200, you must change the LEN parameter to "65535".

TSEND and TRCV Error and Status condition codes

ERROR	STATUS	Description
0	0000	• Send job completed without error (TSEND) • New data accepted: The current length of the received data is shown in RCVD_LEN (TRCV).
0	7000	• No job processing active (TSEND) • Block not ready to receive (TRCV)
0	7001	• Start of job processing, data being sent: During this processing the operating system accesses the data in the DATA send area (TSEND). • Block is ready to receive, receive job was activated (TRCV).
0	7002	• Follow-on instruction execution (REQ irrelevant), job being processed: The operating system accesses the data in the DATA send area during this processing (TSEND). • Follow-on instruction execution, receive job being processed: Data is written to the receive area during this processing. For this reason, an error could result in inconsistent data in the receive area (TRCV).
1	8085	• LEN parameter is greater than the largest permitted value (TSEND) and (TRCV). • LEN or DATA parameter changed since the first instruction execution (TRCV).
1	8086	The ID parameter is not in the permitted address range.
1	8088	The LEN parameter is larger than the memory area specified in DATA.
1	80A1	Communications error: • The specified connection has not yet established (TSEND and TRCV). • The specified connection is currently being terminated. Transmission or a receive job over this connection is not possible (TSEND and TRCV). • The interface is being reinitialized (TSEND). • The interface is receiving new parameters (TRCV).

ERROR	STATUS	Description
1	80C3	Internal lack of resources: A block with this ID is already being processed in a different priority class.
1	80C4	Temporary communications error: • The connection to the communications partner cannot be established at this time. • The interface is receiving new parameter settings, or the connection is currently being established.

Connection Ethernet protocols

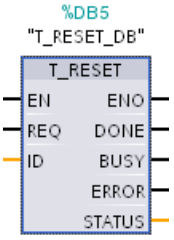
Every CPU has an integrated PROFINET port, which supports standard PROFINET communications. The TSEND_C, TRCV_C, TSEND and TRCV instructions all support the TCP and ISO on TCP Ethernet protocols.

Refer to "Device Configuration: Configuring the Local/Partner connection path (Page 532)" for more information.

12.6.8.15 T_RESET (Terminate and re-establish an existing connection) instruction

The "T_RESET" instruction terminates and then re-establishes an existing connection:

Table 12-42 T_RESET instruction

LAD / FBD	SCL	Description
	**"T_RESET_DB"(req:=_bool_in_, id:=_word_in_, done=>_bool_out_, error=>_bool_out_, status=>_word_out_);**	Use the T_RESET instruction to terminate and then re-establish an existing connection.

The local end points of the connection are retained. They are generated automatically:

- If a connection has been configured and loaded to the CPU.
- If a connection has been generated by the user program, for example, by calling the instruction "TCON (Page 578)".

The "T_RESET" instruction can be executed for all connection types regardless of whether the local interface of the CPU or the interface of a CM/CP was used for the connection. An exception to this is connections for data transfer in ad-hoc mode with TCP, as such connections cannot be referenced with a connection ID.

Once the instruction "T_RESET" has been called using the REQ parameter, the connection specified with the ID parameter is terminated and, if necessary, the data send and receive buffer cleared. Canceling the connection also cancels any data transfer in progress. There is therefore a risk of losing data if data transfer is in progress. The CPU defined as the active connection partner will then automatically attempt to restore the interrupted communication connection. You therefore do not need to call the "TCON (Page 578)" instruction to re-establish the communication connection.

The output parameters DONE, BUSY, and STATUS indicate the status of the job.

Data types for the parameters

The following table shows the parameters of the "T_RESET" instruction:

Parameter	Declaration	Data type	Memory area	Description
REQ	Input	BOOL	I, Q, M, D, L, T, C or constant	Control parameter REQUEST starts the job for terminating the connection specified by ID. The job starts on a rising edge.
ID	Input	CONN_OUC (WORD)	L, D or constant	Reference to the connection to the passive partner which is to be terminated. ID must be identical to the corresponding parameter ID in the local connection description. Range of values: W#16#0001 to W#16#0FFF
DONE	Output	BOOL	I, Q, M, D, L	Status parameter DONE • 0: Job not yet started or still executing. • 1: Job executed without errors.
BUSY	Output	BOOL	I, Q, M, D, L	Status parameter BUSY • 0: Job is complete. • 1: Job is not yet complete.
ERROR	Output	BOOL	I, Q, M, D, L	Status parameter ERROR • 0: No error occurred. • 1: Error occurred during processing. The STATUS parameter supplies detailed information on the type of error
STATUS	Output	WORD	I, Q, M, D, L	Status parameter STATUS Error information (see "STATUS parameter" table).

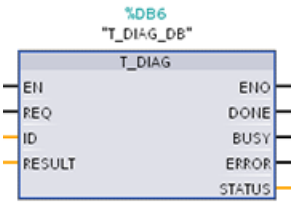
STATUS parameter

Error bit	STATUS* (W#16#...)	Description
0	0000	No error.
0	0001	Connection has not been established.
0	7001	Connection termination launched.
0	7002	Connection being terminated.
1	8081	Unknown connection specified at the ID parameter.

12.6.8.16 T_DIAG (Checks the status of connection and reads information) instruction

The "T_DIAG" instruction checks the status of a connection and reads further information on the local end point of this connection:

Table 12-43 T_DIAG instruction

LAD / FBD	SCL	Description
	**"T_DIAG_DB"(req:=_bool_in_, id:=_word_in_, done=>_bool_out_, error=>_bool_out_, status=>_dword_out_);**	Use the T_DIAG instruction to check the status of a connection and read further information on the local end point of this connection.

The "T_DIAG" instruction operates as follows:

- The connection is referenced by the ID parameter. You can read both connection end points configured in the connection editor and programmed connection end points (e.g. with the "TCON" instruction).

  Temporary connection end points (for example end points created when you connect to an engineering station) cannot be diagnosed, as no connection ID is generated in this process.
- The connection information read is stored in a structure referenced by the RESULT parameter.
- The output parameter STATUS indicates whether it was possible to read the connection information. The connection information in the structure at the RESULT parameter is only valid if the "T_DIAG" instruction has been completed with STATUS = W#16#0000 and ERROR = FALSE.

  Connection information cannot be evaluated if an error occurs.

Possible connection information

The "TDiag_Status" structure can be used to read the connection information at the RESULT parameter. The TDiag_Status structure only contains the most important information about a connection end point (for example, the protocol used, the connection status, and the number of data bytes sent or received).

The structure and parameters of the TDiag_Status structure are described below (see the "TDIAG_Status structure" table).

Data types for the parameters

The following table shows the parameters of the "T_DIAG" instruction:

Parameter	Declaration	Data type	Memory area	Description
REQ	Input	BOOL	I, Q, M, D, L, T, C or constant	Starts the instruction to check the connection specified in the ID parameter when there is a positive edge.
ID	Input	CONN_OUC (WORD)	L, D or constant	Reference to the assigned connection. Range of values: W#16#0001 to W#16#0FFF
RESULT	InOut	VARIANT	D	Pointer to the structure in which the connection information is stored. The structure TDiag_Status can be used at the RESULT parameter (for a description, see the "TDIAG_Status structure" table).
DONE	Output	BOOL	I, Q, M, D, L	Status parameter: • 0: Instruction not yet started or still in progress. • 1: Instruction executed without errors.
BUSY	Output	BOOL	I, Q, M, D, L	Status parameter: • 0: Instruction not yet started or already completed. • 1: Instruction not yet completed. A new job cannot be started.
ERROR	Output	BOOL	I, Q, M, D, L	Status parameter: • 0: No error. • 1: Error occurred.
STATUS	Output	WORD	I, Q, M, D, L	Status of the instruction

Parameters BUSY, DONE, and ERROR

You can check the status of "T_DIAG" instruction execution with the BUSY, DONE, ERROR and STATUS parameters. The BUSY parameter indicates the processing status. You use the DONE parameter to check whether or not an instruction has been executed successfully. The ERROR parameter is set if errors occur during execution of "T_DIAG".

The following table shows the relationship between the BUSY, DONE, and ERROR parameters:

BUSY	DONE	ERROR	Description
1	-	-	The instruction is being processed.
0	1	0	The instruction has been executed successfully. The data in the structure referenced by RESULT are only valid if this is the case.
0	0	1	Instruction completed with an error. The cause of the error is output at the STATUS parameter.
0	0	0	No new instruction has been assigned.

STATUS parameter

The following table shows the meaning of the values at the STATUS parameter:

Error bit	STATUS* (W#16#...)	Description
0	0000	The instruction "T_DIAG" has been executed successfully. The data in the structure referenced at the RESULT parameter can be evaluated.
0	7000	No instruction processing active.
0	7001	Instruction processing launched.
0	7002	Connection information is being read (REQ parameter irrelevant).
1	8086	The value at the ID parameter is outside the valid range (W#16#0001 ... W#16#0FFF).
1	8089	The RESULT parameter points to an invalid data type (structures TDIAG_Status and TDIAG_StatusExt only).
1	80A3	The ID parameter references a connection end point which does not exist. With programmed connections, this error can also occur after the "TDISCON" instruction is called.
1	80B1	The RESULT parameter was changed before the execution of T_DIAG was completed. A change of RESULT is not permitted during the execution of T_DIAG.
1	80C4	Internal error. Access to the connection end point is temporarily unavailable.

TDIAG_Status Structure

The table below details the form of the TDIAG_Status structure. The value of each element is only valid if the instruction has been executed without errors. If an error occurs, the content of the parameters will not change:

Name	Data type	Description
The following parameters are in the TDIAG_Status structure:		
InterfaceID	HW_ANY	Interface ID (LADDR) of the CPU or the CM/CP.
ID	CONN_OUC	ID of the connection diagnosed. Following a successful call, the value of this element is identical to the parameter ID of the "T_DIAG" instruction.
ConnectionType	BYTE	Protocol type used for connection: • 0x01: Not used. • ... • 0x0B: TCP protocol (IP_v4) • 0x0C: ISO-on-TCP protocol (RFC1006) • 0x0D: TCP protocol (DNS) • 0x0E: Dial-in protocol • 0x0F: WDC protocol • 0x10: SMTP protocol • 0x11: TCP protocol • 0x12: TCP and ISO-on-TCP protocol (RFC1006) • 0x13: UDP protocol • 0x14: Reserved • 0x15: PROFIBUS bus access protocol (FDL) • 0x16: ISO 8073 transport protocol (ISO native) • ... • 0x20: SMTP or SMTPS protocol - based on IPv4 • 0x21: SMTP or SMTPS protocol - based on IPv6 • 0x22: SMTP or SMTPS protocol - based on FQDN (**F**ully **Q**ualified **D**omain **N**ame)

Name	Data type	Description
		• ... • 0x70: S7 connection • Other: Reserved
ActiveEstablished	BOOL	• FALSE: Locally, the passive connection end point • TRUE: Locally, the active connection end point
State	BYTE	Current status of the connection end point • 0x00: Not used. • 0x01: Connection terminated. Temporary status, for example, after the "T_RESET" instruction is called. The system then automatically attempts to re-establish the connection. • 0x02: The active connection end point is attempting to establish a connection to the remote communication partner. • 0x03: The passive connection end point is waiting for establishment of the connection to the remote communication partner. • 0x04: Connection established. • 0x05: The connection is being terminated. This may be because the "T_RESET" or "T_DISCON" instruction has been called. Other possible reasons are protocol errors and line breaks. • 0x06..0xFF: Not used.
Kind	BYTE	Mode of the connection end point: • 0x00: Not used. • 0x01: Configured, static connection which has been configured and loaded to the CPU. • 0x02: Configured, dynamic connection which has been configured and loaded to the CPU (not currently supported). • 0x03: Programmed connection generated in the user program with the instruction "TCON". A call of the instruction "TDISCON" or a transition to CPU STOP status has destroyed the connection end point. • 0x04: Temporary, dynamic connection established by the engineering station (ES) or operator station (OS), for example. (this connection type cannot currently be diagnosed as there is no ID). • 0x05..0xFF: Not used.
SentBytes	UDINT	Number of data bytes sent.
ReceivedBytes	UDINT	Number of data bytes received.

12.6.8.17 TMAIL_C (Send an email using the Ethernet interface of the CPU) instruction

Overview

You use the TMAIL_C instruction to send an email using the Ethernet interface of the S7-1200 CPU.

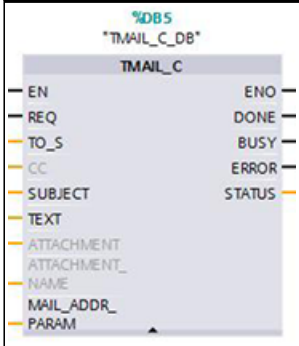
The TMAIL_C instruction has two functionalities:

- Email over the CPU Interface
- Email over a CP Interface

To use the TMAIL_C instruction, you must satisfy these prerequisites:

- You have configured the hardware
- The network infrastructure allows for a communication connection to the mail server

Table 12-44 TMAIL_C instruction

LAD / FBD	SCL	Description
	**"TMAIL_C_DB"(** **req:=_bool_in_,** **to_s:=_string_in_,** **cc:=_string_in_,** **subject:=_string_in_,** **text:=_string_in_,** **attachment:=_variant_in_,** **attachment_name:=_string_in_,** **mail_addr_param:=_string_in_,** **done=>_bool_out_,** **busy=>_bool_out_,** **error=>_bool_out_,** **status=>_word_out_);**	The TMAIL_C instruction sends an email using the Ethernet interface of the S7-1200 CPU.

[1] STEP 7 automatically creates the DB when you insert the instruction.

You define the content of the email and the connection data, using the following parameters:

- Recipient addresses with the TO_S and CC parameters
- Content of the email with the SUBJECT and TEXT parameters
- Optional attachment using VARIANT pointers at the ATTACHMENT and ATTACHMENT_NAME parameters
- Connection data, addressing and authentication for the mail server at the MAIL_ADDR_PARAM parameter (Page 609)

As of TMAIL_C version V6.0 or later and S7-1200 CPU firmware version V4.x, you can use the instruction TMAIL_C to send an email with secure communication over an integrated Ethernet port of your S7-1200 CPU. You define the data required for the sending process at the MAIL_ADDR_PARM parameter (Page 609) with the TMail_V4_SEC or TMail_QDN_SEC SDT.

You cannot send an SMS directly with the TMAIL_C instruction. Whether or not the mail server can forward an email as an SMS depends on your telecommunications provider.

Operation of the instruction

You start the sending of an email with an edge change from "0" to "1" for the REQ parameter. The TMAIL_C instruction indicates the job status by the "BUSY", "DONE", "ERROR" and "STATUS" output parameters.

The TMAIL_C instruction works asynchronously, which means its execution extends over multiple calls. You must specify an instance when you call the instruction "TMAIL_C".

In the following cases, the connection to the mail server will be lost:

- If the CPU switches to STOP while TMAIL_C instruction is active
- If communication problems occur at the Industrial Ethernet bus
  In this case, the transfer of the email will be interrupted and it will not reach its recipient.

The connection is also canceled after the instruction has successfully executed and sent the email.

NOTICE
Changing user programs Change the parts of the user program that directly affect calls of TMAIL_C only when: • The CPU is in "STOP" mode. • No email is being sent (REQ = 0 and BUSY = 0). This relates to deleting and replacing program blocks that contain TMAIL_C calls or calls for the instance of TMAIL_C. Ignoring this restriction can tie up connection resources. The automation system can change to an undefined status with the TCP/IP communication functions via Industrial Ethernet. Perform a warm or cold restart of the CPU after transferring changes. Property damage can occur if the TCP/IP communication functions change to an undefined status.

Data consistency

The TO_S, CC, SUBJECT, TEXT, ATTACHMENT and MAIL_ADDR_PARAM parameters are applied by the TMAIL_C instruction while it is running, which means that they may only be changed after the job has been completed (BUSY = 0).

SMTP authentication

Authentication refers to a procedure for verifying identity, for example, with a password query.

If you are using the S7-1200 CPU interface, the instruction TMAIL_C supports the SMTP authentication procedure AUTH-LOGIN which is required by most mail servers. For information about the authentication procedure of your mail server, refer to your mail server manual or the Web site of your Internet service provider.

- Before you can use the AUTH-LOGIN authentication procedure, the TMAIL_C instruction requires the user name with which it is to log on to the mail server. This user name corresponds to the user name with which you set up a mail account on your mail server. It is transferred via the UserName parameter to the structure at parameter MAIL_ADDR_PARAM.

  If no user name is specified at the MAIL_ADDR_PARAM parameter, the AUTH-LOGIN authentication procedure is not used. The email is then sent without authentication.
- To log on, the TMAIL_C instruction also requires the associated password. This password corresponds to the password you specified when you set up your mail account. It is transferred via the PassWord parameter to the structure at parameter MAIL_ADDR_PARAM.

Data types for the parameters

The following table shows the parameters of the TMAIL_C instruction:

Parameter	Declaration	Data type	Memory area	Description
REQ	Input	BOOL	I, Q, M, D, L, T, C or constant	Control parameter REQUEST: Activates the sending of an email upon a rising edge.
TO_S (Page 615)	Input	STRING	D	Recipient addresses STRING with a maximum length of 180 characters (bytes). For the email address format, please see the example in the parameter description.
CC (Page 615)	Input	STRING	D	CC recipient addresses (optional) STRING with a maximum length of 180 characters (bytes). Same email address format as for the TO_S parameter. If you assign an empty string here, the instruction does not send the email to a CC recipient.
SUBJECT	Input	STRING	D	Subject of the email STRING with a maximum length of 180 characters (bytes).
TEXT	Input	STRING	D	Text of the email (optional) STRING with a maximum length of 180 characters (bytes). If you assign an empty string at this parameter, the instruction sends the email without text.
ATTACHMENT	Input	VARIANT	D	Email attachment (optional) Reference to a char/byte/word/double word/string field (ArrayOfChar, ArrayOfByte, ArrayOfWord, ArrayOfDWord, or String) with a maximum length of 64 KB. Note: If you assign no value or an empty string to the ATTACHMENT parameter, the instruction sends the email without an attachment.
ATTACHMENT_-NAME	Input	VARIANT	D	Email attachment name (optional) Reference to a character string with a maximum length of 50 characters (bytes) to define the file name of the attachment. If an empty string is assigned at this parameter, the email attachment will be sent with the file name "attachment.bin". Using the AttachmentName parameter, you can assign the attachment name that appears when the communication partner receives the email. The TMail_FileReference SDT automatically uses the FileName parameter for the AttachmentName parameter.

Parameter	Declaration	Data type	Memory area	Description
				If using the TMail_FileReference SDT, the AttachmentName parameter does not apply. Leave it blank. If you enter data in the AttachmentName parameter when using the TMail_FileReference SDT, the TMAIL_C instruction produces an error. Refer to "Error condition codes, SFB_STATUS parameter of the instance DB" for further information.
MAIL_ADDR_PARAM (Page 609)	Input	VARIANT	D	Connection parameter and address of the email server To define the connection parameters, use the TMail_V4, TMail_FQDN, TMail_V4_SEC, or TMail_QDN_SEC SDT (see parameter description).
DONE (Page 616)	Output	BOOL	I, Q, M, D, L	Status parameter • DONE = 0: Job not yet started or still executing. • DONE = 1: Job was executed without errors.
BUSY (Page 616)	Output	BOOL	I, Q, M, D, L	Status parameter • BUSY=0: The processing of TMAIL_C was stopped. • BUSY = 1: E-mail transmission is not yet complete.
ERROR (Page 616)	Output	BOOL	I, Q, M, D, L	Status parameter • ERROR = 0: No error has occurred. • ERROR = 1: An error occurred during processing. STATUS supplies detailed information on the type of error.
STATUS (Page 618)	Output	WORD	I, Q, M, D, L	Status parameter Return value or error information of the TMAIL_C instruction (see parameter description).

NOTE

Optional parameters

The instruction sends the optional parameters CC, TEXT, and ATTACHMENT only if the corresponding parameters contain a string of length > 0.

MAIL_ADDR_PARAM parameter

At the MAIL_ADDR_PARAM parameter, you define the connection for sending the email and save the e-mail server address and login details.
The system data type (SDT) you use at the MAIL_ADDR_PARAM parameter depends on the format in which the email server is to be addressed:

SDT	Description	Interface support
TMail_V4	Addressing by IP address (IPv4)	CPU and CP
TMail_V6	Addressing by IP address (IPv6)	CP
TMail_FQDN	Addressing by Fully Qualified Domain Name (FQDN)	CP
TMail_V4_SEC	Secure addressing by IP address (IPv4)	CPU and CP
TMail_V6_SEC	Secure addressing by IP address (IPv6)	CP
TMail_QDN_SEC	Secure addressing by Fully Qualified Domain Name (FQDN)	CPU and CP

TMail_V4: Addressing the mail server by IP address (IPv4)

Parameter	Data type	Description
TMail_v4	Struct	
InterfaceId	LADDR	Hardware identifier of the Ethernet interface
ID	CONN_OUC	Connection ID
ConnectionType	BYTE	Connection type. Select 16#20 as the connection type for IPv4.
ActiveEstablished	BOOL	Active/passive connection establishment. The CPU is always the SMTP client.
CertIndex	BYTE	=0: SMTP used (**S**imple **M**ail **T**ransfer **P**rotocol). SMTP must be used if the email is being sent via the interface of an S7-1200 CPU. ≠0: SMTPS used to secure the connection (CP interface)
WatchDogTime	TIME	Execution watchdog. Use this parameter to define the maximum execution time for the send operation. This value determines how long the TMAIL_C instruction can remain in execution before a timeout is reached and the TMAIL_C instruction execution is stopped. As of TMAIL_C version V6.0, a WatchDogTime value of zero is now allowed, which signals the TMAIL_C instruction to disable the timer during execution. You can still enter a non-zero value for the WatchDogTime to make execution of the TMAIL_C instruction more deterministic. Note: Connection establishment can take longer (approx. one minute) if the connection is slow. When you specify the WatchDogTime parameter, remember to allow for the time required to establish the connection.
MailServerAddress	IP_v4	IP address of the mail server. IPv4 in the following format: XXX.XXX.XXX.XXX (decimal). Example: 192.142.131.237

Parameter	Data type	Description
UserName	STRING[254]	Mail server login name
PassWord	STRING[254]	Mail server password
From	EMAIL_ADDR	Email sender address, which is defined using the following two STRING parameters. For example: "myname@mymailserver.com".
LocalPartPlusAt-Sign	STRING[64]	Local part of sender address, including @ sign. Example: "myname@".
FullQualifiedDo-mainName	STRING[254]	Fully Qualified Domain Name (FQDN for short) of the mail server. Example: "mymailserver.com".

TMail_V6: Addressing the mail server by IP address to IPv6

Parameter	Data type	Description
TMail_V6	Struct	
InterfaceId	LADDR	Hardware identifier of the interface
ID	CONN_OUC	Connection ID
ConnectionType	BYTE	Connection type. Select 16#21 as the connection type for IPv6.
ActiveEstablished	BOOL	Status bit. Set to "1" once the connection is established.
CertIndex	BYTE	=0: SMTP used (**S**imple **M**ail **T**ransfer **P**rotocol). SMTP must be used if the e-mail is being sent via the interface of an S7-1500 CPU. ≠0: SMTPS used to secure the connection before it is established (with CPs/CMs). You use the CertIndex parameter to specify the certificate to be used (see "Project navigation" > "Global security settings" > "Certificate manager").
WatchDogTime	TIME	Execution watchdog. Use this parameter to define the maximum execution time for the send operation. Note: Connection establishment can take longer (approx. one minute) if the connection is slow. When you specify the WATCH_DOG_TIME parameter, remember to allow for the time required to establish the connection. The connection is terminated once the specified time has elapsed.
MailServerAddress	IP_V6	IP address of the mail server (IPv6) in the following format: XXXX.XXXX.XXXX.XXXX.XXXX.XXXX.XXXX.XXXX (hexadecimal). The address is divided into 8 blocks of 2 bytes each (16 bytes in total). Example: 2001:db8:1f11:08d3:290:27ff:0370:2093
UserName	STRING[254]	Mail server login name
PassWord	STRING[254]	Mail server password

Parameter	Data type	Description
From	EMAIL_ADDR	E-mail sender address, which is defined using the following two STRING parameters. For example: "myname@mymailserver.com".
LocalPartPlusAt-Sign	STRING[64]	Local part of sender address, including @ sign. Example: "myname@"
FullQualifiedDo-mainName	STRING[254]	Fully Qualified Domain Name (abbreviated to FQDN) of the mail server. Example: "mymailserver.com"

TMail_FQDN : Addressing the mail server by FQDN

Parameter	Data type	Description
TMail_FQDN	Struct	
InterfaceId	LADDR	Hardware identifier of the Ethernet interface
ID	CONN_OUC	Connection ID
ConnectionType	BYTE	Connection type. Select 16#22 as the connection type for FQDN.
ActiveEstablished	BOOL	Active/passive connection establishment. A Communications Processor (CP) is always the SMTP client.
CertIndex	BYTE	=0: SMTP used (**S**imple **M**ail **T**ransfer **P**rotocol). ≠0: SMTPS used to secure the connection before it is established (CP interface). CertIndex specifies the certificate to be used.
WatchDogTime	TIME	Execution watchdog. Use this parameter to define the maximum execution time for the send operation. Note: Connection establishment can take longer (approx. one minute) if the connection is slow. When you specify the WatchDogTime parameter, remember to allow for the time required to establish the connection.
MailServerAddress	STRING[254]	FQDN (**F**ully **Q**ualified **D**omain **N**ame) of the mail server. The mail server is addressed using the FQDN. Example: "www.mymailserver.com."
UserName	STRING[254]	Mail server login name
PassWord	STRING[254]	Mail server password
From	Struct	Email sender address, which is defined using the following two STRING parameters. For example: "myname@mymailserver.com".
LocalPartPlusAt-Sign	STRING[64]	Local part of sender address, including @ sign. Example: "myname@".
FullQualifiedDo-mainName	STRING[254]	Fully Qualified Domain Name (FQDN for short) of the mail server. Example: "mymailserver.com".

TMail_V4_SEC: Addressing the mail server by IP address (IPv4)

Parameter	Data type	Description
TMail_V4_SEC	Struct	
InterfaceId	LADDR	Hardware identifier of the Ethernet interface Value range: • 0 (new): The operating system selects a suitable integrated port itself. • Hardware identifier of the integrated port to be used.
ID	CONN_OUC	Reference to the connection: Value range: • 0 (new): The operating system selects a free connection ID from the internal range. • 1 to 4095: The connection ID to be used
ConnectionType	BYTE	Connection type. Select 16#20 as the connection type for IPv4.
ActiveEstablishment	BOOL	Active/passive connection establishment. The CPU is always the SMTP client.
WatchDogTime	TIME	Execution watchdog. Use this parameter to define the maximum execution time for the send operation. This value determines how long the TMAIL_C instruction can remain in execution before a timeout is reached and the TMAIL_C instruction execution is stopped. As of TMAIL_C version V6.0, a WatchDogTime value of zero is now allowed, which signals the TMAIL_C instruction to disable the timer during execution. You can still enter a non-zero value for the WatchDogTime to make execution of the TMAIL_C instruction more deterministic. Note: Connection establishment can take longer (approx. one minute) if the connection is slow. When you specify the WatchDogTime parameter, remember to allow for the time required to establish the connection.
MailServerAddress	IP_V4	IP address of the mail server intrinsic in IPv4 format: XXX.XXX.XXX.XXX (decimal place) Example: 192.142.131.237
UserName	STRING[254]	User name You must use your "user name" to access your email inbox in order to identify yourself as the owner of the email inbox to the email provider.
PassWord	STRING[254]	User password You must use your "password" to access your email inbox in order to identify yourself as the owner of the email inbox to the email provider.
From	EMAIL_ADDR	Email sender address, which is defined using the following two STRING parameters. For example: "myname@mymailserver.com"
LocalPartPlusAtSign	STRING[64]	Local part of sender address, including @ sign. Example: "myname@"
FullQualifiedDomainName	STRING[254]	Fully Qualified Domain Name (abbreviated to FQDN) of the mail server. Example: "mymailserver.com"
RemotePort	UINT	TCP port of the mail server

Parameter	Data type	Description
ActivateSecureConn	BOOL	0: SMTP connection (non-secure). In this case, the following parameters are irrelevant. 1: Secure SMTP connection
ExtTLSCapabilities	BYTE	Not currently used
TLSServerCertRef	UDINT	Reference to the X.509 V3 (CA) certificate of the mail server, which the TLS client uses to validate the authentication of the TLS server

TMail_V6_SEC: Addressing of the e-mail server via the IP address in IPv6 format

Parameter	Data type	Description
TMail_V6_SEC	Struct	
InterfaceId	LADDR	Hardware identifier of the Ethernet interface
ID	CONN_OUC	Connection ID
ConnectionType	BYTE	Connection type. Select 16#21 as the connection type for IPv6.
ActiveEstablishment	BOOL	Active/passive connection establishment. Because the CP is always the SMTP client, this parameter must be set to "1".
WatchDogTime	TIME	Execution watchdog. Use this parameter to define the maximum execution time for the send operation. Note: Connection establishment can take longer (approx. one minute) if the connection is slow. When you specify the WatchDogTime parameter, remember to allow for the time required to establish the connection. The connection is terminated once the specified time has elapsed.
MailServerAddress	IP_V6	IP address of the mail server in IPv6 format: XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX (hexadecimal). The address is divided into 8 blocks of 2 bytes each (16 bytes in total). Example: 2001:db8:1f11:08d3:290:27ff:0370:2093
UserName	STRING[254]	User name. This is required if users wants to access their email inbox in order to identify themselves as the owner of the email inbox to the email provider.
PassWord	STRING[254]	User password. This is required if users wants to access their email inbox in order to identify themselves as the owner of the email inbox to the email provider.

Parameter	Data type	Description
From	EMAIL_ADDR	E-mail sender address, which is defined using the following two STRING parameters. For example: "myname@mymailserver.com".
LocalPartPlusAtSign	STRING[64]	Local part of sender address, including @ sign. Example: "myname@"
FullQualifiedDomainName	STRING[254]	Fully Qualified Domain Name (abbreviated to FQDN) of the mail server. Example: "mymailserver.com"
RemotePort	UINT	TCP port of the mail server
ActivateSecureConn	BOOL	0: SMTP connection (non-secure). In this case, the following parameters are irrelevant. 1: Secure SMTP connection
ExtTLSCapabilities	BYTE	Not currently used
TLSServerCertRef	UDINT	Reference to the X.509 V3 (CA) certificate of the mail server, which is used by the TLS client to validate the authentication of the TLS server.

TMail_QDN_SEC: Addressing the mail server by FQDN

Parameter	Data type	Description
TMail_QDN_SEC	Struct	
InterfaceId	LADDR	Hardware identifier of the Ethernet interface Value range: • 0 (new): The operating system selects a suitable integrated port itself. • Hardware identifier of the integrated port to be used.
ID	CONN_OUC	Reference to the connection: Value range: • 0 (new): The operating system selects a free connection ID from the internal range. • 1 to 4095: The connection ID to be used
ConnectionType	BYTE	Connection type. Select 16#22 as the connection type for FQDN.
ActiveEstablishment	BOOL	Active/passive connection establishment. The CPU is always the SMTP client.
WatchDogTime	TIME	Execution watchdog. Use this parameter to define the maximum execution time for the send operation. This value determines how long the TMAIL_C instruction can remain in execution before a timeout is reached and the TMAIL_C instruction execution is stopped. As of TMAIL_C version V6.0, a WatchDogTime value of zero is now allowed, which signals the TMAIL_C instruction to disable the timer during execution. You can still enter a non-zero value for the WatchDogTime to make execution of the TMAIL_C instruction more deterministic. Note: Connection establishment can take longer (approx. one minute) if the connection is slow. When you specify the WatchDogTime parameter, remember to allow for the time required to establish the connection.

Parameter	Data type	Description
MailServerQDN	STRING[254]	FQDN (**F**ully **Q**ualified **D**omain **N**ame) of the mail server. The mail server is addressed using the fully qualified domain name, which must end with "." Example: "www.mymailserver.com."
UserName	STRING[254]	User name You must use your "user name" to access your email inbox in order to identify yourself as the owner of the email inbox to the email provider.
PassWord	STRING[254]	User password You must use your "password" to access your email inbox in order to identify yourself as the owner of the email inbox to the email provider.
From	EMAIL_ADDR	Email sender address, which is defined using the following two STRING parameters. For example: "myname@mymailserver.com"
LocalPartPlusAt-Sign	STRING[64]	Local part of sender address, including @ sign. Example: "myname@"
FullQualifiedDo-mainName	STRING[254]	Fully Qualified Domain Name (abbreviated to FQDN) of the mail server. Example: "mymailserver.com"
RemotePort	UINT	TCP port of the mail server
ActivateSecureConn	BOOL	0: SMTP connection (non-secure). In this case, the following parameters are irrelevant. 1: Secure SMTP connection
ExtTLSCapabilities	BYTE	Not currently used
TLSServerCertRef	UDINT	Reference to the X.509 V3 (CA) certificate of the mail server, which the TLS client uses to validate the authentication of the TLS server

TO_S and CC parameters

For TMAIL_C instructions prior to version 6.0 and S7-1200 CPU firmware V4.4, the following rules apply when entering the TO_S and CC parameters:

- Enter a space and an opening pointed bracket "<" before each address.
- Enter a closing pointed bracket ">" after each address.
- Enter a comma between the addresses in TO and CC.

The following are examples of these TO_S and CC parameter strings:

- <wenna@mydomain.com>, <ruby@mydomain.com>
- <admin@mydomain.com>, <judy@mydomain.com>

As of TMAIL_C instruction version 6.0 or later and S7-1200 CPU firmware V4.x, only the following rule applies when entering the parameters:

- Enter a comma or semicolon between the addresses in TO and CC.

The following are examples of these TO_S and CC parameter strings:

- wenna@mydomain.com, ruby@mydomain.com
- admin@mydomain.com, judy@mydomain.com

For runtime and memory space reasons, the TMAIL_C instruction does not perform a syntax check of parameter TO_S or CC.

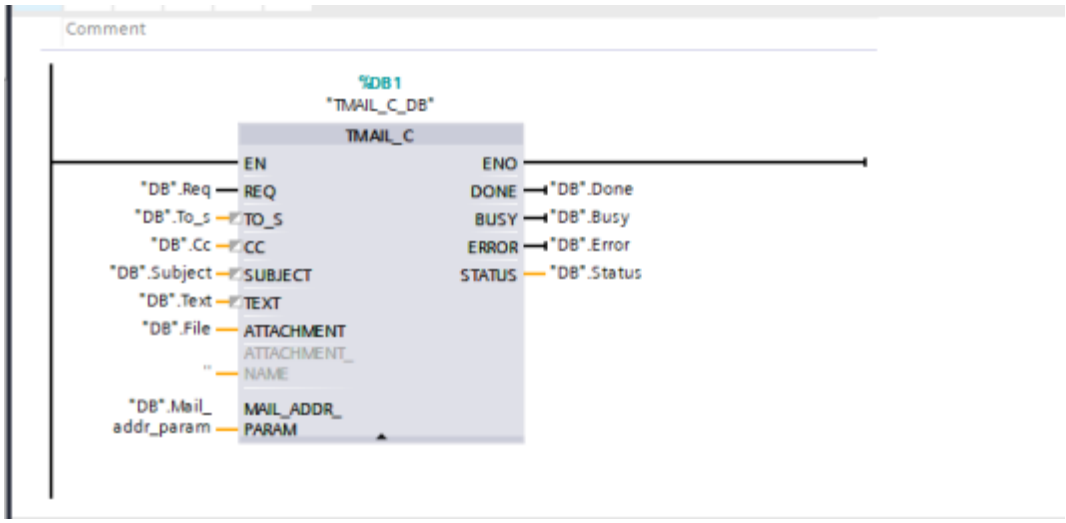
DONE, BUSY and ERROR parameters

The output parameters DONE, BUSY and ERROR are each displayed for only one cycle if the status of the BUSY output parameter changes from "1" to "0".
The following table shows the relationship between DONE, BUSY, and ERROR. Using this table, you can determine the current status of the instruction "TMAIL_C and when the sending of the email is complete.

DONE	BUSY	ERROR	Description
0	1	0	The job is being processed.
1	0	0	Job successfully completed.
0	0	1	The job ended with an error. The cause of the error can be found in the STATUS (Page 618) parameter.
0	0	0	The TMAIL_C instruction was not assigned a (new) job.

Sending data logs, recipes, and user files using email attachments

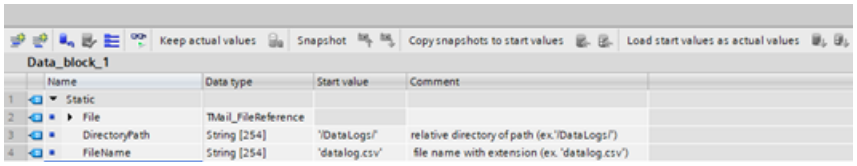
As of TMAIL_C version V6.0 or later and S7-1200 CPU firmware version V4.x, you can add and access the TMail_FileReference SDT using the Attachment parameter of the TMAIL_C instruction. You can then address a file path on the SIMATIC memory card (SMC). If no memory card is present, you can still access the recipe and data log directories on the PLC's internal load storage.
The TMail_FileReference SDT automatically uses the FileName parameter for the AttachmentName parameter.



TMail_FileReference SDT

The TMail_FileReference SDT consists of two parameters, both of which are SIMATIC strings:

- In the DirectoryPath parameter, you can address the directory of the desired file.
- The FileName parameter denotes the name of the file and the extension (if applicable) of the file that you wish to access in the directory, which is specified by the previous parameter.



The TMAIL_C instruction restricts you to the DataLogs, Recipes, or UserFiles directories when addressing the DirectoryPath parameter. You can also address subdirectories within these directories.

Beyond the above base directory restriction, the File Addressing Rules section below prescribes the rules that you must follow to address subdirectories and file names.

The size of the file that you can send is not restricted by the TMAIL_C instruction. You should keep this in mind when constructing your program.

File Addressing Rules

There are certain rules that must be followed to properly address a file using the TMail_FileReference SDT with the TMAIL_C instruction. The following subsections describe the specifics for the DirectoryPath and FileName, respectively. In general, the following applies to both parameters in the TMail_FileReference SDT and failure to follow these rules results in the TMAIL_C instruction producing an error status:

- You cannot use an empty string as a subdirectory or file name.
- You cannot use any ASCII control characters (Hex Range: 0x00 to 0x1F) in either parameter string.
- You cannot use the following reserved characters in either parameter string:
  - < (less than)
  - > (greater than)
  - : (colon)
  - " (double quote)
  - / (forward slash) (This character is allowed in the DirectoryPath as a separator)
  - \ (backslash)
  - | (vertical bar or pipe)
  - ? (question mark)
  - * (asterisk)
- No subdirectory or file name can end with a space or a period.

DirectoryPath

When entering the desired directory into the DirectoryPath parameter of the SDT, keep the following in mind. The root directory is inferred by the PLC's firmware logic and is not necessary for you to know. You can optionally enter a leading and trailing slash (/). If the user omits either slash, the firmware will automatically add these to the path. Thus, each of the following DirectoryPath entries are valid:

- /DataLogs/
- /DataLogs
- DataLogs/
- DataLogs

It is also possible to access a path at a greater depth than the base directory by using the following form, '/DataLogs/dir1/' where each (/) denotes a new directory. The maximum depth is eight, including the root directory.

In addition to the rules set forth in the File Addressing Rules section, you must be aware that the use of relative paths is strictly prohibited. Thus, '/DataLogs/' is an illegal path name. In addition, the use of a period in any subdirectory component to represent the current directory is prohibited (for example, '/DataLogs/').

FileName

When utilizing the FileName parameter of the SDT, keep in mind the rules laid out in the File Addressing Rules section. In addition to this, you must also be aware that the PLC's operating system limits the file name to less than 60 characters. If you attempt to address a file name greater than or equal to 60 characters, the TMAIL_C instruction aborts its operation and produces an error.

Aside from these exceptions, you can attach any file regardless of size or extension. The addressed file may or may not include a file extension.

Error condition codes

STATUS parameter

The following table shows the return values of TMAIL_C at the STATUS parameter:

Return value STATUS* (W#16#...):	Explanation	Notes
0000	The processing of TMAIL_C was completed without errors.	Error-free completion of TMAIL_C does not mean that the email sent will necessarily arrive. Incorrectly entering the recipient addresses does not generate a status error of the TMAIL_C instruction. In this case, there is no guarantee that the email will be sent to other recipients, even if these were entered correctly.
7001	TMAIL_C is active (BUSY = 1).	First call: Job triggered.
7002	TMAIL_C is active (BUSY = 1).	Intermediate call: Job already active.
8xxx	The processing of TMAIL_C was completed with an error code of the communication instructions called internally.	For detailed information, refer to the STATUS parameter descriptions for the TCON, TDISCON, TSEND and TRCV (Page 578) communication instructions.
8009	Internal function error	An internal function has returned an error. You can find detailed information in the SFB_STATUS parameter of the instance DB. Its possible values are described below.
8010	Error during connection establishment	You will find further information on evaluation in the SFB_STATUS parameter of the instance data block. The error code displayed at the SFB_STATUS parameter is explained in the STATUS parameter description for the TCON (Page 578) instruction.

Return value STATUS* (W#16#...):	Explanation	Notes
8011	Error sending the data	You will find further information on evaluation in the SFB_STATUS parameter of the instance data block. The error code displayed at the SFB_STATUS parameter is explained in the STATUS parameter description for the TSEND (Page 578) instruction.
8012	Error receiving the data	You will find further information on evaluation in the SFB_STATUS parameter of the instance data block. The error code displayed at the SFB_STATUS parameter is explained in the STATUS parameter description for the TRCV (Page 578) instruction.
8013	Error during connection establishment	You will find further information on evaluation in the SFB_STATUS parameter of the instance data block. The error code displayed at the SFB_STATUS parameter is explained in the STATUS parameter description for the TCON (Page 578) and TDISCON (Page 578) instructions.
8014	Establishment of a connection is not possible.	You may have entered an incorrect mail server IP address (MailServerAddress (Page 609)) or too short a time span (WatchDogTime (Page 609)) for connection establishment. It is also possible that the CPU has no connection to the network or that the CPU configuration is incorrect.
8015	Incorrect data type for MAIL_ADDR_PARAM	The only valid data types are the system data types (structures) Tmail_v4 and TMail_FQDN.
8016	Incorrect data type for the ATTACHMENT parameter	The valid data types are in the following list: • ArrayOfChar • ArrayOfByte • ArrayOfWord • ArrayOfDWord • String Note: The ArrayOfChar and String data types are only valid with TMAIL_C instruction version V5.0 or later.
8017	Incorrect data length for the ATTACHMENT parameter	Data length must be <= 65534 bytes.
82xx, 84xx, or 85xx	The error message originates from the mail server and corresponds, except for the "8", to the error number of the SMTP protocol. The following lines list several error codes that can occur.	You will find more detailed information on the SMTP error code and other error codes in the SMTP protocol on the Internet or in the error documentation of the mail server. You can also view the most recent error message from the mail server in your instance DB in the BUFFER1 parameter. You will find the last data sent by the TMAIL_C instruction under DATEN in the instance DB.
8450	Action not executed: Mailbox not available/cannot be reached	Try again later.

Return value STATUS* (W#16#...):	Explanation	Notes
8451	Action aborted: Local processing error	Try again later.
8500	Syntax error: Error not recognized. This also includes the error when a command string is too long. This can also occur when the email server does not support the LOGIN authentication procedure.	Check the parameters of TMAIL_C. Try to send an email without authentication. To do this, replace the content of the UserName parameter with an empty string. If no user name is specified, the LOGIN authentication procedure is not used.
8501	Syntax error: Incorrect input at a parameter	Possible cause: Incorrect address at the TO_S or CC parameter (see also: TO_S and CC parameters (Page 615)).
8502	Command unknown or not implemented	Check your entries, in particular the FROM parameter. It may be incomplete and you may have forgotten the "@" or "." (see also: TO_S and CC parameters (Page 615)).
8535	SMTP authentication incomplete	You have possibly entered an incorrect user name or incorrect password.
8550	Mail server cannot be reached. You have no access rights.	You may have entered an incorrect user name or password, or the mail server may not support your login. Another cause of error could be a mistake in the domain name after the "@" at the TO_S or CC parameter (see also: TO_S and CC parameters (Page 615)).
8552	Action aborted: Assigned memory size has been exceeded	Try again later.
8554	Transfer failed	Try again later.
* You can display error codes as integer or hexadecimal values in the program editor.		

SFB_STATUS parameter of the instance DB

With version V6.0 or later of the TMAIL_C instruction, the following return values are possible at the SFB_STATUS parameter of the instance DB:

Return values at the SFB_STATUS parameter of the instance DB (W#16#...)	Explanation
8085	The connection ID (ID parameter) is already being used by a configured connection.
8086	The ID parameter is outside the valid range.
8087	Maximum number of connections reached; no further connections possible
8088 *	The file does not exist or is currently unavailable.
8089 *	Unable to open the file because the number of simultaneously opened files has exceeded the system's limit. The limit per filesystem is 26 on the S7-1200.

* These error codes are added to the TMAIL_C instruction to assist in diagnosing improper file path addressing.

Return values at the SFB_STATUS parameter of the instance DB (W#16#...)	Explanation
808A *	The DirectoryPath contains a directory other than DataLogs, Recipes, or UserFiles, or one of the addressed subdirectories violates the previously-mentioned addressing rules. Refer to DirectoryPath (Page 616) for further information.
808B *	The FileName contains an illegal character sequence or has been left blank. Refer to FileName (Page 616) for further information.
808C *	The AttachmentName parameter must be blank when addressing a file path as an attachment.
8092	The TO_S and CC parameters are empty or the From sub-parameter is empty or incomplete.
8093	The MAIL_ADDR_PARAM parameter requires the connection to be upgraded to a secure connection, but the mail server does not support the STARTTLS command.
8095	Invalid response from mail server. The mail server may not be RFC-compliant.
809A	The SDT structure at the MAIL_ADDR_PARAM parameter is not supported at an integrated interface.
809B	Invalid interface ID in SDT at MAIL_ADDR_PARAM parameter
80A1	The specified connection or the remote port is already being used.
80A3	ID is used by a connection created by the user program.
80A4	IP address of the remote endpoint of the connection is invalid or it corresponds to the IP address of the local partner.
80A7	Communication error: You executed TDISCON before TMAIL_C had completed.
80B7	Remote port is 0 or IP address of the partner endpoint was set to 0.0.0.0.
80C3	Too few resources in the CPU
80C4	Temporary communication error: • The connection cannot be established at this time. • The connection cannot be established because the firewalls on the connection path are not open for the required ports. • The interface is currently receiving new parameters. • The configured connection is currently being removed by a TDISCON instruction.
80C5	The mail server refuses to establish the connection, has terminated the connection, or is actively ending it.
80C6	The connection partner cannot be reached (network error).
80C7	Execution timeout
80C8	Attempt being made to re-establish an existing connection.

* These error codes are added to the TMAIL_C instruction to assist in diagnosing improper file path addressing.

Return values at the SFB_STATUS parameter of the instance DB (W#16#...)	Explanation
80C9	Validation of the connection partner failed. The mail server does not correspond to the defined partner at the MailServerAddress parameter.
80CE	The IP address of the local interface is 0.0.0.0.
80D0	The MailServerAddress parameter contains an empty string in the attempt to use DNS.
80D1	The MailServerAddress parameter is not a fully qualified domain name. The period at the end may be missing.
80D2	You did not configure a DNS server address.
80D3	The Fully Qualified Domain Name (FQDN) could not be resolved. Possible causes: • The DNS server cannot be reached (for example. the DNS server has been shut down or the remote port cannot be reached). • An error occurred during communication with the DNS server. • The DNS server returned a valid DNS response; however, the response contained no IPv4 address.
80E0	Communication with the mail server failed due to a message with errors. Possible causes: • Invalid message authentication code • Message decoding failed. • Error decompressing a message • Internal capacity overflow
80E1	Error during the handshake. Possible causes: • Abort by the user • Security not high enough • Renewed negotiation is not supported • SSL/TLS version is not supported. • Decryption error
80E2	Certificate not supported / invalid Possible cause: The time-of-day of the module concerned is not set or the module is not synchronized. Example: The default setting for the date of the module is 1/1/2012, and the date was not set during commissioning. The validity period of the certificate starts on 20 August 2016 and ends on 20 August 2024. In this case, the date of the module is outside the validity period of the certificate; the certificate is invalid for the module.
80E3	Mail server certificate has been discarded.
80E4	No valid certification authority found for the mail server certificate.
80E5	Mail server certificate expired.

* These error codes are added to the TMAIL_C instruction to assist in diagnosing improper file path addressing.

Return values at the SFB_STATUS parameter of the instance DB (W#16#...)	Explanation
80E6	Integrity errors in the Transport-Layer-Security (TLS) protocol
80E7	Unsupported extension in mail server certificate
80E9	TLS server without server certificate is not supported

* These error codes are added to the TMAIL_C instruction to assist in diagnosing improper file path addressing.

12.6.8.18 UDP

UDP is a standard protocol described by RFC 768: User Datagram Protocol. UDP provides a mechanism for one application to send a datagram to another; however, delivery of data is not guaranteed. This protocol has the following features:

- A quick communications protocol
- Suitable for small-sized to medium data amounts (up to 2048 bytes)
- UDP is a simpler transport control protocol than TCP, with a thin layer that yields low overheads
- Can be used very flexibly with many third-party systems
- Routing-capable
- Uses port numbers to direct the datagrams
- Messages are unacknowledged: The application is required to take responsibility for error recovery and security
- Programming effort is required for data management due to the SEND / RECEIVE programming interface

UDP supports broadcast communication. To use broadcast, you must configure the IP address portion of the ADDR configuration. For example: A CPU with an IP address of 192.168.2.10 and subnet mask of 255.255.255.0 would use a broadcast address of 192.168.2.255.

For further information, see "Configuring connections > Creating UDP/FDL connections with broadcast/multicast" in the TIA Portal Information System

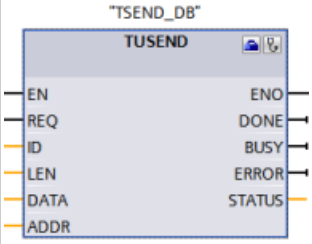
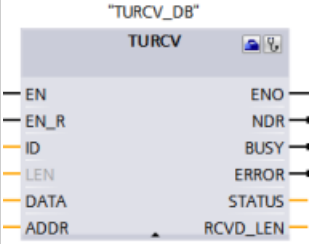
12.6.8.19 TUSEND and TURCV

The following instructions control the UDP communication process:

- TCON establishes the communication between the client and server (CPU) PC.
- TUSEND and TURCV send and receive data.
- TDISCON disconnects the communication between the client and server.

Refer to TCON, TDISCON, TSEND, and TRCV (Page 578) in the "TCP and ISO-on-TCP" section for more information on the TCON and TDISCON communication instructions.

Table 12-45 TUSEND and TURCV instructions

LAD / FBD	SCL	Description
	**"TUSEND_DB"(req:=_bool_in_, ID:=_word_in_, len:=_udint_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, data:=_variant_inout_);**	The TUSEND instruction sends data via UDP to the remote partner specified by the parameter ADDR. To start the job for sending data, call the TUSEND instruction with REQ = 1.
	**"TURCV_DB"(en_r:=_bool_in_, ID:=_word_in_, len:=_udint_in_, ndr=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, rcvd_len=>_udint_out_, data:=_variant_inout_);**	The TURCV instruction receives data via UDP. The parameter ADDR shows the address of the sender. After successful completion of TURCV, the parameter ADDR contains the address of the remote partner (the sender). TURCV does not support ad hoc mode. To start the job for receiving data, call the TURCV instruction with EN_R = 1.

[1] STEP 7 automatically creates the DB when you insert the instruction.

TCON, TDISCON, TUSEND, and TURCV operate asynchronously, which means that the job processing extends over multiple instruction executions.

⚠ WARNING

Data transfer via UDP

RFC 768 specifies that UDP transfers data to the partner without acknowledgement, making it a non-secure method. The lack of acknowledgement can result in loss of data without any indication or notification. Transferring more than 1472 bytes significantly increases the risk of undetected transmission errors.

Design your program so that safety-critical functionality does not rely on successfully transmitting and receiving UDP messages. Instead, use a connection-oriented communication protocol.

Failure to follow these precautions can cause death or severe personal injury.

⚠ WARNING

Unsecured data transfer

RFC 768 specifies that UDP transfers data to the remote partner without acknowledgement, making it an unreliable method. This lack of acknowledgement can result in data loss without any indication from the block.

Design your program so that safety-critical functionality does not rely on successfully transmitting and receiving UDP messages. Instead, use a connection-oriented communication protocol.

Failure to follow these precautions can cause death or severe personal injury.

Table 12-46 TUSEND and TURCV data types for the parameters

Parameter and type		Data type	Description
REQ (TUSEND)	IN	Bool	Starts the send job on a rising edge. The data is transferred from the area specified by DATA and LEN.
EN_R (TURCV)	IN	Bool	• 0: CPU cannot receive. • 1: Enables the CPU to receive. The TURCV instruction is ready to receive, and the receive job is processed.
ID	IN	Word	Reference to the associated connection between the user program and the communication level of the operating system. ID must be identical to the associated parameter ID in the local connection description. Range of values: W#16#0001 to W#16#0FFF.
LEN	IN	UDInt	Number of bytes to be sent (TUSEND) or received (TURCV). • Default = 0. The DATA parameter determines the length of the data to be sent or received. • Otherwise, range of values: 1 to 2048
DONE (TUSEND)	IN	Bool	Status parameter DONE (TUSEND): • 0: Job is not yet started or still running. • 1: Job completed without error.
NDR (TURCV)	OUT	Bool	Status parameter NDR (TURCV): • 0: Job not yet started or still running. • 1: Job has successfully completed.
BUSY	OUT	Bool	• 1: Job is not yet completed. A new job cannot be triggered. • 0: Job has completed.
ERROR	OUT	Bool	Status parameters with the following values: • 0: No error • 1: Error occurred during processing. STATUS provides detailed information on the type of error.
STATUS	OUT	Word	Status information including error information. (Refer to the Error and Status condition codes in the table below.)
RCVD_LEN	OUT	UDInt	Number of bytes received (TURCV)
DATA	IN_OUT	Variant	Address of the sender area (TUSEND) or receive area (TURCV): • The process image input table • The process image output table • A memory bit • A data block
ADDR	IN_OUT	Variant	Pointer to the address of the receiver (for TUSEND) or sender (for TURCV) (for example, P#DB100.DBX0.0 byte 8). The pointer may point to any memory area. A structure of 8 bytes is required as follows: • First 4 bytes contain the remote IP address. • Next 2 bytes specify the remote port number. • Last 2 bytes are reserved.

The job status is indicated at the output parameters BUSY and STATUS. STATUS corresponds to the RET_VAL output parameter of asynchronously functioning instructions.

The following table shows the relationships between BUSY, DONE (TUSEND), NDR (TURCV), and ERROR. Using this table, you can determine the current status of the instruction (TUSEND or TURCV) or when the sending (transmission) / receiving process is complete.

Table 12-47 Status of BUSY, DONE (TUSEND) / NDR (TURCV), and ERROR parameters

BUSY	DONE / NDR	ERROR	Description
TRUE	irrelevant	irrelevant	The job is being processed.
FALSE	TRUE	FALSE	The job was completed successfully.
FALSE	FALSE	TRUE	The job was ended with an error. The cause of the error can be found in the STATUS parameter.
FALSE	FALSE	FALSE	The instruction was not assigned a (new) job.

[1] Due to the asynchronous function of the instructions: For TUSEND, you must keep the data in the sender area consistent until the DONE parameter or the ERROR parameter assumes the value TRUE. For TURCV, the data in the receiver area are only consistent when the NDR parameter assumes the value TRUE.

Table 12-48 TUSEND and TURCV condition codes for ERROR and STATUS

ERROR	STATUS	Description
0	0000	• Send job completed without error (TUSEND). • New data were accepted. The current length of the received data is shown in RCVD_LEN (TURCV).
0	7000	• No job processing active (TUSEND) • Block not ready to receive (TURCV)
0	7001	• Start of job processing, data being sent (TUSEND): During this processing, the operating system accesses the data in the DATA send area. • Block is ready to receive, receive job was activated (TURCV).
0	7002	• Follow-on instruction execution (REQ irrelevant), job being processed (TUSEND): During this processing, the operating system accesses the data in the DATA send area. • Follow-on instruction execution, job being processed: During this processing, the TURCV instruction writes data to the receive area. For this reason, an error could result in inconsistent data in the receive area.
1	8085	LEN parameter is greater than the largest permitted value, has the value 0 (TUSEND), or you changed the value of the LEN or DATA parameter since the first instruction execution (TURCV).
1	8086	The ID parameter is not in the permitted address range.
1	8088	• LEN parameter is larger than the memory area (TUSEND) or receive area (TURCV) specified in DATA. • Receive area is too small (TURCV).
1	8089	ADDR parameter does not point to a data block.
1	80A1	Communications error: • The specified connection between user program and communications layer of the operating system has not yet been established. • The specified connection between the user program and the communication layer of the operating system is currently being terminated. Transmission (TUSEND) or a receive job (TURCV) over this connection is not possible. • The interface is being reinitialized.
1	80A4	IP address of the remote connection end point is invalid; it is possible that it matches the local IP address (TUSEND).

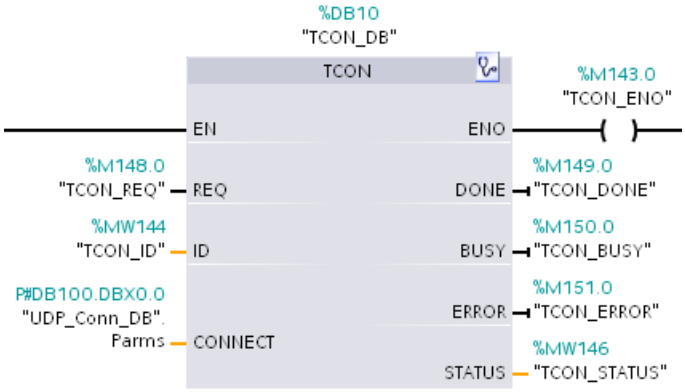
ERROR	STATUS	Description
1	80B3	• The set protocol variant (connection_type parameter in the connection description) is not UDP. Please use the TSEND or TRCV instruction. • ADDR parameter: Invalid settings for port number (TUSEND)
1	80C3	• A block with this ID is already being processed in a different priority class. • Internal lack of resources
1	80C4	Temporary communications error: • The connection between the user program and the communication level of the operating system cannot be established at this time (TUSEND). • The interface is receiving new parameters (TUSEND). • The connection is currently being reinitiated (TURCV).

Connection Ethernet protocols

Every CPU has an integrated PROFINET port, which supports standard PROFINET communications. The TUSEND and TURCV instructions support the UDP Ethernet protocol. Refer to "Configuring the Local/Partner connection path" (Page 532)" in the "Device configuration" chapter for more information.

Operations

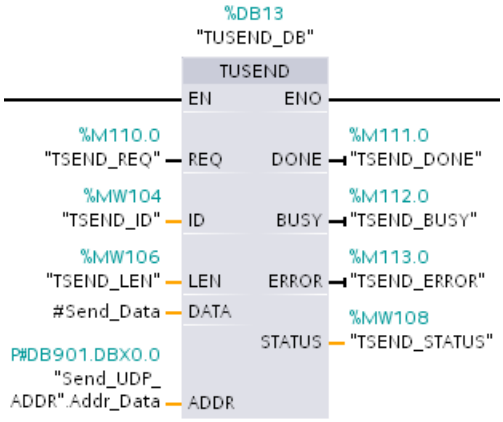
Both partners are passive in UDP communication. Typical parameter start values for the "TCON_Param" data type are shown in the following figures. Port numbers (LOCAL_TSAP_ID) are written in a 2-byte format. All ports except for 161, 34962, 34963, and 34964 are allowed.



UDP_Conn_DB

	Name	Data type	Offset	Initial value	Comment
1	Static				
2	Parms	TCON_Param	0.0		
3	BLOCK_LENGTH	UInt	0.0	64	byte length of SDT
4	ID	CONN_OUC	2.0	1	reference to the connection
5	CONNECTION_TYPE	USInt	4.0	19	17: TCP/IP, 18: ISO on TCP
6	ACTIVE_EST	Bool	5.0	false	active/passive connection establishment
7	LOCAL_DEVICE_ID	USInt	6.0	1	1: local IE interface
8	LOCAL_TSAP_ID_L...	USInt	7.0	2	byte length of local TSAP id/port number
9	REM_SUBNET_ID_...	USInt	8.0	0	byte length of remote subnet id
10	REM_STADDR_LEN	USInt	9.0	0	byte length of remote IP address
11	REM_TSAP_ID_LEN	USInt	10.0	0	byte length of remote port/TSAP id
12	NEXT_STADDR_LEN	USInt	11.0	0	byte length of next station address
13	LOCAL_TSAP_ID	Array[1..16] of Byte	12.0		TSAP id/local port number
14	LOCAL_TSAP_I...	Byte		B#16#07	
15	LOCAL_TSAP_I...	Byte		B#16#D0	

The TUSEND instruction sends data through UDP to the remote partner specified in the "TADDR_Param" data type. The TURCV instruction receives data through UDP. After a successful execution of the TURCV instruction, the "TADDR_Param" data type shows the address of the remote partner (the sender), as shown in the figures below.



Send_UDP_ADDR

	Name	Data type	Offset	Initial value	Comment
1	Static				
2	Addr_Data	TADDR_Param	0.0		
3	REM_IP_ADDR	Array[1..4] of USint	0.0		remote station address
4	REM_IP_ADDR[1]	USInt		192	
5	REM_IP_ADDR[2]	USInt		168	
6	REM_IP_ADDR[3]	USInt		2	
7	REM_IP_ADDR[4]	USInt		10	
8	REM_PORT_NR	UInt	4.0	2000	remote port number
9	RESERVED	Word	6.0	0	ununsed; has to be 0

12.6.8.20 T_CONFIG

The T_CONFIG instruction can change the Ethernet address, the PROFINET device name, or the IP addresses of the NTP servers for time-of-day synchronization from within the user program. The following features can be adjusted permanently or temporarily:

- IP address
- Subnet mask
- Router address
- Station name
- IP addresses of up to four NTP servers

NOTE

Located in the CPU "Properties", "Ethernet address" page, the "IP address is set directly at the device" (Page 635) radio button allows you to change the IP address online or by using the "T_CONFIG" instruction after the program is downloaded.

Located in the CPU "Properties", "Ethernet address" page, the "PROFINET device name is set directly at the device" (Page 636) radio button allows you to change the PROFINET device name online or by using the "T_CONFIG" instruction after the program is downloaded.

Located in the CPU "Properties", "Time synchronization" page, the "Enable time synchronization via NTP server" (Page 638) box allows you to change the IP addresses of up to four NTP servers.

NOTE

You cannot execute more than one T_CONFIG instruction at a time.

NOTE

Changes to the IP address or name of station of the CPU can be temporary or permanent. Changes to the NTP server IP addresses can only be temporary:

– A permanent change indicates that the change is retentive, meaning that the change persists through a power failure.
– A temporary change indicates that the change is volatile and reverts to the original value after a power loss.

Table 12-49 T_CONFIG instruction

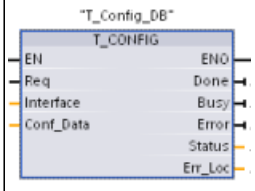
LAD / FBD	SCL	Description
	**"T_CONFIG_DB"(Req:=_bool_in_, Interface:=_uint_in_, Conf_Data:=_variant_in_, Done=>_bool_out_, Busy=>_bool_out_, Error=>_bool_out_, Status=>_dword_out_, Err_Loc=>_dword_out_);**	Use the T_CONFIG instruction to change the IP configuration parameters from your user program. T_CONFIG works asynchronously. The execution extends over multiple calls.

Table 12-50 T_CONFIG data types for the parameters

Parameter and type		Data type	Description
REQ	Input	Bool	Starts the instruction on the rising edge.
INTERFACE	Input	HW_Interface	ID of network interface
CONF_DATA	Input	Variant	Reference to the structure of the configuration data; CONF_DATA is defined by a struct containing up to four System Data Types (SDT).
DONE	Output	Bool	• 0: Job has not yet started or is still running. • 1: Job was executed without error.
BUSY	Output	Bool	• 0: The job is complete. • 1: The job is not yet complete. A new job cannot be triggered.
ERROR	Output	Bool	Status parameters with the following values: • 0: No error • 1: Error occurred during processing. STATUS provides detailed information on the type of error.
STATUS	Output	DWord	Status information including error information. (Refer to the Error and Status condition codes in the table below.)
ERR_LOC	Output	DWord	Fault location (field ID and subfield location within the CONF_DATA structure)

The IP configuration information is placed in the CONF_DATA data block, along with a Variant pointer on parameter CONF_DATA referenced above. The successful execution of the T_CONFIG instruction ends with the handover of the IP configuration data to the network interface.

The status and error messages of the instruction "T_CONFIG" are output at the parameters STATUS and ERR_LOC:

- The cause of the error is output at the parameter STATUS.
- The location of the error that occurred is output at the parameter ERR_LOC. The following options are available here:
  - 16#0000_0000: No error or error when calling the instruction (for example, errors when assigning parameters to the instruction or in communication with the PROFINET interface).
  - 16#0001_0000: Error with the configuration data in the parameters of the system data type IF_CONF_HEADER.
  - 16#0001_000x: Error in the configuration data in the parameters of system data type IF_CONF_V4 or IF_CONF_NOS or IF_CONF_NTP (x specifies the position of the bad sub-block in the T_CONFIG structure. If the T_CONFIG structure contains, for example, a sub-block for the IP address and a sub-block for the station name, and the error is located in the sub-block for the station name, ERR_LOC has the value 0001_0002.)

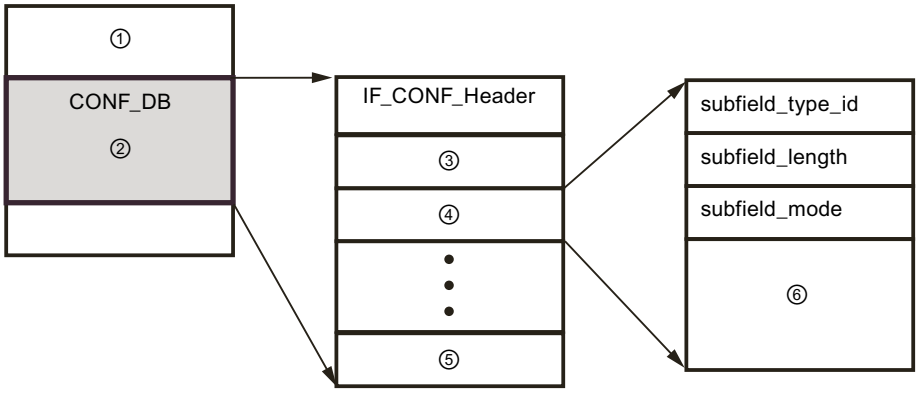
The following table shows the possible values for the parameters STATUS and ERR_LOC:

STATUS*	ERR_LOC*	Explanation
0000_0000	0000_0000	Order processing completed without errors.
0070_0000	0000_0000	No job processing active.
0070_0100	0000_0000	Start of the order processing.
0070_0200	0000_0000	Intermediate call (REQ irrelevant).
C08x_yy00	0000_0000	General error information.
C080_8000	0000_0000	Error at call of the instruction: The hardware ID at the parameter Interface is invalid.
C080_8100	0000_0000	Error at call of the instruction: The hardware ID at the parameter Interface does not address a PROFINET interface.
C080_8700	0000_0000	Error at call of the instruction: Incorrect length of the data block at the parameter CONF_DATA.
C080_8800	0001_0000	Error in the system data type IF_CONF_HEADER: The parameter FieldType has an invalid value. Use the value "0" for FieldType.
C080_8900	0001_0000	Error in the system data type IF_CONF_HEADER: The parameter FieldId has an invalid value or was used several times. Use the value "0" for FieldId.
C080_8A00	0001_0000	Error in the system data type IF_CONF_HEADER: Incorrect number at the parameter SubfieldCount. Enter the correct number of system data types IF_CONF_V4, IF_CONF_NOS, or IF_CONF_NTP being used.
C080_8B00	0001_000x	Error in the system data type IF_CONF_V4, IF_CONF_NOS, or IF_CONF_NTP: The parameter Id has an invalid value. For IF_CONF_V4 use "30", for IF_CONF_NOS "40", for IF_CONF_NTP "17".
C080_8C00	0001_000x	Error in the system data type IF_CONF_V4, IF_CONF_NOS, or IF_CONF_NTP: Incorrect data type system used, wrong order or multiple use of a system data type.
C080_8D00	0001_000x	Error in the system data type IF_CONF_V4, IF_CONF_NOS, or IF_CONF_NTP: The parameter Length has an incorrect or invalid value.
C080_8E00	0001_000x	Error in the system data type IF_CONF_V4, IF_CONF_NOS, or IF_CONF_NTP: The parameter Mode has an incorrect or invalid value. • With IF_CONF_V4 and IF_CONF_NOS only the values "1" (permanent) or "2" (temporary) are permitted. • With IF_CONF_NTP only the value "2" (temporary) is permitted.
C080_9000	0001_000x	Error in the system data type IF_CONF_V4, IF_CONF_NOS, or IF_CONF_NTP: Configuration data cannot be applied. Possible cause: • With IF_CONF_V4: In the hardware configuration, the setting "Set IP address on the device" was not selected.. • With IF_CONF_NOS: In the hardware configuration, the setting "Set PROFINET device name on the device" was not selected.. • With IF_CONF_NTP: In the hardware configuration, the setting "Enable time synchronization via NTP server " was not selected and no IP address was set for NTP servers..
C080_9400	0001_000x	Error in the system data type IF_CONF_V4, IF_CONF_NOS, or IF_CONF_NTP: A parameter value is undefined or invalid.
C080_9500	0001_000x	Error in the system data type IF_CONF_V4, IF_CONF_NOS, or IF_CONF_NTP: The values of two parameters are inconsistent.

STATUS*	ERR_LOC*	Explanation
C080_C200	0000_0000	Error at call of the instruction: The configuration data cannot be transferred. Possible cause: The PROFINET interface is not accessible.
C080_C300	0000_0000	Error at call of the instruction: Insufficient resources (for example, multiple calling of "T_CONFIG" with different parameters).
C080_C400	0000_0000	Error at call of the instruction: Temporary communication error. Time indication for change to daylight saving time.
C080_D200	0000_0000	Error at call of the instruction: Call not possible. Instruction is not supported by the selected PROFINET interface.

CONF_DATA Data block

The following diagram shows how the configuration data to be transferred is stored in the configuration DB.



① Configuration DB
② Configuration data
③ Subfield 1
④ Subfield 2
⑤ Subfield *n*
⑥ Subfield-specific parameters

The configuration data of CONF_DB consists of a field that contains a header (IF_CONF_Header) and several subfields. IF_CONF_Header provides the following elements:

- field_type_id (data type UInt): Zero
- field_id (data type UInt): Zero
- subfield_cnt (data type UInt): Number of subfields

Each subfield consists of a header (subfield_type_id, subfield_length, subfield_mode) and the subfield-specific parameters. Each subfield must consist of an even number of bytes. The subfield_mode can support a value of 1 or 2. Please refer to the tables below.

NOTE

Only one field (IF_CONF_Header) is currently allowed. Its parameters field_type_id and field_id must have the value zero. Other fields with different values for field_type_id and field_id are subject to future extensions.

Table 12-51 Subfields supported

subfield_type_id	Data type	Explanation
30	IF_CONF_V4	IP parameters: IP address, subnet mask, router address
40	IF_CONF_NOS	PROFINET IO device name (Name of station)
17	IF_CONF_NTP	Network Time Protocol (NTP)

Table 12-52 Elements of the IF_CONF_V4 data type

Name		Data type	Start value	Description
Id		UInt	30	subfield_type_id
Length		UInt	18	subfield_length
Mode		UInt	0	subfield_mode (1: permanent or 2: temporary)
InterfaceAddress		IP_V4	-	Interface address
ADDR		Array [1..4] of Byte		
	ADDR[1]	Byte	0	IP address high byte: 200
	ADDR[2]	Byte	0	IP address high byte: 12
	ADDR[3]	Byte	0	IP address low byte: 1
	ADDR[4]	Byte	0	IP address low byte: 144
SubnetMask		IP_V4	-	Subnet mask
ADDR		Array [1..4] of Byte		
	ADDR[1]	Byte	0	Subnet mask high byte: 255
	ADDR[2]	Byte	0	Subnet mask high byte: 255
	ADDR[3]	Byte	0	Subnet mask low byte: 255
	ADDR[4]	Byte	0	Subnet mask low byte: 0
DefaultRouter		IP_V4	-	Default router
ADDR		Array [1..4] of Byte		
	ADDR[1]	Byte	0	Router high byte: 200
	ADDR[2]	Byte	0	Router high byte: 12
	ADDR[3]	Byte	0	Router low byte: 1
	ADDR[4]	Byte	0	Router low byte: 1

Table 12-53 Elements of the IF_CONF_NOS data type

Name	Data type	Start value	Description
Id	UInt	40	subfield_type_id
Length	UInt	246	subfield_length
Mode	UInt	0	subfield_mode (1: permanent or 2: temporary)
NOS (Name of station)	Array[1..240] of Byte	0	Station name: You must occupy the ARRAY from the first byte. If the ARRAY is longer than the station name to be assigned, you must enter a zero byte after the actual station name (in conformity with IEC 61158-6-10). Otherwise, NOS is rejected and the "T_CONFIG (Page 629)" instruction enters the error code DW#16#C0809400 in STATUS. If you occupy the first byte with zero, the station name is deleted.

The station name is subject to the following limitations:

- A name component within the station name, i.e., a character string between two dots, must not exceed 63 characters.
- No special characters such as umlauts, brackets, underscore, slash, blank space, etc. The only special character permitted is the dash.
- The station name must not begin or end with the "-" character.
- The station name must not begin with a number.
- The station name form n.n.n.n (n = 0, ... 999) is not permitted.
- The station name must not begin with the string "port-xyz" or "port-xyz-abcde" (a, b, c, d, e, x, y, z = 0, ... 9).

NOTE

You can also create an ARRAY "NOS" that is shorter then 240 bytes, but not less than 2 bytes. In this case, you must adjust the "Length" (length of subfield) tag accordingly.

Table 12-54 Elements of the IF_CONF_NTP data type

Name	Data type	Start value	Description
Id	UInt	17	subfield_type_id
Length	UInt	22	subfield_length
Mode	UInt	0	subfield_mode (2: temporary)
NTP_IP	Array[1...4] of IP_V4	-	IP addresses of NTP servers
NTP_IP[1]	IP_V4		IP addresses of NTP server 1
ADDR	Array[1...4] of Byte	0	
ADDR[1]	Byte	0	IP address high byte
ADDR[2]	Byte	0	IP address high byte
ADDR[3]	Byte	0	IP address low byte
ADDR[4]	Byte	0	IP address low byte
NTP_IP[2]	IP_V4		IP addresses of NTP server 2
ADDR	Array[1...4] of Byte	0	
ADDR[1]	Byte	0	IP address high byte
ADDR[2]	Byte	0	IP address high byte
ADDR[3]	Byte	0	IP address low byte
ADDR[4]	Byte	0	IP address low byte
NTP_IP[3]	IP_V4		IP addresses of NTP server 3
ADDR	Array[1...4] of Byte	0	
ADDR[1]	Byte	0	IP address high byte
ADDR[2]	Byte	0	IP address high byte
ADDR[3]	Byte	0	IP address low byte
ADDR[4]	Byte	0	IP address low byte
NTP_IP[4]	IP_V4		IP addresses of NTP server 4
ADDR	Array[1...4] of Byte	0	
ADDR[1]	Byte	0	IP address high byte

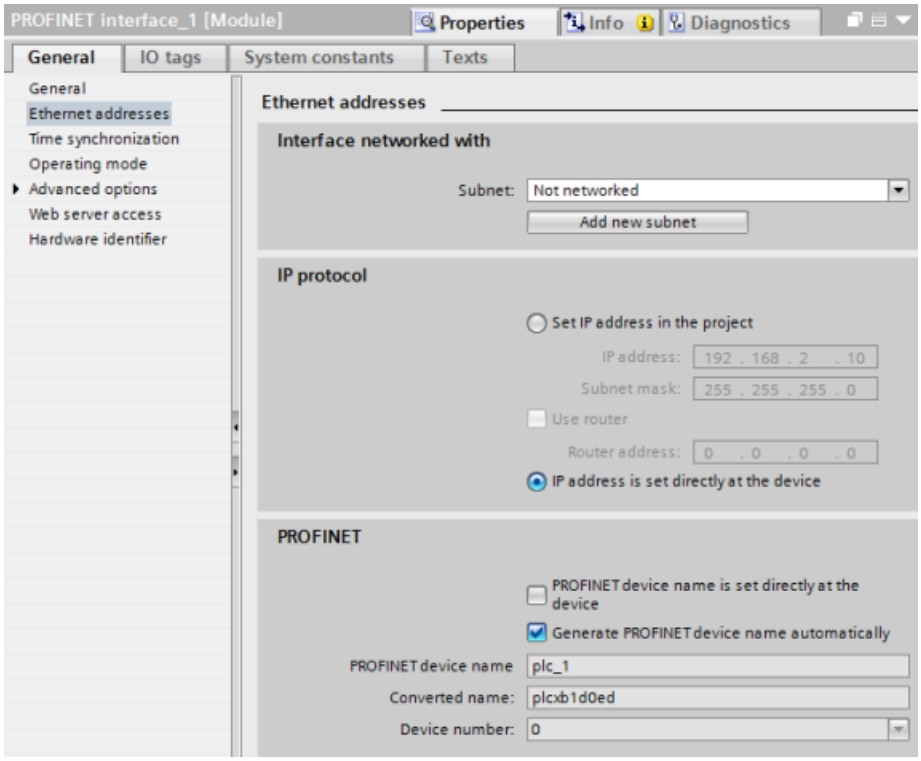
Name		Data type	Start value	Description
	ADDR[2]	Byte	0	IP address high byte
	ADDR[3]	Byte	0	IP address low byte
	ADDR[4]	Byte	0	IP address low byte

Example: Using the T_CONFIG instruction to change IP parameters

In the following example, in the "addr" subfield, the "InterfaceAddress" (IP address), "SubnetMask", and "DefaultRouter" (IP router) are changed. In the CPU "Properties", "Ethernet address" page, you must select the "IP address is set directly at the device" radio button to enable you to change the IP parameters using the "T_CONFIG" instruction after the program is downloaded.

CONF_DATA_1

	Name	Data type	Start value
1	Static		
2	Conf_data	Struct	
3	header	IF_CONF_Header	
4	FieldType	UInt	0
5	FieldId	UInt	0
6	SubfieldCount	UInt	1
7	addr	IF_CONF_v4	
8	Id	UInt	30
9	Length	UInt	18
10	Mode	UInt	1
11	InterfaceAddress	IP_V4	
12	ADDR	array [1..4] of Byte	
13	ADDR[1]	Byte	192
14	ADDR[2]	Byte	168
15	ADDR[3]	Byte	2
16	ADDR[4]	Byte	30
17	SubnetMask	IP_V4	
18	ADDR	array [1..4] of Byte	
19	ADDR[1]	Byte	255
20	ADDR[2]	Byte	255
21	ADDR[3]	Byte	255
22	ADDR[4]	Byte	0
23	DefaultRouter	IP_V4	
24	ADDR	array [1..4] of Byte	
25	ADDR[1]	Byte	192
26	ADDR[2]	Byte	168
27	ADDR[3]	Byte	2
28	ADDR[4]	Byte	1

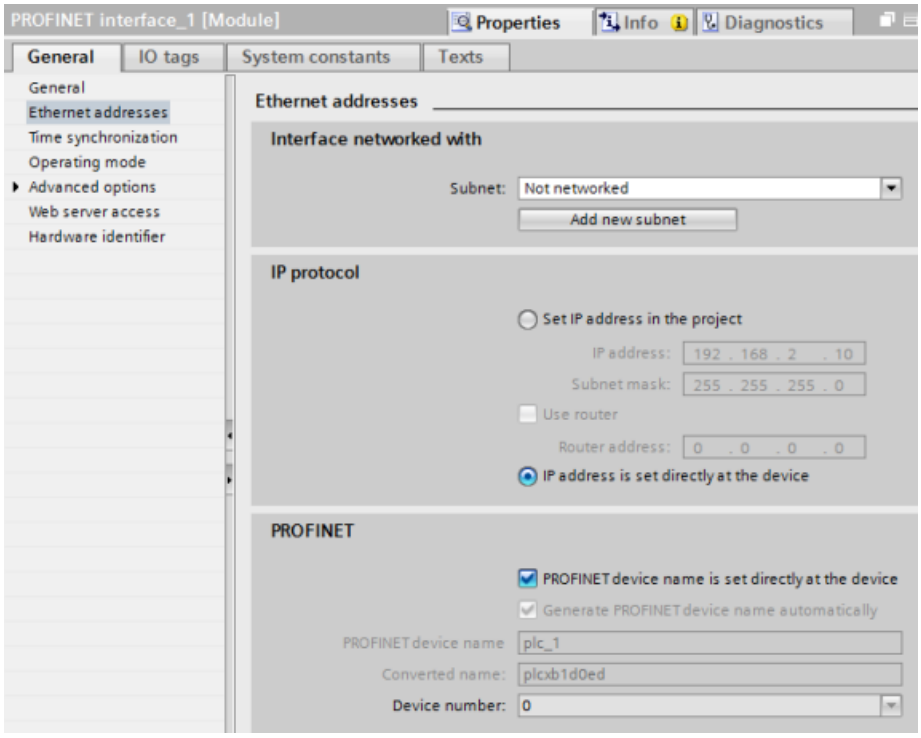


Example: Using the T_CONFIG instruction to change IP parameters and PROFINET IO device names

In the following example, both the "addr" and "nos" (Name of station) subfields are changed. In the CPU "Properties", "Ethernet address" page, you must select the "PROFINET device name is set directly at the device" check box to enable you to change the PROFINET device name using the "T_CONFIG" instruction after the program is downloaded.

CONF_DATA_2

	Name	Data type	Start value
1	Static		
2	Conf_data	Struct	
3	header	IF_CONF_Header	
4	FieldType	UInt	0
5	FieldId	UInt	0
6	SubfieldCount	UInt	2
7	addr	IF_CONF_v4	
8	Id	UInt	30
9	Length	UInt	18
10	Mode	UInt	1
11	InterfaceAddress	IP_V4	
12	ADDR	array [1..4] of Byte	
13	SubnetMask	IP_V4	
14	ADDR	array [1..4] of Byte	
15	DefaultRouter	IP_V4	
16	ADDR	array [1..4] of Byte	
17	nos	IF_CONF_NOS	
18	Id	UInt	40
19	Length	UInt	246
20	Mode	UInt	1
21	NOS	array [1..240] of Byte	

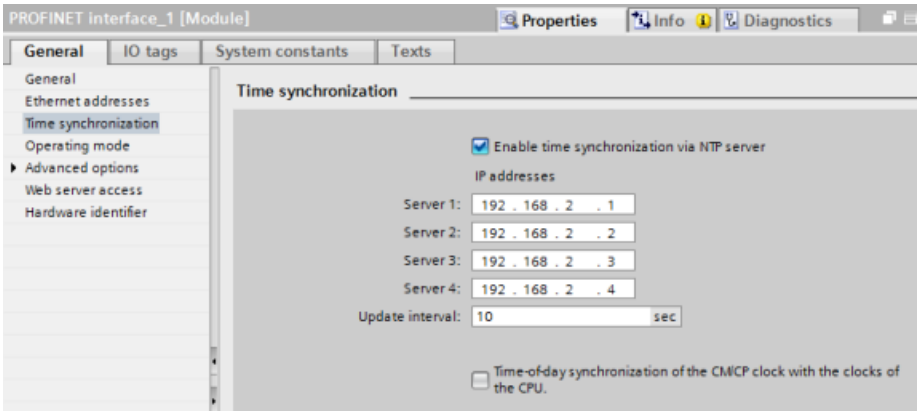

PROFINET interface_1 [Module]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
Ethernet addresses
Time synchronization
Operating mode
Advanced options
Web server access
Hardware identifier
Ethernet addresses
Interface networked with
Subnet:
Not networked
Add new subnet
IP protocol
Set IP address in the project
IP address:
192 . 168 . 2 . 10
Subnet mask:
255 . 255 . 255 . 0
Use router
Router address:
0 . 0 . 0 . 0
IP address is set directly at the device
PROFINET
PROFINET device name is set directly at the device
Generate PROFINET device name automatically
PROFINET device name
plc_1
Converted name:
plcxb1d0ed
Device number:
0

Example: Using the T_CONFIG instruction to change IP addresses in the NTP servers

In the following example, in the "ntp" (Network Time Protocol (NTP) server) subfield, the T_CONFIG instruction changes the IP addresses of up to four NTP servers.
In the CPU Properties, PROFINET interface [X1], Time synchronization page, you configure NTP synchronization by selecting the "Enable time synchronization via NTP server" check box as shown in the figure below. You can then change the IP addresses in the NTP servers using the "T_CONFIG" instruction after the program is downloaded.

CONF_DATA_3

	Name	Data type	Start value
1	Static		
2	Conf_Data	Struct	
3	header	IF_CONF_Header	
4	FieldType	UInt	0
5	FieldId	UInt	0
6	SubfieldCount	UInt	1
7	ntp	IF_CONF_NTP	
8	Id	UInt	17
9	Length	UInt	22
10	Mode	UInt	2
11	NTP_IP	Array[1..4] of IP_V4	
12	NTP_IP[1]	IP_V4	
13	ADDR	Array[1..4] of Byte	
14	ADDR[1]	Byte	192
15	ADDR[2]	Byte	168
16	ADDR[3]	Byte	2
17	ADDR[4]	Byte	5
18	NTP_IP[2]	IP_V4	
19	ADDR	Array[1..4] of Byte	
20	ADDR[1]	Byte	192
21	ADDR[2]	Byte	168
22	ADDR[3]	Byte	2
23	ADDR[4]	Byte	6
24	NTP_IP[3]	IP_V4	
25	ADDR	Array[1..4] of Byte	
26	ADDR[1]	Byte	192
27	ADDR[2]	Byte	168
28	ADDR[3]	Byte	2
29	ADDR[4]	Byte	7
30	NTP_IP[4]	IP_V4	
31	ADDR	Array[1..4] of Byte	
32	ADDR[1]	Byte	192
33	ADDR[2]	Byte	168
34	ADDR[3]	Byte	2
35	ADDR[4]	Byte	8



12.6.8.21 Common parameters for instructions

REQ input parameter

Many of the OUC instructions use the REQ input to initiate the operation on a low to high transition. The REQ input must be high (TRUE) for one execution of an instruction, but the REQ input can remain TRUE for as long as you choose. The instruction does not initiate another operation until it has been executed with the REQ input FALSE so that the instruction can reset the history state of the REQ input. This is required so that the instruction can detect the low to high transition to initiate the next operation.

When you place one of these instructions in your program, STEP 7 prompts you to identify the instance DB. Use a unique DB for each instruction call. This ensures that each instruction properly handles inputs such as REQ.

ID input parameter

The ID parameter is a reference to the "Local ID (hex)" on the "Network view" of "Devices and networks" in STEP 7 and is the ID of the network that you want to use for this communication block. The ID must be identical to the associated parameter ID in the local connection description.

DONE, NDR, ERROR, and STATUS output parameters

The following parameters are common to the OUC instructions and provide outputs describing the completion status:

Table 12-55 Open User Communication instruction output parameters

Parameter	Data type	Default	Description
DONE	Bool	FALSE	Is set TRUE for one execution to indicate that the last request completed without errors; otherwise, FALSE.
NDR	Bool	FALSE	Is set TRUE for one execution to indicate that the requested action has completed without error and new data has been received; otherwise, FALSE.
BUSY	Bool	FALSE	Is set TRUE when active to indicate that: • The job is not yet complete. • A new job cannot be triggered. Is set FALSE when job is complete.
ERROR	Bool	FALSE	Is set TRUE for one execution to indicate that the last request completed with errors, with the applicable error code in STATUS; otherwise, FALSE.
STATUS	Word	0	Is set to a status value as follows: • If the DONE or NDR bit is set, then STATUS is set to 0 or to an informational code. • If the ERROR bit is set, then STATUS is set to an error code. • If none of the above bits are set, then the instruction returns status results that describe the current state of the function. STATUS retains its value for the duration of the execution of the function.

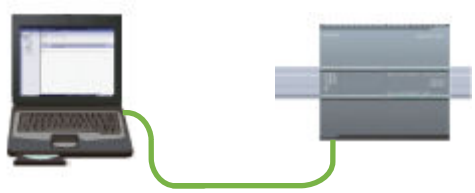
NOTE

Note that DONE, NDR, and ERROR are set for one execution only.

If you use the TCON instruction to set up and establish a passive communications connection, do not use the following restricted port addresses:

- ISO TSAP (passive):
  - 01.00, 01.01, 02.00, 02.01, 03.00, 03.01
  - 10.00, 10.01, 11.00, 11.01, ... BF.00, BF.01
- TCP port (passive) and UDP port (passive):
  - 20, 80, 102, 5001, 34962, 34963, 34964

12.6.9 Communication with a programming device



A CPU can communicate with a STEP 7 programming device on a network.

Figure

Consider the following when setting up communications between a CPU and a programming device:

- Configuration/Setup: Hardware configuration is required.
- No Ethernet switch is required for one-to-one communications; an Ethernet switch is required for more than two devices in a network.

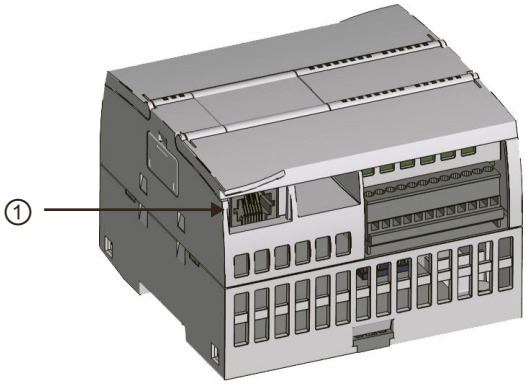
12.6.9.1 Establishing the hardware communications connection

The PROFINET interfaces establish the physical connections between a programming device and a CPU. Since Auto-Cross-Over functionality is built into the CPU, either a standard or crossover Ethernet cable can be used for the interface. An Ethernet switch is not required to connect a programming device directly to a CPU.

Follow the steps below to create the hardware connection between a programming device and a CPU:

1. Install the CPU (Page 47).
2. Plug the Ethernet cable into the PROFINET port shown below.

3. Connect the Ethernet cable to the programming device.

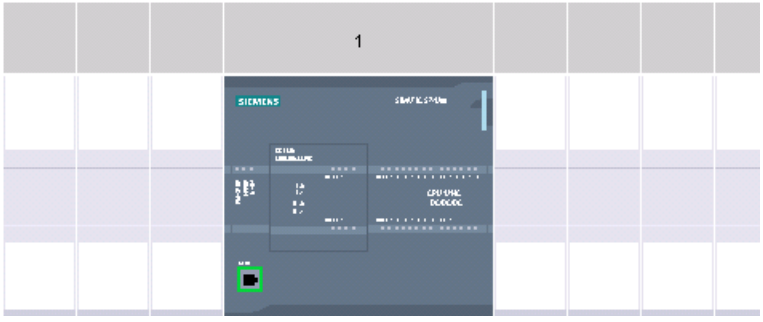


① PROFINET port

An optional strain relief is available to strengthen the PROFINET connection. For ordering information, see Spare parts and other hardware (Page 1277).

12.6.9.2 Configuring the devices

If you have already created a project with a CPU, open your project in STEP 7.
If not, create a project and insert a CPU (Page 122) into the rack. In the project below, a CPU is shown in the "Device View".



12.6.9.3 Assigning Internet Protocol (IP) addresses

Assigning the IP addresses

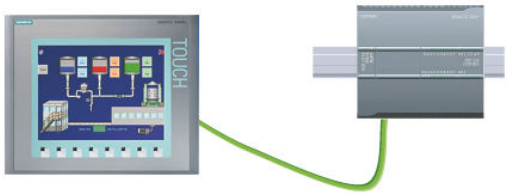
In a PROFINET network, each device must also have an Internet Protocol (IP) address. This address allows the device to deliver data on a more complex, routed network:

- If you have programming or other network devices that use an onboard adapter card connected to your plant LAN or an Ethernet-to-USB adapter card connected to an isolated network, you must assign IP addresses to them. Refer to "Assigning IP addresses to programming and network devices" (Page 535) for more information.
- You can also assign an IP address to a CPU or network device online. This is particularly useful in an initial device configuration. Refer to "Assigning an IP address to a CPU online" (Page 535) for more information.
- After you have configured your CPU or network device in your project, you can configure parameters for the PROFINET interface, to include its IP address. Refer to "Configuring an IP address for a CPU in your project" (Page 537) for more information.

12.6.9.4 Testing your PROFINET network

After completing the configuration, you must download your project to the CPU. The download operation sets all IP addresses for devices configured as "Set IP address in the project".
The CPU "Download to device" function and its "Extended download to device" dialog can show all accessible network devices and whether or not unique IP addresses have been assigned to all devices. Refer to "Testing the PROFINET network" (Page 542) for more information.

12.6.10 HMI-to-PLC communication



Figure

The CPU supports PROFINET communications connections to HMIs (Page 36). The following requirements must be considered when setting up communications between CPUs and HMIs:

Configuration/Setup:

- The PROFINET port of the CPU must be configured to connect with the HMI.
- The HMI must be setup and configured.

- The HMI configuration information is part of the CPU project and can be configured and downloaded from within the project.
- No Ethernet switch is required for one-to-one communications; an Ethernet switch is required for more than two devices in a network.

NOTE

The rack-mounted CSM1277 4-port Ethernet switch can be used to connect your CPUs and HMI devices. The PROFINET port on the 1211, 1212, and 1214 CPUs does not contain an Ethernet switching device.

Supported functions:

- Read/write data to the CPU
- Trigger messages based upon information retrieved from the CPU
- Read system diagnostics

Table 12-56 Required steps in configuring communications between an HMI and a CPU

Step	Task
1	Establishing the hardware communications connection A PROFINET interface establishes the physical connection between an HMI and a CPU. Since Auto-Cross-Over functionality is built into the CPU, you can use either a standard or crossover Ethernet cable for the interface. An Ethernet switch is not required to connect an HMI and a CPU. Refer to "Communication with a programming device: Establishing the hardware communications connection" (Page 640) for more information.
2	Configuring the devices Refer to "Communication with a programming device: Configuring the devices" (Page 641) for more information.
3	Configuring the logical network connections between an HMI and a CPU Refer to "HMI-to-PLC communication: Configuring the logical network connections between two devices" (Page 643) for more information.
4	Configuring an IP address in your project Use the same configuration process; however, you must configure IP addresses for the HMI and the CPU. Refer to "Device configuration: Configuring an IP address for a CPU in your project" (Page 538) for more information.
5	Testing the PROFINET network You must download the configuration for each CPU and HMI device. Refer to "Device configuration: Testing the PROFINET network" (Page 542) for more information.

Supported HMI tags and subscriptions

The CPU supports 400 tags per HMI and up to 40 HMI subscriptions.

12.6.10.1 Configuring logical network connections between two devices

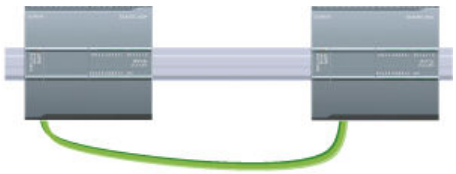
After you configure the rack with the CPU, you are now ready to configure your network connections.

In the Devices and Networks portal, use the "Network view" to create the network connections between the devices in your project. First, click the "Connections" tab, and then select the connection type with the dropdown, just to the right (for example, an ISO on TCP connection).

To create a PROFINET connection, click the green (PROFINET) box on the first device, and drag a line to the PROFINET box on the second device. Release the mouse button and your PROFINET connection is joined.

Refer to "Device Configuration: Creating a network connection" (Page 531) for more information.

12.6.11 PLC-to-PLC communication



Figure

A CPU can communicate with another CPU on a network by using the TSEND_C and TRCV_C instructions.

Consider the following when setting up communications between two CPUs:

- Configuration/Setup: Hardware configuration is required.
- Supported functions: Reading/Writing data to a peer CPU
- No Ethernet switch is required for one-to-one communications; an Ethernet switch is required for more than two devices in a network unless the devices have a built in switch.

Table 12-57 Required steps in configuring communications between two CPUs

Step	Task
1	Establishing the hardware communications connection A PROFINET interface establishes the physical connection between two CPUs. Since Auto-Cross-Over functionality is built into the CPU, you can use either a standard or crossover Ethernet cable for the interface. An Ethernet switch is not required to connect the two CPUs. Refer to "Communication with a programming device: Establishing the hardware communications connection" (Page 640) for more information.
2	Configuring the devices You must configure two CPUs in your project. Refer to "Communication with a programming device: Configuring the devices" (Page 641) for more information.
3	Configuring the logical network connections between two CPUs Refer to "PLC-to-PLC communication: Configuring logical network connections between two devices" (Page 645) for more information.
4	Configuring an IP address in your project Use the same configuration process; however, you must configure IP addresses for two CPUs (for example, PLC_1 and PLC_2). Refer to "Device configuration: Configuring an IP address for a CPU in your project" (Page 538) for more information.
5	Configuring transmit (send) and receive parameters You must configure TSEND_C and TRCV_C instructions in both CPUs to enable communications between them. Refer to "Configuring communications between two CPUs: Configuring transmit (send) and receive parameters" (Page 645) for more information.
6	Testing the PROFINET network You must download the configuration for each CPU. Refer to "Device configuration: Testing the PROFINET network" (Page 542) for more information.

12.6.11.1 Configuring logical network connections between two devices

After you configure the rack with the CPU, you are now ready to configure your network connections.

In the Devices and Networks portal, use the "Network view" to create the network connections between the devices in your project. First, click the "Connections" tab, and then select the connection type with the dropdown, just to the right (for example, an ISO on TCP connection).

To create a PROFINET connection, click the green (PROFINET) box on the first device, and drag a line to the PROFINET box on the second device. Release the mouse button and your PROFINET connection is joined.

Refer to "Device Configuration: Creating a network connection" (Page 531) for more information.

12.6.11.2 Configuring the Local/Partner connection path between two devices

Configuring General parameters

You specify the communication parameters in the "Properties" configuration dialog of the communication instruction. This dialog appears near the bottom of the page whenever you have selected any part of the instruction.

Refer to "Device configuration: Configuring the Local/Partner connection path (Page 532)" for more information.

In the "Address Details" section of the Connection parameters dialog, you define the TSAPs or ports to be used. The TSAP or port of a connection in the CPU is entered in the "Local TSAP" field. The TSAP or port assigned for the connection in your partner CPU is entered under the "Partner TSAP" field.

12.6.11.3 Configuring transmit (send) and receive parameters

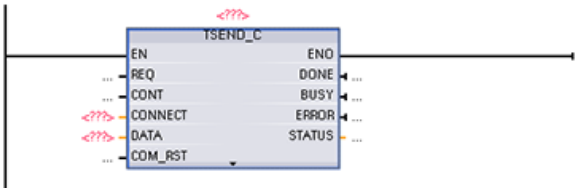
Communication blocks (for example, TSEND_C and TRCV_C) are used to establish connections between two CPUs. Before the CPUs can engage in PROFINET communications, you must configure parameters for transmitting (or sending) messages and receiving messages. These parameters dictate how communications operate when messages are being transmitted to or received from a target device.

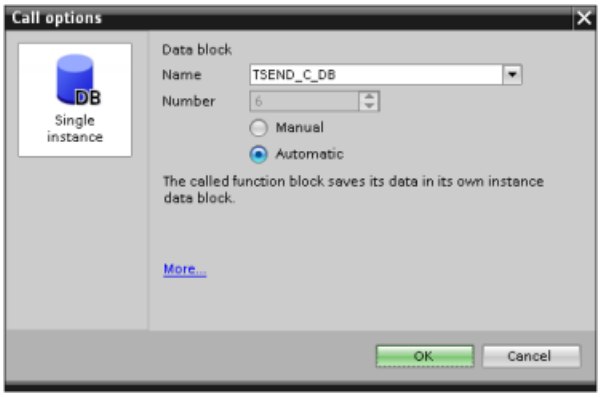
Configuring the TSEND_C instruction transmit (send) parameters

TSEND_C instruction

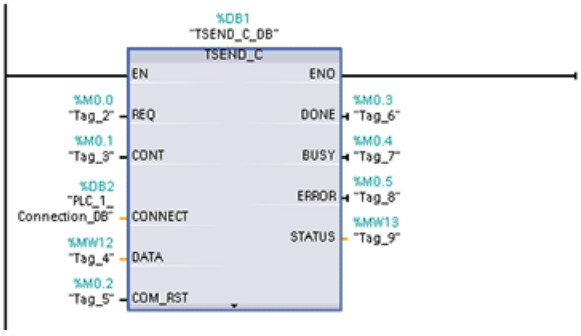
The TSEND_C instruction (Page 562) creates a communications connection to a partner station. The connection is set up, established, and automatically monitored until it is commanded to disconnect by the instruction. The TSEND_C instruction combines the functions of the TCON, TDISCON and TSEND instructions.

From the Device configuration in STEP 7, you can configure how a TSEND_C instruction transmits data. To begin, you insert the instruction into the program from the "Communications" folder in the "Instructions" task card. The TSEND_C instruction is displayed, along with the Call options dialog where you assign a DB for storing the parameters of the instruction.





You can assign tag memory locations to the inputs and outputs, as shown in the following figure:



Configuring General parameters

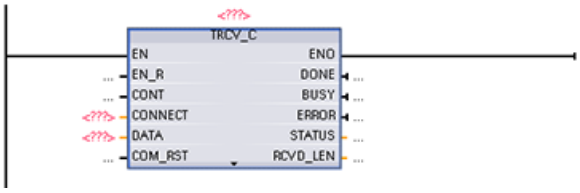
You specify the parameters in the Properties configuration dialog of the TSEND_C instruction. This dialog appears near the bottom of the page whenever you have selected any part of the TSEND_C instruction.

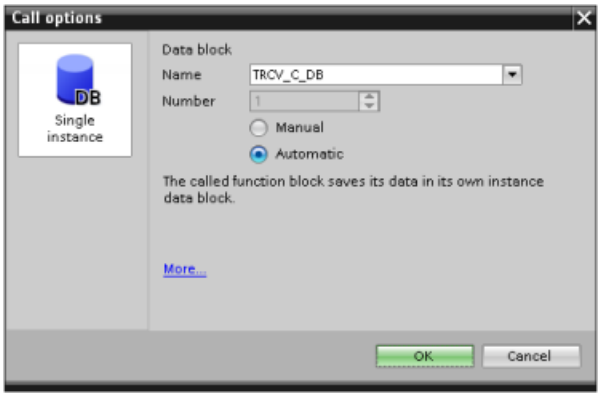
Configuring the TRCV_C instruction receive parameters

TRCV_C instruction

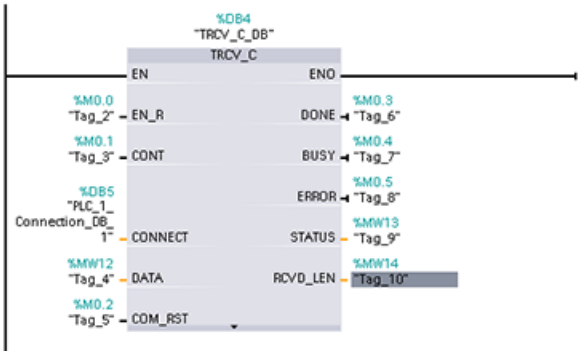
The TRCV_C instruction (Page 562) creates a communications connection to a partner station. The connection is set up, established, and automatically monitored until it is commanded to disconnect by the instruction. The TRCV_C instruction combines the functions of the TCON, TDISCON, and TRCV instructions.

From the CPU configuration in STEP 7, you can configure how a TRCV_C instruction receives data. To begin, insert the instruction into the program from the "Communications" folder in the "Instructions" task card. The TRCV_C instruction is displayed, along with the Call options dialog where you assign a DB for storing the parameters of the instruction.





You can assign tag memory locations to the inputs and outputs, as shown in the following figure:



Configuring the General parameters

You specify the parameters in the Properties configuration dialog of the TRCV_C instruction. This dialog appears near the bottom of the page whenever you have selected any part of the TRCV_C instruction.

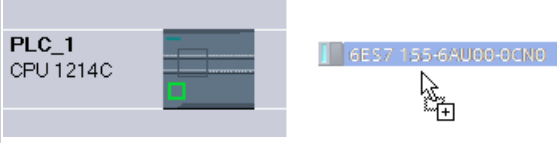
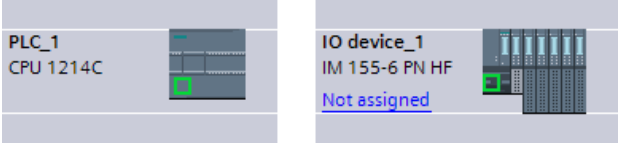
12.6.12 Configuring a CPU and PROFINET IO device

12.6.12.1 Adding a PROFINET IO device

In the Network view, use the hardware catalog to add PROFINET IO devices.

For example, expand the following containers in the hardware catalog to add an ET 200SP IO device: Distributed I/O, ET 200SP, Interface modules, and PROFINET. You can then select the interface module from the list of ET 200SP devices (sorted by part number) and add the ET 200SP IO device.

Table 12-58 Adding an ET 200SP IO device to the device configuration

Insert the IO device	Result
	

You can now connect the PROFINET IO device to the CPU:

1. Right-click the "Not assigned" link on the device and select "Assign new IO controller" from the context menu to display the "Select IO controller" dialog.
2. Select your S7-1200 CPU (in this example, "PLC_1") from the list of IO controllers in the project.
3. Click "OK" to create the network connection.

You can also go to the "Devices and networks" portal and use the "Network view" to create the network connections between the devices in your project:

1. To create a PROFINET connection, click the green (PROFINET) box on the first device, and drag a line to the PROFINET box on the second device.
2. Release the mouse button and your PROFINET connection is joined.

Refer to "Device Configuration: Configuring the CPU for communication" (Page 163) for more information.

12.6.12.2 Assigning CPUs and device names

Assigning CPUs and device names

Network connections between the devices also assign the PROFINET IO device to the CPU, which is required for that CPU to control the device. To change this assignment, click the PLC Name shown on the PROFINET IO device. A dialog box opens that allows the PROFINET IO device to be disconnected from the current CPU and reassigned or left unassigned, if desired.

The devices on your PROFINET network must have an assigned name before you can connect with the CPU. Use the "Network view" to assign names to your PROFINET devices if the devices have not already been assigned a name or if the name of the device is to be changed. Right-click the PROFINET IO device and select "Assign device name" to do this.

For each PROFINET IO device, you must assign the same name to that device in both the STEP 7 project and to the PROFINET IO device in the PROFINET network. (You can use either the STEP 7 "Online & diagnostics" tool or the PRONETA commissioning, configuration, and diagnostics tool to assign the device name in the PROFINET network.) If a name is missing or does not match in either location, the PROFINET IO data exchange mode will not run. Refer to "Online and diagnostic tools: Assigning a name to a PROFINET device online (Page 1053)" for more information.

12.6.12.3 Assigning Internet Protocol (IP) addresses

Assigning the IP addresses

In a PROFINET network, each device must also have an Internet Protocol (IP) address. This address allows the device to deliver data on a more complex, routed network:

- If you have programming or other network devices that use an onboard adapter card connected to your plant LAN or an Ethernet-to-USB adapter card connected to an isolated network, you must assign IP addresses to them. Refer to "Assigning IP addresses to programming and network devices" (Page 535) for more information.
- You can also assign an IP address to a CPU or network device online. This is particularly useful in an initial device configuration. Refer to "Assigning an IP address to a CPU online" (Page 537) for more information.
- After you have configured your CPU or network device in your project, you can configure parameters for the PROFINET interface, to include its IP address. Refer to "Configuring an IP address for a CPU in your project" (Page 538) for more information.

12.6.12.4 Configuring the IO cycle time

Configuring the IO cycle time

A PROFINET IO device is supplied with new data from the CPU within an "IO cycle" time period. The update time can be separately configured for each device and determines the time interval in which data is transmitted from the CPU to and from the device.

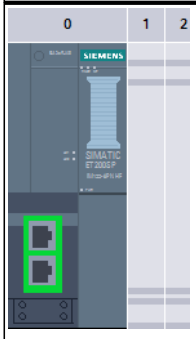
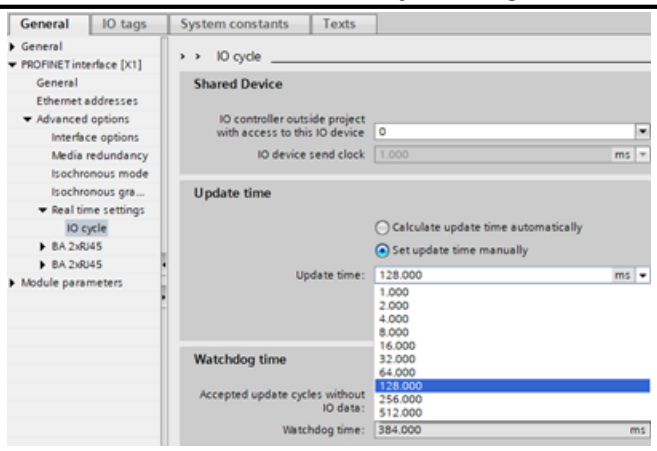
STEP 7 calculates the "IO cycle" update time automatically in the default setting for each device of the PROFINET network, taking into account the volume of data to be exchanged and the number of devices assigned to this controller. If you do not want to have the update time calculated automatically, you can change this setting.

To access the IO cycle parameters, click the PROFINET port on the ET 200SP IO device. From Properties dialog, select "Advanced options > Realtime settings > IO cycle".

Define the IO cycle "Update time" with the following selections:

- To have a suitable update time calculated automatically, select "Calculate update time automatically".
- To set the update yourself, select "Set update time manually" and choose the required update time in ms from the dropdown menu.

Table 12-59 Configuring the ET 200SP PROFINET IO cycle time

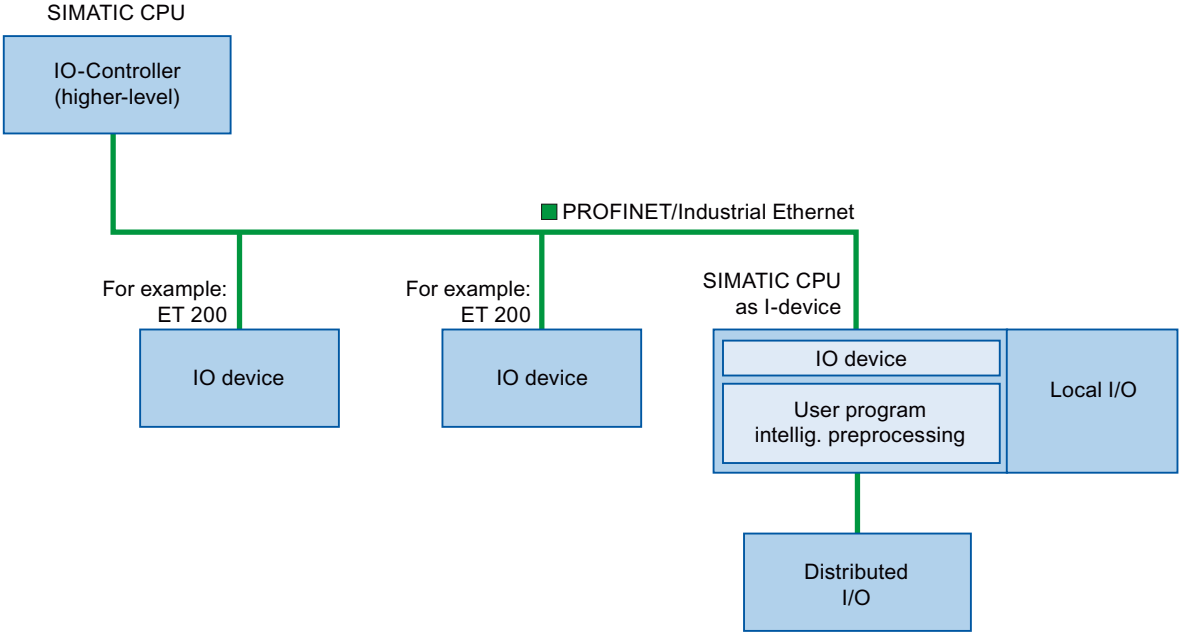
ET 200SP PROFINET IO device	ET 200SP PROFINET IO cycle dialog
	

12.6.13 Configuring a CPU and PROFINET I-device

12.6.13.1 I-device functionality

The "I-device" (intelligent IO device) functionality of a CPU facilitates data exchange with an IO controller and operation of the CPU as intelligent preprocessing unit of sub processes, for example. The I-device is linked as an IO device to a "higher-level" IO controller.

The pre-processing is handled by the user program on the CPU. The process values acquired in the centralized or distributed (PROFINET IO or PROFIBUS DP) I/O are pre-processed by the user program and made available through a PROFINET IO interface to the CPU of a higher-level station.



"I-device" naming conventions

In the remainder of this description, a CPU or a CP with I-device functionality is simply called an "I-device".

12.6.13.2 Properties and advantages of the I-device

Fields of application

Fields of application of the I-device:

- Distributed processing:
  A complex automation task can be divided into smaller units/subprocesses. This results in manageable processes which lead to simplified subtasks.
- Separating subprocesses:
  Complicated, widely distributed and extensive processes can be subdivided into several subprocesses with manageable interfaces by using I-devices. These subprocesses can be stored in individual STEP 7 projects if necessary, which can later be merged to form one master project.
- Know-how protection:
  Components can only be delivered with a GSD file for the I-device interface description instead of with a STEP 7 project. The user can protect his program since it no longer has to be published.

Properties

Properties of the I-device:

- Unlinking STEP 7 projects:
  Creators and users of an I-device can have completely separated STEP 7 automation projects. The GSD file forms the interface between the STEP 7 projects. This allows a link to standard IO controllers through a standardized interface.
- Real-time communication:
  The I-device is provided with a deterministic PROFINET IO system through a PROFINET IO interface.

Advantages

The I-device has the following advantages:

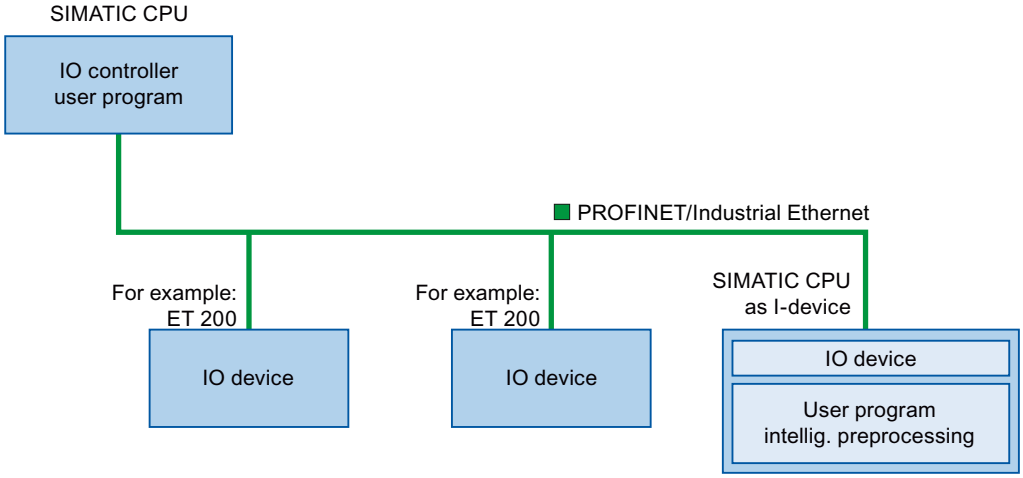
- Simple linking of IO controllers
- Real-time communication between IO controllers
- Relieving the IO controller by distributing the computing capacity to I-devices
- Lower communications load by processing process data locally
- Manageable, due to processing of subtasks in separate STEP 7 projects

12.6.13.3 Characteristics of an I-device

An I-device is included in an IO system like a standard IO device.

I-device without lower-level PROFINET IO system

The I-device does not have its own distributed I/O. The configuration and parameter assignment of the I-devices in the role of an IO device is the same as for a distributed I/O system (for example, ET 200).



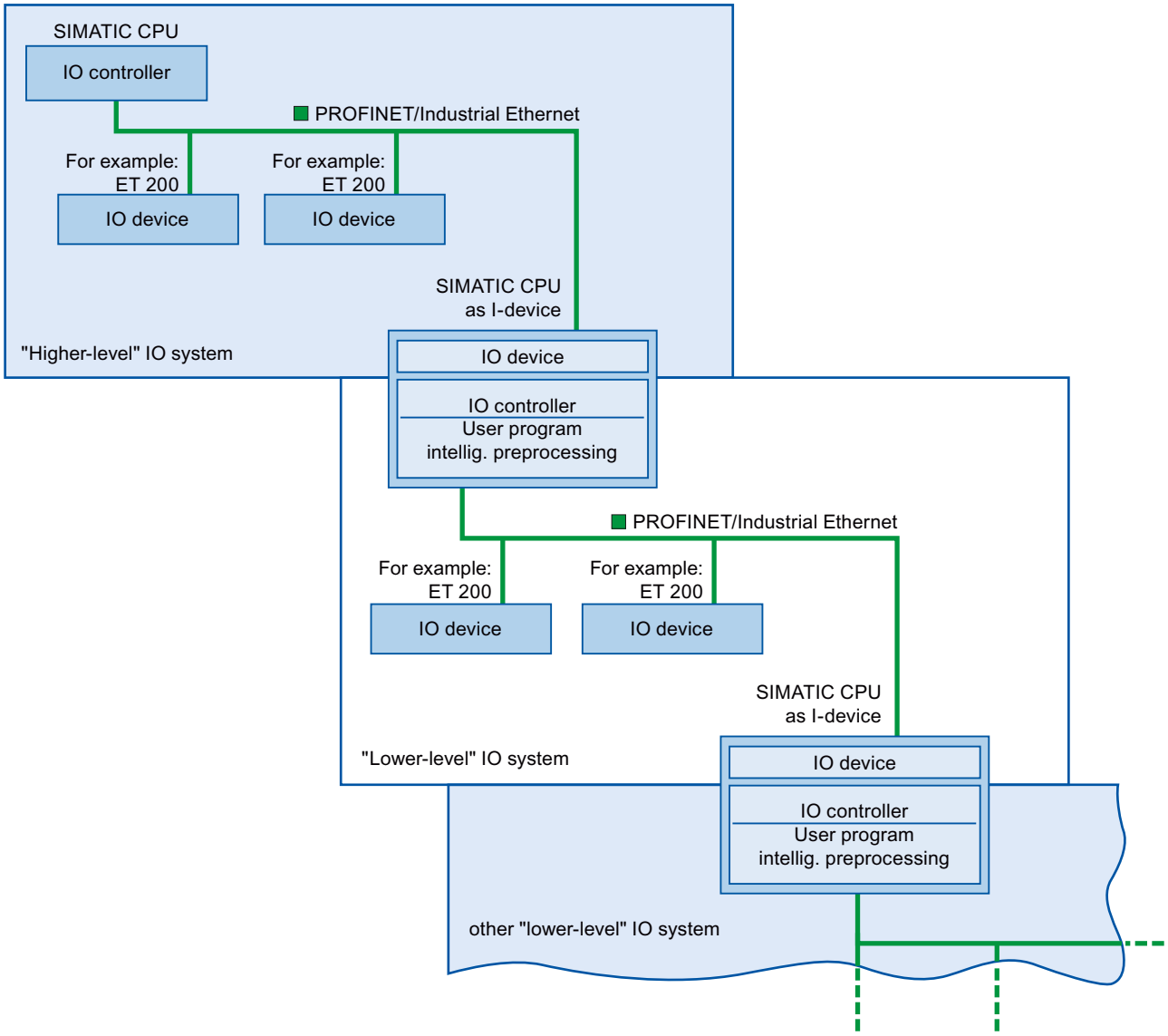
I-device with lower-level PROFINET IO system

Depending on the configuration, an I-device can also be an IO controller on a PROFINET interface in addition to having the role of an IO device.

This means that the I-device can be part of a higher-level IO system through its PROFINET interface and as an IO controller can support its own lower-level IO system.

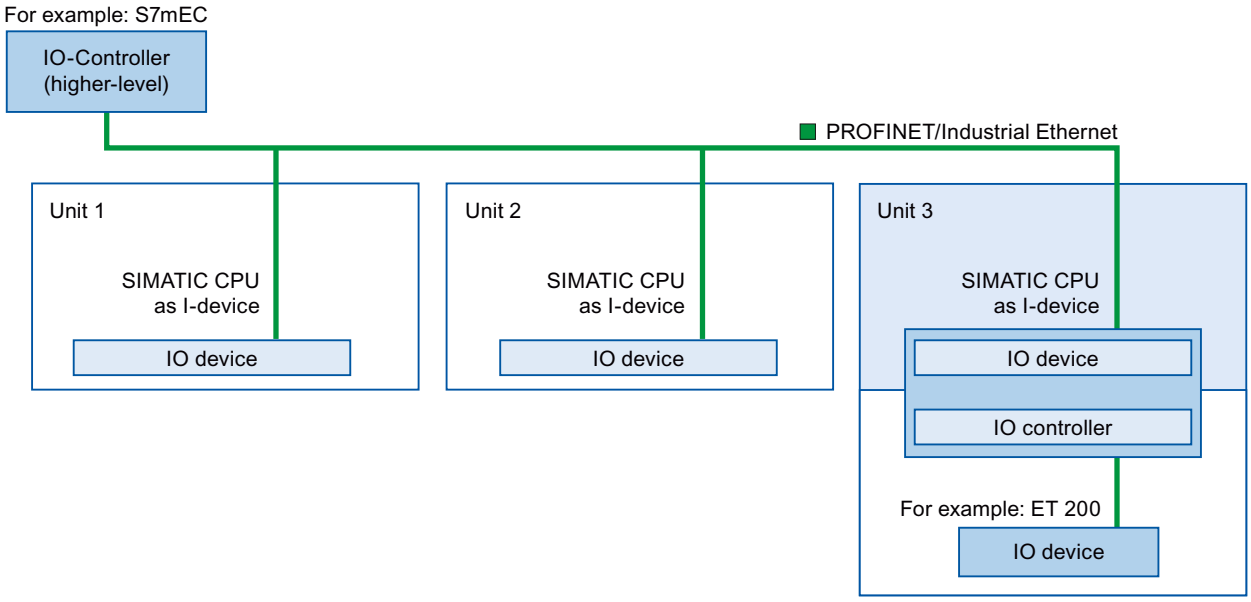
The lower-level IO system can, in turn, contain I-devices (see figure below). This makes hierarchically structured IO systems possible.

In addition to its role as IO controller, an I-device can also be used through a PROFIBUS interface as DP master for a lower-level PROFIBUS system.



Example: I-device as IO device and IO controller

The I-device as IO device and IO controller is explained based on the example of a print process. The I-device controls a unit (a subprocess). One unit is used, for example, to insert additional sheets such as flyers or brochures in a package of printed material.



Unit 1 and unit 2 each consist of an I-device with centralized I/O. The I-device along with the distributed I/O system (for example, ET 200) forms unit 3.

The user program on the I-device is responsible for preprocessing the process data. For this task, the user program of the I-device requires default settings (for example, control data) from the higher-level IO controller. The I-device provides the higher-level IO controller with the results (for example, status of its subtask).

12.6.13.4 Data exchange between higher- and lower-level IO system

Transfer areas are an interface to the user program of the I-device CPU. Inputs are processed in the user program and outputs are the result of the processing in the user program.

The data for communication between IO controller and I-device is made available in the transfer areas. A transfer area contains an information unit that is exchanged consistently between IO controller and I-device. You can find more information on configuration and use of transfer areas in "Configuring the I-device" (Page 657).

Input transfer areas behave differently upon network loss between controller and I-device

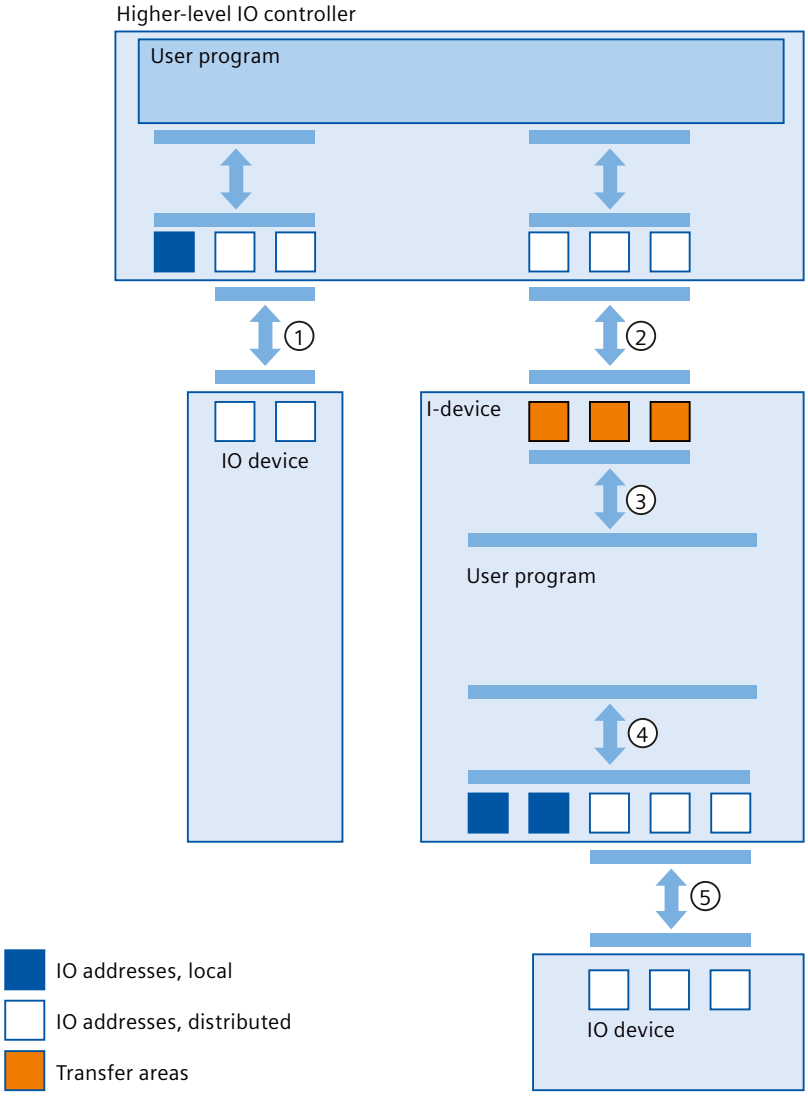
On the controller, the CPU writes zero to the input transfer areas upon network loss. On the I-device, the input transfer areas retain their last values.

You can configure your system to avoid this condition for the general I-device case (non-shared I-device). To do this, clear the input transfer areas for the I-device in a "Rack or Station Failure OB" for a coming event. Follow these steps:

1. Add a "Rack or Station Failure OB" to your project. (This OB defaults to the number OB 86).
2. Add logic to the OB to write the values of the inputs for the I-device to zero when the startup variable of LADDR indicates the value of the I-device hardware ID and the startup variable of Event_Class indicates a "coming" event:
   - You can find the I-device hardware ID in the Default tag table in the "System constants" tab. The hardware ID is a type of "HW_Device", and the name of the tag indicates that it is an I-device (for example, "Local~PROFINET_interface_1~IODevice").
   - A value of "16#39" in the Event_Class indicates a "coming" event. If the "Event_Class" input variable contains the value of "16#39", this indicates that the "Rack or Station Failure OB" is now active (as opposed to being cleared).

Data exchange flow

The next figure shows the data exchange between the higher- and lower-level IO system. The individual communication relations are explained below based upon the numbers:



① **Data exchange between higher-level IO controller and normal IO-device**
In this way, the IO controller and IO devices exchange data through PROFINET.

② **Data exchange between higher-level IO controller and I-device**
In this way, the IO controller and the I-device exchange data through PROFINET.
The data exchange between a higher-level IO controller and an I-device is based upon the conventional IO controller / IO device relationship.
For the higher-level IO controller, the transfer areas of the I-devices represent submodules of a pre-configured station.
The output data of the IO controller is the input data of the I-device. Analogously, the input data of the IO controller is the output data of the I-device.

③ **Transfer relationship between the user program and the transfer area**
In this way, the user program and the transfer area exchange input and output data.

④ **Data exchange between the user program and the I/O of the I-device**
In this way, the user program and the centralized / distributed I/O exchange input and output data.

⑤ **Data exchange between the I-device and a lower-level IO device**
In this way, the I-device and its IO devices exchange data. The data transfer is through PROFINET.

12.6.13.5 Configuring the I-device

There are basically two possibilities for configuration:

- Configuration of an I-device within a project
- Configuration of an I-device that is used in another project or in another engineering system.

STEP 7 allows you to configure an I-device for another project or for another engineering system by exporting a configured I-device to a GSD file. You import the GSD file in other projects or engineering systems as with other GSD files. The transfer areas for the data exchange, among other data, are stored in this GSD file.

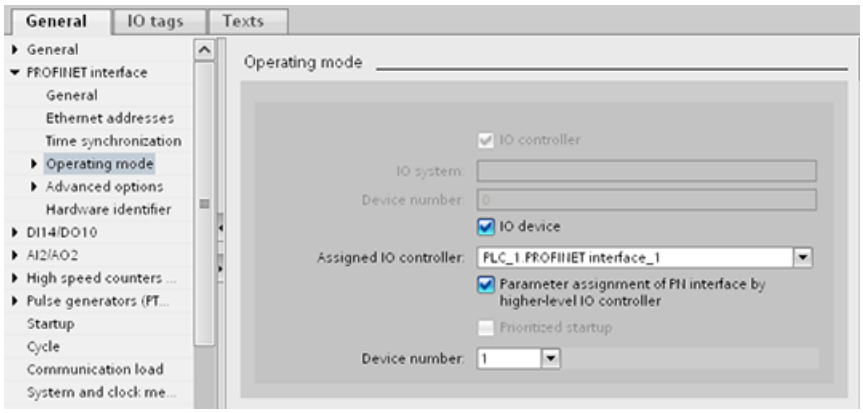
NOTE

When you use the S7-1200 as a shared I-device and as a controller, ensure that you increase the PROFINET I-device and PROFINET IO Update times to alleviate the communications performance impact. The system is very stable and works well when you select 2 ms for the Update time of a single PROFINET I-device time and you select 2 ms for the Update time of a single PROFINET IO time.

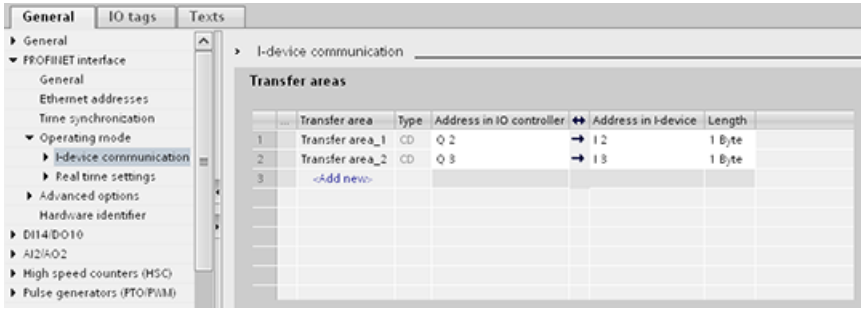
Configuration of an I-device within a project

1. Drag-and-drop a PROFINET CPU from the hardware catalog into the network view.
2. Drag-and-drop a PROFINET CPU, which can also be configured as an IO device, from the hardware catalog into the network view. This device is configured as an I-device (for example, CPU 1215C).
3. Select the PROFINET interface for the I-device.
4. In the Inspector window in the area navigation choose "Operating mode" and select the check box "IO device".

5. Now you have the option of choosing the IO controller in the "Assigned IO controller" drop-down list.
   Once you have chosen the IO controller, the networking and the IO system between both devices are displayed in the network view.



6. With the "Parameter assignment of PN interface by higher-level IO controller" check box, you specify whether the interface parameters will be assigned by the I-device itself or by a higher-level IO controller.
   If you operate the I-device with a lower-level IO system, then the parameters of the I-device PROFINET interface (for example, port parameter) cannot be assigned with the higher-level IO controller.
7. Configure the transfer areas. The transfer areas are found in the area navigation section "I-device communication":
   – Click in the first field of the "Transfer area" column. STEP 7 assigns a default name which you can change.
   – Select the type of communication relation: you can currently only select CD or F-CD.
   – Addresses are automatically preset; you can correct addresses if necessary, and determine the length of the transfer area which is to be consistently transferred.



8. A separate entry is created in the area navigation for each transfer area. If you select one of these entries, you can adjust the details of the transfer area, or correct them and comment on them.

NOTE

If you configure an S7-1200 as an I-device, the maximum size of a transfer area is 1024 input or output bytes. There are possible constraining factors depending on local I/O as well as address space limitations on the controlling device.

Configuring an I-device with a GSD file

If you use an I-device in another project, or if the I-device is used in another engineering system, then configure the higher-level IO controller and the I-device as described above.

However, click on the "Export" button after configuring the transfer areas so a new GSD file is created from the I-device. This GSD file represents the configured I-device in other projects.

The "Export" button is found in the "I-device communication" section of the Inspector window.

The hardware configuration is compiled and the export dialog opened.

Assign a name for the I-device proxy as well as a description in the fields provided. Click the "Export" button to complete your process.

Finally, import the GSD file, for example, in another project.

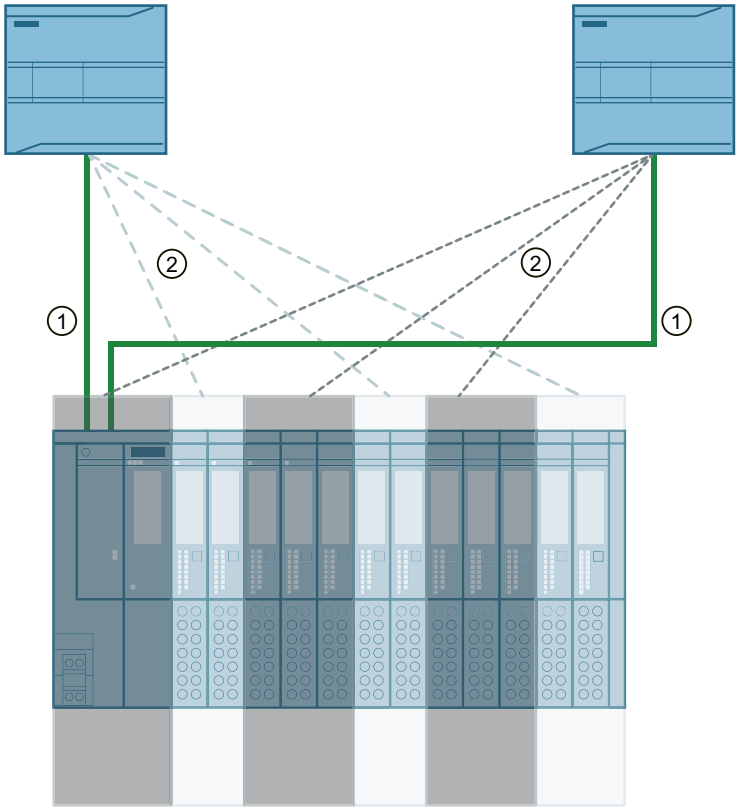
12.6.14 Shared devices

12.6.14.1 Shared device functionality

Numerous IO controllers are often used in larger or widely distributed systems.

Without the "Shared Device" function, each I/O module of an IO device is assigned to the same IO controller. If sensors that are physically close to each other must provide data to different IO controllers, several IO devices are required.

The "Shared Device" function allows the modules or submodules of an IO device to be divided up among different IO controllers. This allows flexible automation concepts. You have, for example, the possibility of combining I/O modules lying near each other into an IO device.



① PROFINET

② Logical assignment

Principle

Access to the submodules of the shared device is then divided up among the individual IO controllers. Each submodule of the shared device is assigned exclusively to one IO controller.

Requirement (GSD configuration)

- STEP 7
- S7-1200 CPU with firmware of V4.1 or later as IO controller
- IO device supports the shared device function, e.g. interface module IM 155-5 PN ST
- GSD file for configuring the IO device is installed
- An S7-1200 CPU configured as an I-device supports the Shared Device functionality. You must export the PROFINET GSD file for the I-device from STEP 7 and then import it into STEP 7 (TIA Portal).

Configuring the access

The IO device must be present in several projects so that the modules or submodules of an IO device can be assigned to different IO controllers. A separate project is required for each IO controller.

You use the "Shared device" parameter of the interface module to determine the modules or submodules to which the IO controller has access:

- If the local IO controller has access to the configured module, select the name of the IO controller from the list.
- If the IO controller from a different project and not the local IO controller is to have access to the configured module, select the entry "---".

The configuration is consistent regarding access if each module or submodule in exactly one project is assigned to an IO controller.

Module or submodule is assigned to another IO controller

The paragraph below describes the consequences of the "---" setting of the "Shared device" parameter from the point of view of the local IO controller.

In this case, the local IO controller does not have access to the module configured in this way. Specifically, this means:

- No data exchange with the module or submodule
- No reception of alarms or diagnostics, which means no display of the diagnostics status in the online view
- No parameter assignment of the module or submodule

Setting of the real-time properties

STEP 7 calculates the communication load and thus the resulting update times. You must enter the number of project-external IO controllers in the project in which the PROFINET interface of the shared device is assigned to the IO controller so that a calculation is possible with shared device configurations.

The maximum possible number of IO controllers for the shared device depends on the device. This number is stored in the GSD file of the shared device.

You can set a very short send clock (minimum of 1 ms) with an S7-1200 CPU as IO controller. The send clock can be shorter than the shortest send clock supported by the shared device. In this case, the shared device is operated by the IO controller with a send clock that it supports (send clock adaptation).

Example: A CPU supports send clocks starting from 1 ms. A configured IO device supports send clocks starting at 1.25 ms; another IO device supports send clocks starting at 1 ms. In this case, you have the option of setting the short send clock of 1 ms for the CPU. The CPU operates the "slow" IO device with the send clock of 1.25 ms.

Rules for the configuration

- IO controllers that use the shared device are created in different projects. In each project, care must be taken that the shared device is configured identically in each station. Only one IO controller may ever have full access to a submodule. Inconsistencies in the configuration result in a failure of the shared device.
- I/O addresses of a module or submodule can only be edited if a module or submodule is assigned to the IO controller in the same project.
- The shared device must have the same IP parameters and the same device name in each project.
- The send clock must be identical for all IO controllers that have access to the shared device.
- The S7 subnet ID of the subnet to which the shared device is connected must be identical in all projects.
- The following functions are only available if the PROFINET interface of the shared device is assigned to the local IO controller:
  - Prioritized startup
  - Parameter assignment of the port properties

Boundary conditions

The following boundary conditions result because a shared device configuration is distributed across several projects:

- The addresses of modules or submodules that are not assigned to this IO controller are missing in the address overview of each IO controller that has access to a shared device.
- The modules or submodules that are not assigned are not taken into consideration in the configuration limit calculation for the shared device during the consistency check. For this reason, you must verify for yourself that the maximum number of submodules or the maximum amount of cyclic IO data for the shared device will not be exceeded. For information on the maximum quantities, refer to the documentation for the devices you are using.
- Configuration errors such as the assignment of a module or submodule to several IO controllers are not detected in STEP 7.
- CPUs that are loaded with a shared device configuration do not have any information on whether the IO device is a shared device. Modules or submodules that are assigned to other IO controllers and therefore other CPUs are missing in the loaded configuration. These modules or submodules are therefore displayed neither in the CPU web server nor in the CPU display.

12.6.14.2 Example: Configuring a shared device (GSD configuration)

This example describes how to configure a distributed I/O system as a shared device with STEP 7.

A "distributed" configuration with different engineering tools for different IO controller families is possible. The procedure described below is based on STEP 7 and is limited to configuration with two IO controllers of the S7-1200 series that share one shared device.

The example creates two projects with one IO controller each:

- Controller1
- Controller2

You must create the shared device in both projects, even though it is physically one and the same IO device.

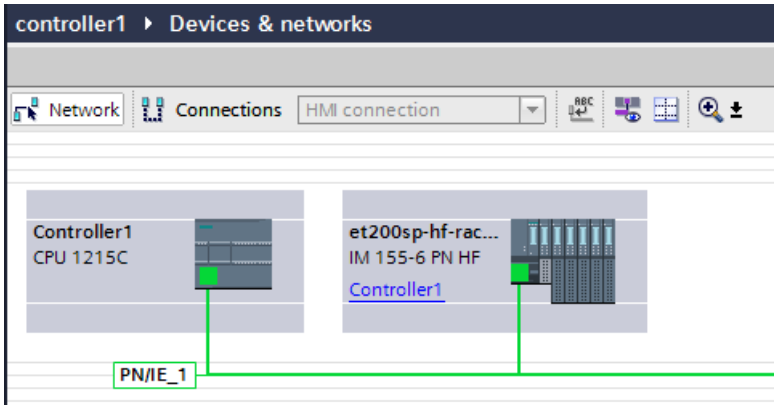
Requirements

- STEP 7
- IO device supports shared device functionality (for example, ET 200SP IM 155-6 PN HF V3.1).
- GSD file for configuring the IO device as a shared device is installed.

Procedure: Creating project 1

To create the first project with a shared device, follow these steps:

1. Start STEP 7.
2. Create a new project with the name "Controller1".
3. Insert a CPU 1215C from the hardware catalog in the network view. Name it "Controller1".
4. Insert an IO device with the "Shared Device" function (for example, an ET 200SP) from the hardware catalog (hardware catalog: Other field devices > PROFINET IO > I/O).
5. Assign the IO controller "Controller1" to the IO device.



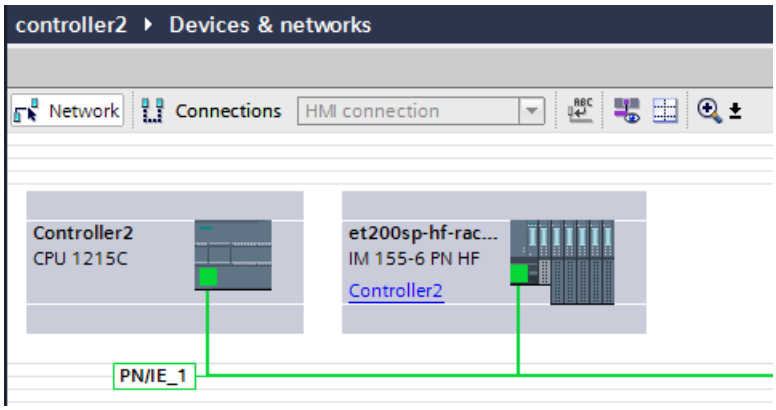
6. Double-click the IO device and insert all required modules and submodules from the hardware catalog in the device overview table.
7. Assign the module parameters.
8. Save the project.

Procedure: Creating project 2

To create the second project with a shared device, follow these steps:

1. Start STEP 7 once again.
   A new instance of STEP 7 opens.
2. In the new instance, create a new project with the name "Controller2".
3. Insert a CPU 1215C in the network view. Name it "Controller2".

4. Copy the IO device from the project "Controller1" and insert it in the network view of project "Controller2".
5. Assign the IO controller "Controller2" to the IO device.



6. Save the project.

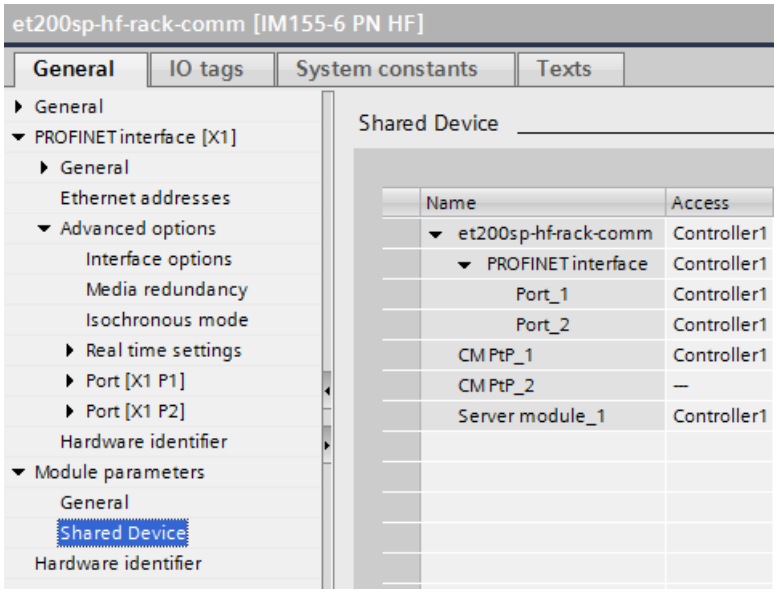
Both projects now have an identically structured IO device that must be configured in the next step for the different types of IO controller access.

Procedure: Configuring access to the shared device

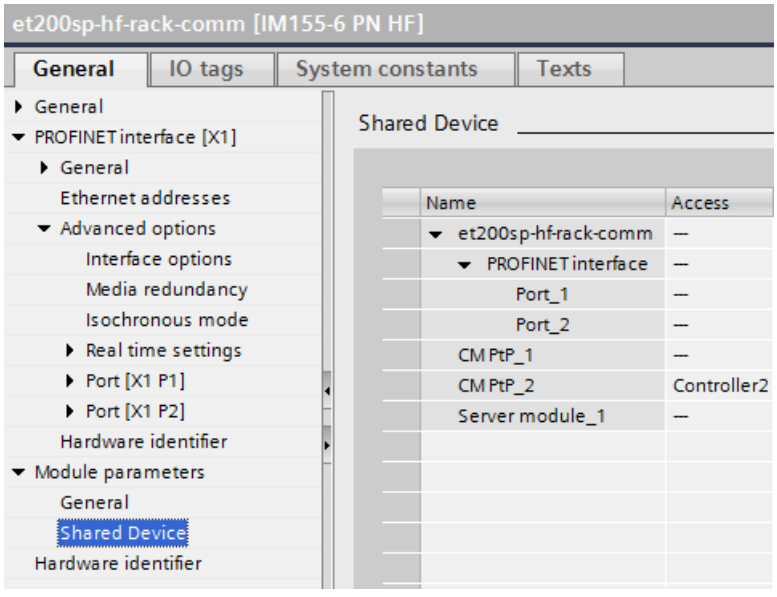
The modules and submodules you insert in the shared device are automatically assigned to the local CPU. To change the assignment, follow these steps:

1. Select the interface module in the network or device view of project "Controller1".
2. Select the "Shared Device" area in the Inspector window.
   A table shows which CPU has access to the respective module or submodule for all configured modules. The default setting is that the local CPU has access to all modules and submodules.

3. Keep the "Controller1" setting for all modules and submodules that are to remain in the address range of the local CPU.
   Select the setting "---" for all modules and submodules that are to be located in the address range of the CPU from the "Controller2" project (Controller2). This means that an IO controller outside the project is to have access to the module or submodule.



4. Select the interface module in the network or device view of project "Controller2".
5. Select the "Shared Device" area in the Inspector window.
   A table shows which CPU has access to the respective module or submodule for all configured modules.
6. Select the setting "---" for all modules and submodules that are to be located in the address range of the CPU from the "Controller1" project (Controller1).



7. Finally, check whether the settings for access are "complementary" for each module or submodule in both projects. This means that if the local CPU has access in one project, the option "---" must be set in the other project and vice versa.

   Note: The option "---" for the PROFINET interface and therefore for the ports makes the associated parameters read-only and not changeable. Parameters of the PROFINET interface and port parameters can only be edited in the project in which the PROFINET interface is assigned to the local CPU. The ports can be interconnected in both projects regardless of this.
8. Check whether the same IP address parameters and device name are set for the shared device in all projects.

   Check whether the same S7 subnet ID is set in all projects for the subnet to which the shared device is connected (subnet properties, "General" area in the Inspector window).

NOTE

If you make changes to the shared device: Make the same changes in each project on the shared device. Make sure that only one IO controller has access to a module or submodule.

Procedure: Adjusting the real-time settings

To ensure that all IO controllers and shared devices are operated with the appropriate send clock and that the update times are calculated correctly based on the communication load, you must adjust and check the following settings:

1. Select the project whose IO controllers have access to the PROFINET interface and the ports of the shared device.
2. Select the interface module of the shared device in the network view.
3. In the Inspector window, navigate to the "PROFINET interface > Advanced options > Real time settings > IO cycle" area.
4. In the "Shared device" area, set the number of project-external IO controllers. The maximum number depends on the IO device (specification in GSD file).
5. You must set the same send clock for each IO controller that has access to modules and submodules of the shared device:

- If you configure the IO controller with STEP 7 (TIA Portal):
  - Open the corresponding project.
  - Select the PROFINET interface of the IO controller.
  - Select the "Advanced options > Real time settings > IO communication" area in the Inspector window and set the shared send clock.
- If you configure the IO controller with a different engineering tool:
  - Select the PROFINET interface of the shared device in STEP 7 (TIA Portal) and read out the send clock on the shared device ("Advanced options > Real time settings" area).
  - Enter the read send clock in the engineering tool.

NOTE

If you configure all IO controllers that have access to the shared device in STEP 7 (TIA Portal), you can set shorter send clocks on the IO controller than supported by the shared device (send clock adaptation).

Compiling and loading

You must compile the configurations for the different IO controllers and load them to the CPUs one after the other.
Due to the distributed configuration with separate projects, STEP 7 does not output consistency errors in the case of incorrect access parameter assignment. These are examples of incorrect access parameter assignment:

- Several IO controllers have access to the same module
- IP address parameters or send clocks are not identical

These errors do not show up until controller operation and are output as configuration errors.

12.6.14.3 Example: Configuring an I-device as a shared device

This example describes how to configure an S7-1200 as an I-device with STEP 7 Version V13 SP1 or higher and then use it in two projects as a shared device.
A "distributed" configuration with different engineering tools for different IO controller families is possible. The procedure described below is based on STEP 7 and is limited to a configuration with two IO controllers of the S7-1200 family that share the transfer areas of an I-device as a shared device. The I-device itself is a CPU 1215C.
The example creates three projects with one IO controller each:

- S7-1200-I-Device
- Controller1
- Controller2

You use the S7-1200-I-Device project to configure the I-device. You use the PROFINET GSD variant of S7-1200-I-Device in the Controller1 and Controller2 projects in order to assign the transfer areas in the respective higher-level IO controller.

Shared I-device concept

The shared I-device concept requires a minimum of three separate projects:

- I-device project: You configure and program an I-device to perform a particular automation task. You define transfer areas as the I/O interface for the higher level controllers and assign these transfer areas to different IO controllers. For the connection to higher-level IO controllers, you provide a PROFINET GSD file and use the transfer areas to access the I-device.
- Controllers that share the I-device (two projects): You use the I-device as a PROFINET GSD variant during configuration of the PROFINET IO system and, in this process, specify the I/O addresses under which the IO controllers access the transfer areas.

NOTE

If you configure an S7-1200 as an I-device, the maximum size of a transfer area is 1024 input or output bytes. There are possible constraining factors depending on local I/O as well as address space limitations on the controlling device.

I-device

You assign the following parameters for an S7-1200 CPU as an I-device:

- Centralized and distributed I/O
- Desired transfer areas
- Number of IO controllers having access to this I-device (always greater than 1 for a shared device)

NOTE

You configure the I-device without a higher-level IO controller. As a result, you can only use the local I/O addresses of the transfer area (corresponds with the "Address in the I-device") to create the user program for editing the addresses from the transfer area. You download the I-device, completely configured except for the connection to the higher-level IO controller, to the S7-1200 CPU.

You export a PROFINET GSD file from the I-device configuration.

Controllers that share the I-device

You must install the PROFINET GSD file created from the I-device configuration in all engineering systems that you use in configuring a PROFINET IO system with this shared I-device. If you configure all uses of this I-device with STEP 7, install the GSD file in STEP 7.

You configure the I-device as a GSD variant on the PROFINET IO system in the projects involved. You can find this I-device under "Other field devices > PROFINET IO > PLCs & CPs" following installation.

In each of the projects involved, you assign transfer areas exclusively to the higher-level IO controllers (default setting: all). You set the other transfer areas to "---" (not assigned). When you do so, the local IO controller cannot access this transfer area, and you can assign the transfer area to another IO controller in another project.

Requirements

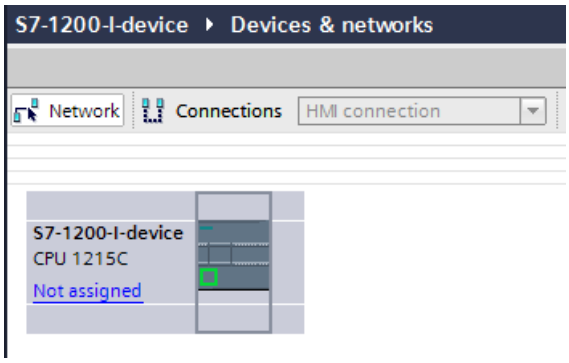
- IO device supports shared device functionality (for example, ET 200SP IM 155-6 PN HF V3.1).
- GSD file for configuring the IO device as a shared device is installed.

Procedure: Creating the S7-1200-I-device project

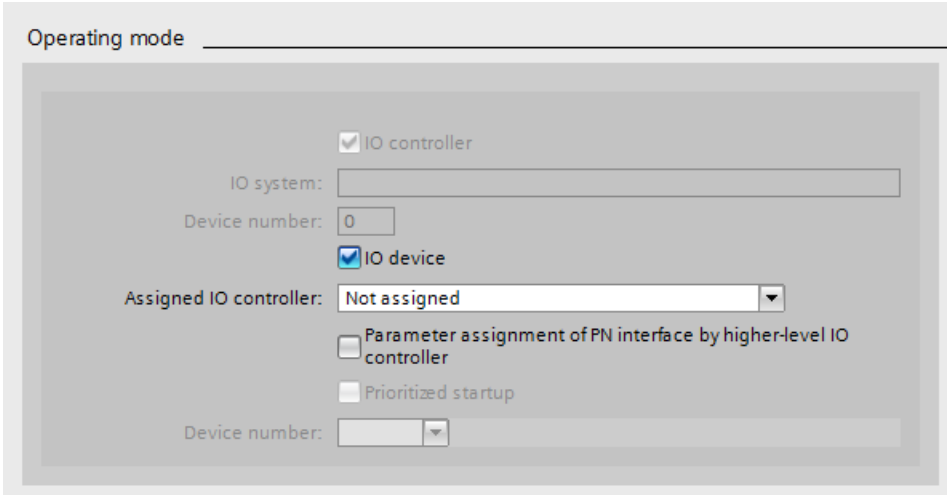
To create the project with a shared I-device, follow these steps:

1. Start STEP 7.
2. Create a new project with the name "S7-1200-I-device".

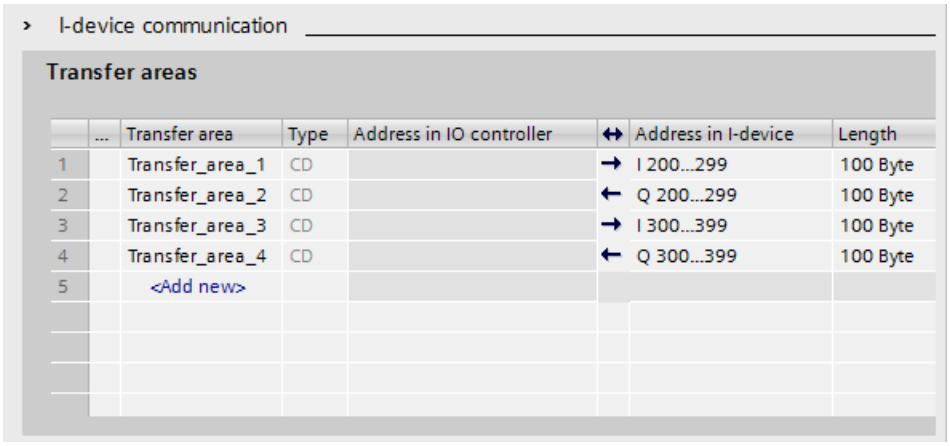
3. Insert a CPU 1215C from the hardware catalog in the network view. Assign the name "S7-1200-I-device".



4. Double-click the IO device and configure all required modules and submodules.
5. Assign the module parameters. In particular, you must configure the following settings for the CPU in the area of the PROFINET interface [X1]:
   – Enable the "IO device" option in the "Operating mode" area.

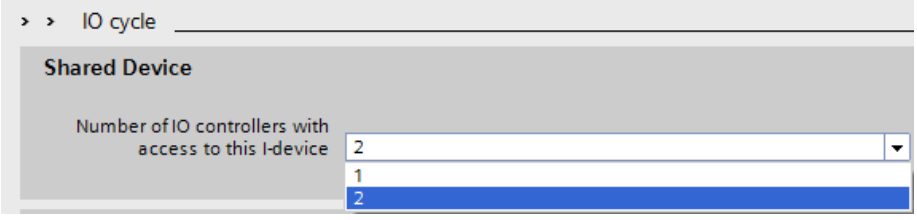


   – Configure the transfer areas in the "Operating mode" > "I-device communication". The "Address in IO controller" column remains empty because no IO controller is assigned.



Note: To change an input area to an output area, and vice versa, you must navigate to the area of the corresponding transfer area.

– Select the number of IO controllers (at least two) that will access the shared I-device during operation ("Operating mode" > "Real time settings" > "IO cycle").



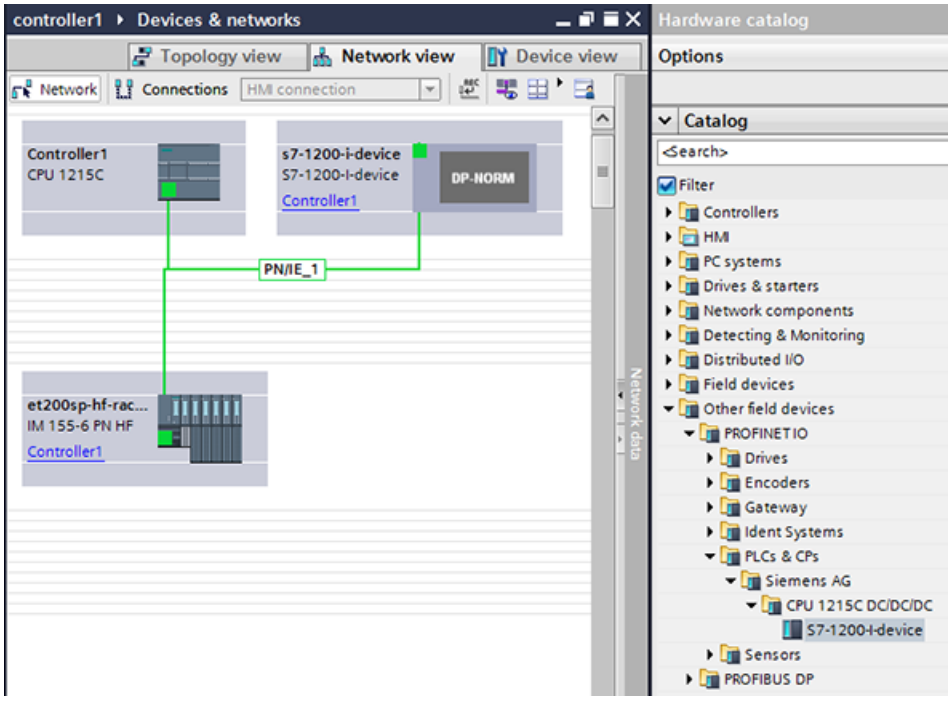
6. Save the project.
7. From the General tab, select PROFINET interface [X1] > Operating mode > I-device communication. From the "Export generic station description file (GSD)" area, click the Export button. If you do not change the name in the Export dialog, the GSD file uses an assigned format name (for example, "GSDML-V2.31-#Siemens-PreConf_S7-1200-I-Device-20130925-123456").

Procedure: Creating the Controller1 project

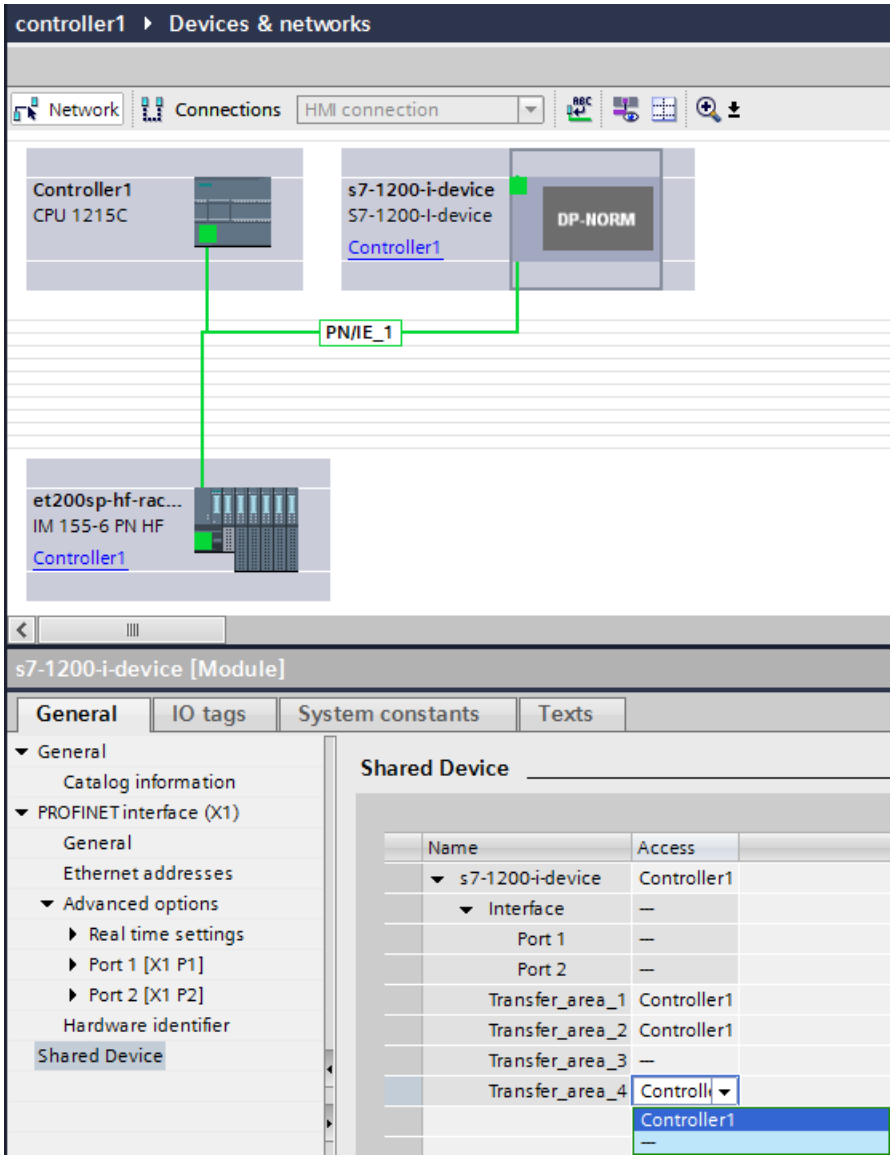
To create the first project with a shared I-device, follow these steps:

1. Start STEP 7.
2. From the Options menu, select "Manage general station description files (GSD)".
3. From the "Manage general station description files" dialog, install the PROFINET GSD file that you exported.
4. Create a new project with the name "Controller1".
5. Insert the CPU 1215C in the network view. The name of the CPU should be "Controller1".
6. Insert the I-device from the hardware catalog (Hardware catalog: Other field devices > PROFINET IO > PLCs & CPs).

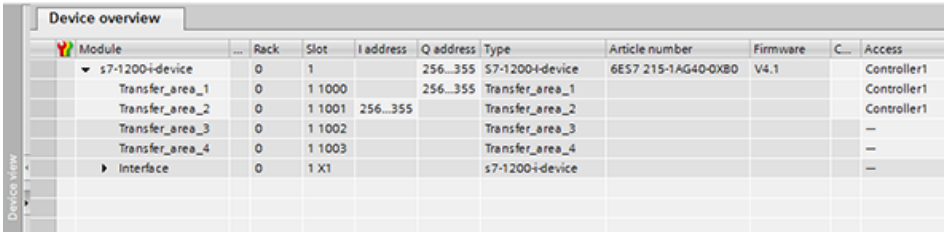
7. Assign the IO controller "Controller1" to the I-device.



8. Select the "Shared device" area in the properties of the I-device:
   - In the table, all transfer areas and the PROFINET interface are assigned to the local IO controller (Controller1).
   - Define the transfer areas to which the Controller1 CPU should **not** have access. Select the "---" entry for these areas. These transfer areas are provided for Controller2.



9. You can adapt the addresses from the Device view of the IO controller in the Device overview. To open the device overview, double-click the I-device.



Module	...	Rack	Slot	I address	Q address	Type	Article number	Firmware	C...	Access
s7-1200-i-device		0	1		256...355	S7-1200-I-device	6ES7 215-1AG40-0XB0	V4.1		Controller1
Transfer_area_1		0	1 1000		256...355	Transfer_area_1				Controller1
Transfer_area_2		0	1 1001	256...355		Transfer_area_2				Controller1
Transfer_area_3		0	1 1002			Transfer_area_3				—
Transfer_area_4		0	1 1003			Transfer_area_4				—
Interface		0	1 X1			s7-1200-i-device				—

10. Save the project.

Procedure - Creating the Controller2 project

To create the second project with a shared device, follow these steps:

1. Start STEP 7 once again.
   A new instance of STEP 7 opens.
2. In the new instance, create a new project with the name "Controller2".
3. Insert the CPU 1215C in the network view. Assign the name "Controller2".
4. Insert the I-device from the hardware catalog (Hardware catalog: Other field devices > PROFINET IO > PLCs & CPs).
5. Assign the IO controller "Controller2" to the I-device.
6. Adapt the access to the transfer areas as in the Controller1 project. Ensure that no duplicate assignments result.
7. Adapt the parameters of the subnet and PROFINET interface. Because the shared I-device involves the same device in different projects, these data must match.
8. Save the project.

Both projects now have an identically configured shared I-device. The IO controller access and the parameters of the PROFINET interface should still be checked in the different projects during the next step.

Summary - Assigning parameters for access to the shared device

The transfer areas are automatically assigned to the local IO controller. To change the assignment, follow these steps:

1. Click the "S7-1200-I-Device" device in the network view of the "Controller1" project, and select the "Shared device" area.
2. A table shows which CPU has access to each of the configured transfer areas. The default setting is that the local CPU has access to all modules and submodules.
3. Keep the setting "Controller1" for all transfer areas that are to remain in the address range of the local CPU.
   Select the setting "---" for all transfer areas that are to be located in the address range of the "Controller2" CPU from the "Controller2" project. This means that an IO controller outside the project is to have access to the transfer area.
4. Follow the same procedure for the remaining projects.
5. Finally, check whether the settings for access are "complementary" for each module or submodule in both projects. This means that if the local CPU has access in one project, the option "---" must be set in the other project and vice versa.
   Note: The option "---" for the PROFINET interface and therefore for the ports makes the associated parameters read-only and not changeable. Parameters of the PROFINET interface and port parameters can only be edited in the project in which the PROFINET interface is assigned to the local CPU. The ports can be interconnected in both projects regardless of this.
6. Check whether the same IP address parameters and device name are set for the shared device in all projects.
   Check whether the same S7 subnet ID is set in all projects for the subnet to which the shared device is connected (subnet properties, "General" area in the Inspector window).

NOTE

If you make changes to the I-device (for example, change the number or length of the transfer areas), export the I-device as a GSD file again. Re-install the GSD file in each project that uses the I-device as a shared device. Make sure that only one IO controller has access to a transfer area.

NOTE

When you use the S7-1200 as a shared I-device and as a controller, ensure that you increase the PROFINET I-device and PROFINET IO Update times to alleviate the communications performance impact. The system is very stable and works well when you select 2 ms for the Update time of a single PROFINET I-device time and you select 2 ms for the Update time of a single PROFINET IO time.

You specify the "IO cycle" parameters in the "Properties" configuration dialog of the PROFINET I-device or IO. Refer to "Configuring the IO cycle time" (Page 649) for further information.

Procedure - Adjusting the real-time settings

To ensure that all IO controllers and shared devices are operated with the appropriate send clock and that the update times are calculated correctly based on the communication load, you must adjust and check the following settings:

1. You must set the same send clock for each IO controller that has access to modules and submodules of the shared device:

- If you configure the IO controller with STEP 7 (TIA Portal), perform these steps:
  - Open the corresponding project.
  - Select the PROFINET interface of the IO controller.
  - Select the "Advanced options > Real time settings > IO cycle" area in the Inspector window and set the shared send clock.
- If you configure the IO controller with a different engineering tool, perform these steps:
  - Select the PROFINET interface of the shared device in STEP 7 (TIA Portal) and read out the send clock on the shared device ("Advanced options > Real time settings" area)
  - Enter the read send clock in the engineering tool.

NOTE

If you configure **all** IO controllers that have access to the shared I-device in STEP 7 (TIA Portal), you can set shorter send clocks on the IO controller than supported by the shared device (send clock adaptation).

Compiling and downloading

You must compile the configurations for the different IO controllers and download them to the CPUs one after the other.

Due to the distributed configuration with separate projects, STEP 7 does not output consistency errors in the case of incorrect access parameter assignment. These are examples of incorrect access parameter assignment:

- Several IO controllers have access to the same module.
- IP address parameters or send clocks are not identical.

These errors do not show up until controller operation and are output as configuration errors.

12.6.15 Media Redundancy Protocol (MRP)

The following CPUs support MRP functionality as a MRP Manager and a client.

- CPU 1215C
- CPU 1217C
- CPU 1215FC

As a "Client" the 1215/1217 must operate in an MRP ring by forwarding MRP packets over its interface and reporting connection breaks to a manager in the network.

As a "Manager" the 1215/1217 must send MRP packets around the network, detect open ports in the ring, manage blocked ports, and negotiate manager status with other potential managers.

The S7-1200 CPU family has three models (see above) that support the MRP protocol, and the configuration parameters used to initialize MRP client and manager operation. These CPUS have two PN ports.

With these three CPUs you can set up an MRP ring with the S7-1200 as either a client or a manager. When acting as a manager, the CPU uses test frames to check and make sure the ring is not interrupted. When acting as a client, it forwards these test frames instead of making the check itself. This allows the S7-1200 to be used in both roles if needed.

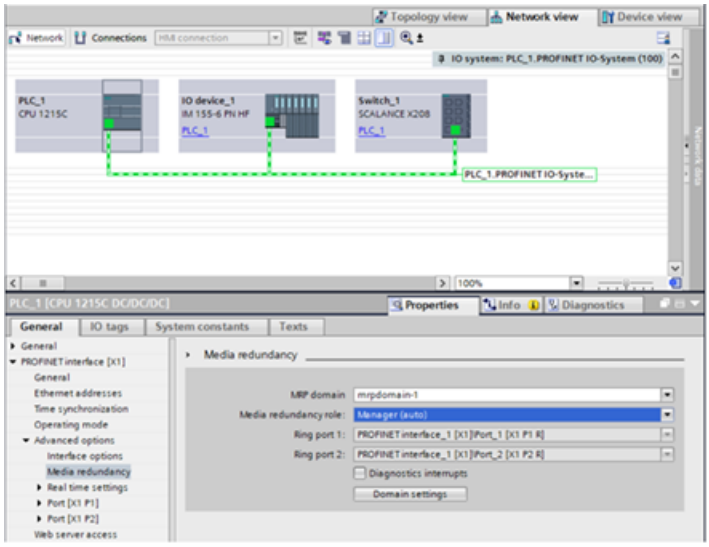


Figure 12-1 Media redundancy configuration STEP 7

MRP Manager (auto) role and Manager

You can use the S7-1200 (1215C/1217C) as a Manager and Manager (auto) role in a Media Redundancy Ring (MRP). MRP allows you to connect their devices into a ring configuration. The MRP Manager typically forces data to flow in one linear direction by blocking a port of the ring. When this ring configuration experiences an interruption, the Manager detects the interruption and unblocks the port, allowing data to flow in the other direction. MRP allows

the network to remain operational because of a broken wire or failed device. MRP Specification allows a maximum of 50 devices in a ring configuration.

MRP Manager

The MRP Manager allows the S7-1200 PLC to act as the redundancy manager. When configured for this role, the S7-1200 uses test frames to communicate with client PLCs to ensure connection within the ring is not interrupted. If an interruption to a client is detected, the S7-1200, acting as the MRP Manager, will inform client devices within the ring of the change immediately using the ring ports. TIA Portal only allows one device to be set to MRP Manager in an MRP Loop.

MRP Manager (auto) role

When multiple devices are assigned the MRP Manager (auto) role, they negotiate for Manager status amongst one another. If the negotiated MRP Manager is disconnected from the configuration, the remaining devices set as Manager (auto) will renegotiate the Manager role amongst themselves until the original configuration returns. When the original manager returns successfully, they will renegotiate the manager status back, and resume the original configuration.

NOTE

Reconfiguration of ring

The reconfiguration of the ring can take up to 200 ms. For this reason, the PROFINET watchdog time for each device must be set higher than 200 ms.

NOTE

MRP Manager (auto) mode is default

If there is not a project, the CPU will, by default, be in the MRP Manager (auto) mode. This is important to know if you plug an out-of-the-box device into a non-ring topology and notice test frames on your network.

S7-1200 (1214C, 1212C, and 1211C CPUs) cannot enable MRP Manager and Manager (auto) functionality. The menu options in TIA Portal are not available for these CPUs.

The S7-1200 does not support MRPD because the S7-1200 does not have IRT (Isochronous Realtime) capability.

Diagnostic interrupts can be toggled on and off in the media redundancy configuration window of the TIA portal to allow the manager and clients to provide relevant MRP change reports such as:

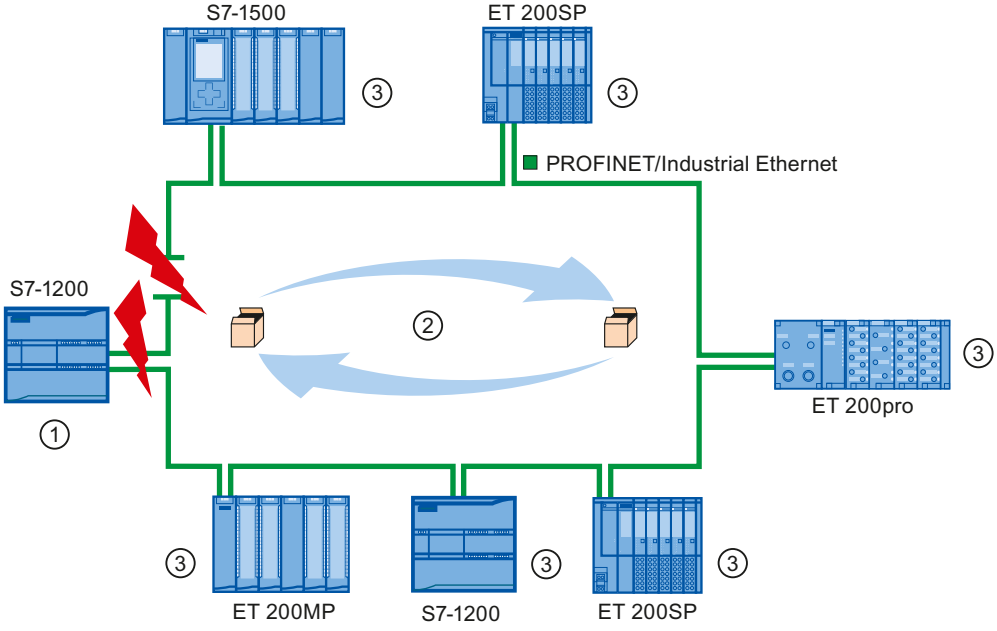
- A neighbor device of the ring port not supporting MRP
- A ring port being connected to a non-ring port neighbor
- A ring port connected to a different MRP Domain
- (Manager only) Interruption / return diagnostic interrupts when the MRP ring is interrupted and when the original configuration returns

12.6.15.1 Media redundancy with ring topologies

In order to increase the network availability of an Industrial Ethernet network with optical or electrical linear bus topologies, you can convert a linear bus topology to a ring topology by joining the ends together.

Devices in a ring topology can be IO devices, IO controllers, external switches, and/or the integrated switches of communication modules.

To set up a ring topology with media redundancy, you need to bring together the two free ends of a linear bus topology in one device. Closing the linear bus topology to form a ring is achieved with two ports (ring ports) of a device in the ring. One device of the resulting ring then takes over the role of the MRP manager. All other devices in the ring are MRP clients.



① MRP manager (Can be an S7-1500 CPU, an S7-1200 CPU 1215C, an S7-1200 CPU 1215FC, or an S7-1200 CPU 1217C)

② Test frames

③ MRP clients

The ring ports of a device are the ports that establish the connection to the two neighboring devices in the ring topology. The ring ports are selected and set in the configuration of the relevant device (is also preset, if applicable).

How media redundancy works in a ring topology

The data paths between the individual devices are automatically reconfigured if the ring is interrupted at any point. The devices are available again after reconfiguration.

In the MRP manager, one of the two ring ports is blocked in uninterrupted network operation for normal communication so that no data frames are circulated. The MRP manager monitors the ring for interruptions. It does this by sending test frames both from ring port 1 and ring port 2. The test frames run round the ring in both directions until they arrive at the other ring port of the MRP manager.

An interruption of the ring can be caused by loss of the connection between two devices or by failure of a device in the ring.

If the test frames of the MRP manager no longer arrive at the other ring port during an interruption of the ring, the MRP manager connects its two ring ports. This substitute path once again restores a functioning connection between all remaining devices in the form of a linear bus topology.

The time between the ring interruption and restoration of a functional linear topology is known as the reconfiguration time.

As soon as the interruption is eliminated, the original transmission paths are established again, the two ring ports of the MRP manager are disconnected, and the MRP clients informed of the change. The MRP clients then use the original paths again to the other devices.

Media redundancy method

The standard method of media redundancy in SIMATIC is Media Redundancy Protocol (MRP) with a typical reconfiguration time of 200 ms. Up to 50 devices can participate per ring.

NOTE

Reconfiguration of ring

The reconfiguration of the ring can take up to 200 ms. The PROFINET watchdog time for each device must be set higher than 200 ms.

12.6.15.2 Using Media Redundancy Protocol (MRP)

The "MRP" process works in conformity with Media Redundancy Protocol (MRP), which is specified in IEC 61158 Type 10 "PROFINET".

Requirements

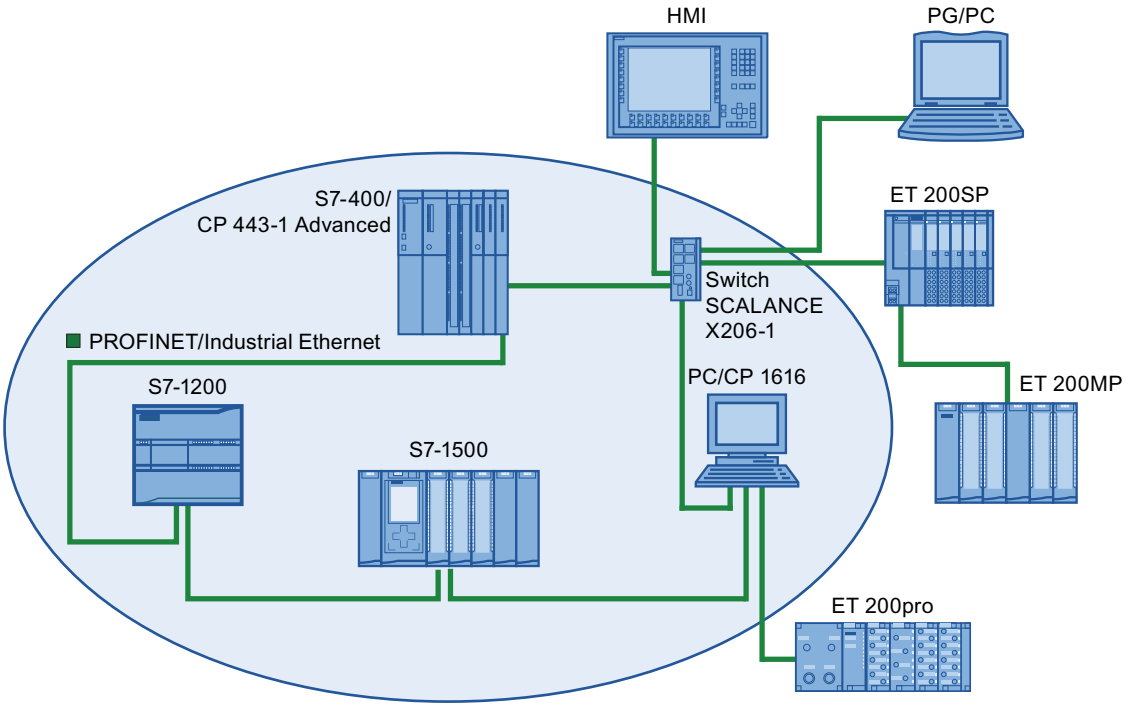
The following requirements must be met for error-free operation with MRP:

- The ring in which you want to use MRP may only consist of devices that support this function.
- "MRP" must be activated for all devices in the ring.
- All devices must be interconnected using their ring ports.
- At least one MRP manager or Role "Manager" must be available.
- The ring must contain not more than 50 devices. Otherwise, reconfiguration times of greater than or equal to 200 ms can occur.
- All partner ports within the rings must have identical settings.

Topology

The following schematic shows a possible topology for devices in a ring with MRP. The devices inside the shaded oval are in the redundancy domain.

This is an example of a ring topology with MRP:



The following rules apply to a ring topology with media redundancy using MRP:

- All devices in the ring belong to the same redundancy domain.
- One device in the ring must be configured for the role of MRP manager or MRP manager(auto).
  - Only one device in the ring can be an MRP manager; all other devices must be MRP clients.
  - If there is no MRP manager, multiple devices can be configured as MRP manager(auto).

You can connect non MRP-compliant devices to the network through ports not configured as ring ports. You can only do this with devices that have more than two ports (for example, a SCALANCE X switch or a PC with a CP1616).

Boundary conditions

You can have the following communication possibilities:

- MRP and RT: RT operation is possible with the use of MRP.

NOTE

The RT communication is disrupted (station failure) if the reconfiguration time of the ring is greater than the selected watchdog time of the IO device. You must select a watchdog time greater than 200 ms for your IO devices. Refer to the "Watchdog time" section below for further information.

- MRP and TCP/IP (TSEND, HTTP, ...): The TCP/IP communication with MRP is possible because lost data packages are resent, if applicable.

- MRP and prioritized startup:
  - If you configure MRP in a ring, you cannot use the "prioritized startup" function in PROFINET applications on the devices involved.
  - If you want to use the "prioritized startup" function, then you must disable MRP in the configuration (the device cannot be part of the ring).
- MRP on PROFINET devices with more than two ports: If you operate a PROFINET device with more than two ports in a ring, you should set a sync boundary on the ports that are not in the ring. By setting the sync boundary, you define a boundary for a sync domain. You cannot forward sync frames transmitted to synchronize devices within a sync domain.

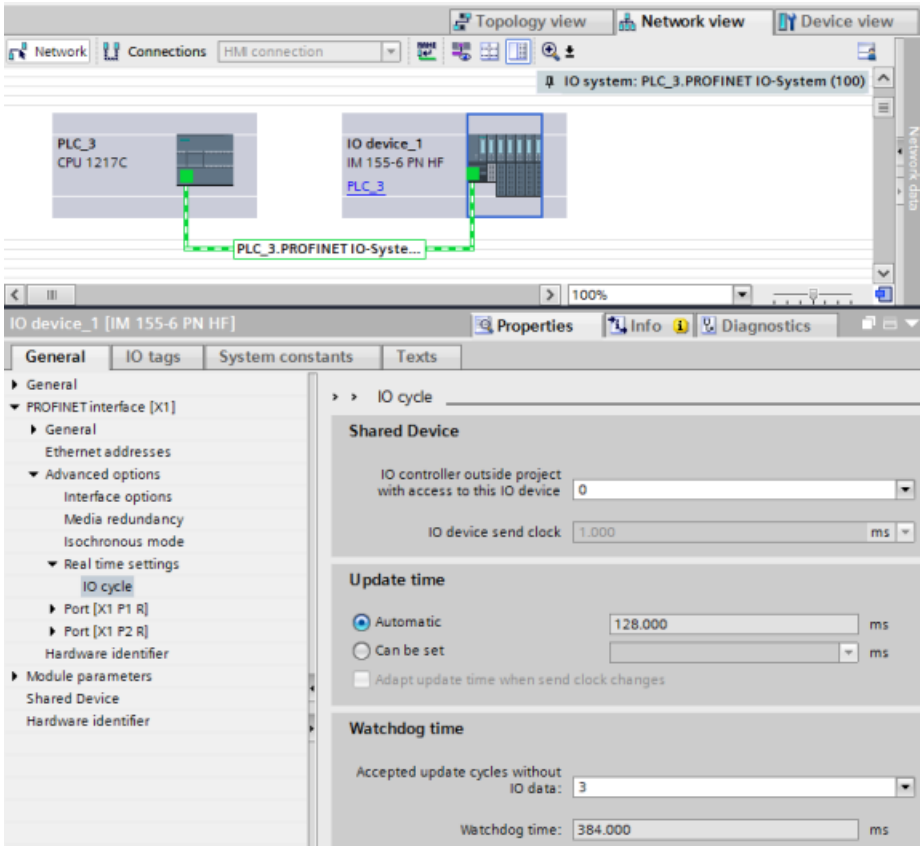
Watchdog time

The PROFINET watchdog time is the time interval that an IO controller or IO device permits, without receiving IO data. If the IO device is not supplied by the IO controller with data within the watchdog time, the device detects the missing frames and outputs substitute values. This is reported in the IO controller as a station failure.

You can configure the watchdog time for PROFINET IO devices. Do not enter the watchdog time directly, but as "Accepted update cycles without IO data". The resulting watchdog time is automatically calculated from the number of update cycles.

To assign the watchdog time, follow these steps:

1. Select the PROFINET interface of the IO device in the Network or Device view.
2. In the properties of the interface, navigate to: Advanced options > Realtime settings > IO cycle
3. Select the required number of cycles from the drop-down list.



12.6.15.3 Configuring media redundancy

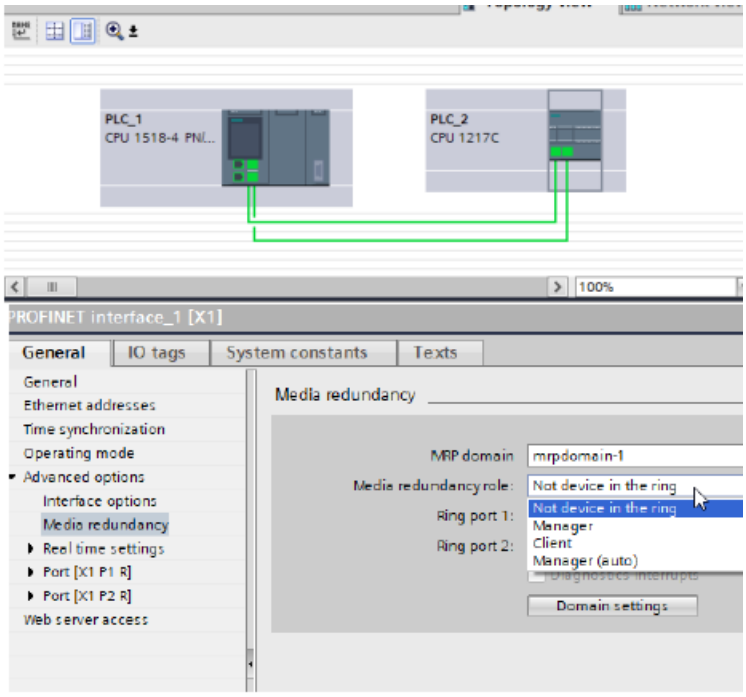
All of the components in your application must support Media Redundancy Protocol (MRP).

Procedure

To configure media redundancy, proceed as follows:

1. Establish a ring by means of appropriate port interconnections (for example, in the topology view).
2. Select a PROFINET device for which you want to configure media redundancy.

3. In the Inspector window, navigate to "PROFINET" interface [X1]">"Advanced options">"Media redundancy".



4. Under "Media redundancy role", assign the "Manager (Auto)", "Client", or "Not device in the ring" role to the device.
   When you configure a ring in the TIA Portal Topology view, the TIA Portal automatically sets the Media Redundancy role for you. If a device can be a Manager, the TIA Portal sets the Media redundancy role as "Manager (Auto)". For the S7-1200, the Media Redundancy role can now be set to either "Client" or "Manager".

   NOTE

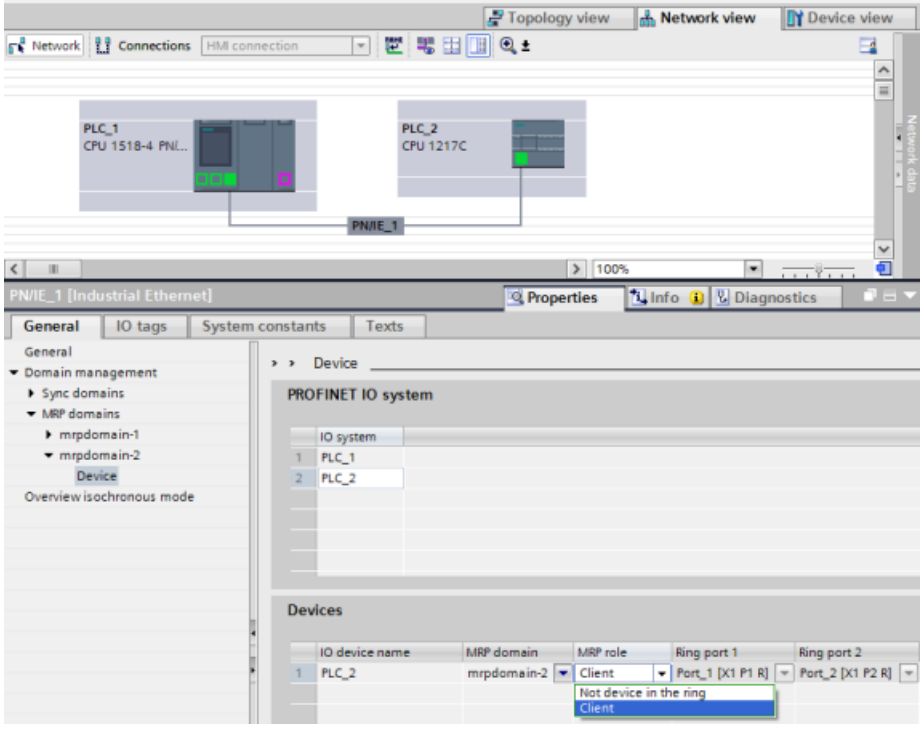
   You can assign the "Manager" or "Manager (Auto)" MRP roles to the S7-1200 CPU 1215C/1215FC/1217C.

5. Repeat steps 2 to 4 for all PROFINET devices in the ring.

Or:

1. Highlight the PROFINET IO system in the network view.
2. Click on the PROFINET IO system.

3. Navigate to the device of the required MRP domain in the inspector window.



4. For the PROFINET devices, set the "Manager (Auto)", "Client", or "Not device in the ring" role.

"Media redundancy" setting option: MRP role

Depending on the device used, the roles "Manager", "Manager (Auto)", "Client", and "Not device in the ring" are available.

Rules:

- A ring can have only one device with the role of "Manager". No additional devices with the role of "Manager" or "Manager (Auto)" are permissible. All other devices in the ring can only have the role of "Client". Devices not in the ring can have the role "Not device in the ring".
- If a ring has no device with the "Manager" role, the ring must at least have one device with the role "Manager (Auto)". A ring can have any number of devices with the roles "Client" and "Manager (Auto)".

"Media redundancy" setting option: Ring port 1 and Ring port 2

Select one at a time those ports you want to configure as ring port 1 or ring port 2. The drop-down list box shows the selection of possible ports for each device type. If the ports are set at the factory, then the fields are unavailable.

NOTE

Ring port configuration is not necessary in the S7-1200 because the S7-1200 CPU has only two ports.

Diagnostic interrupts

If diagnostic interrupts to the MRP state are to be output in the local CPU, select the "Diagnostic interrupts" check box. The following diagnostic interrupts can be configured:

- Wiring or port error:
  The CPU generates diagnostic interrupts for the following errors in the ring ports:
  - A neighbor of the ring port does not support MRP.
  - A ring port is connected to a non-ring port.
  - A ring port is connected to the ring port of another MRP domain.
- Interruption / return (MRP manager only):
  If the ring is interrupted and the original configuration is returned, the CPU generates diagnostic interrupts. If both of these interrupts occur within 0.2 seconds, this indicates an interruption of the ring.

You can respond to these events in the user program by programming the appropriate response in the diagnostic error interrupt OB (OB 82).

NOTE

Third-party devices as MRP manager

To assure error-free operation when a third party device is used as MRP manager in a ring, you must assign the fixed role of "Client" to all other devices in the ring before you close the ring. Otherwise, circulating data frames and network failure could occur.

12.6.16 S7 routing

From the STEP 7 Network view, you can create a complex communication topology by connecting devices in different S7 subnets. You can connect classic S7-300/S7-400 CPUs and CPs as well as the latest S7 CPUs and CPs and can include HMIs and PC stations such as an OPC server.

Once you decide which devices must communicate and establish the necessary connections using STEP 7, the Engineering System (ES) can download the corresponding routing tables to the various S7 routers as part of the hardware configuration. After you download the routing tables to the various S7 routers, the ES or other communication partners can communicate with each device even though the devices are on different S7 subnets. This is possible because the CPUs and/or CPs, in between, act as S7 routers. The CPUs and/or CPs forward incoming connection requests to the next S7 router until the connection request reaches the targeted device, and the devices establish the S7 connection.

The CPU uses the write record mechanism to transfer the routing tables required by the CP devices in the local base. The routing tables establish the route from one device to another at the time of a connection request, which includes a remote S7 Subnet_ID. The device receiving the connection request interrogates its routing table, finds the next station in the path to the target S7 subnet, and forwards the connection request. Eventually, the

connection request reaches the intended target and the response traverses the route in the reverse direction.

The S7-1200 CPUs have a single PN interface and up to three CP devices connected to the local communication bus. Therefore, you have two options for routing within the S7-1200 station:

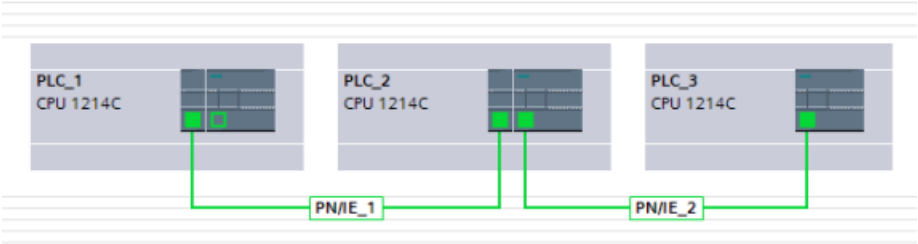
- Routing between the CPU and a CP
- Routing from one CP to another CP

Refer to S7-1200 CPs at Siemens Industry Online Support for further information on all S7-1200 CPs that support the S7 routing function (https://support.industry.siemens.com/cs/us/en/view/584459).

12.6.16.1 S7 routing between CPU and CP interfaces

Since the S7-1200 CPUs are limited to a single PN interface, a stand-alone CPU cannot serve the function of a router. You can never connect a stand-alone CPU to more than one S7 subnet at a time. When you install CP modules in the local base of the CPU, you can connect to multiple S7 subnets and utilize routing.

In the example system below, in order for PLC_1 to communicate with PLC_3, the Engineering System (ES) must rout messages through PLC_2. The ES must download the routing table for PLC_2, and PLC_2 must provide the routing table for the CP module in its local base. With these routing tables in place, PLC_1 and PLC_3 can communicate with each other, even though not directly connected.

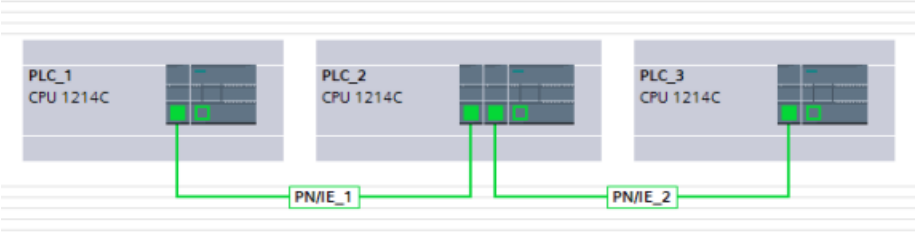


In order to check routing from either S7 subnet to the other S7 subnet, PLC_1 must establish a transport connection to PLC_3, and PLC_3 must establish a connection to PLC_1. Doing so, makes sure that routing from the PLC's PN/IE interface to a CP module is possible as well as routing from a CP module to the PLC's PN/IE interface.

12.6.16.2 S7 routing between two CP interfaces

Since the S7-1200 CPUs support up to three CP modules, you can connect all three modules to different S7 subnets. When you install at least two CP modules in the local base of the CPU and connect to different S7 subnets, you can utilize routing.

In the example system below, in order for PLC_1 to communicate with PLC_3, the Engineering System (ES) must rout messages by PLC_2 from the CP module to the CP module in its local base. The ES must download the routing table for PLC_2, and PLC_2 must provide the routing table for the two CP modules. With these routing tables in place, PLC_1 and PLC_3 can communicate with each other, even though not directly connected. Also, you should note that routing takes place from CP module to CP module without messages being sent over the PN/IE interface of PLC_2.



12.6.17 SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more.

Network management systems use SNMP to monitor network-attached devices for conditions that warrant administrative attention. SNMP uses various services and tools for detection and diagnostics of the network topology. You can find information about the properties of devices capable of SNMP in the Management Information Base (MIB) files. You must have the required rights to access the MIB files.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. Managing applications can query (and sometimes set) these variables.

SNMP uses the UDP transport protocol and has two network components:

- SNMP manager: Monitors the network nodes
- SNMP client: Collects the various network-specific information in the individual network nodes and stores it in a structured form in the Management Information Base (MIB). You can use this data to perform detailed network diagnostics.

For security reasons, SNMP is disabled by default on S7-1200 CPUs, preventing read and write access of SNMP variables. You must enable SNMP to remotely view and edit SNMP variables.

NOTE

S7-1200 CPUs prior to V4.6 enable SNMP by default. If you downgrade the firmware to a version earlier than V4.6, you can only disable SNMP from the STEP 7 program.

After enabling SNMP, certain conditions might require you to disable it. Examples of these conditions include the following:

- The security settings in your network do not allow the use of SNMP.
- You use your own SNMP solution (for example, with your own communications instructions).

If SNMP is disabled on the device, some functions and tools that rely on access to SNMP variables are unavailable or inoperable. For example, topology detection in TIA Portal is inoperable, and some functions of the SIMATIC Automation Tool V4.x and prior, are inoperable.

You can enable or disable SNMP from the device configuration and STEP 7 program.

NOTE

Restoring the CPU to factory defaults disables SNMP.

Enabling and disabling SNMP from the device configuration

To enable or disable SNMP follow these steps:

1. From the Project Tree, under the CPU, double-click Device configuration.
2. From the General tab of the device properties, expand Advanced configuration and select SNMP.
   The Inspector window displays the SNMP configuration settings.
3. To enable SNMP, select the "Activate SNMP" checkbox or to disable SNMP, deselect it.
4. Enter a Read-only community string or use the default (public) and enter a Read-write community string or use the default (private).

   NOTE

   Follow these conventions when entering Read-only and Read-write community strings:

   – Names must be at least 8 characters long, but no more than 240 characters long.
   – Names can include any letter of the alphabet or number.
   – Names cannot end or begin with a period or hyphen.

   NOTE

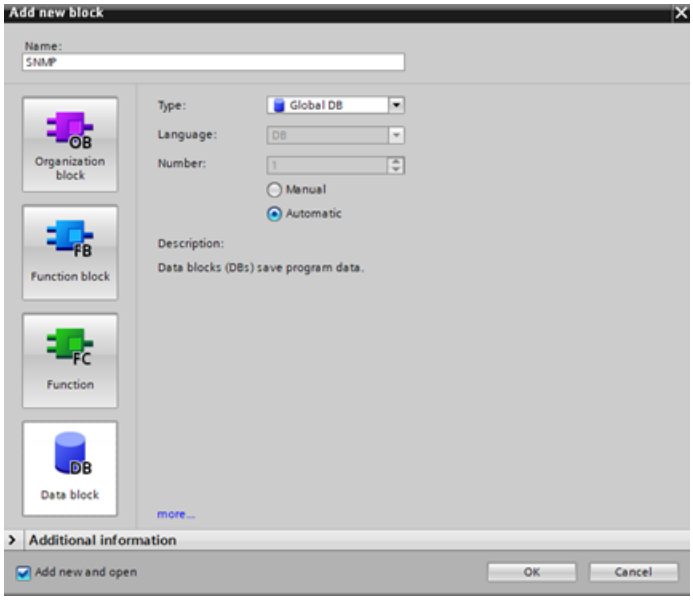
   To share SNMP data between the STEP 7 project and the PLC, the community name entered in the STEP 7 project must match the community name entered for the host when creating the SNMP database connection.

5. Download the configuration to the CPU.

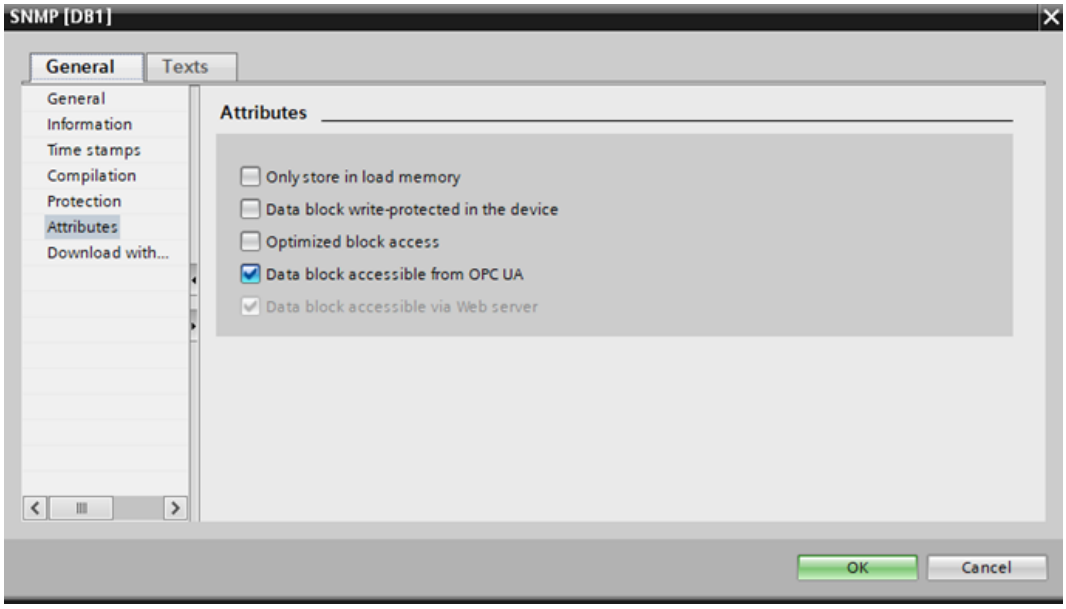
Enabling and disabling SNMP from the STEP 7 program

To enable or disable SNMP follow these steps:

1. Create a data block (DB):

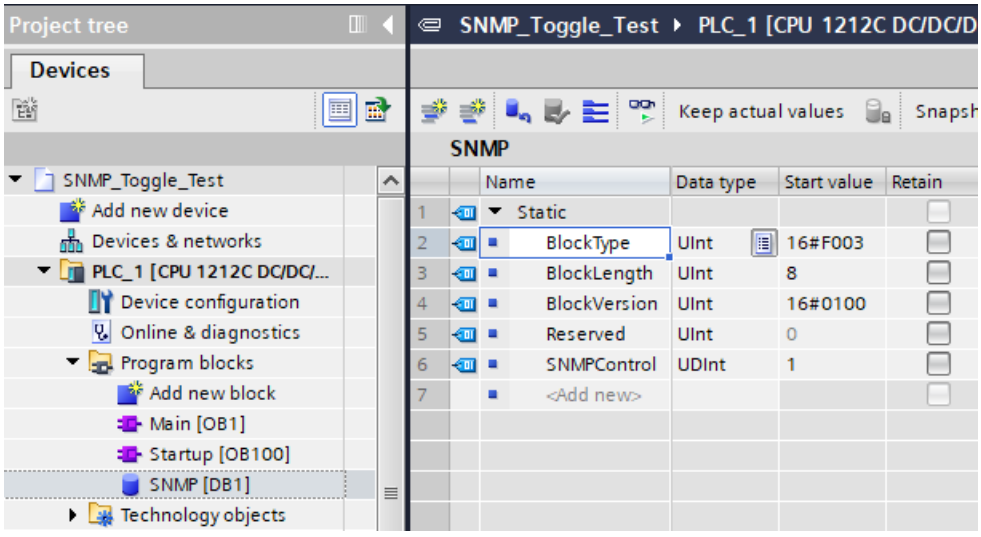


2. Select the Properties of the newly-created DB.
3. Select the Attributes tab. Deselect the check box for "Optimized block access":

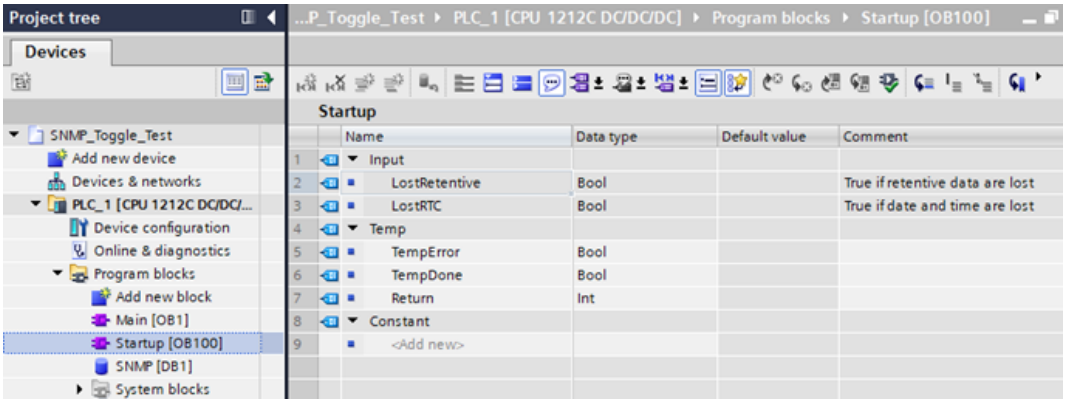


4. Click the OK button.
   When prompted, recompile your program.

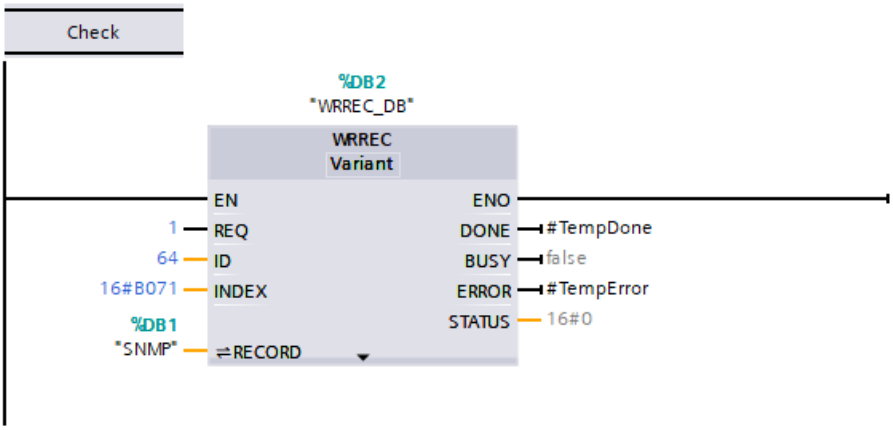
5. In the DB block interface, create the following static tags with the values shown. You will use these tags in your program to enable or disable the internal SNMP implementation. Change the Start value of the SNMPControl tag to enable or disable SNMP. Entering a Start value of 1 enables SNMP, while entering a Start value of 0 disables SNMP:



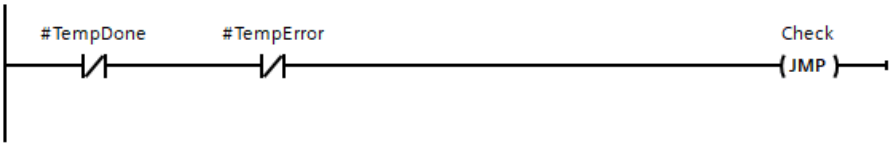
6. Add the Temporary variables, as shown below, to any program block (OB, FB, or FC) that executes when you want to enable or disable SNMP. This example uses Startup OB (OB100) to enable SNMP at the beginning of the program's execution:



7. Using the LAD editor insert a Label (Jump label) into Network 1 of the Startup OB (OB100). In the example below, the Label is named "Check." Then, in the same network, insert a WRREC (Write Record) instruction with the inputs and outputs shown:



8. Enter the following code for Network 2. This code ensures that the WRREC call completes, enabling or disabling SNMP before leaving the Startup OB (OB100):



9. Download the STEP 7 project software to the CPU.

NOTE

You cannot set community strings from the STEP 7 program. You can activate configured community strings from the STEP 7 program. When activating SNMP from the STEP 7 program, SNMP is active in RUN mode and is non-retentive. Because it is non-retentive, after a POWER OFF/ ON transition SNMP reverts to the settings selected in the device configuration. When activating SNMP from the device configuration, SNMP is active at download and is retentive.

12.6.18 Diagnostics

Refer to "Organization blocks (OBs)" (Page 66) for information on how to use organization blocks (OBs) for diagnostics with these communication networks.

12.6.19 Distributed I/O and diagnostic instructions

Refer to Distributed I/O (PROFINET, PROFIBUS, or AS-i) (Page 330) for information on Distributed I/O and Diagnostics instructions.
Refer to Diagnostic events for distributed I/O (Page 718) for handling diagnostic events.

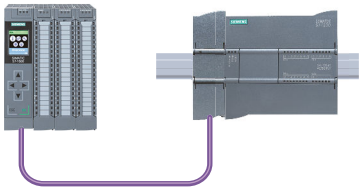
12.7 PROFIBUS

A PROFIBUS system uses a bus master to poll slave devices distributed in a multi-drop fashion on an RS485 serial bus. A PROFIBUS slave is any peripheral device (I/O transducer, valve, motor drive, or other measuring device) that processes information and sends its output to the master. The slave forms a passive station on the network since it does not have bus access rights, and can only acknowledge received messages, or send response messages to the master upon request. All PROFIBUS slaves have the same priority, and all network communication originates from the master.

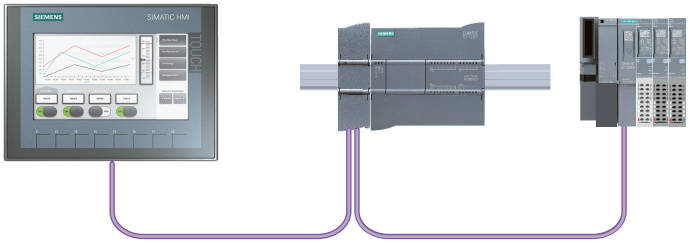
A PROFIBUS master forms an "active station" on the network. PROFIBUS DP defines two classes of masters. A class 1 master (normally a central programmable controller (PLC) or a PC running special software) handles the normal communication or exchange of data with the slaves assigned to it. A class 2 master (usually a configuration device, such as a laptop or programming console used for commissioning, maintenance, or diagnostics purposes) is a special device primarily used for commissioning slaves and for diagnostic purposes.

The S7-1200 is connected to a PROFIBUS network as a DP slave with the CM 1242-5 communication module. The CM 1242-5 (DP slave) module can be the communications partner of DP V0/V1 masters. If you want to configure the module in a third-party system, there is a GSD file available for the CM 1242-5 (DP slave) that ships with the module and on Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/49852283)pages on the Internet.

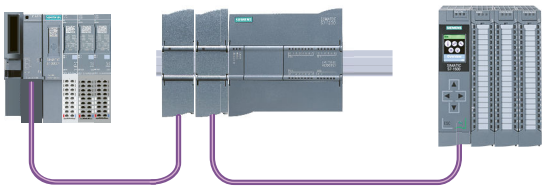
In the figure below, the S7-1200 is a DP slave to an S7-1500 controller:



The S7-1200 is connected to a PROFIBUS network as a DP master with the CM 1243-5 communication module. The CM 1243-5 (DP master) module can be the communications partner of DP V0/V1 slaves. In the figure below, the S7-1200 is a master controlling an ET 200SP DP slave:



If a CM 1242-5 and a CM 1243-5 are installed together, an S7-1200 can perform as both a slave of a higher-level DP master system and a master of a lower-level DP slave system, simultaneously:



You can configure a maximum of three PROFIBUS CMs per station, in which there can be any combination of DP master or DP slave CMs. DP masters can each control a maximum of 32 slaves.

The configuration data of the PROFIBUS CMs is stored on the local CPU. This allows simple replacement of these communications modules when necessary.

To use PROFIBUS, the PROFIBUS Master CM firmware must be at least V1.3.

NOTE

Always update the PROFIBUS CM firmware to the latest version available (http://support.automation.siemens.com/WW/view/en/42131407). You can perform a firmware update by any of these methods:

- Using the online and diagnostic tools of STEP 7 (Page 1055)
- Using a SIMATIC memory card (Page 117)
- Using the Web server "Module Information" standard Web page (Page 777)
- Using the SIMATIC Automation Tool (https://support.industry.siemens.com/cs/ww/en/view/98161300)

12.7.1 Communications services of the PROFIBUS CMs

The PROFIBUS CMs use the PROFIBUS DP-V1 protocol.

Types of communication with DP-V1

The following types of communication are available with DP-V1:

- Cyclic communication (CM 1242-5 and CM 1243-5)
  Both PROFIBUS modules support cyclic communication for the transfer of process data between DP slave and DP master.
  Cyclic communication is handled by the operating system of the CPU. No software blocks are required for this. The I/O data is read or written directly from/to the process image of the CPU.
- Acyclic communication (CM 1243-5 only)
  The DP master module also supports acyclic communication using software blocks:
  - The "RALRM" instruction is available for interrupt handling.
  - The "RDREC" and "WRREC" instructions are available for transferring configuration and diagnostics data.

Functions not supported by the CM 1243-5: SYNC/FREEZE and Get_Master_Diag

Other communications services of the CM 1243-5

The CM 1243-5 DP master module supports the following additional communications services:

- S7 communication
  - PUT/GET services
    The DP master functions as a client and server for queries from other S7 controllers or PCs via PROFIBUS.
  - PG/OP communication
    The PG functions allow the downloading of configuration data and user programs from a PG and the transfer of diagnostics data to a PG.
    Possible communications partners for OP communication are HMI panels, SIMATIC panel PCs with WinCC flexible or SCADA systems that support S7 communication.

12.7.2 Reference to the PROFIBUS CM user manuals

Further information

You can find detailed information on the PROFIBUS CMs in the manuals for the devices. You can find these on the Internet in the pages of Siemens Industrial Automation Customer Support under the following entry IDs:

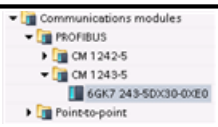
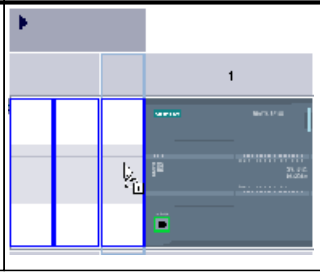
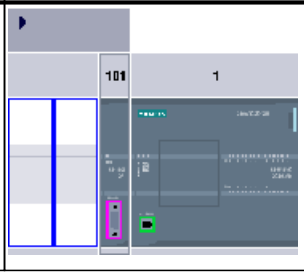
- CM 1242-5 (hhttps://support.industry.siemens.com/cs/ww/en/view/61029535)
- CM 1243-5 (https://support.industry.siemens.com/cs/ww/en/view/49851842)

12.7.3 Configuring a DP master and slave device

12.7.3.1 Adding the CM 1243-5 (DP master) module and a DP slave

In the "Devices and networks" portal, use the hardware catalog to add PROFIBUS modules to the CPU. These modules are connected to the left side of the CPU. To insert a module into the hardware configuration, select the module in the hardware catalog and either double-click or drag the module to the highlighted slot.

Table 12-60 Adding a PROFIBUS CM 1243-5 (DP master) module to the device configuration

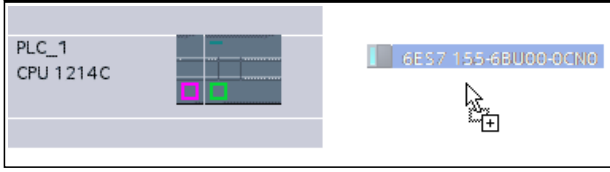
Module	Select the module	Insert the module	Result
CM 1243-5 (DP master)			

Use the hardware catalog to add DP slaves as well. For example, to add an ET 200SP DP slave, in the Hardware Catalog, expand the following containers:

- Distributed I/O
- ET 200SP
- Interface modules
- PROFIBUS

Next, select "6ES7 155-6BU00-0CN0" (IM155-6 DP HF) from the list of part numbers, and add the ET 200SP DP slave as shown in the figure below.

Table 12-61 Adding an ET 200SP DP slave to the device configuration

Insert the DP slave	Result
	

12.7.3.2 Configuring logical network connections between two PROFIBUS devices

After you configure the CM 1243-5 (DP master) module, you are now ready to configure your network connections.

In the Devices and Networks portal, use the "Network view" to create the network connections between the devices in your project. To create the PROFIBUS connection, select the purple (PROFIBUS) box on the first device. Drag a line to the PROFIBUS box on the second device. Release the mouse button and your PROFIBUS connection is joined.

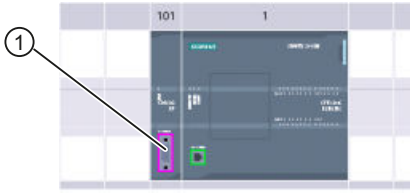
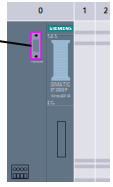
Refer to "Device Configuration: Creating a network connection" (Page 531) for more information.

12.7.3.3 Assigning PROFIBUS addresses to the CM 1243-5 module and DP slave

Configuring the PROFIBUS interface

After you configure logical network connections between two PROFIBUS devices, you can configure parameters for the PROFIBUS interfaces. To do so, click the purple PROFIBUS box on the CM 1243-5 module, and the "Properties" tab in the inspector window displays the PROFIBUS interface. The DP slave PROFIBUS interface is configured in the same manner.

Table 12-62 Configuring the CM 1243-5 (DP master) module and ET 200SP DP slave PROFIBUS interfaces

CM 1243-5 (DP master) module	ET 200SP DP slave
	

① PROFIBUS port

Assigning the PROFIBUS address

In a PROFIBUS network, each device is assigned a PROFIBUS address. This address can range from 0 through 127, with the following exceptions:

- Address 0: Reserved for network configuration and/or programming tools attached to the bus
- Address 1: Reserved by Siemens for the first master
- Address 126: Reserved for devices from the factory that do not have a switch setting and must be re-addressed through the network
- Address 127: Reserved for broadcast messages to all devices on the network and may not be assigned to operational devices

Thus, the addresses that may be used for PROFIBUS operational devices are 2 through 125.

In the Properties window, select the "PROFIBUS address" configuration entry. STEP 7 displays the PROFIBUS address configuration dialog, which is used to assign the PROFIBUS address of the device.

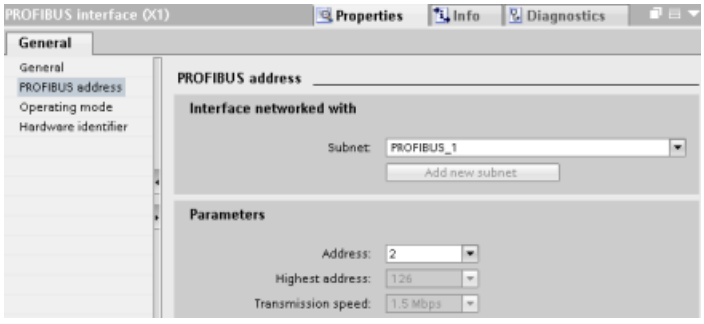


Table 12-63 Parameters for the PROFIBUS address

Parameter		Description
Subnet	Name of the Subnet to which the device is connected. Click the "Add new subnet" button to create a new subnet. "Not connected" is the default. Two connection types are possible: • The "Not connected" default provides a local connection. • A subnet is required when your network has two or more devices.	
Parameters	Address	Assigned PROFIBUS address for the device
	Highest address	The highest PROFIBUS address is based on the active stations on the PROFIBUS (for example, DP master). Passive DP slaves independently have PROFIBUS addresses from 1 to 125 even if the highest PROFIBUS address is set to 15, for example. The highest PROFIBUS address is relevant for token forwarding (forwarding of the send rights), and the token is only forwarded to active stations. Specifying the highest PROFIBUS address optimizes the bus.
	Transmission rate	Transmission rate of the configured PROFIBUS network: The PROFIBUS transmission rates range from 9.6 Kbits/sec to 12 Mbits/sec. The transmission rate setting depends on the properties of the PROFIBUS nodes being used. The transmission rate should not be greater than the rate supported by the slowest node. The transmission rate is normally set for the master on the PROFIBUS network, with all DP slaves automatically using that same transmission rate (auto-baud).

12.7.4 Distributed I/O and diagnostic instructions

Refer to Distributed I/O (PROFINET, PROFIBUS, or AS-i) (Page 330) for information on Distributed I/O and Diagnostics instructions.

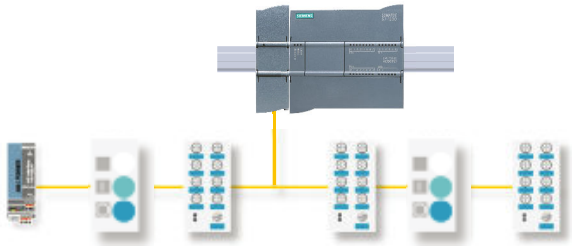
Refer to Diagnostic events for distributed I/O (Page 718) for handling diagnostic events.

12.8 AS-i

The S7-1200 AS-i master CM 1243-2 allows the attachment of an AS-i network to an S7-1200 CPU.

The actuator/sensor interface, or AS-i, is a single master network connection system for the lowest level in automation systems. The CM 1243-2 serves as the AS-i master for the network. Using a single AS-i cable, sensors and actuators (AS-i slave devices) can be connected to the CPU through the CM 1243-2. The CM 1243-2 handles all AS-i network coordination and relays data and status information from the actuators and sensors to the CPU through the I/O addresses assigned to the CM 1243-2. You can access binary or analog values depending on the slave type. The AS-i slaves are the input and output channels of the AS-i system and are only active when called by the CM 1243-2.

In the figure below, the S7-1200 is an AS-i master controlling AS-i I/O module digital/analog slave devices.



To use AS-i with S7-1200 V4.0 CPUs, you must upgrade the AS-i Master CM firmware to V1.1. You can make this upgrade using the webserver or a SIMATIC memory card.

NOTE

For V4.0 S7-1200 CPUs, if using the web server or a SIMATIC memory card to upgrade from V1.0 to V1.1 AS-i firmware, you must update the AS-i firmware in the AS-i Master CM 1243-2 according to the following procedure:

1. Download the firmware upgrade to the AS-i Master CM 1243-2.
2. When the download is complete, power cycle the S7-1200 CPU to complete the firmware upgrade process in the AS-i Master CM 1243-2.
3. Repeat steps 1 and 2 for each additional AS-i Master CM 1243-2. The S7-1200 PLC allows a maximum of three AS-i Master CM 1243-2.

NOTE

It is recommended that you always update the AS-i CM firmware to the latest version available (http://support.automation.siemens.com/WW/view/en/43416171)at the Siemens Service and Support Web site.

12.8.1 Configuring an AS-i master and slave device

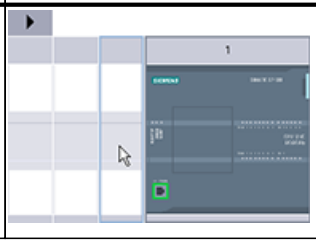
The AS-i master CM 1243-2 is integrated into the S7-1200 automation system as a communication module.

You can find detailed information on the AS-i master CM 1243-2 in the "AS-i master CM 1243-2 and AS-i data decoupling unit DCM 1271 for SIMATIC S7-1200" Manual (https://support.industry.siemens.com/cs/ww/en/ps/15750/man).

12.8.1.1 Adding the AS-i master CM 1243-2 and AS-i slave

Use the hardware catalog to add AS-i master CM1243-2 modules to the CPU. These modules are connected to the left side of the CPU, and a maximum of three AS-i master CM1243-2 modules can be used. To insert a module into the hardware configuration, select the module in the hardware catalog and either double-click or drag the module to the highlighted slot.

Table 12-64 Adding an AS-i master CM1243-2 module to the device configuration

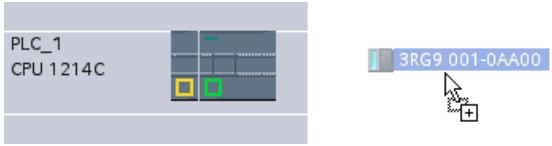
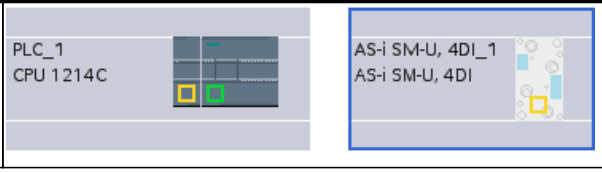
Module	Select the module	Insert the module	Result
CM 1243-2 AS-i Master			

Use the hardware catalog to add AS-i slaves as well. For example, to add an "I/O module, compact, digital, input" slave, in the Hardware Catalog, un-check Filter (if checked) and expand the following containers:

Field devices > AS-Interface > Input/Output modules IP6x, compact modules > Digital > Input > User modules > AS-i SM-U, 4DI

Next, select "3RG9 001-0AA00" from the list of part numbers, and add the "I/O module, compact, digital, input" slave as shown in the figure below.

Table 12-65 Adding an AS-i slave to the device configuration

Insert the AS-i slave	Result
	

12.8.1.2 Configuring logical network connections between two AS-i devices

After you configure the AS-i master CM1243-2, you are now ready to configure your network connections.

In the Devices and Networks portal, use the "Network view" to create the network connections between the devices in your project. To create the AS-i connection, select the yellow (AS-i) box on the first device. Drag a line to the AS-i box on the second device. Release the mouse button and your AS-i connection is joined.

Refer to "Device Configuration: Creating a network connection" (Page 531) for more information.

12.8.1.3 Configuring the properties of the AS-i master CM1243-2

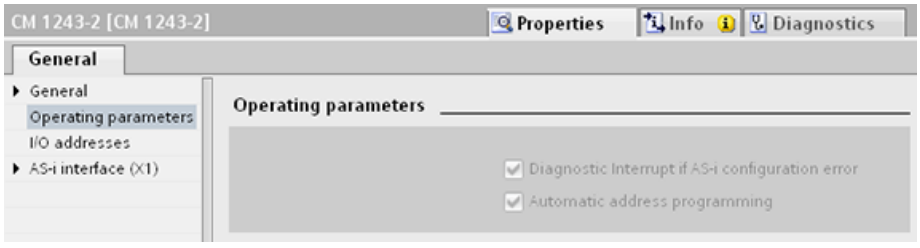
To configure parameters for the AS-i interface, click the yellow AS-i box on the AS-i master CM1243-2 module, and the "Properties" tab in the inspector window displays the AS-i interface.
In the STEP 7 inspector window, you can view, configure, and change general information, addresses and operating parameters:

Table 12-66 AS-i master CM1243-2 module properties

Property	Description
General	Name of the AS-i master CM 1243-2
Operating parameters	Parameters for the response of the AS-i master
I/O addresses	Address area for the slave I/O addresses
AS-i interface (X1)	Assigned AS-i network

NOTE

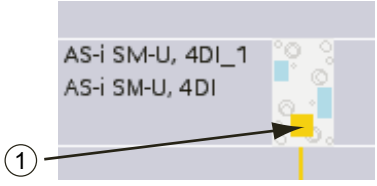
"Diagnostic interrupt for faults in the AS-i configuration" and "Automatic address programming" are always active and are therefore shown in gray.



12.8.1.4 Assigning an AS-i address to an AS-i slave

Configuring the AS-i slave interface

To configure parameters for the AS-i interface, click the yellow AS-i box on the AS-i slave, and the "Properties" tab in the inspector window displays the AS-i interface.



① AS-i port

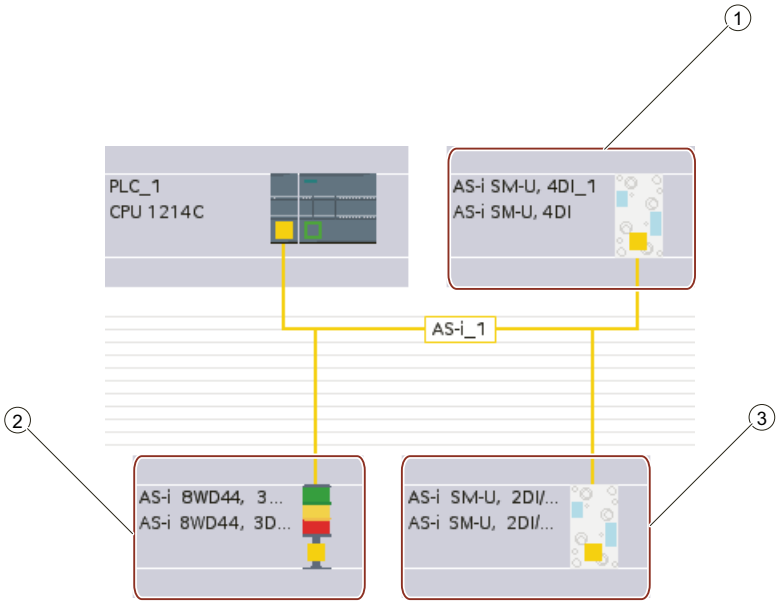
Assigning the AS-i slave address

In an AS-i network, each device is assigned an AS-i slave address. This address can range from 0 through 31; however, address 0 is reserved only for new slave devices. The slave addresses are 1(A or B) to 31(A or B) for a total of up to 62 slave devices.

"Standard" AS-i devices use the entire address, having a number address without the A or B designation. "A/B node" AS-i devices use the A or B portion of each address, enabling each of the 31 addresses to be used twice. The address space range is 1A to 31A plus 1B to 31B.

Any address in the range of 1 - 31 can be assigned to an AS-i slave device; in other words, it does not matter whether the slaves begin with address 21 or whether the first slave is actually given the address 1.

In the example below, three AS-i devices have been addressed as "1" (a standard type device), "2A" (an A/B node type device), and "3" (a standard type device):

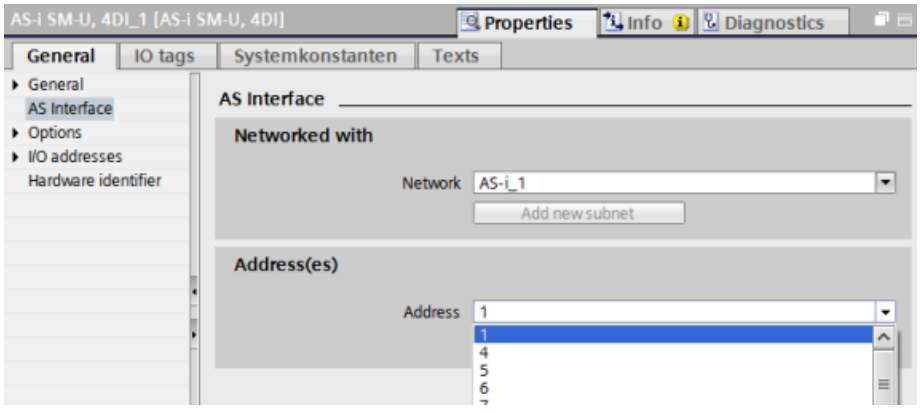


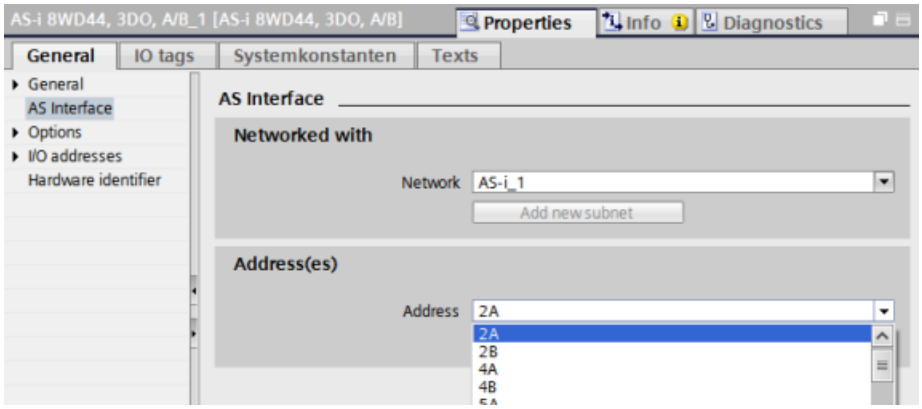
① AS-i slave address 1; Device: AS-i SM-U, 4DI; article number: 3RG9 001-0AA00

② AS-i slave address 2A; Device: AS-i 8WD44, 3DO, A/B; article number: 8WD4 428-0BD

③ AS-i slave address 3; Device: AS-i SM-U, 2DI/2DO; article number: 3RG9 001-0AC00

Enter the AS-i slave address here:





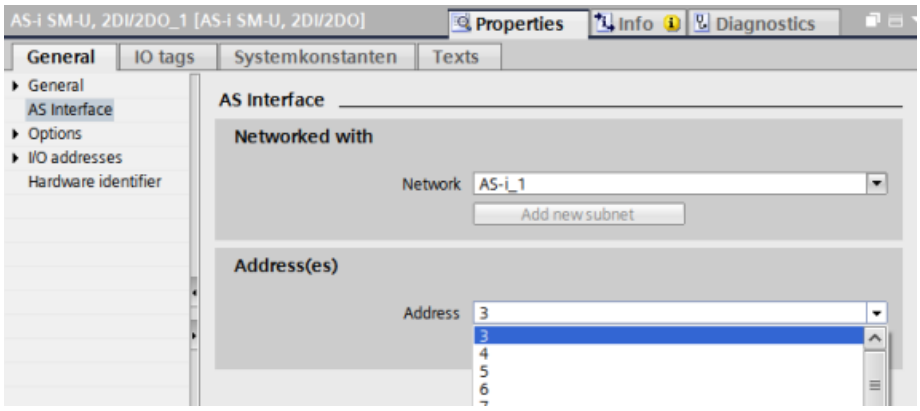


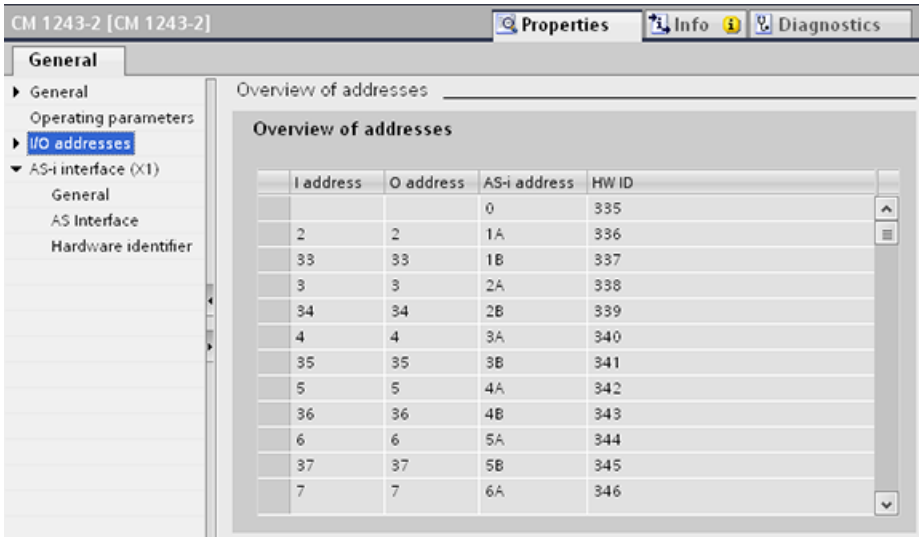
Table 12-67 Parameters for the AS-i interface

Parameter	Description
Network	Name of the network to which the device is connected
Address(es)	Assigned AS-i address for the slave device in range of 1(A or B) to 31(A or B) for a total of up to 62 slave devices

12.8.2 Exchanging data between the user program and AS-i slaves

12.8.2.1 STEP 7 configuration

The AS-i master reserves a 62-byte data area in the I/O area of the CPU. Access to the digital data is performed here in bytes; for each slave, there is one byte of input and one byte of output data.
The assignment of the AS-i connections of the AS-i digital slaves to the data bits of the assigned byte is indicated in the inspection window of the AS-i master CM 1243-2.



I address	O address	AS-i address	HW ID
		0	335
2	2	1A	336
33	33	1B	337
3	3	2A	338
34	34	2B	339
4	4	3A	340
35	35	3B	341
5	5	4A	342
36	36	4B	343
6	6	5A	344
37	37	5B	345
7	7	6A	346

You can access the data of the AS-i slaves in the user program by using the displayed I/O addresses with the appropriate bit logic operations (for example, "AND") or bit assignments.

NOTE

"System assignment" is automatically activated if you do not configure the AS-i slaves with STEP 7.

If you do not configure any slaves, you must inform the AS-i master CM1243-2 about the actual bus configuration using the online function "ACTUAL > EXPECTED".

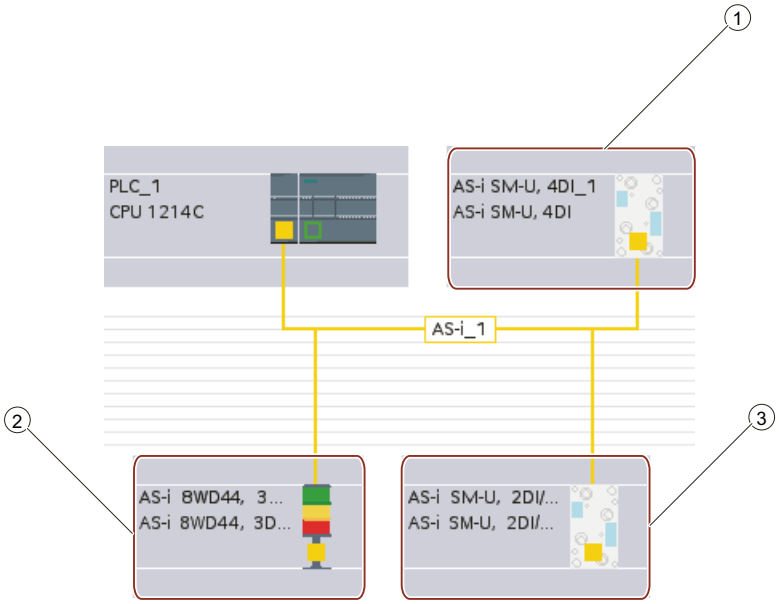
Further information

You can find detailed information on the AS-i master CM 1243-2 in the "AS-i master CM 1243-2 and AS-i data decoupling unit DCM 1271 for SIMATIC S7-1200" Manual (https://support.industry.siemens.com/cs/ww/en/ps/15750/man).

12.8.2.2 Configuring AS-i slaves with STEP 7

Transferring AS-i digital values

The CPU accesses the digital inputs and outputs of the AS-i slaves through the AS-i master CM1243-2 in cyclic operation. The data is accessed through I/O addresses or by means of a data record transfer.



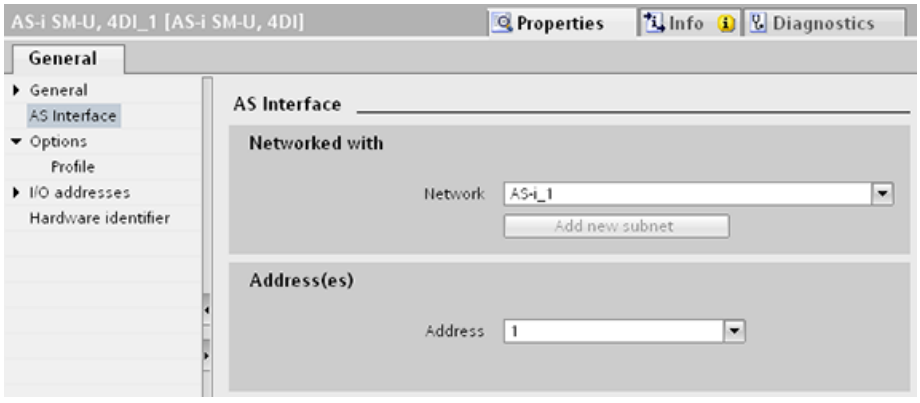
① AS-i slave address 1

② AS-i slave address 2A

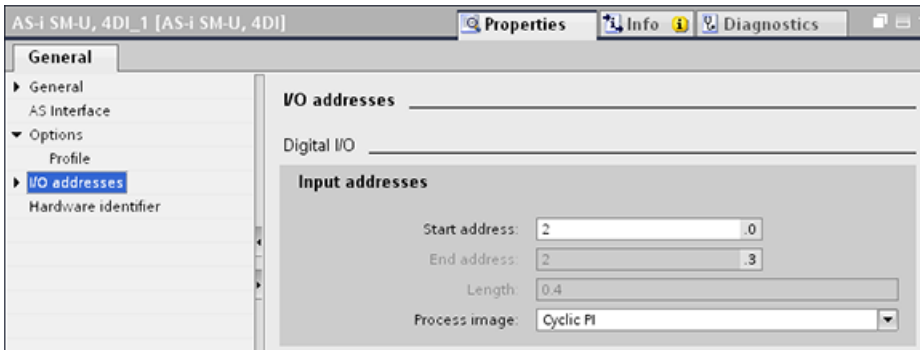
③ AS-i slave address 3

Access to the digital data is performed here in bytes (in other words, one byte is assigned to each AS-i digital slave). When you configure the AS-i slaves in STEP 7, the I/O address for accessing the data from the user program is displayed in the inspection window for the respective AS-i slave.

The digital input module (AS-i SM-U, 4DI) in the AS-i network above has been assigned slave address 1. By clicking on the digital input module, the "AS interface" tab in the device "Properties" displays the slave address, as shown below:

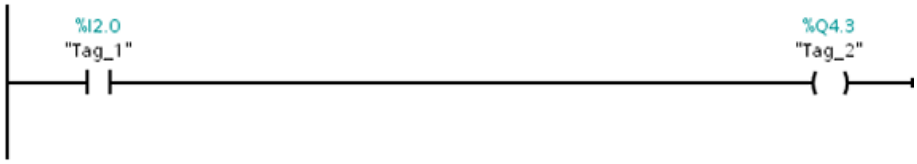


The digital input module (AS-i SM-U, 4DI) in the AS-i network above has been assigned I/O address 2. By clicking on the digital input module, the "I/O addresses" tab in the device "Properties" displays the I/O address, as shown below:



You can access the data of the AS-i slaves in the user program by using their I/O addresses with the appropriate bit logic operations (for example, "AND") or bit assignments. The following simple program illustrates how the assignment works:

Input 2.0 is polled in this program. In the AS-i system, this input belongs to slave1 (Input byte 2, bit 0). Output 4.3, which is then set, corresponds to AS-i slave 3 (Output byte 4, bit 3)



Transferring AS-i analog values

You can access analog data of an AS-i slave through the process image of the CPU if you have configured this AS-i slave in STEP 7 as an analog slave.

If you did not configure the analog slave in STEP 7, you can only access the data of the AS-i slave through the acyclic functions (data record interface). In the user program of the CPU, AS-i calls are read and written using the RDREC (read data record) and WRREC (write data record) distributed I/O instructions.

NOTE

A configuration of the AS-i slaves specified through STEP 7 and downloaded into the S7 station is transferred by the CPU on the AS-i master CM1243-2 during S7 station start-up. Any existing configuration that was determined through the "System assignment" online function (Page 702) ("ACTUAL -> EXPECTED") will be overwritten.

Further information

You can find detailed information on the AS-i master CM 1243-2 in the "AS-i master CM 1243-2 and AS-i data decoupling unit DCM 1271 for SIMATIC S7-1200" Manual (http://support.automation.siemens.com/WW/view/en/50414115/133300).

12.8.3 Distributed I/O instructions

Refer to Distributed I/O (PROFINET, PROFIBUS, or AS-i) (Page 330) for information on Distributed I/O and Diagnostics instructions.

Refer to DPNRM_DG (Read diagnostic data from a PROFIBUS DP slave) (Page 355) for handling diagnostic events.

12.8.4 Working with AS-i online tools

You must go online in STEP 7 to view and change the AS-i operational modes.

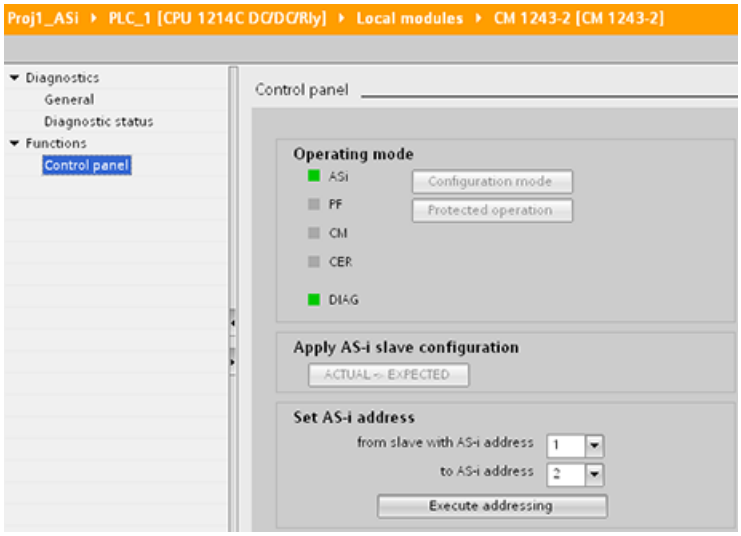
To change the AS-i operational modes, follow these steps:

1. Select the AS-i master CM1243-2 module from the device configuration of your PLC.
2. Click the "Go online" button in the toolbar.
3. Select the "Online and diagnostics" command from the "Online" menu or from the project tree.

Under "Operating mode" for the Control panel, you see two modes:

- Configuration mode:
  - You can make required changes in your AS-i slave device and CPU I/O addresses.
  - The green "CM" LED is ON.
- Protected operation:
  - You cannot change AS-i slave device and CPU I/O addresses.
  - The green "CM" LED is OFF.

If your mode is configuration mode, you can set the AS-i slave address. A new slave that has not been assigned an address always has address 0. The master detects it as a new slave without an address assignment. It is not included in normal communication until assigned an address.



Configuration error

When the yellow "CER" LED is ON, there is an error in the AS-i slave device configuration. Select the "ACTUAL > EXPECTED" button to overwrite the AS-i master CM1243-2 module slave device configuration with the AS-i field network slave device configuration.

12.9 S7 communication

12.9.1 GET and PUT (Read and write from a remote CPU)

You can use the GET and PUT instructions to communicate with S7 CPUs through PROFINET and PROFIBUS connections. This is only possible if the "Permit access with PUT/GET communication from remote partner" function is activated for the partner CPU in the "Protection & Security" property of the local CPU properties:

- Accessing data in a remote CPU: An S7-1200 CPU can only use absolute addresses in the ADDR_x input field to address variables of remote CPUs (S7-200/300/400/1200).
- Accessing data in a standard DB: An S7-1200 CPU can only use absolute addresses in the ADDR_x input field to address DB variables in a standard DB of a remote S7 CPU.
- Accessing data in an optimized DB: An S7-1200 CPU cannot access DB variables in an optimized DB of a remote S7-1200 CPU.
- Accessing data in a local CPU: An S7-1200 CPU can use either absolute or symbolic addresses as inputs to the RD_x or SD_x input fields of the GET or PUT instruction, respectively.

NOTE

GET/PUT operation is not automatically enabled for V4.x

To enable GET/PUT access, follow these steps:

1. Enable the Anonymous user under "Security settings" > "Users and roles".
2. Assign any access level to the Anonymous user.
3. In the CPU's "Device configuration" inspector window, select the "Properties" tab > "Protection & Security" and click the check box to "Permit access to the PUT/GET communication from remote partner".

WARNING

Avoiding security risks from physical network attacks

If an attacker can physically access your networks, the attacker can possibly read and write data.

For example, I/O exchange through PROFIBUS, PROFINET, AS-i, or other I/O bus, GET/PUT, T-Block, and communication modules (CMs) have no security features. You must protect these forms of communication by limiting physical access. If an attacker can physically access your networks using these forms of communication, the attacker can possibly read and write data.

If you fail to protect these forms of communication, death or severe personal injury can result.

For security information and recommendations, see the "Operational Guidelines" white paper on the Siemens Industrial Cybersecurity Web site (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

Table 12-68 GET and PUT instructions

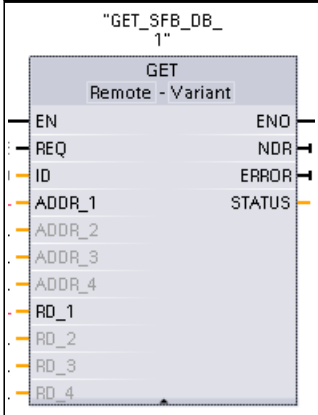
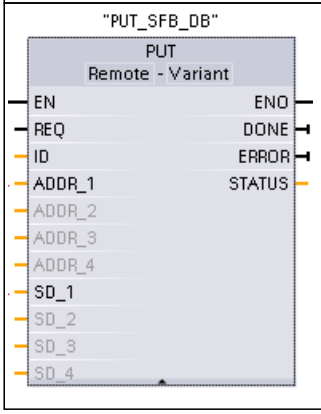
LAD / FBD	SCL	Description
	**"GET_DB"(req:=_bool_in_, ID:=_word_in_, ndr=>_bool_out_, error=>_bool_out_, status=>_word_out_, addr_1:=_remote_inout_, [...addr_4:=_remote_inout_,] rd_1:=_variant_inout_ [,...rd_4:=_variant_inout_]);**	Use the GET instruction to read data from a remote S7 CPU. The remote CPU can be in either RUN or STOP mode. STEP 7 automatically creates the DB when you insert the instruction.
	**"PUT_DB"(req:=_bool_in_, ID:=_word_in_, done=>_bool_out_, error=>_bool_out_, status=>_word_out_, addr_1:=_remote_inout_, [...addr_4:=_remote_inout_,] sd_1:=_variant_inout_, [....sd_4:=_variant_inout_]);**	Use the PUT instruction to write data to a remote S7 CPU. The remote CPU can be in either RUN or STOP mode. STEP 7 automatically creates the DB when you insert the instruction.

Table 12-69 Data types for the parameters

Parameter and type		Data type	Description
REQ	Input	Bool	A low to high (positive edge) signal starts the operation.
ID	Input	CONN_PRG (Word)	S7 connection ID (Hex)
NDR (GET)	Output	Bool	New Data Ready: • 0: request has not yet started or is still running • 1: task was completed successfully
DONE (PUT)	Output	Bool	DONE: • 0: request has not yet started or is still running • 1: task was completed successfully
ERROR STATUS	Output Output	Bool Word	• ERROR=0 STATUS value: – 0000H: neither warning nor error – <> 0000H: Warning, STATUS supplies detailed information • ERROR=1 There is an error. STATUS supplies detailed information about the nature of the error.
ADDR_1	InOut	Remote	Pointer to the memory areas in the remote CPU that stores the data to be read (GET) or that is sent (PUT).
ADDR_2	InOut	Remote	
ADDR_3	InOut	Remote	

Parameter and type		Data type	Description
ADDR_4	InOut	Remote	Pointer to the memory areas in the remote CPU that stores the data to be read (GET) or that is sent (PUT).
RD_1 (GET) SD_1 (PUT)	InOut	Variant	Pointer to the memory areas in the local CPU that stores the data to be read (GET) or sent (PUT). Data types allowed: Bool (only a single bit allowed), Byte, Char, Word, Int, DWord, DInt, or Real. Note: If the pointer accesses a DB, you must specify the absolute address, such as: P# DB10.DBX5.0 Byte 10 In this case, 10 represents the number of bytes to GET or PUT.
RD_2 (GET) SD_2 (PUT)	InOut	Variant	
RD_3 (GET) SD_3 (PUT)	InOut	Variant	
RD_4 (GET) SD_4 (PUT)	InOut	Variant	

You must ensure that the length (number of bytes) and data types for the ADDR_x (remote CPU) and RD_x or SD_x (local CPU) parameters match. The number after the identifier "Byte" is the number of bytes referenced by the ADDR_x, RD_x, or SD_x parameter.

NOTE

The total number of bytes received on a GET instruction or the total number of bytes sent on a PUT instruction is limited. The limitations are based on how many of the four possible address and memory areas you use:

- If you use only ADDR_1 and RD_1/SD_1, a GET instruction can get 222 bytes and a PUT instruction can send 212 bytes.
- If you use ADDR_1, RD_1/SD_1, ADDR_2, and RD_2/SD_2, a GET instruction can get a total of 218 bytes and a PUT instruction can send a total of 196 bytes.
- If you use ADDR_1, RD_1/SD_1, ADDR_2, RD_2/SD_2, ADDR_3, and RD_3/SD_3 a GET instruction can get a total of 214 bytes and a PUT instruction can send a total of 180 bytes.
- If you use ADDR_1, RD_1/SD_1, ADDR_2, RD_2/SD_2, ADDR_3, RD_3/SD_3, ADDR_4, RD_4/SD_4 a GET instruction can get a total of 210 bytes and a PUT instruction can send a total of 164 bytes.

The sum of the number of bytes of each of your address and memory area parameters must be less than or equal to the defined limits. If you exceed these limits, the GET or PUT instruction returns an error.

On the rising edge of the REQ parameter, the read operation (GET) or write operation (PUT) loads the ID, ADDR_1, and RD_1 (GET) or SD_1 (PUT) parameters.

- For GET: The remote CPU returns the requested data to the receive areas (RD_x), starting with the next scan. When the read operation has completed without error, the NDR parameter is set to 1. A new operation can only be started after the previous operation has completed.
- For PUT: The local CPU starts sending the data (SD_x) to the memory location (ADDR_x) in the remote CPU. When the write operation has completed without error, the remote CPU returns an execution acknowledgement. The DONE parameter of the PUT instruction is then set to 1. A new write operation can only be started after the previous operation has completed.

NOTE

To ensure data consistency, always evaluate when the operation has been completed (NDR = 1 for GET, or DONE = 1 for PUT) before accessing the data or initiating another read or write operation.

The ERROR and STATUS parameters provide information about the status of the read (GET) or write (PUT) operation.

Table 12-70 Error information

ERROR	STATUS (decimal)	Description
0	11	• New job cannot take effect since previous job is not yet completed. • The job is now being processed in a priority class having lower priority.
0	25	Communication has started. The job is being processed.
1	1	Communications problems, such as: • Connection description not loaded (local or remote) • Connection interrupted (for example: cable, CPU is turned off, or CM/CB/CP is in STOP mode) • Connection to partner not yet established
1	2	Negative acknowledgement from the partner device. The task cannot be executed.
1	4	Errors in the send area pointers (RD_x for GET, or SD_x for PUT) involving the data length or the data type.
1	8	Access error on the partner CPU
1	10	Access to the local user memory not possible (for example, attempting to access a deleted DB)
1	12	When the SFB was called: • An instance DB was specified that does not belong to GET or PUT • No instance DB was specified, but rather a shared DB • No instance DB found (loading a new instance DB)
1	20	• Exceeded the maximum number of parallel jobs/instances • The instances were overloaded at CPU-RUN This status is possible for first execution of the GET or PUT instruction
1	27	There is no corresponding GET or PUT instruction in the CPU.

12.9.2 Creating an S7 connection

Connection mechanisms

To access remote connection partners with PUT/GET instructions, the user must also have permission.

By default, the "Permit access with PUT/GET communication from remote partner" option is not enabled. In this case, read and write access to CPU data is only possible for communication connections that require configuration or programming both for the local CPU and for the communication partner. Access through BSEND/BRCV instructions is possible, for example.

If the local CPU is used only as a server, the CPU cannot program or configure communication with the communication partner. The following connections are therefore not possible during the operation of the CPU:

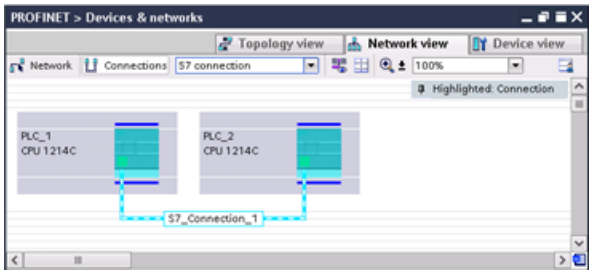
- PUT/GET, FETCH/WRITE or FTP access through communication modules
- PUT/GET access from other S7 CPUs
- HMI access through PUT/GET communication

If you want to allow access to CPU data from the client side, that is, you do not want to restrict the communication services of the CPU, you can configure the access protection for the S7-1200 CPU (Page 151) for this level of security.

Connection types

The connection type that you select creates a communication connection to a partner station. The connection is set up, established, and automatically monitored.

In the Devices and Networks portal, use the "Network view" to create the network connections (Page 531) between the devices in your project. First, click the "Connections" tab, and then select the connection type with the dropdown, just to the right (for example, an S7 connection). Click the green (PROFINET) box on the first device, and drag a line to the PROFINET box on the second device. Release the mouse button and your PROFINET connection is joined.



Click the "Highlighted: Connection" button to access the "Properties" configuration dialog of the communication instruction.

12.9.3 Configuring the Local/Partner connection path between two devices

Configuring General parameters

You specify the communication parameters in the "Properties" configuration dialog of the communication instruction. This dialog appears near the bottom of the page whenever you have selected any part of the instruction.

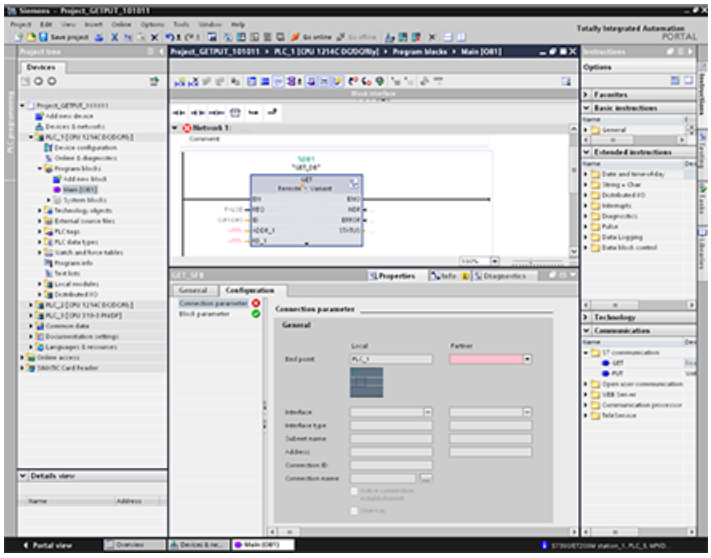
Refer to "Device configuration: Configuring the Local/Partner connection path (Page 532)" for more information.

In the "Address Details" section of the Connection parameters dialog, you define the TSAPs or ports to be used. The TSAP or port of a connection in the CPU is entered in the "Local TSAP" field. The TSAP or port assigned for the connection in your partner CPU is entered under the "Partner TSAP" field.

12.9.4 GET/PUT connection parameter assignment

The GET/PUT instructions connection parameter assignment is a user aid for configuring CPU-to-CPU S7 communication connections.

After inserting a GET or PUT block, STEP 7 displays the connection parameter assignment dialog for the GET/PUT instructions:



The inspector window displays the properties of the connection whenever you have selected any part of the instruction. You can configure the communication parameters in the "Configuration" tab of the "Properties" for the communication instruction.

NOTE

GET/PUT operation is not automatically enabled for V4.x

To enable GET/PUT access (Page 151), go to the CPU "Device configuration", inspector window "Properties" tab, "Protection & Security" property.

12.9.4.1 Connection parameters

The "Connection parameters" page allows you to configure the necessary S7 connection and to configure the parameter "Connection ID" that is referenced by the GET/PUT block parameter "ID". The page's content has information about the local endpoint and allows you to define the local interface. You can also define the partner end point.

The "Block parameters" page allows you to configure the additional block parameters.

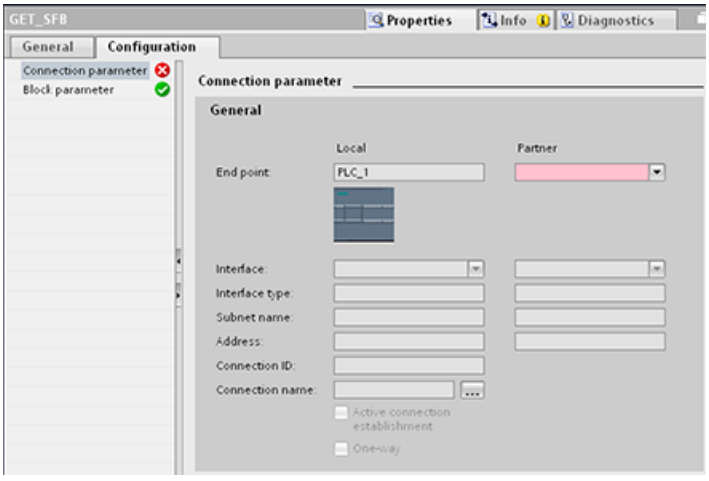


Table 12-71 Connection parameter: General definitions

Parameter		Definition
Connection parameter: General	End point	"Local End point": Name assigned to the Local CPU "Partner End point": Name assigned to the Partner (remote) CPU Note: In the "Partner End point" dropdown list, the system displays all potential S7 connection partners of the current project as well as the option "unspecified". An unspecified partner represents a communication partner which is not currently in the STEP 7 project (for example, a third party device communication partner).
	Interface	Name assigned to the interfaces Note: You can change the connection by changing the Local and Partner interfaces
	Interface type	Type of interface
	Subnet name	Name assigned to the subnets
	Address	Assigned IP addresses Note: You can specify the remote address of a third party device for an "unspecified" communication partner.
	Connection ID	ID number: Automatically generated by the GET/PUT connection parameter assignment
	Connection name	Local and Partner CPU data storage location: Automatically generated by the GET/PUT connection parameter assignment
	Active connection establishment	Checkbox to select Local CPU as the active connection
	One-way	Checkbox to specify a one-way or two-way connection; read-only Note: In a PROFINET GET/PUT connection, both the local and partner devices can act as a server or a client. This allows a two-way connection, and the "One-way" checkbox is unchecked. In a PROFIBUS GET/PUT connection, in some cases, the Partner device can only act as a server (for example, an S7-300), and the "One-way" checkbox is checked.

Connection ID parameter

There are three ways to change the system-defined connection IDs:

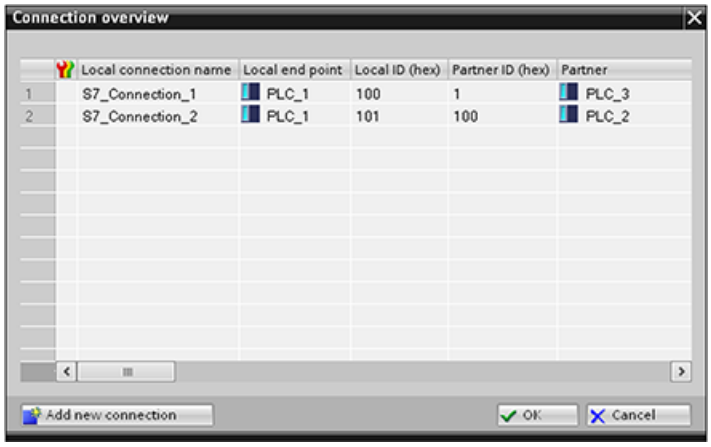
1. The user can change the current ID directly on the GET/PUT block. If the new ID belongs to an already existing connection, the connection is changed.
2. The user can change the current ID directly on the GET/PUT block, but the new ID does not already exist. A new S7 connection is created by the system.
3. The user can change the current ID through the "Connection overview" dialog: The user-input is synchronized with the ID-parameter on the corresponding GET/PUT block.

NOTE

The parameter "ID" of the GET/PUT block is not a connection name, but a numerical expression which is written like the following example: W#16#1

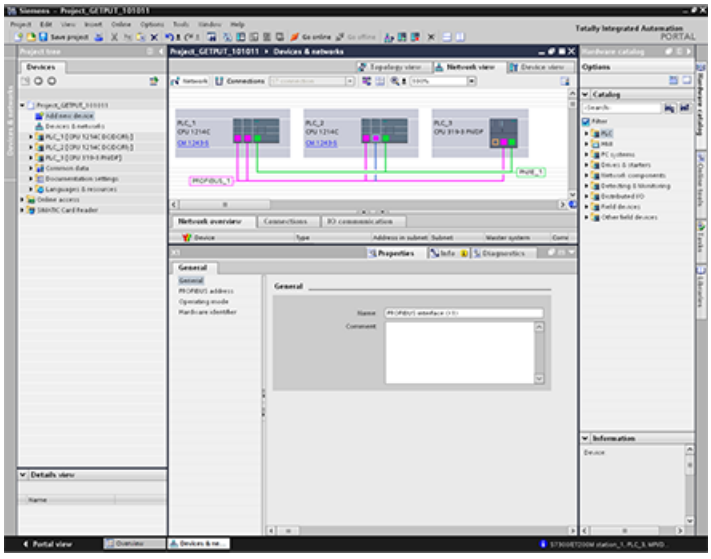
Connection name parameter

The connection name is editable through a special user control, the "Connection overview" dialog. This dialog offers all the available S7 connections which could be selected as an alternative for the current GET/PUT communication. The user can create a completely new connection in this table. Click the button to the right of the "Connection name" field to start the "Connection overview" dialog.



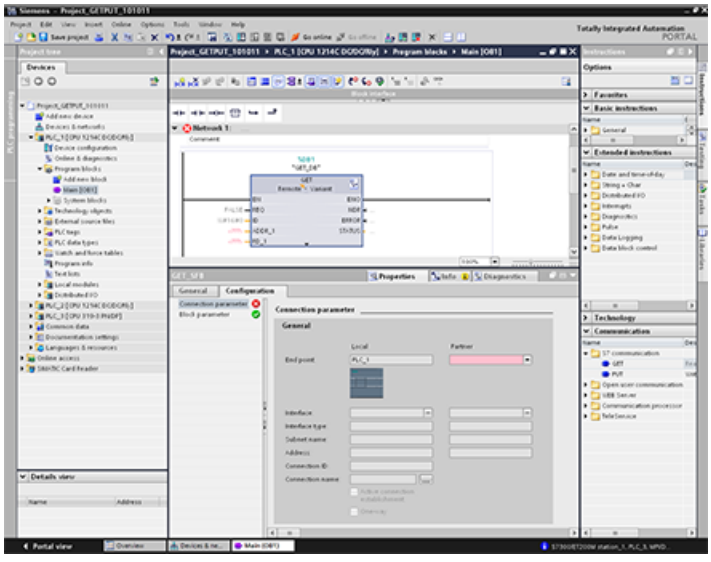
12.9.4.2 Configuring a CPU-to-CPU S7 connection

Given the configuration of PLC_1, PLC_2, and PLC_3 as shown in the figure below, insert GET or PUT blocks for "PLC_1".



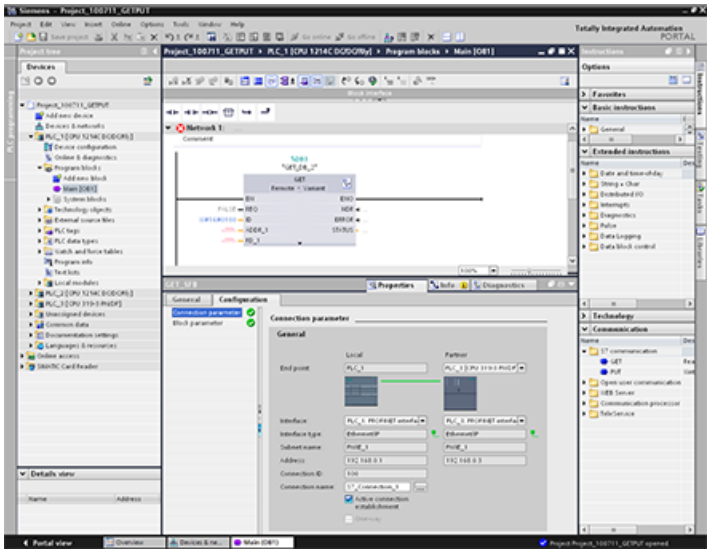
For the GET or PUT instruction, the "Properties" tab is automatically displayed in the inspector window with the following menu selections:

- Connection parameter
- Block parameter



Configuring a PROFINET S7 connection

For the "Partner End point", select "PLC_3".



The system reacts with the following changes:

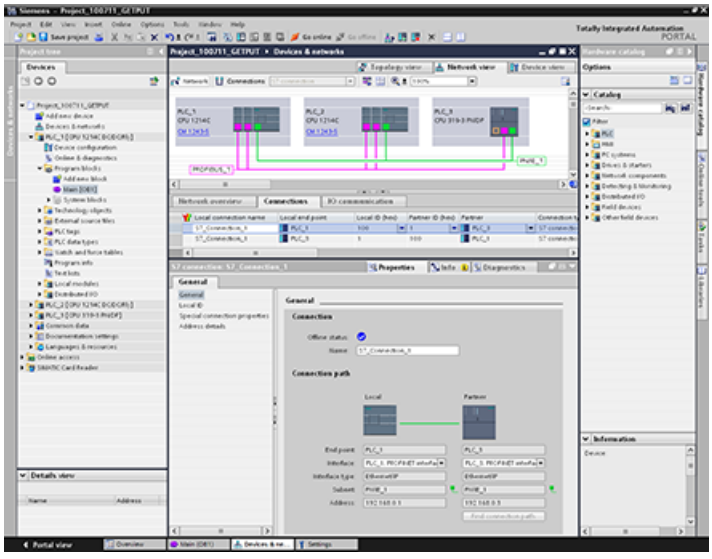
Table 12-72 Connection parameter: General values

Parameter		Definition
Connection parameter: General	End point	"Local End point" contains "PLC_1" as read-only. "Partner End point" field contains "PLC_3[CPU319-3PN/DP]": • The color switches from red to white • The "Partner" device image is shown. • A connection line appears between the PLC_1- and PLC_3 device images (green Ethernet line).
	Interface	"Local Interface" contains "CPU1214C DC/DC/DC, PROFINET interface (R0/S1)". "Partner Interface" contains: "CPU319-3PN/DP, PROFINET interface (R0/S2)".
	Interface type	"Local Interface type" contains "Ethernet/IP"; control is read-only. "Partner Interface type" contains "Ethernet/IP"; control is read-only. Interface type images are shown at the right beside the Local and Partner "Interface type" (green Ethernet icon).
	Subnet name	"Local Subnet name" contains "PN/IE_1"; control is read only. "Partner Subnet name" contains "PN/IE_1"; control is read only.
	Address	"Local Address" contains the Local IP address; control is read only. "Partner Address" contains the Partner IP address; control is read only.
	Connection ID	"Connection ID" contains "100". In the Program editor, in the Main [OB1], the GET/PUT block "Connection ID" value also contains "100".
	Connection name	"Connection name" contains the default connection name (for example, "S7_Connection_1"); control is enabled.
	Active connection estab-lishment	Checked and enabled to select the Local CPU as the active connection.
	One-way	Read-only and unchecked. Note: "PLC_1" (an S7-1200 CPU 1214CDC/DC/Relay) and "PLC_3" (an S7-300 CPU 319-3PN/DP) can both act as a server and a client in a PROFINET GET/PUT con-nection, allowing a two-way connection.

The GET/PUT icon in the Property View tree also changes from red to green.

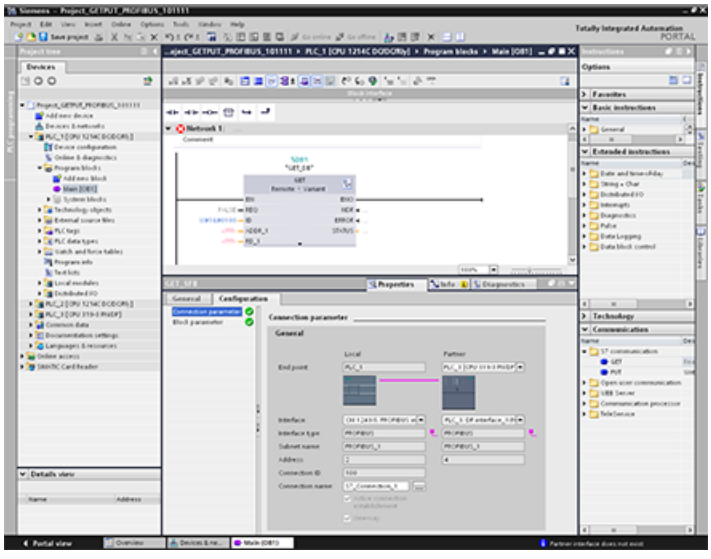
Completed PROFINET S7 connection

In the "Network view", a two-way S7 connection is shown in the "Connections" table between "PLC_1" and "PLC_3".



Configuring a PROFIBUS S7 connection

For the "Partner End point", select "PLC_3".



The system reacts with the following changes:

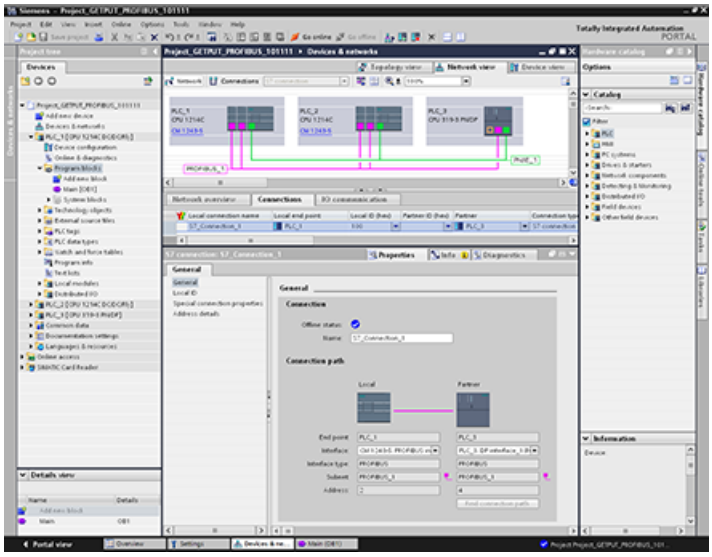
Table 12-73 Connection parameter: General values

Parameter		Definition
Connection parameter: General	End point	"Local End point" contains "PLC_1" as read-only. "Partner End point" field contains "PLC_3[CPU319-3PN/DP]": • The color switches from red to white • The "Partner" device image is shown. • A connection line appears between the PLC_1- and PLC_3 device images (purple PROFIBUS line).
	Interface	"Local Interface" contains "CPU1214C DC/DC/DC, PROFIBUS interface (R0/S1)". "Partner Interface" contains: "CPU319-3PN/DP, PROFIBUS interface (R0/S2)".
	Interface type	"Local Interface type" contains "PROFIBUS"; control is read-only. "Partner Interface type" contains " PROFIBUS "; control is read-only. Interface type images are shown at the right beside the Local and Partner "Interface type" (purple PROFIBUS icon).
	Subnet name	"Local Subnet name" contains " PROFIBUS _1"; control is read only. "Partner Subnet name" contains " PROFIBUS _1"; control is read only.
	Address	"Local Address" contains the Local IP address; control is read only. "Partner Address" contains the Partner IP address; control is read only.
	Connection ID	"Connection ID" contains "100". In the Program editor, in the Main [OB1], the GET/PUT block "Connection ID" value also contains "100".
	Connection name	"Connection name" contains the default connection name (for example, "S7_Connection_1"); control is enabled.
	Active connection establishment	Read-only, checked, and enabled to select the Local CPU as the active connection.
	One-way	Read-only and checked. Note: "PLC_3" (an S7-300 CPU319-3PN/DP) can act only as a server (cannot also be a client) in a PROFIBUS GET/PUT connection, allowing only a one-way connection.

The GET/PUT icon in the Property View tree also changes from red to green.

Completed PROFIBUS S7 connection

In the "Network view", a one-way S7 connection is shown in the "Connections" table between "PLC_1" and "PLC_3".



12.10 Diagnostic events for distributed I/O

NOTE

With a PROFIBUS IO system, after a download or power cycle, the CPU will go to RUN mode unless the hardware compatibility is set to allow acceptable substitute modules (Page 136) and one or more modules is missing or is not an acceptable substitute for the configured module.

As shown in the following table, the CPU supports diagnostics that can be configured for the components of the distributed I/O system. Each of these errors generates a log entry in the diagnostics buffer.

Table 12-74 Handling of diagnostic events for PROFINET and PROFIBUS

Type of error	Diagnostic information for the station?	Entry in the diagnostics buffer?	CPU operating mode
Diagnostic error	Yes	Yes	Stays in RUN mode
Rack or station failure	Yes	Yes	Stays in RUN mode
I/O access error [1]	No	Yes	Stays in RUN mode
Peripheral access error [2]	No	Yes	Stays in RUN mode
Pull / plug event	Yes	Yes	Stays in RUN mode

[1] I/O access error example cause: A module that has been removed.

[2] Peripheral access error example cause: Acyclic communication to a submodule that is not communicating.

Use the GET_DIAG instruction (Page 406) for each station to obtain the diagnostic information. This will allow you to programmatically handle the errors encountered on the

device and if desired take the CPU to STOP mode. This method requires you to specify the hardware device from which to read the status information.

The GET_DIAG instruction uses the "L address" (LADDR) of the station to obtain the health of the entire station. This L Address can be found within the Network Configuration view and by selecting the entire station rack (entire gray area), the L Address is shown in the Properties Tab of the station. You can find the LADDR for each individual module either in the properties for the module (in the device configuration) or in the default tag table for the CPU.

12.11 What to do when you cannot access the CPU by the IP address

In case you cannot reach a CPU by the IP address, you can set an emergency (temporary) IP address for the CPU. The emergency IP address enables you to re-establish communication with the CPU in order to download a device configuration with a valid IP address.

Reasons why you might need an emergency IP address

Your CPU might be inaccessible if someone downloaded a project with one of the following problems:

- The IP address of the PROFINET interface of the CPU is a duplicate of another device on the network.
- The subnet is incorrect for the CPU.
- The subnet mask makes the CPU unreachable.

In these cases, the CPU is no longer accessible from STEP 7.

Assigning an emergency IP address

You can assign an emergency IP address under the following conditions:

- The device configuration in STEP 7 has "Set IP address in the project" for the IP protocol.
- The CPU is in STOP mode.

Under these conditions, you can use a DCP tool to set the IP address of the device to an emergency IP address. The SIMATIC Automation Tool, for example, has a DCP Set IP address command. You can set an emergency IP address regardless of the protection level (Page 151) of the CPU. After you set a temporary IP address with a DCP tool, the Maintenance LED on the CPU turns on. The Diagnostics Buffer also includes an entry indicating that you enabled an emergency address of an Ethernet interface.

Restoring an IP address after assigning an emergency IP address

The diagnostics buffer informs you when you have enabled or disabled an emergency IP address. You can reset the emergency IP address by powering the CPU off and on.

After you have assigned an emergency IP address, you can then download a STEP 7 project with a valid IP address for the CPU. After you download the project, power cycle the CPU.

12.12 OPC UA Server

S7-1200 CPUs support the OPC UA Micro-Embedded Profile. For more information on the OPC UA Micro-Embedded Profile, visit the TIA Portal Information system.

Additionally, S7-1200 CPUs support the following:

- User management
- Communications security
- Subscriptions
- Program tag reading and writing
- Method calls

User management access control (UMAC) (Page 147) allows you to centrally manage a CPU's local users, including OPC UA users, from one location in the STEP 7 project: "Security settings > Users and roles". For CPUs with older projects, see Access control for the S7-1200 CPU (Page 151).

S7-1200 CPUs support a subset of OPC UA functionality, as described in the following sections. For additional information on OPC UA servers, visit the OPC Foundation Web site (https://opcfoundation.org/).

12.12.1 OPC UA server configuration

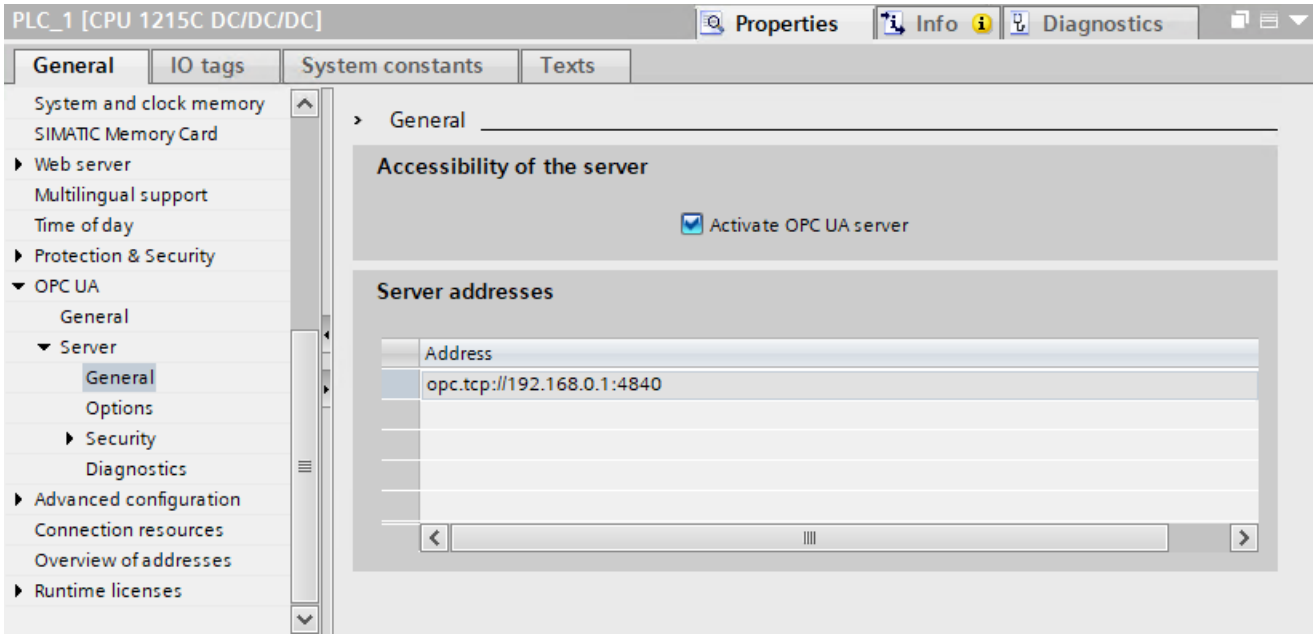
To use the OPC UA server, you must configure the OPC UA settings in the Device configuration of the CPU in the TIA Portal.

12.12.1.1 Activating the OPC UA server

By default, the OPC UA server is inactive. Activate the OPC UA server by selecting the checkbox for "Activate OPC UA server" in the CPU's hardware properties.

To activate the OPC UA server, follow these steps:

1. Select the General tab in the Device Configuration view.
2. In the General window, select "OPC UA".
3. In the OPC UA>Server>General window, select the "Activate OPC UA server" checkbox.



12.12.1.2 Behavior of the OPC UA server in operation

The OPC UA server is operational once you activate the server and download the project to the S7-1200 CPU.

Behavior in STOP mode of the CPU

An activated OPC UA server is operational even when the CPU is switched to "STOP". The OPC UA server continues responding to requests from OPC UA clients.

Server response in detail:

- When requesting the values of PLC tags, the CPU is returning the values written before it was set to "STOP" mode.
- You can write values to the OPC UA server while in "STOP" mode. However, the CPU is not processing the values because the user program is not executing while in "STOP" mode. Any values written while in "STOP" mode are readable by OPC UA clients from the OPC UA server of the CPU.

Loading of the CPU with running OPC UA server

Loading certain objects while the OPC UA server is running can cause the CPU to stop. If the CPU stops, you are prompted to restart the server. Restarting the server interrupts active connections. You must re-establish the connections when the server restarts.

The following parameters affect the duration of the restart:

- The scope of the data structure
- The number of variables visible in the OPC UA address space
- The setting for downward compatible data type definition according to OPC UA specification to V1.03 (TypeDictionary enabled)
- The Settings for the communication load and minimum cycle time (Page 136)

The OPC UA server behavior is as follows:

- Downloading objects while the CPU is in the "STOP" mode causes the OPC UA server to stop and restart. STEP 7 does not display a warning.
- Downloading objects while the CPU is in "RUN" mode causes the OPC UA server to stop when the objects are or maybe OPC UA-relevant. The modified OPC UA data causes the OPC UA server to restart after re-initialization.
  STEP 7 displays a warning in the preview dialog before loading OPC-UA-relevant objects into the CPU and stopping the OPC UA server. If a server restart is incompatible with your running process, you can cancel the download. These warnings are only displayed when the OPC UA server is running. If the OPC UA server is not enabled, modified OPC UA data has no influence on the download process.

Examples of how a running OPC UA server reacts during loading

Example 1:

Desired action: You want to add another code block to the program. Data blocks, inputs, outputs, and flags are not affected.

Server reaction: The running OPC UA server is not interrupted.

Example 2:

Desired action: You want to load a new data module and you have flagged the data module as not OPC UA relevant.

Server reaction: The running OPC UA server is not interrupted.

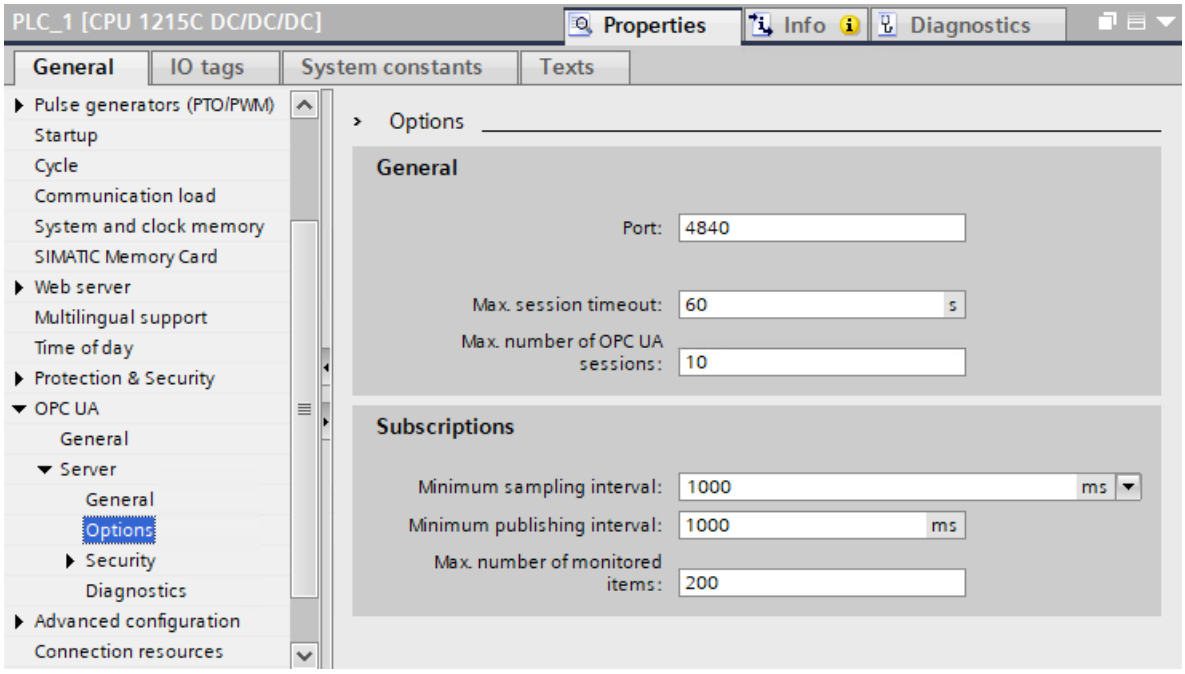
Example 3:

Desired action: You want to overwrite a data module.

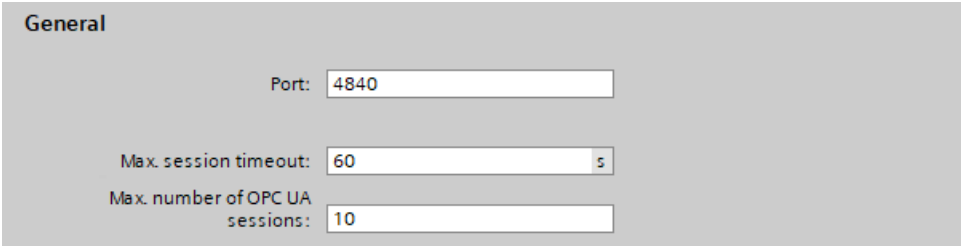
Server reaction: Because STEP 7 cannot determine whether the changes affect OPC UA relevant data, a warning appears indicating the server is restarting.

12.12.1.3 Settings for the OPC UA server

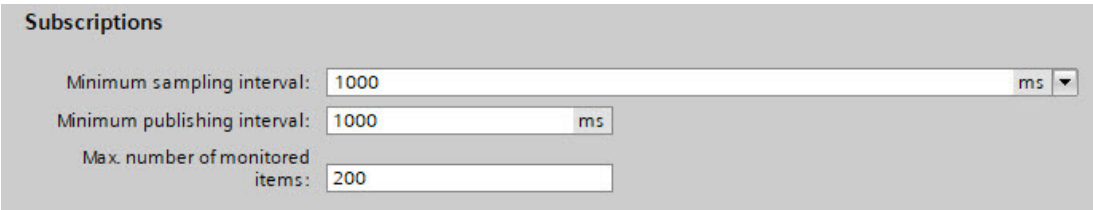
From the Options dialog you can adjust the OPC UA server settings:



The following General settings and Subscriptions settings tables give further information about the server's configurable settings.
The default values for each row work with the default CPU communication load (Page 81) of 20%. Increase the CPU communication load percentage to suit your needs. The current load of communication activities (for example, PROFINET) affects the CPU percentage load.



General settings	Range	Default
Ports	1024 - 49151	4840
Max. session timeout	1s - 600000s	60s
Max. number of OPC UA sessions	1 - 10	10



Subscriptions settings	Range	Default
Minimum sampling interval	100 ms, 250 ms, 500 ms, 1000 ms, 5000 ms, 10000 ms	1000 ms
Minimum publishing interval	200 ms - 20000000 ms	1000 ms
Max. number of monitored items	100 - 1000	200

12.12.1.4 Limitations of the OPC UA server

When using OPC UA server interfaces, you must comply with the following limitations:

- Number of server interfaces
- Number of OPC UA nodes
- Number of server methods or server method instances if you have implemented methods

Interface, method, and subscription limitations

The following tables apply to S7-1200 CPUs and S7-1200 Fail-safe CPUs; consider these limitations when compiling and loading a configuration. Violating a server limitation results in an error message.

Interface limitations	Max.
OPC UA server interfaces[1]	2
User-defined nodes on server interface[2]	2000
Namespaces[3]	18

1 A server interface can be a "Companion specification" type or a "Server interface" type.

2 The maximum number includes nodes internally defined by the server interface.

3 This is the total number of defined namespaces for all server interface types: "Interface", "Companion specification", and "Reference namespace".

Method limitations	Max.
Server methods[1]	20
Server method instance DBs for all server interfaces and associated server methods	20
Server method input arguments	20
Server method output arguments	20

1 Any methods above this limit are non-executable, and result in a client runtime error. You can use multiple instances of the same method.

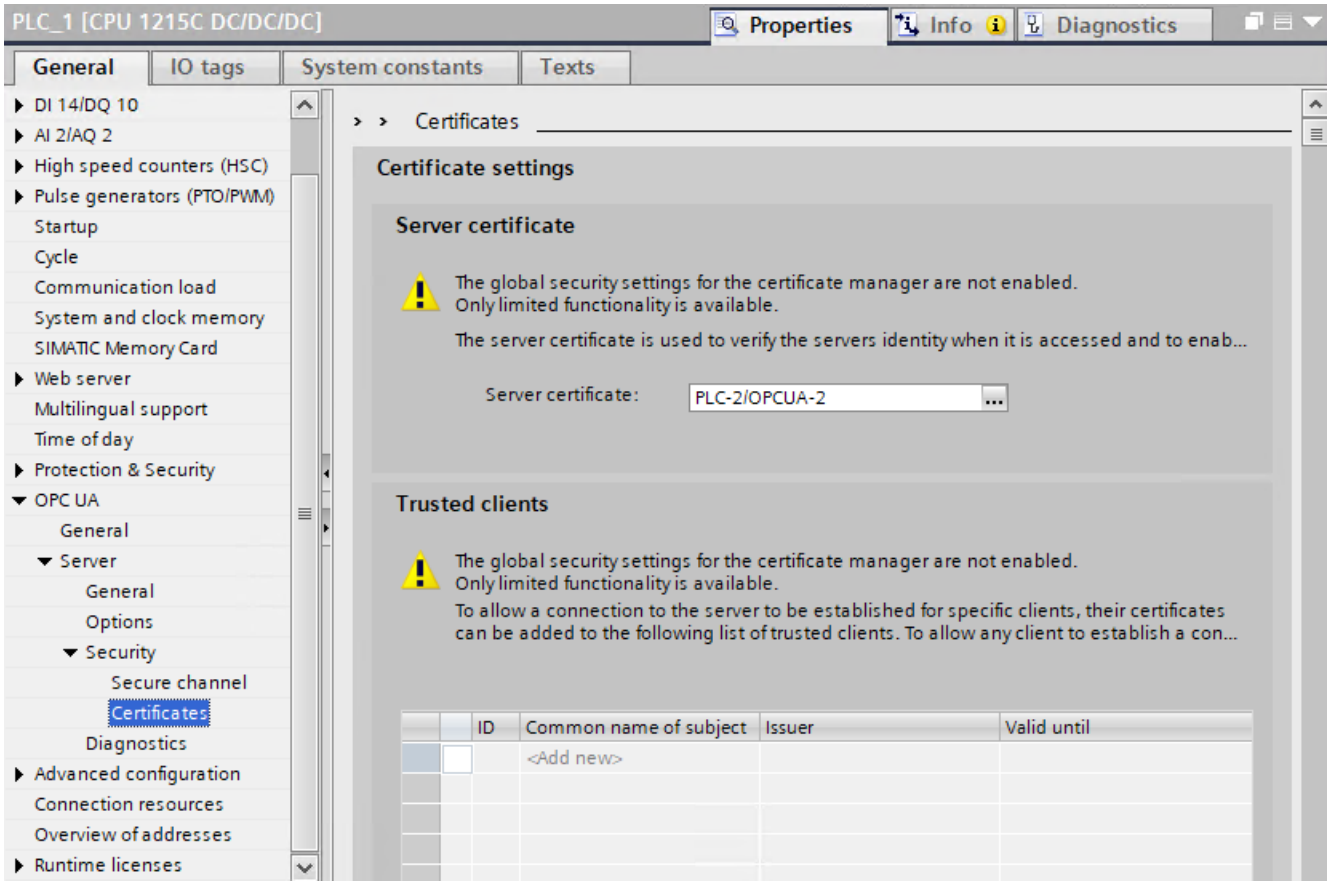
Subscription limitations	Max.
Concurrent subscriptions[1]	50
Subscriptions per session	5

[1] Concurrent Subscriptions is equal to the configured number of concurrent sessions multiplied by the maximum number of subscriptions per session.

12.12.2 OPC UA server security

Server security is one of several security methods available to secure communication. TIA Portal security and PLC security are two other security methods.

The OPC UA server requires a certificate (Page 529) for activation. When you activate the server, TIA Portal generates a certificate. You can change this certificate in the PLC properties.



NOTE

S7-1200 certificate limit

The S7-1200 has a system certificate limit of 64.

All certificates count against this number (for example, Web certificates, OPC UA certificates, and OUC certificates).

If you have more than 64 certificates, the TIA Portal displays an error stating that you have exceeded the maximum number of 64 certificates. You must remove some certificates from the PLC configuration.

12.12.2.1 Supported security policies

Selecting a supported security policy at runtime determines the security of communications between the client and server.

To select your OPC UA security policy, follow these steps:

1. Select the General tab in the Device Configuration view.
2. In the General window, select "OPC UA".
3. Under OPC UA, select "Server > Security > Secure Channel".
4. Select the security policy you need from the list of available server policies.

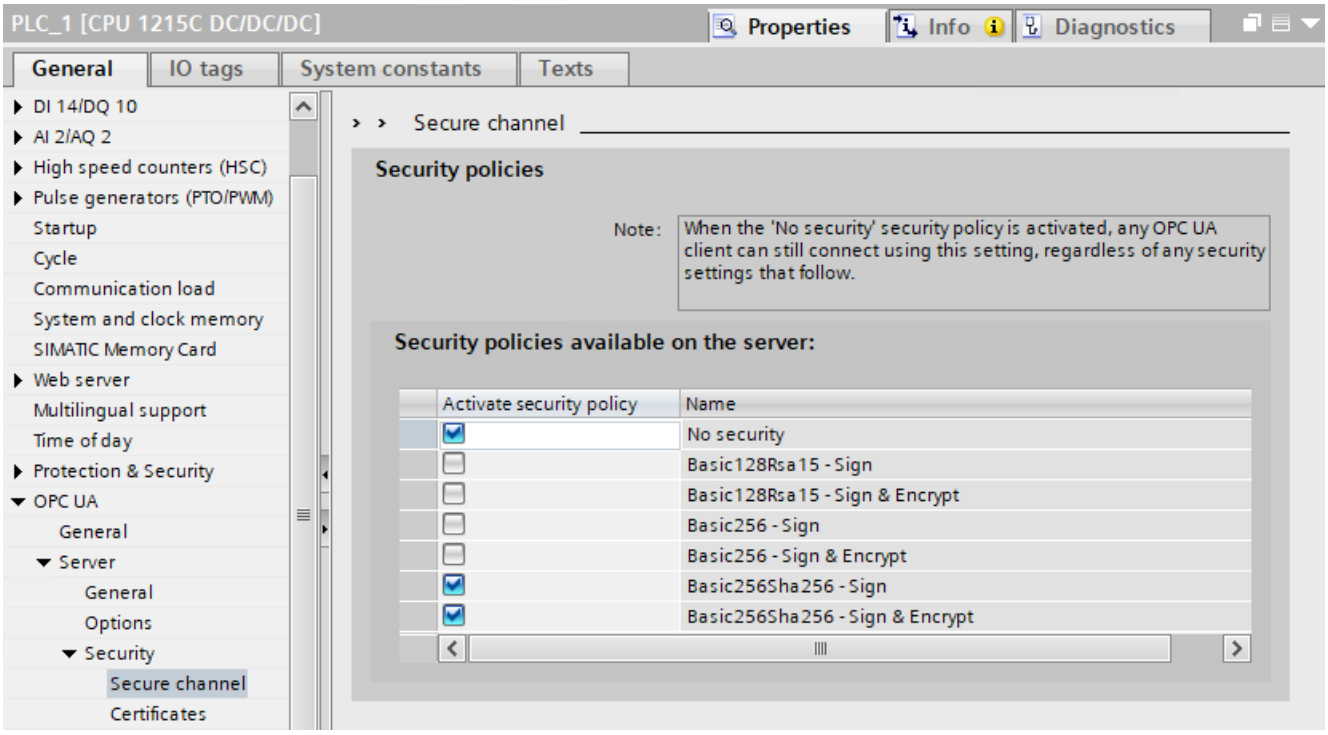


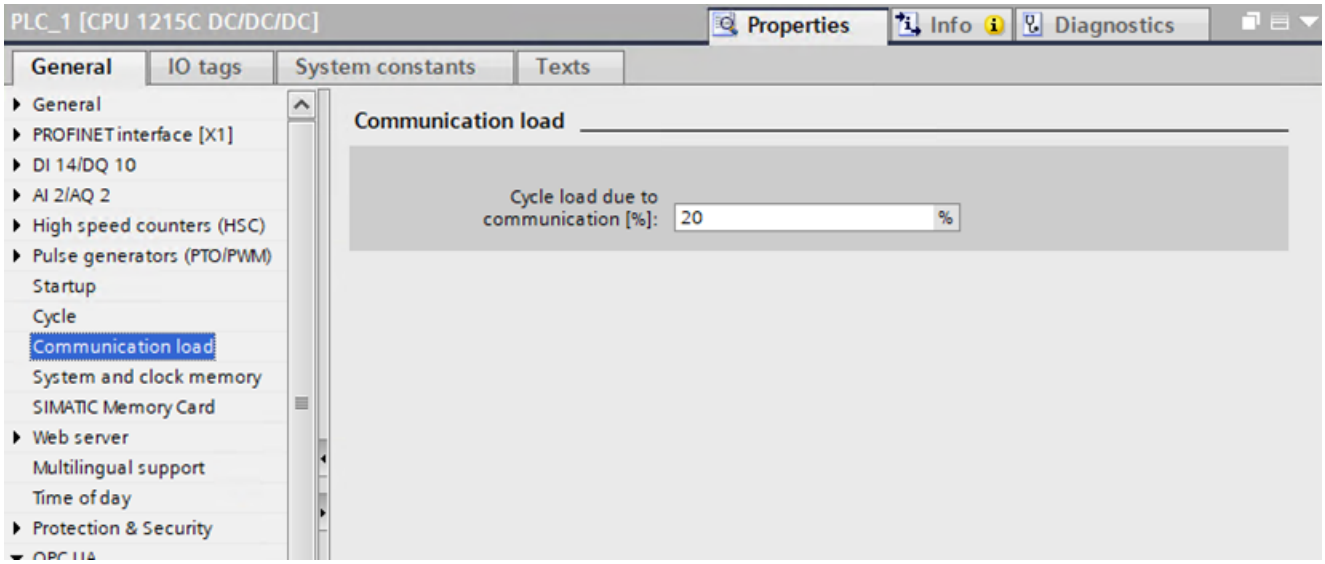
Table 12-75 OPC UA security polices supported by the S7-1200

Security policy	Enabled by default?
No security	Yes
Basic128Rsa15 – sign	No
Basic128Rsa15 – sign & encrypt	No
Basic256 – sign	No
Basic256 – sign & encrypt	No
Basic256Sha256 – sign	Yes
Basic256Sha256 – sign & encrypt	Yes

Establishing a secure OPC UA connection

Using enhanced security policies when establishing an initial connection between the OPC UA client and the S7-1200 server can significantly increase connection time, especially during RUN mode. This can cause the OPC UA client to time out before a connection is established and interrupt online connections to external devices such as TIA portal, HMIs, etc.

To prevent the OPC UA client from timing out, you can increase the OPC UA client's session connection time to 60 seconds.
To maintain online connections to external devices, you can increase the communications load percentage.



If necessary, to avoid increasing the communications load while establishing the initial OPC UA connection, you can do one of the following:

- Abort any online connections to external devices and once the initial OPC UA connection is established, reconnect.
- Re-establish online connections to external devices once they have timed out.

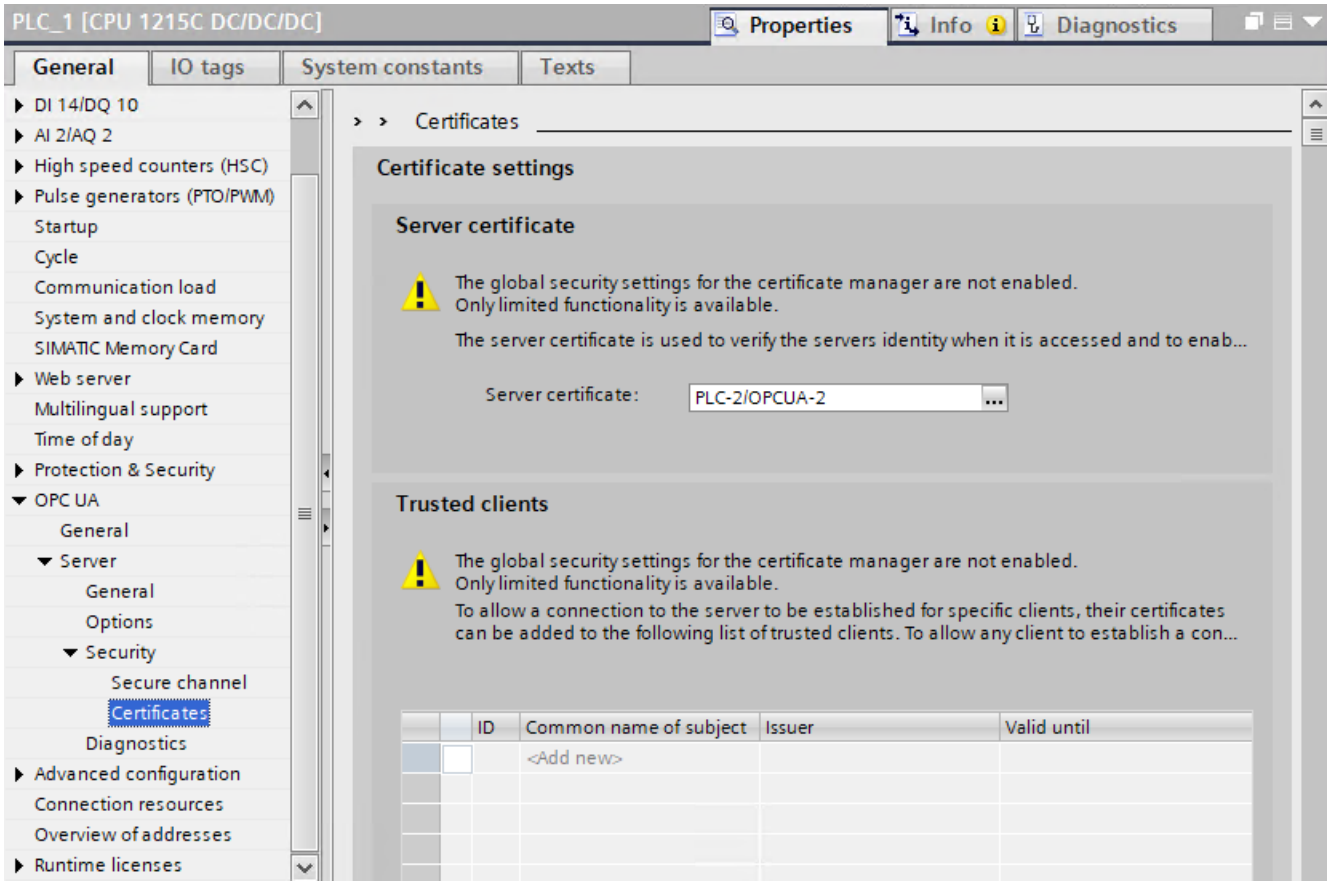
NOTE

Increasing the cycle load due to communication proportionately increases the scan cycle time relative to active communication in progress.

12.12.2.2 Trusted clients

You can configure the OPC UA server to only allow connections from trusted clients. The default server configuration automatically accepts client certificates.
You define the list of trusted clients. The server uses certificates to identify trusted clients. If selected, only clients that present trusted certificates at runtime are allowed to connect to the server.

To specify trusted clients, add their certificates to the "Trusted clients" list in TIA Portal under "Hardware properties > OPC UA security > Secure channel > Trusted clients".



12.12.2.3 Assigning OPC UA user rights for V4.7 configured CPUs

If the firmware version of the CPU in your STEP 7 project is V4.7 or later, you can assign OPC UA users with User Management & Access Control (UMAC) (Page 147).

Assign roles and rights by doing the following:

1. Select "Security Settings" in the STEP 7 project tree.
2. Double-click "Users and roles".

From Users and Roles, you can add a user, create a new role, assign rights to the new role, and assign the role to a user.

To add a user, do the following:

1. Select the "Users" tab on the top, right side of the window.
2. Double-click "add a new user", then select "Add new local user" from the pop-up.
3. Enter the User name and Password. Runtime timeout defaults to 30 minutes but can be configured by entering the time manually in the field or using the arrows to change the time by one minute increments . The UM domain ID and Comment fields are optional.

NOTE

In addition to defining a user name and password using UMAC, you must enable corresponding OPC UA user function rights for the client and the server.

NOTE

The value in the column "Runtime timeout" (max. session duration) in the Users table under the Users tab does not evaluate the CPU for OPC UA runtime rights; users are not automatically logged out after a certain period of time.

To automatically log users out, you must use OPC UA specific mechanisms like the parameter "Max. session timeout" which is located under "OPC UA > Server > Options" on the "Properties" tab.

To create a new role, follow these steps:

1. Select the "Roles" tab from the top, right side of the window.
2. In the "Roles" section, double-click "Add new role".
3. Enter the Role Name, Description, Runtime timeout, and optional Comment.

Assign rights to the role in the following way:

1. Click the "Runtime rights" tab in the bottom window.
2. Select your PLC from the "Runtime rights" dropdown at left. This will populate all of the Function rights you can assign for that PLC.
3. Select the check boxes that you wish to assign for this role.

To assign a role to a user, do the following:

1. Select the "Users" tab on the top, right side of the window.
2. Click the check box and highlight the name of the user you want to assign with a role.
3. Click the "Assigned roles" tab in the bottom window.
4. Select the check box next to the role(s) you want to assign to the user.

After you download the configuration to the CPU, only authorized users can access OPC UA functions for which they have privileges.

OPC UA user role runtime rights

The default "Anonymous" user is disabled for security. You can enable the anonymous user by selecting the checkbox and agreeing to the security warning. For more information on working with the anonymous user, see "Managing users and roles > Activating or deactivating anonymous user" in the TIA Portal Information System.

Assignable user role runtime rights are as follows:

- OPC UA server access
- User authentication of the OPC UA client
- Mange certificates

WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server or OPC UA users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

- Enable Access control (Page 147) under "Protection & Security > Access control".
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Enable the setting "Only allow secure PG/PC and HMI communication" under "Protection & Security > Connection mechanisms".
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC from a location outside your protected network.
- Enable access to the Web server only with the HTTPS protocol.
- Perform error-checking and range-checking on your variables in your program logic because Web server or OPC UA users can change PLC variables to invalid values.
- For the OPC UA server: In your STEP 7 Device configuration, navigate to "Properties > OPC UA > Server > Security" and deselect "No security" in "Security policies available on the server for the secure channel".

Disruption of process operations can result in death, severe personal injury, and/or property damage.

12.12.2.4 Authenticating OPC UA users for CPUs with project configurations earlier than V4.7

User Management Access Control (UMAC) is only available when the configured firmware version of the CPU in the project is V4.7.

If you have a CPU configured in your STEP 7 project to use a firmware version earlier than V4.7, you authenticate OPC UA users under "Properties > OPC UA > Server > Security > User authentication".

For more information on how to add and authenticate OPC UA users for projects with older CPU versions, see OPC UA user authentication (https://support.industry.siemens.com/cs/us/en/view/109814829/159773719435).

WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server or OPC UA users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

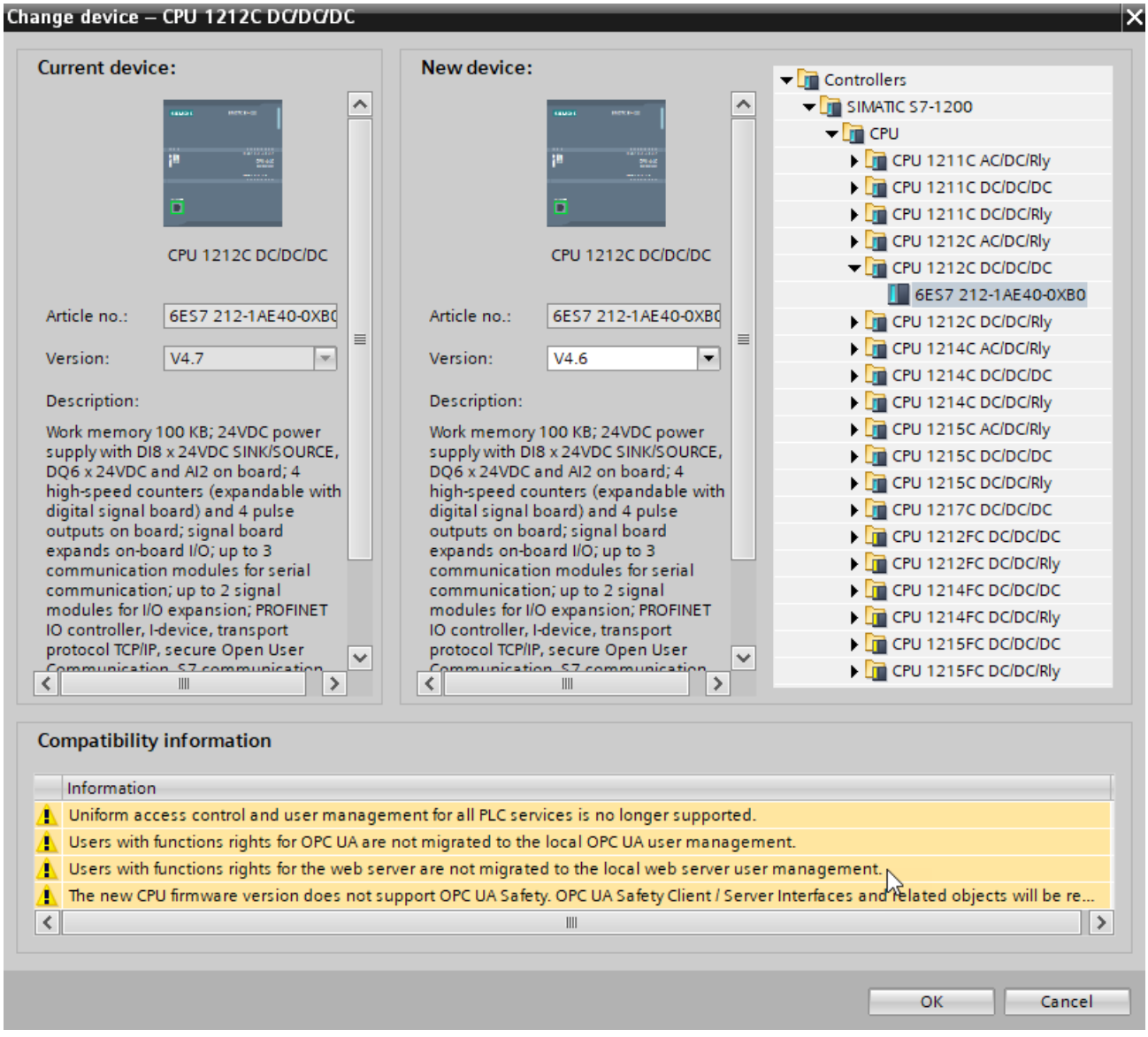
- Enable Access control (Page 147) under "Protection & Security > Access control".
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Enable the setting "Only allow secure PG/PC and HMI communication" under "Protection & Security > Connection mechanisms".
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC from a location outside your protected network.
- Enable access to the Web server only with the HTTPS protocol.
- Perform error-checking and range-checking on your variables in your program logic because Web server or OPC UA users can change PLC variables to invalid values.
- For the OPC UA server: In your STEP 7 Device configuration, navigate to "Properties > OPC UA > Server > Security" and deselect "No security" in "Security policies available on the server for the secure channel".

Disruption of process operations can result in death, severe personal injury, and/or property damage.

12.12.2.5 OPC UA user compatibility

Upgrading configured firmware from an earlier version to V4.7

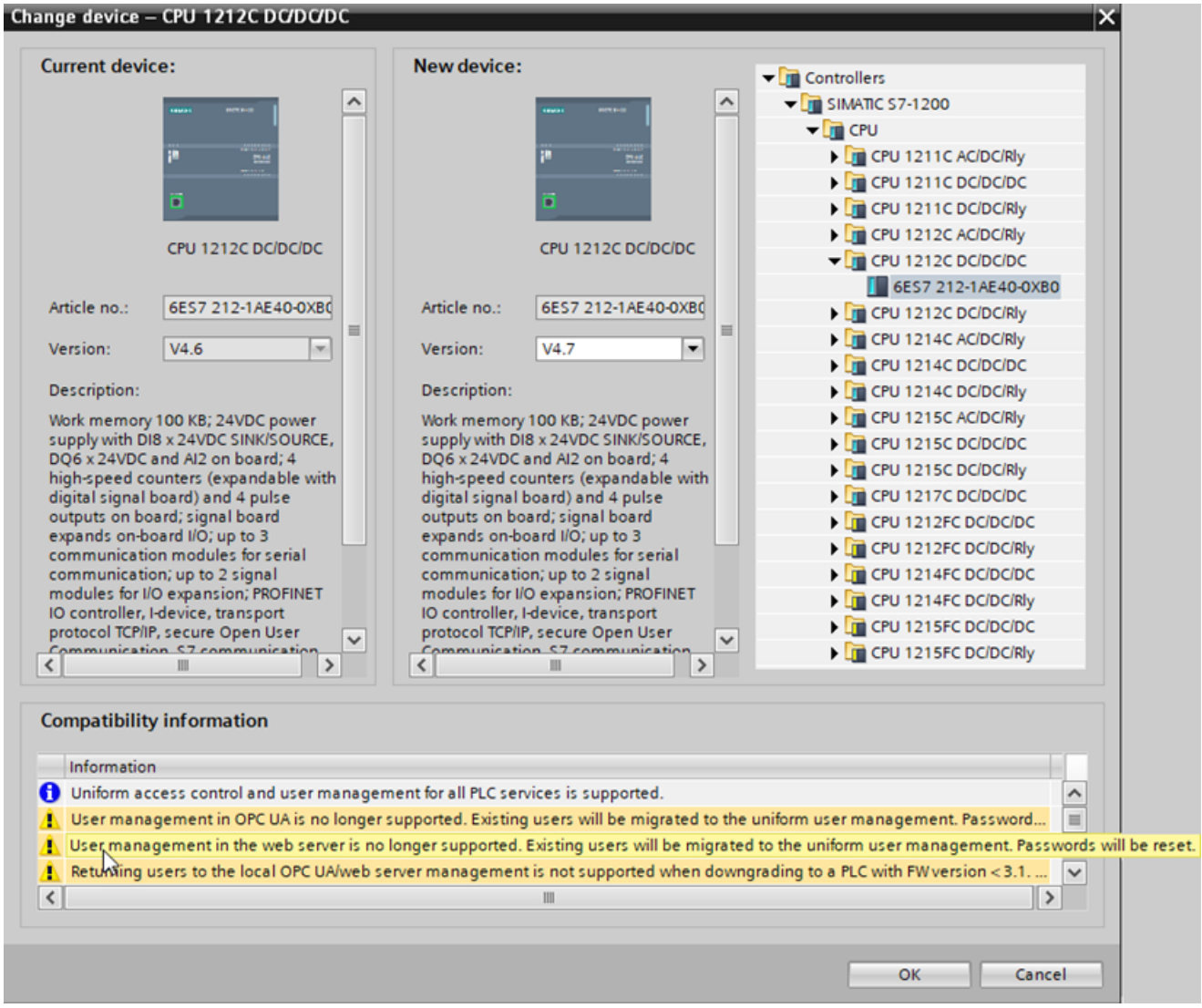
When you upgrade the configured firmware version in your STEP 7 project to V4.7, STEP 7 migrates users that you previously configured in "User management" to "Users and Roles". You reassign user passwords in the Project tree under "Security settings > Users and roles > Users."



For more information about OPC UA user rights when upgrading firmware in the STEP 7 project, see "Editing devices and networks > Configuring devices and networks > Creating configurations > Configuring automation systems > Functional description of S7-1200 CPUs > Setting the operating behavior > Protection and Security > Settings for users and roles > Information about compatibility" in the TIA Portal Information System.

Downgrading configured firmware from V4.7 to an earlier version

When you downgrade the configured firmware version in your STEP 7 project from V4.7 to an earlier version, users configured in the Project tree under "Security settings > Users and roles > Users" will not be migrated. OPC UA users must be reconfigured from the CPU's "Properties" tab under "OPC UA > Server > Security > User authentication" in the "User management" area.



For more information about OPC UA user rights when downgrading firmware in the STEP 7 project, see "Editing devices and networks > Configuring devices and networks > Creating configurations > Configuring automation systems > Functional description of S7-1200 CPUs > Setting the operating behavior > Protection and Security > Settings for users and roles > Information about compatibility" in the TIA Portal Information System.

12.12.3 OPC UA server interface

The S7-1200 OPC UA server supports the standard SIMATIC server interface. It does not support the automatic publishing of CPU and DB tags using this selection. You must define the structure and content of the server interface in TIA Portal and then download to the PLC.

To add a server interface, perform the following steps:

1. In the project tree, click the PLC name.
2. Select "OPC UA communication."
3. Select "Server interfaces."
4. Select "Add new server interface" and click OK.
5. In the new server interface, enter variables from your PLC program.
6. Download the server to your PLC.

When you are adding a server interface, note that the OPC UA elements of the screen lists all available tags. You can drag the elements from the "OPC UA elements" window to the "OPC UA server interface" window. There is a consistency checker to verify the service interface contents. You can export the interface to an XML file.

You define the OPC UA server interface when you add an OPC UA server interface to your project.

To define the OPC UA server interface, select one of the following options from the OPC UA server creation dialog:

- Select "Server interface", Type: Interface
- Select "Companion specification", Type: Companion specification
- Select "Companion specification", Type: Reference namespace

12.12.3.1 Supported data types

The OPC Foundation (https://opcfoundation.org/) defines a set of supported data types that describe the structure of the Value attribute of Variables and their VariableTypes. The S7-1200 supports a subset of those data types (Page 95), as well as other defined types that derive from those data types.

The following table lists the data types that the S7-1200 supports:

SIMATIC type	OPC UA type name	Node identifier
Bool	Boolean	i=1
SInt	SByte	i=2
USInt	Byte	i=3
Int	Int16	i=4
UInt	UInt16	i=5
DInt	Int32	i=6
UDInt	UInt32	i=7
Real	Float	i=10
LReal	Double	i=11
WString	String	i=12
DWord	StatusCode	i=19
DATE	UInt16	i=5

SIMATIC type	OPC UA type name	Node identifier
TOD	UInt32	i=7
TIME	Int32	i=6
DTL	Structure	N/A

Note that this list represents supported base node types. It does not represent a complete list of supported node types since many SIMATIC data types map to the base node types. Any SIMATIC data type that maps to a base node type is also a supported node type.

The S7-1200 CPUs support server methods as well as structured data types (structures and arrays).

The S7-1200 CPUs do not support Unions.

The S7-1200 accepts a download of a server with unsupported types. However, the PLC returns an error if the client attempts to read or write to a node with an unsupported type.

12.12.3.2 PLC representation

The OPC UA server interface provides nodes that represent the PLC with properties that describe the PLC. These are available whenever the OPC UA server is active.

The standard SIMATIC server interface provides the following information:

Attribute	**Value**		
NodeId	Ns=SI;s=PLC		
BrowseName	SI:<PLC> Where <PLC> is the name the user has assigned to the PLC in their TIA Portal project		
References	**NodeClass**	**BrowseName**	**Comment**
ComponentOf the DeviceSet Object			
OrganizedBy the Objects folder			
HasTypeDefinition	ObjectType	SimaticDeviceType	Derived from device type
HasProperty	Variable	DeviceManual	
HasProperty	Variable	DeviceRevision	
HasProperty	Variable	EngineeringRevision	
HasProperty	Variable	HardwareRevision	
HasProperty	Variable	Icon	
HasProperty	Variable	Manufacturer	
HasProperty	Variable	Model	
HasProperty	Variable	OperatingMode	
HasProperty	Variable	OrderNumber	
HasProperty	Variable	RevisionCounter	
HasProperty	Variable	SerialNumber	
HasProperty	Variable	SoftwareRevision	

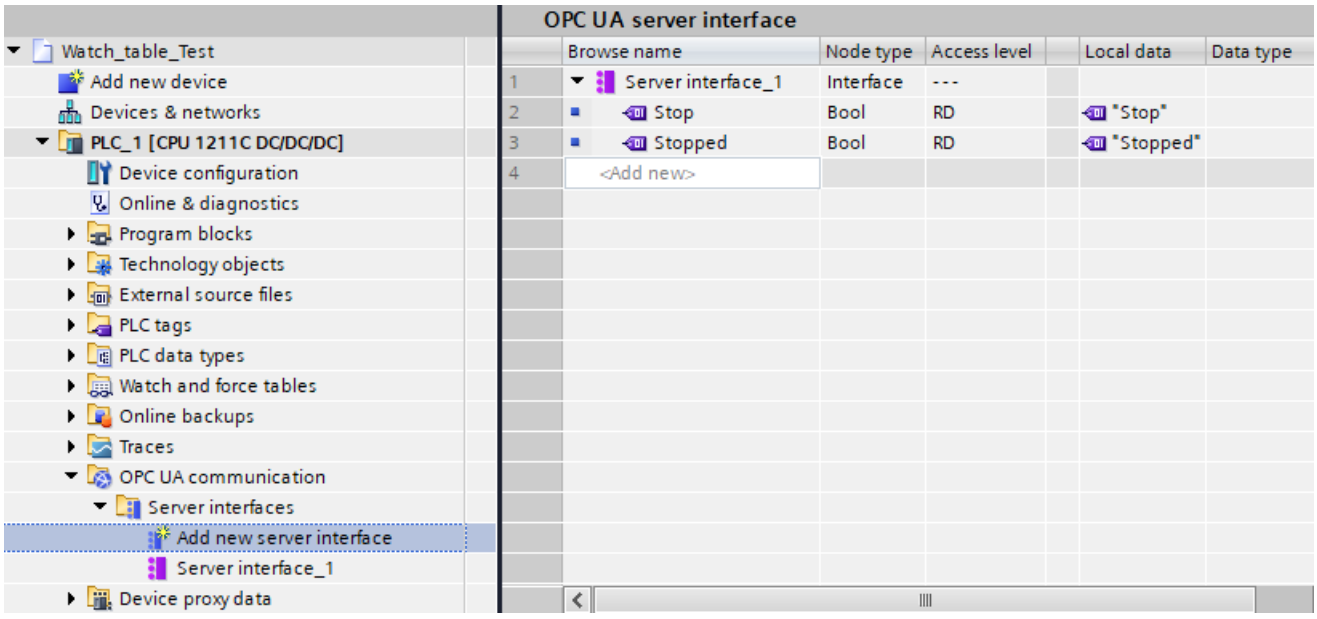
12.12.3.3 Downloadable server interfaces

You create and edit components of the OPC UA server interface in TIA Portal. You can define OPC UA server interfaces in two ways:

- Companion specification externally-created XML files
- Server interface defined directly in the TIA Portal based on data block elements and global tags you include in your program

When downloaded, these components define the server interface that is visible to an OPC UA client.

You must set specific TAG attributes for the TAG to be readable/writable from OPC UA.



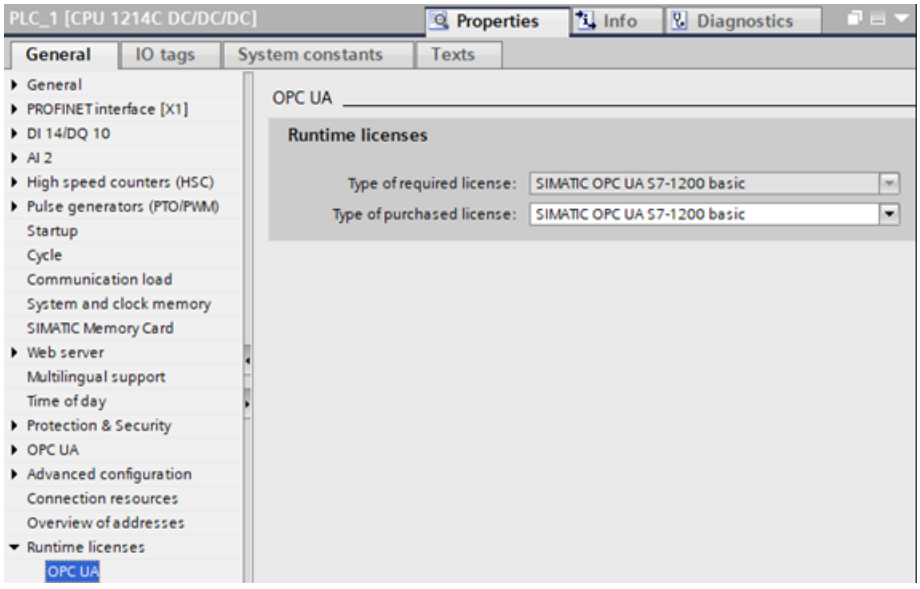
Runtime license required

The OPC UA server for the S7-1200 CPU requires a runtime license to operate. The following licenses are available:

- SIMATIC OPC UA S7-1200 Basic DVD 6ES7823-0BA00-2BA0
- SIMATIC OPC UA S7-1200 Basic DL 6ES7823-0BE00-2BA0

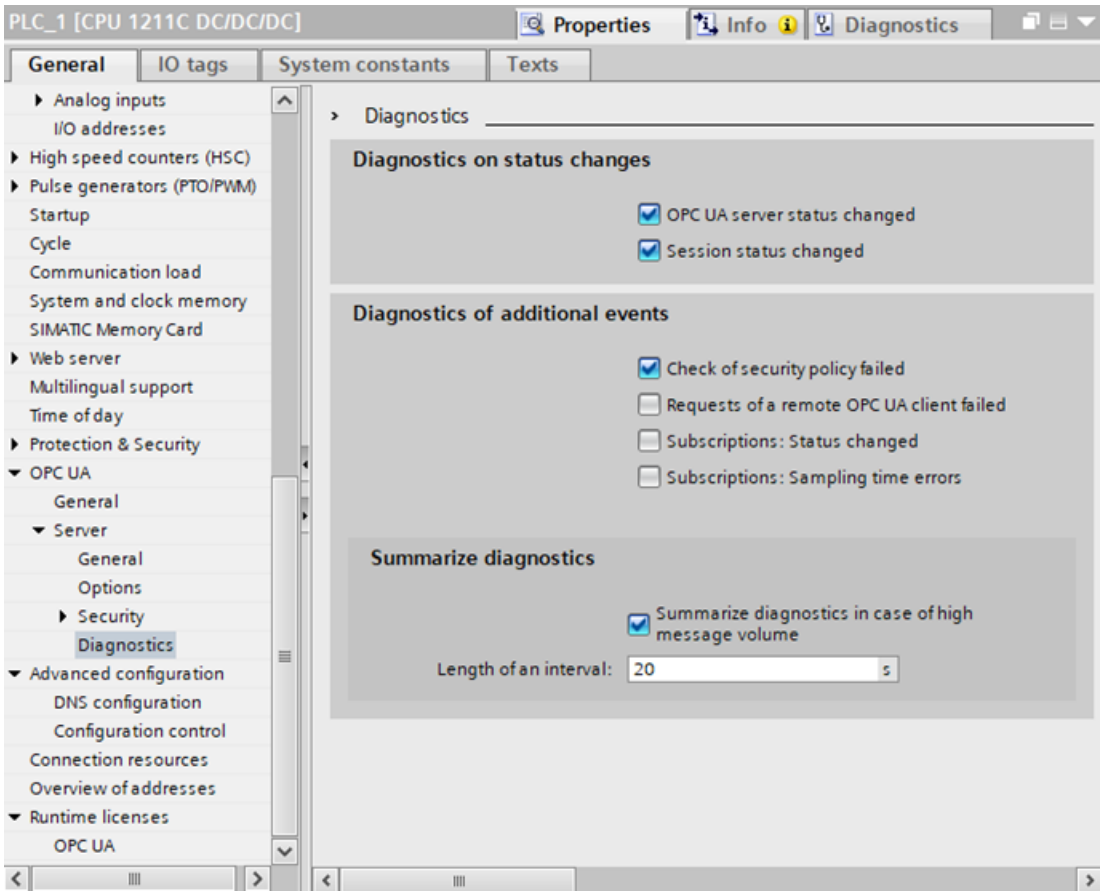
To find the required license type select "Properties > General > Runtime licenses > OPC-UA > Type of required license." To confirm purchase of the required license, follow these steps:

1. Click "Runtime licenses > OPC UA" in the properties of the CPU.
2. Select the required license from the "Type of purchased license" drop-down list.



12.12.4 OPC UA Diagnostics Buffer

You configure the OPC UA diagnostics in the TIA Portal and download the settings to the PLC. You can check the diagnostics buffer entries using the OPC UA client.



Diagnostics messages on status change do not appear with high frequency. Each of these messages has a high importance for the usage of OPC UA.

Summarizing diagnostics messages applies only to the diagnostic messages of the OPC UA Server. You can choose different settings for the CPU-global security events.

To limit the number of diagnostic messages in the case of high message volume, you can specify a message collection interval in seconds. The value range is 1 to 7200 seconds.

NOTE

Enabled/disabled OPC UA server

You can only change the settings of the OPC UA diagnostics menu when OPC UA server is enabled.

When you disable the OPC UA server, all settings become gray and are read-only.

12.12.4.1 OPC UA Limits reached

The server tells you when a system limit is reached, for example if it cannot provide data or when you cannot use the server/client in the normal way.
The OPC UA server has specific system limits for the number of subscriptions/monitored items, number of registered items, sampling rate of subscriptions, and number of connected clients.
When you reach any of these specific system limits, the server creates a diagnostics buffer entry.
The creation of a new diagnostics buffer entry causes a diagnostic message to display:
OPC UA Server: Exceeded limit of <Name of Limit>.
The diagnostic message specifies one of the following limits:

- Number of Sessions
- Number of Monitored Items
- Number of Subscriptions
- Number of Registered Nodes
- Number of Server Methods
- Number of Monitored Items per Call
- Number of Nodes per Browse
- Number of Nodes per Read
- Number of Nodes per RegisterNodes
- Number of Nodes per TranslateBrowsePathsToNodeIds
- Number of Nodes per Write
- Number of Nodes per MethodCall
- Memory Consumption

NOTE

If a service request exceeds a configured limit or a system limit, the server will respond with a service fault in the most cases.

The following use cases are shown below:

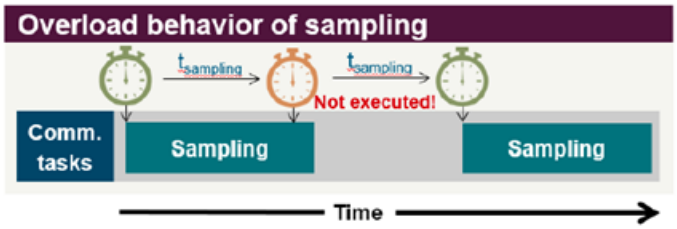
Table 12-76 Use cases for "OPC UA limits reached"

User action	Expected behavior	Limit
Client creates more sessions as allowed by HWCN	The CPU adds a diagnostic message with exceeded limit to the diagnostics buffer.	Sessions
Client creates more Monitored Items as allowed by HWCN	The CPU adds a diagnostic message with exceeded limit to the diagnostics buffer.	Monitored Items
Client creates more Subscriptions as allowed (depends on PLC type)	The CPU adds a diagnostic message with statuscode <Statuscode> to the diagnostics buffer.	Client tries to connect with an unsupported identity token

User action	Expected behavior	Limit
Clients registers more nodes as allowed by HWCN	The CPU adds a diagnostic message with exceeded limit to the diagnostics buffer.	Registered Nodes
Client triggers a BadOutOfMemory response from the server by a high number of sessions/ subscriptions/ registered Nodes	The CPU adds a diagnostic message with exceeded limit to the diagnostics buffer.	Memory Consumption
Client exceeds an operational limit of a service. (amount of operations in a single request exceeds the limit specified by the server)	The CPU adds a diagnostic message with exceeded limit to the diagnostics buffer.	Nodes per Browse Nodes per Read Nodes per Write Nodes per MethodCall Nodes per RegisterNodes Nodes per Translate

Diagnostic message for "Overload behavior of subscriptions"

With an OPC UA subscription on different variables the OPC UA server checks the items for value change at predefined sampling intervals. This check, the "Sampling", needs a certain time that is independent of the number and data type of the items. Once sampling is complete the server publishes the results and sends the items to the client. If there are too many items in the queue, an "Overload" of the communication stack might occur. The CPU cannot check all the items in the specified sampling interval and jumps to the next sampling job.



If you cannot reach the set sampling rate, the server triggers a "Sampling Overload" diagnostics buffer entry.

Examples of OPC UA sampling overload diagnostic messages:

OPC UA server: Sampling rate 100 ms could not be reached. Overload of Subscription ID 12345678

OPC UA server: Sampling rate could not be reached. -Summary message for 3 occurrences during the last 20 second(s)

12.12.4.2 OPC UA Security events

The OPC UA server alerts you whenever security events occur so you can react if the OPC UA server is vulnerable or if it detects an attack. The occurrence of specific OPC UA security events in the OPC UA server/client system triggers the entry of a message in the diagnostics buffer.

Denying a session or connection attempt due to incorrect authentication data is an example of a possible security event.

The OPC UA Server uses this message to report security problems:
"OPC UA Server: Security checks failed"

When a security check fails it generates warning messages and the operation does not execute.

Often, other security components like OpenSSL, UMAC 711, or OPC UA Stack return a status code and the server writes the status code into the diagnostic message.

Any time you get a negative response, the server generates a message. The most common use cases are shown below:

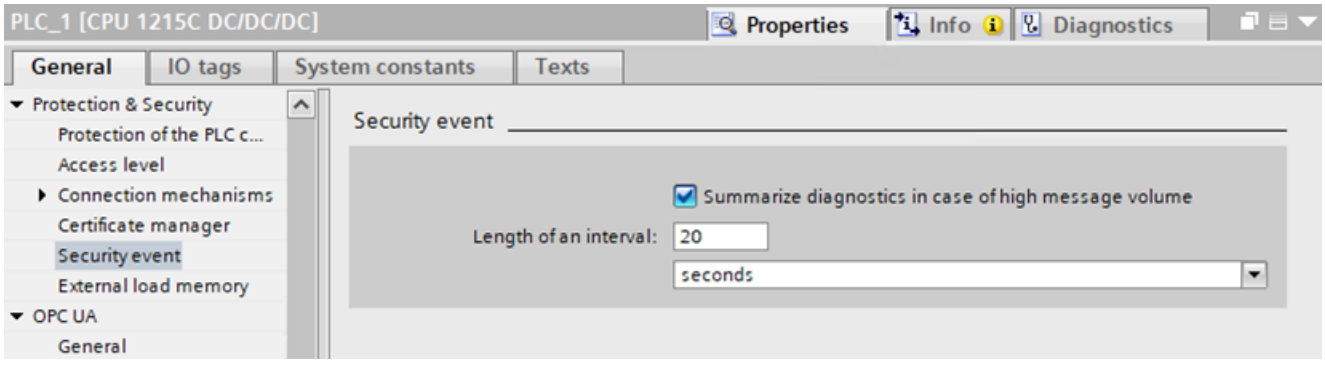
User action	Expected behavior	Statuscode
Client tries to connect with an unsupported security model	The CPU adds the diagnostic message with statuscode <Statuscode> to the diagnostics buffer.	16#8054_0000 (BadSecurityModeRejected)
Client tries to connect with an unsupported security policy	The CPU adds the diagnostic message with statuscode <Statuscode> to the diagnostics buffer.	16#8055_0000 (BadSecurityPolicyRejected)
Client tries to connect with an unsupported identity token	The CPU adds the diagnostic message with statuscode <Statuscode> to the diagnostics buffer.	16#8020_0000 (BadIdentityTokenInvalid)
Client tries to connect with the wrong authentication (username or password wrong)	The CPU adds the diagnostic message with statuscode <Statuscode> to the diagnostics buffer.	16#8021_0000 (BadIdenditytokenRejected)
Client tries to connect with an invalid certificate (there are several possible reasons for invalidity of certificates)	The CPU adds the diagnostic message with statuscode <Statuscode> to the diagnostics buffer.	Depends on reason for invalidity e.g. 16#8014_0000 (BadCertificateTimeInvalid) 16#801A_0000 (BadCertificateUntrusted)

Types of Security messages

There are two types of security messages: CPU-wide security messages and Security of OPC UA messages.

CPU-Wide security messages

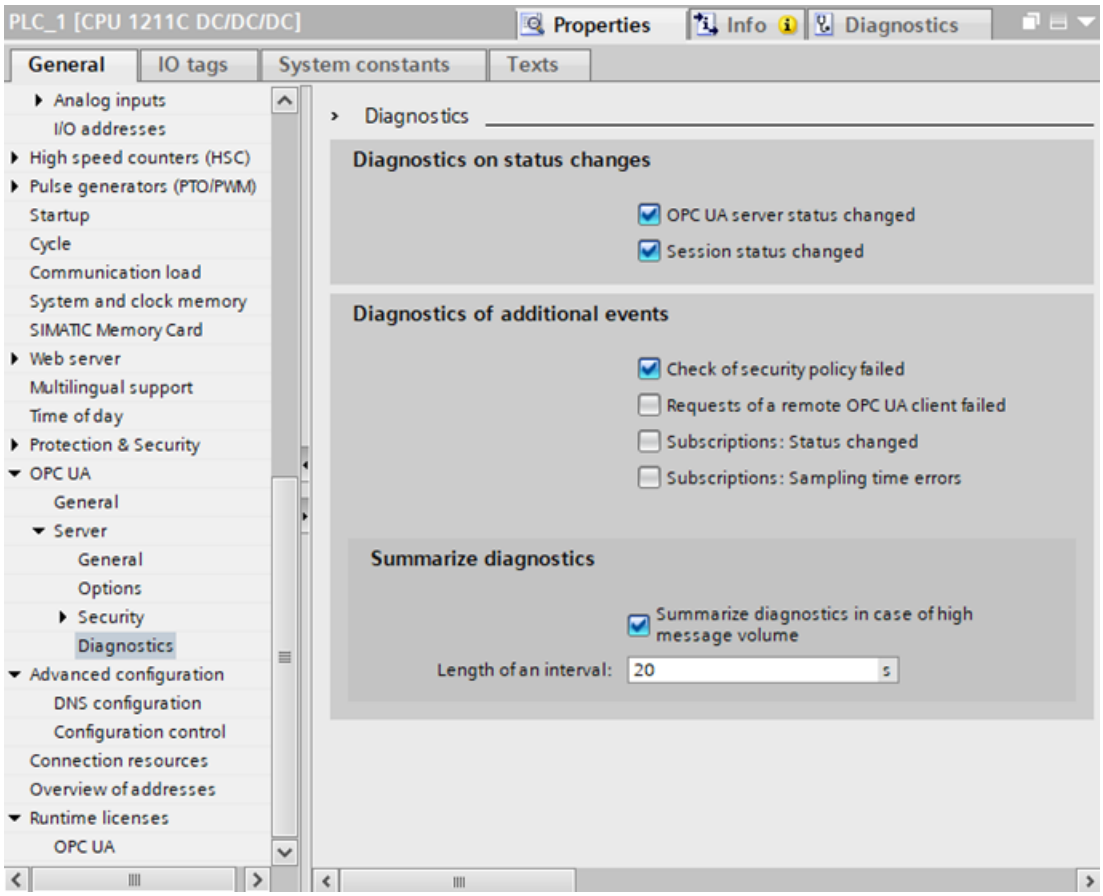
CPU-wide security messages are diagnostic messages generated in scenarios defined as CPU-wide critical by the security officer. Such messages are using a special Alarm-Domain. This allows HMIs to filter for them and to handle them differently. Such security messages are authentication failures that can occur when you try to log on to the CPU's Web- or the OPC UA -Server. There is a configuration dialog in TIA-Portal beneath the item "Protection & Security".



Security of OPC UA messages

The OPC UA server generates messages from OPC UA concerning server security and uses the standard alarm domain or checks during certificate verification.

Enable or disable the "Check of security policy failed" option in the TIA-Portal property view, as shown below.



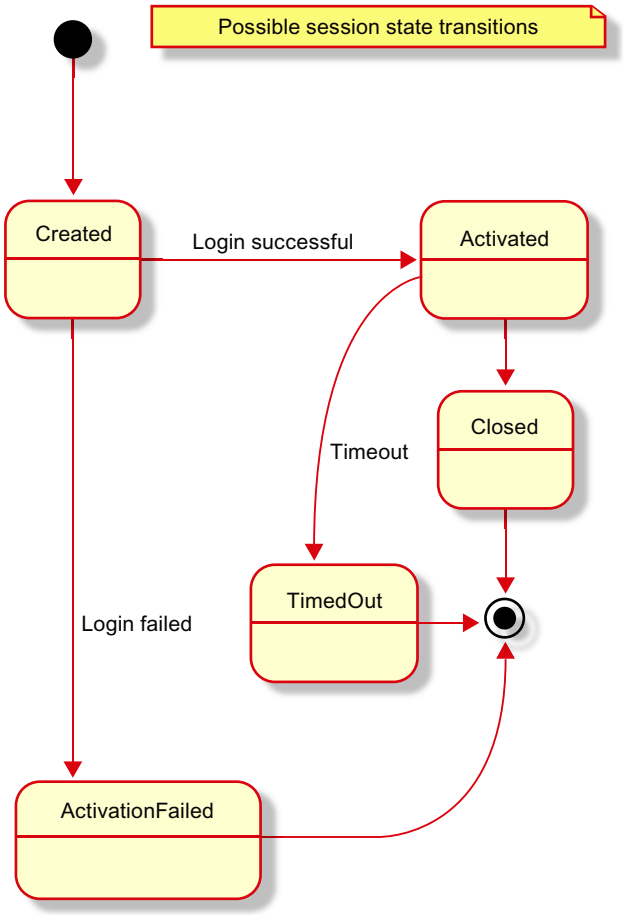
OPC UA server connection information

With the OPC UA diagnostics buffer, you can see the status of clients using the OPC UA server. For example, the diagnostics buffer shows the following information:

- When a client connects to your OPC UA server
- When the client disconnects from your OPC UA server

The server writes a diagnostic message to the diagnostics buffer when the state of a session changes. The possible session state transitions are:

- Created
- Activated
- Closed
- TimedOut
- ActivationFailed



The following use cases are implemented:

Table 12-77 Implemented use cases for OPC UA Server security activated

User action	Expected behavior	Security policies
Starting the OPC UA Server (for example, power cycle)	The S7-1200 CPU adds a diagnostic message with lowest security policy (Page 726) to the diagnostics buffer.	None, Basic128Rsa15, Basic256, Basic256Sha256,

Table 12-78 Implemented use cases for OPC UA session state changed

Precondition	User action	Expected behavior	States
OPC UA Server running, no client connected	Client connects to OPC UA Server and passes correct credentials	The S7-1200 CPU generates a diagnostic message showing the state change.	Created, Activated
OPC UA Server running, no client connected	Client connects to OPC UA Server and passes wrong credentials	The S7-1200 CPU generates a diagnostic message showing the state change.	Created, Activation failed
OPC UA Server running, Client is connected	Client closes session correctly	The S7-1200 CPU generates a diagnostic message showing the state change.	Closed
OPC UA Server running, Client is connected	Client sends no more messages to the server until session times out	The S7-1200 CPU generates a diagnostic message showing the state change.	TimedOut

OPC UA Server started/stopped

Use the OPC UA diagnostics buffer to see the global status of the OPC UA server. Diagnostic buffer messages show when the OPC UA server starts and stops. You can also see additional information, such as if the generic interface is on, or how many server interfaces or namespaces are active.

The OPC UA server can be in any of the following states:

- Running
- Failed
- NoConfiguration
- Suspended
- Shutdown
- Test
- CommunicationFault
- Unknown
- Starting
- Restarting

State change reasons: download/power cycle, instruction called by user program, remote request. The possible server-state transitions are shown below.

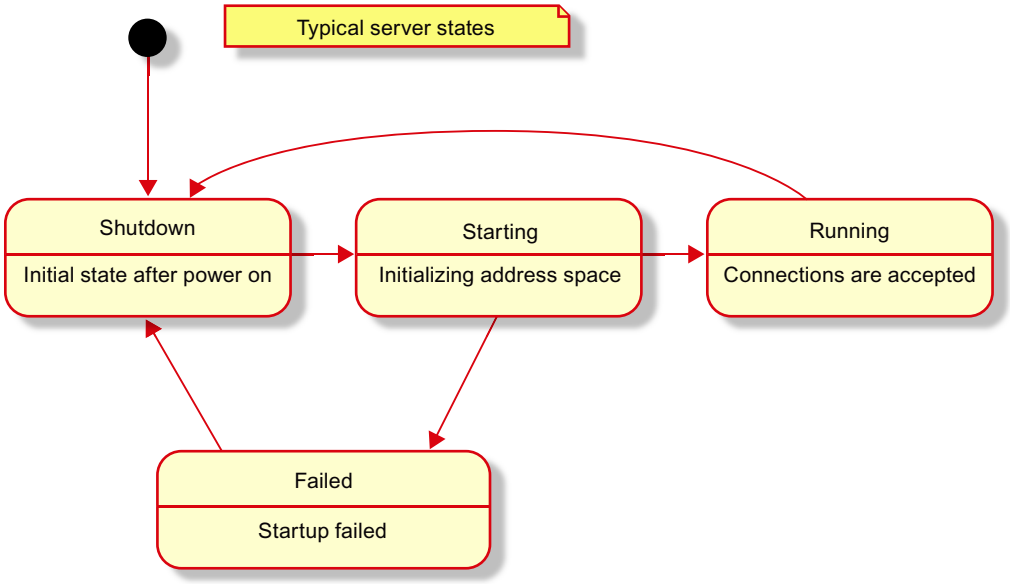


Table 12-79 Implemented use cases for OPC UA session state changed

Precondition	User action	Expected behavior	States
OPC UA Server running	HW download with activated OPC UA Server	The S7-1200 CPU generates a diagnostic message showing the state change. Reason: Download / Power Cycle	Shutdown, Starting, Running
OPC UA Server stopped	HW download with activated OPC UA Server	The S7-1200 CPU generates a diagnostic message showing the state change.	Created, Activated
OPC UA Server running	HW download with disabled OPC UA Server	The S7-1200 CPU generates a diagnostic message showing the state change.	Created, Activation failed
OPC UA Server running	HW download with activated OPC UA Server and too large type dictionary (too many structures)	The S7-1200 CPU generates a diagnostic message showing the state change.	Closed
OPC UA Server stopped	HW download with activated OPC UA Server and too large type dictionary	The S7-1200 CPU generates a diagnostic message showing the state change.	TimedOut

NOTE

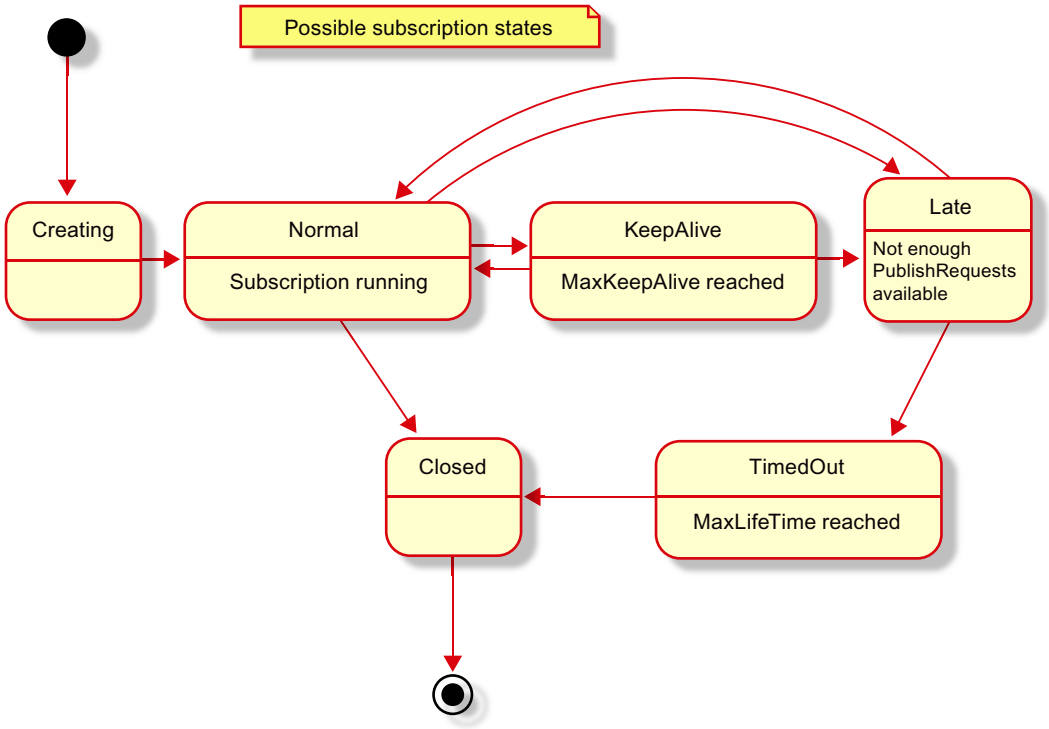
Software download

A software download also results in a OPC UA Server restart.

OPC UA session/subscription timeout

You can see when an OPC UA session or subscription has timed out and which sessions or subscriptions are still active.
When you change the state of an OPC UA session or subscription, the server writes information about the state change to the OPC UA diagnostics buffer. The possible OPC UA subscription states are as follows:

- Created
- Closed
- Normal
- Late
- KeepAlive
- TimedOut



A running subscription often changes between the states "Normal" and "KeepAlive" (when the monitored values changes only occasionally). There are no messages triggered for the "KeepAlive" state. The following use cases are implemented:

Table 12-80 Implemented use cases for OPC UA Server security activated

User action	Expected behavior	Security policies
OPC UA Server was started (for example, power cycle)	The S7-1200 CPU adds a diagnostic message with lowest security policy (Page 726) to the diagnostics buffer.	None, Basic128Rsa15, Basic256, Basic256Sha256,

12.12.4.3 OPC UA Wrong usage

The OPC UA server notifies you when a "wrong usage" occurs.

A "wrong usage" occurs when a client requests data or tries to use a function in a way not intended. Sending an invalid request causes the server to display a "wrong usage" diagnostic message.

Requesting an invalid NodeID causes the "wrong usage" diagnostic message to display. You can identify an invalid NodeID by browsing.

The "wrong usage" diagnostic message does not display during the following events:

- A client tries to read optional attributes
- A client exceeds subscriptions
- A client exceeds the server's session limits

Note: The namespace "http://opcfoundation.org/UA/" (ns=0) is a special namespace handled by the OPC Foundation (or the SDK) and diagnostics functions are limited. Not every "wrong usage" in this namespace triggers a message (for example, registering an unknown node)

The server writes the diagnostic message "OPC UA Server: Wrong usage of service <Service-Name> in session ID <Session-ID>" to the diagnostics buffer when it detects the "wrong usage" of a service. It only considers services that the S7-1200 OPC UA server supports:

- FindServers
- GetEndpoints
- FindServersOnNetwork
- CreateSession
- ActivateSession
- CloseSession
- Cancel
- Browse
- BrowseNext
- TranslateBrowsePathsToNodeIds
- RegisterNodes
- UnregisterNodes
- Write
- Read
- Call
- CreateMonitoredItems
- ModifyMonitoredItems
- DeleteMonitoredItems
- SetMonitoringMode
- SetTriggering
- CreateSubscription
- ModifySubscription
- DeleteSubscription
- Publish
- Republish
- SetPublishingMode

- OpenSecureChannel
- CloseSecureChannel

12.12.4.4 Summary messages for OPC UA

The following is an example of a "wrong usage" OPC UA Diagnostics buffer message:

Table 12-81 Summary of messages for OPC UA from Wrong usage of service

Message	Single Event	Summary Event
OPC UA Wrong Usage		
Example	OPC UA Server: Wrong usage of service Read in session ID 12345678	OPC UA Server: Wrong usage of a service. – Summary Message. - Summary Message for 3 occurrences during the last 20 second(s)

12.12.5 OPC UA Method calls

Providing user programs for server methods

You can provide OPC UA methods through the user program on the OPC UA server of an S7-1200 CPU.

Using OPC UA methods, you can trigger specific actions on the controller and transfer data consistently.

For example, OPC UA methods can use an OPC UA client to process a manufacturing job with the method call of the S7-1200.

OPC UA methods, an implementation of "Remote Procedure Calls", provide an efficient mechanism for interactions between different communication nodes. The mechanism provides both job confirmation and feedback values, eliminating the need to program handshaking mechanisms.

How does an OPC UA method work?

An OPC UA method in principle operates like a know-how protected function block that you call during runtime.

The OPC UA client only "sees" defined inputs and outputs. The content of the function block (the method or algorithm) remains hidden to the external OPC UA client. The OPC UA client receives feedback on successful execution and values returned by the function block (method), or an error message if execution is not successful.

As the programmer, you have full control over and responsibility for the program context in which the OPC UA method runs.

Rules for programming a method and runtime behavior

- Make sure that the values returned by the OPC UA method are consistent with the input values provided by the OPC UA client.
- Follow the rules on assigning name and the structure of parameters, and the permitted data types (see description of the OPC UA server instructions).
- Behavior during runtime: The OPC UA server accepts one call per instance. The method instance is not available for other OPC UA clients until the call is complete or has timed out. The instance times out when you reach the maximum amount of time allowed for establishing a connection to the server.

Implementing a server method

Implementing a server method involves the following tasks:

- Defining optional input and output parameters for the server method
- Querying the server method call with OPC_UA_ServerMethodPre
- Writing the server method
- Responding to the server method with the OPC_UA_ServerMethodPost

Defining optional input and output parameters for the server method

An OPC UA method can optionally define input or output parameters. Neither type of parameter is required. The OPC UA client supplies input parameters to the OPC UA method at runtime. The OPC UA method returns output parameters to the OPC UA client at runtime, when the method completes.

Follow these steps to define OPC UA method input parameters:

1. Within the Static section of the FB interface, define a struct named UAMethod_InParameters. Mark this struct as “Accessible from HMI/OPC UA/Web API” and “Writable from HMI/OPC UA/Web API”.
2. Within this struct, define the OPC UA method input parameters. The input parameters can have any valid name. The data types for an OPC UA method input parameter can be scalar types (Int, Real, etc.), structured data types, or arrays.

Follow these steps to define OPC UA method output parameters:

1. Within the Static section of the FB interface, define a struct named UAMethod_OutParameters. Mark this struct as “Accessible from HMI/OPC UA/Web API”.
2. Within this struct, define the OPC UA method output parameters. The output parameters can have any valid name. The data types for an OPC UA method output parameter can be scalar types (Int, Real, etc.), structured data types, or arrays

The following is an example of user-defined input and output parameters for an OPC UA method:

		Name	Data type	Accessible from HMI/OPC UA/Web API	Writable from HMI/OPC UA/Web API
7		Static		☐	☐
8		UAMethod_InParameters	Struct	☑	☑
9		a	Int	☑	☑
10		b	Int	☑	☑
11		UAMethod_OutParameters	Struct	☑	☑
12		SUM	Int	☑	☑

Querying the server method call with OPC_UA_ServerMethodPre

Call the "OPC_UA_ServerMethodPre" instruction in your user program from your server method.

This instruction asks the OPC UA server of the S7-1200 CPU whether the server method was called from an OPC UA client.

Once an OPC UA client calls the server method, the server method receives any input parameters from the OPC UA client.

Writing the server method

In the section of the server method between the calls to OPC_UA_ServerMethodPre and OPC_UA_ServerMethodPost, you provide the actual user program. You have the same options as in any other user program (for example, access to other function blocks or global data blocks). If the server method uses input parameters, these parameters are available to you. The server method must only execute this section if an OPC UA client has called the server method and the server method has called OPC_UA_ServerMethodPre.

After successful execution of the method, set the output parameters of the server method (if the method has output parameters.)

Responding to the server method with the OPC_UA_ServerMethodPost

To complete the server method, call the "OPC_UA_ServerMethodPost" instruction.
Use the parameters to notify the "OPC_UA_ServerMethodPost" instruction of the processing status of the user program.
Once the user program successfully executes, the relevant parameters notify the OPC UA server. The OPC UA server then sends the output parameters of the server method to the OPC UA client.

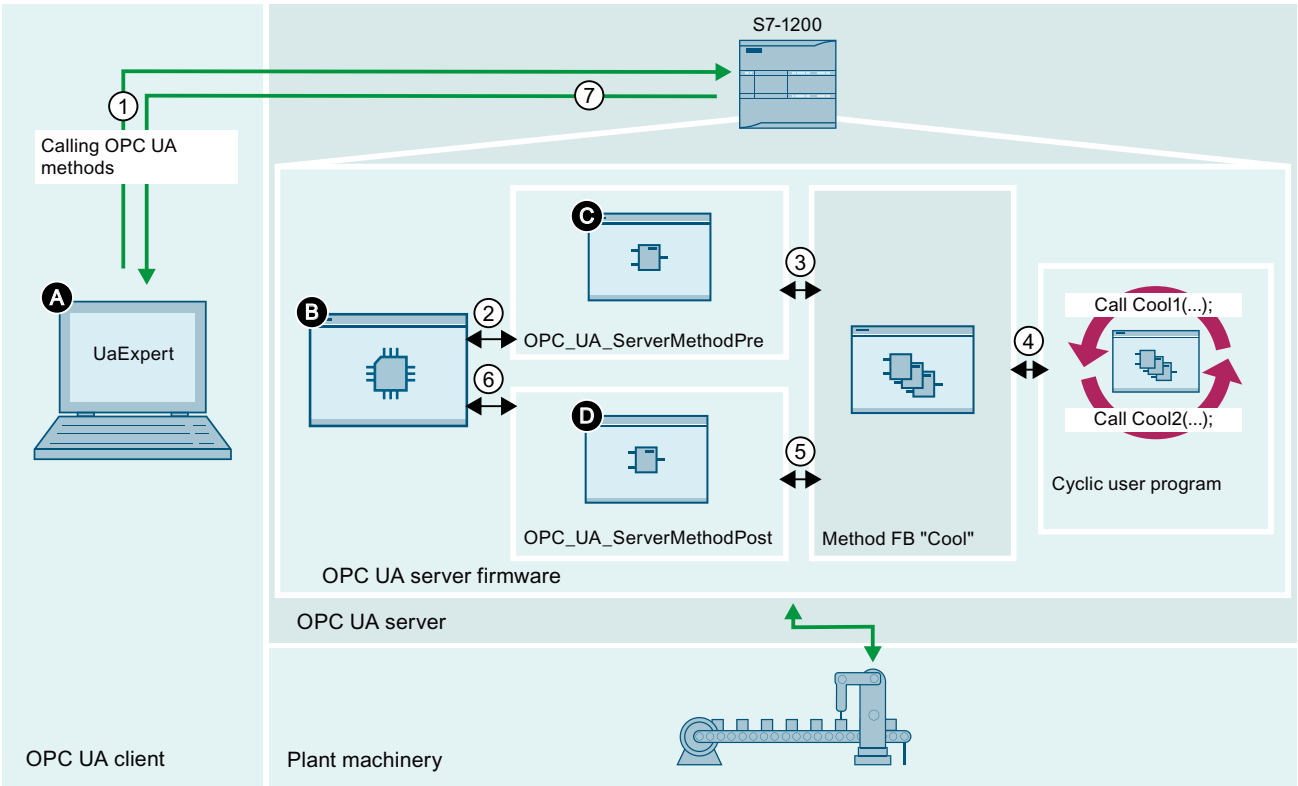
Information about server methods

Always use the "OPC_UA_ServerMethodPre" and the "OPC_UA_ServerMethodPost" as a pair when writing an OPC UA method. OPC UA methods will not function unless you add both methods.

For a detailed description of the "OPC_UA_ServerMethodPre" and "OPC_UA_ServerMethodPost" visit the TIA Portal Information system.

Integrating the server method

The diagram below shows how an OPC UA client calls the server method "Cool":



A The OPC UA client calls the OPC UA server method and manages its "Done" status.

① The OPC UA method calls between the OPC UA client and the OPC UA server method are asynchronous.

B The OPC UA server firmware waits for OPC UA client calls, manages calls in the queue, and forwards "Done" information from the cyclic user program to the OPC UA client.

② This call transfers data from the OPC UA server to the instance of the user program, method FB "Cool".

C The instruction, OPC_UA_ServerMethodPre, asks the OPC UA server of the CPU if the OPC UA server method has been called by an OPC UA client. Once an OPC UA client calls the OPC UA server method, the OPC_UA_ServerMethodPre instruction sets a flag to indicate the OPC UA client is calling the OPC UA server method. If there are input parameters from the OPC UA client, the OPC_UA_ServerMethodPre instruction provides them to the method FB "Cool". The user program, method FB "Cool", must first call the OPC_UA_ServerMethodPre instruction.

③ Method FB "Cool" performs a synchronous call of the OPC_UA_ServerMethodPre instruction. The OPC_UA_ServerMethodPre instruction is a multi-instance static variable that stores input data from the OPC UA client. The return value from the synchronous call indicates whether a client did or did not call the OPC UA server method.

④ The cyclic user program asynchronously calls the method FB "Cool" with the required instance parameters.

⑤ This synchronous call checks the status, complete or "busy," of the OPC UA server method.

D The OPC_UA_ServerMethodPost, once the OPC UA server method is complete, forwards the output data of the method instance to the OPC UA server. The OPC_UA_ServerMethodPost also notifies the method instance and the OPC UA server that the method is complete.

⑥ This call transfers data to the OPC UA server from the instance of the user program, method FB "Cool".

⑦ The OPC UA server firmware sends information back to the OPC UA client.

How this example works

The CPU executes the instance "Cool1" of the server method FB "Cool" in the cyclic user program ④.

The instance "Cool1" calls the instruction "OPC_UA_ServerMethodPre" to query ③ whether an OPC UA client has called the server method FB "Cool" ①.

- If the server method FB "Cool" has not called OPC_UA_ServerMethodPre, program execution returns directly to the cyclic user program over ③ and ④. The CPU resumes the cyclic user program after "Cool1".
- If the server method FB "Cool" has already called OPC_UA_ServerMethodPre, OPC_UA_ServerMethodPre returns information directly to the server method FB "Cool" over ③. The method FB "Cool" now executes and accesses data from the plant machinery.

Once the OPC UA server method is complete, the server method FB "Cool" then calls the instruction "OPC_UA_ServerMethodPost" ⑤ to notify the firmware (B) that the instruction has executed ⑥.The firmware returns this information over ⑦ to the calling OPC UA client (A). The CPU resumes the cyclic user program after "Cool1".

12.12.5.1 Boundary conditions for using server methods

If you provide server methods, assign the data types as shown below (SIMATIC data type - OPC UA data type). Do not use other assignments.
STEP 7 does not prevent incorrect assignments. You are responsible for making compliant selections and data type assignments.
You can also use the listed data types, for example, as elements of structures/arrays/UDTs for input and output parameters of self-created server methods (UAMethod_InParameters and UAMethod_OutParameters).

SIMATIC data type	OPC UA data type
BOOL	Boolean
SINT	SByte
INT	INT16
DINT	INT32
USINT	Byte
UINT	UINT16
UDINT	UINT32
REAL	Float
LREAL	Double
WSTRING	String
DINT	Enumeration (Encoding Int32) and all derived data types

Web server

13

The Web server for the S7-1200 provides Web page access to data about your CPU and process data.

You can access the S7-1200 Web pages from a PC or from a mobile device. For devices with small screens, the Web server supports a collection of basic pages (Page 769).

You use a Web browser to access the IP address of the S7-1200 CPU or the IP address of a Web server-enabled CP (communications processor) module (Page 766) in the local rack with the CPU to establish the connection. The S7-1200 supports multiple concurrent connections.

NOTE

Web server multiple concurrent connections

The S7-1200 Web server allows for 30 concurrent connections (assuming that you have enough dynamic connections). Open browser instances can consume between 2 to 8 connections each. The Web server allows up to 7 logged-in users but Siemens recommends that you keep the number of concurrent users as low as possible. An average of 7 users at a time is typically okay under average workloads.

Standard Web pages

The S7-1200 includes standard Web pages (Page 768) that you can access from the Web browser of your PC (Page 764) or from a mobile device (Page 765):

- Introduction (Page 772) - entry point to the standard Web pages
- Start Page (Page 773) - general information about the CPU
- Diagnostics (Page 773) - detailed information about the CPU including serial, order, and version numbers, program protection, and memory usage
- Diagnostics Buffer (Page 776) - the diagnostics buffer
- Module Information (Page 777)- information about the local and remote modules and the ability to update firmware for modules
- Communication (Page 781) - information about the network addresses, physical properties of the communication interfaces, statistics, parameters, as well as a connection summary and diagnostic information
- Tag status (Page 784) - CPU variables and I/O, accessible by address or PLC tag name
- Watch tables (Page 786) - watch tables that you configured in STEP 7
- Online backup (Page 787) - ability to backup an online CPU or restore a previously-made online backup

- Data Logs (Page 789)- ability to view a list of all data logs on the PLC, download a data log from the PLC to your computer, delete a data log from the PLC, and retrieve and clear a data log from the PLC
- User Files (Page 792)- ability to view a list of user files on the PLC, download a user file from the PLC to your computer, upload a user file from your computer to the PLC, and delete a user file on your PLC
- User-defined pages (Page 796)- create user-defined Web pages to access CPU data
- File Browser (Page 794) - browser for files stored internally in the CPU or on a memory card, for example, data logs and recipes
- Login (Page 769) - log in as a different user, or log out.

These pages are included in the S7-1200 CPU firmware, and are available in English, German, French, Spanish, Italian, and Simplified Chinese. Additional configuration is needed in TIA Portal to view PLC diagnostic messages (chapter 15). All pages except for the Introduction and Start page require additional user privileges (Page 757) that you configure in STEP 7 to view the page.

User-defined Web pages

The S7-1200 also provides support for you to create user-defined Web pages that can access CPU data. You can develop these pages with the HTML authoring software of your choice, and include pre-defined "AWP" (Automation Web Programming) commands in your HTML code to access CPU data. Refer to the User-defined Web pages (Page 796) chapter for specific information on the development of user-defined Web pages, and the associated configuration and programming in STEP 7.

You can access the user-defined pages from either a PC or mobile device from the standard or basic Web pages. You can also configure one of your user-defined Web pages to be the entry page (Page 812) for the Web server.

Web API

The S7-1200 CPU also provides a Web API (Page 833) that is an interface for you to read and write process data.

Web browser requirement

Siemens has tested the Web server standard pages and verifies support of the following Web browsers:

- Microsoft Edge V116.0
- Mozilla Firefox V116.0.3
- Opera V102.0
- Google Chrome V116.0
- Android browser V7.x, 8.x, 10.x, 11.x, and 12.x
- Mobile Chrome for Android V7.x, 8.x, 10.x, 11.x, and 12.x
- Mobile Safari and Chrome for iOS V12.5.1 and V16.5

When using the HTML Browser control in a WinCC project, the Web server supports the following Siemens HMI Panels for the standard pages:

- Basic Panels
  - Gen 2 KTP400 to KTP1200
- Comfort Panels
  - TP700 to TP2200
  - KP400 to KP1500
  - KTP400
  - TP700 Comfort Outdoor
- Mobile Panels
  - Gen 2 KTP700[F], KTP900[F]
- Unified Comfort Panels
  - Basic Panel (2nd Gen)
  - Mobile Panel (2nd Gen)

For browser-related restrictions that can interfere with the display of standard or user-defined Web pages, see the Constraints (Page 834) section.

Web server performance

Many factors can affect the performance of the Web server. The S7-1200 CPU and the programming device must share time with other tasks that consume resources and processing time. If you have poor performance with the Web server, try these adjustments to improve Web server performance:

- Increase the communication load (Page 81) on the PLC from 20% to 50%.
- Configure a minimum scan time (Page 81). Setting a minimum scan time provides increased communication time between the S7-1200 CPU and the programming device.
- Increase the "Update interval" time in TIA Portal from the default 10s.
- Use the S7-1200 CPU's Ethernet interface instead of a CP module (Page 766) to access the Web server.

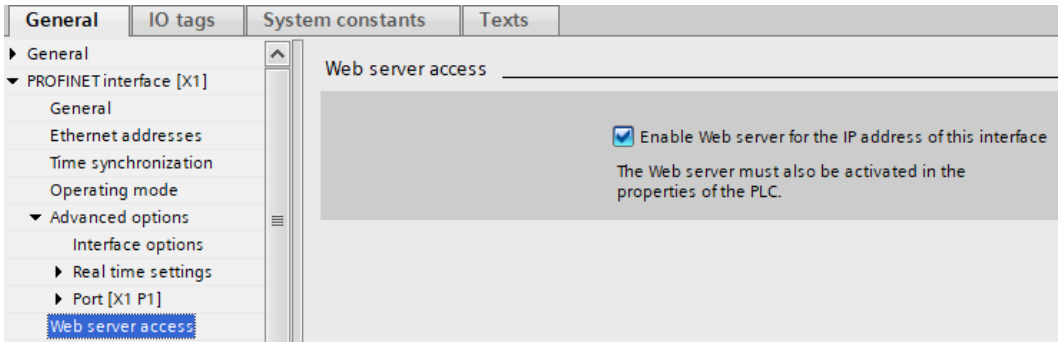
13.1 Enabling the Web server

You enable the Web server in STEP 7 from Device Configuration for the CPU to which you intend to connect.

To enable the Web server, follow these steps:

1. Select the CPU in the Device Configuration view.
2. In the inspector window, select "Web server" from the CPU properties.
3. Select the check box for "Activate web server on all modules of this device".
4. For increased security, ensure that "Permit access only with HTTPS" is selected to require secure access to the Web server over TLS (Page 557). To use HTTPS for secure communication, you must configure a Web server certificate. Configure Web server certificates from Device configuration for the CPU. From the CPU properties, select Web server > Security to configure Web server certificates (Page 529).
5. If you select "Enable automatic update" for "Automatic update", standard Web pages will refresh by default every ten seconds. You can also enter a custom refresh time period in seconds for the "Update interval" field.

6. Depending upon the type of interface access used, you must ensure that Web server access is enabled for that interface:
   - PLC PROFINET: Ensure that the "Enable Web server for the IP address of this interface" property is enabled on the PLC for the Web server to be accessible through the PLC PROFINET interface.
   - WanCP PROFINET port: If you are using a WanCP device, ensure that the property "Enable Web server for the IP address of this interface" property is checked in order to have the Web server accessible through the particular WanCP PROFINET port.



WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server or OPC UA users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

- Enable Access control (Page 147) under "Protection & Security > Access control".
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Enable the setting "Only allow secure PG/PC and HMI communication" under "Protection & Security > Connection mechanisms".
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC from a location outside your protected network.
- Enable access to the Web server only with the HTTPS protocol.
- Perform error-checking and range-checking on your variables in your program logic because Web server or OPC UA users can change PLC variables to invalid values.
- For the OPC UA server: In your STEP 7 Device configuration, navigate to "Properties > OPC UA > Server > Security" and deselect "No security" in "Security policies available on the server for the secure channel".

Disruption of process operations can result in death, severe personal injury, and/or property damage.

After you download the device configuration, you can use the standard Web pages to access the Introduction and Start page of the CPU. To access additional pages, you must configure one or more Web server users (Page 757).

If you created and enabled user-defined Web pages (Page 796), you can access them from the standard or basic Web page navigation menu.

NOTE

Device exchange: Replacing a V3.0 CPU with a V4.x CPU

If you replace an existing V3.0 CPU with a V4.x CPU (Page 1285) and convert your V3.0 project to a V4.x project, note that STEP 7 and the V4.x CPU retain the Web server settings for

- "Activate web server on all modules of this device"
- "Permit access only with HTTPS"

NOTE

If a "Download in RUN" (Page 1072) is in progress, standard and user-defined Web pages do not update data values or permit you to write data values until the download is complete. The Web server discards any attempts to write data values while a download is in progress.

13.2 Web server user management

13.2.1 Assigning Web server user privileges for V4.7 configured CPUs

If the firmware version of the CPU in your STEP 7 project is V4.7 or later, you can assign user privileges for accessing the CPU through the Web server with User Management & Access Control (UMAC) (Page 147).

Assign roles and rights by doing the following:

1. Select "Security Settings" in the STEP 7 project tree.
2. Double-click "Users and roles".

From Users and Roles, you can add a user, create a new role, assign rights to the new role, and assign the role to a user.

To add a user, do the following:

1. Select the "Users" tab on the top, right side of the window.
2. Double-click "add a new user", then select "Add new local user" from the pop-up.
3. Enter the User name and Password. Runtime timeout defaults to 30 minutes but can be configured by entering the time manually in the field or using the arrows to change the time by one minute increments . The UM domain ID and Comment fields are optional.

To create a new role, follow these steps:

1. Select the "Roles" tab from the top, right side of the window.
2. In the "Roles" section, double-click "Add new role".
3. Enter the Role Name, Description, Runtime timeout, and optional Comment.

Assign rights to the role in the following way:

1. Click the "Runtime rights" tab in the bottom window.
2. Select your PLC from the "Runtime rights" dropdown at left. This will populate all of the Function rights you can assign for that PLC.
3. Select the check boxes that you wish to assign for this role.

To assign a role to a user, do the following:

1. Select the "Users" tab on the top, right side of the window.
2. Click the check box and highlight the name of the user you want to assign with a role.
3. Click the "Assigned roles" tab in the bottom window.
4. Select the check box next to the role(s) you want to assign to the user.

After you download the configuration to the CPU, only authorized users can access Web server functions for which they have privileges.

Web server access levels

The default "Anonymous" user is disabled for security. You can enable the Anonymous user by selecting the checkbox and agreeing to the security warning. For more information on working with the anonymous user, see "Managing users and roles > Activating or deactivating anonymous user" in the TIA Portal Information System.

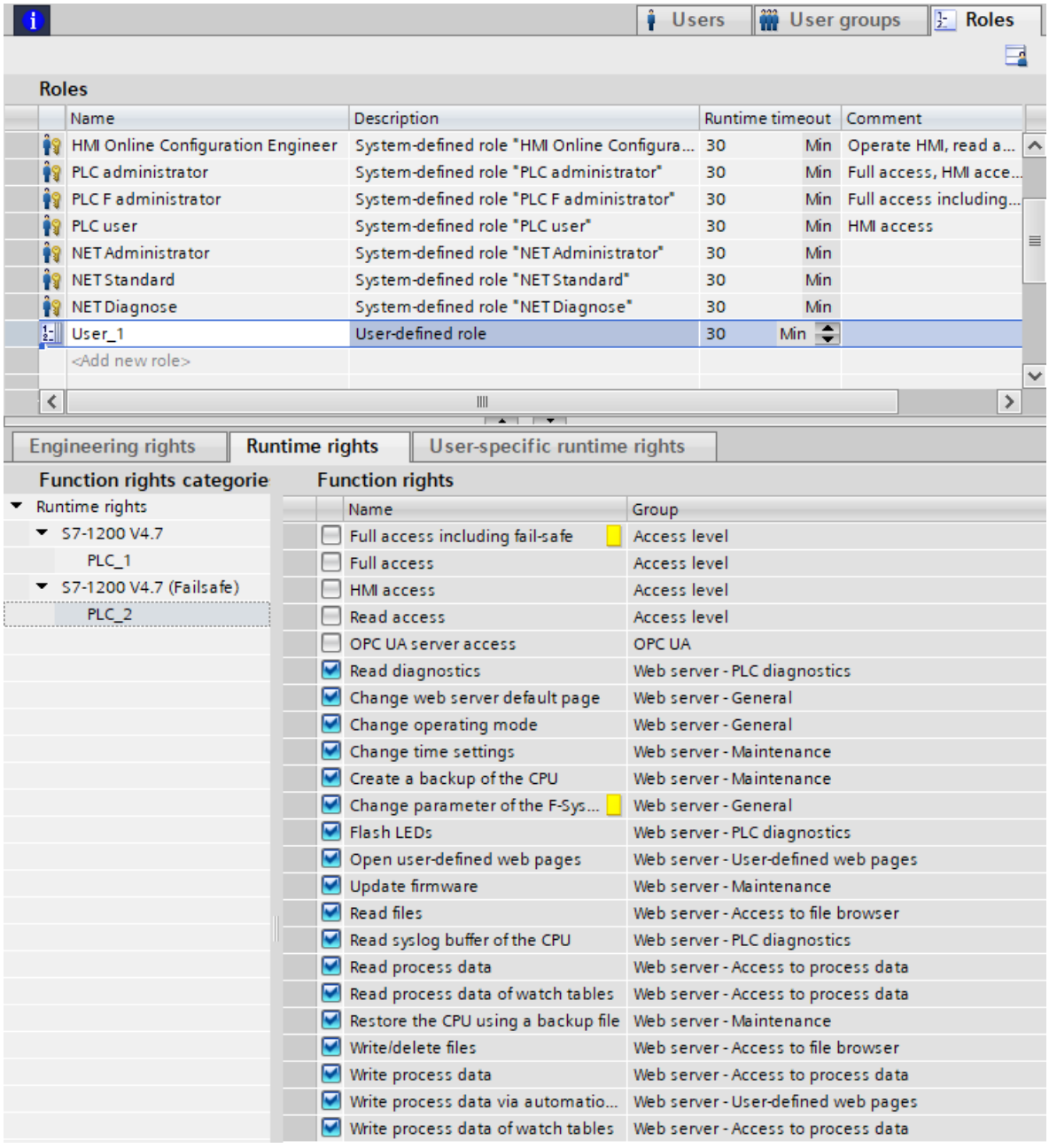
Assignable user privileges are as follows:

- Read diagnostics
- Change web server default page
- Change operating mode
- Change time settings
- Create a backup of the CPU
- Change parameter of the F-System (F-Admin)[1]
- Flash LEDs
- Open user-defined web pages
- Update firmware
- Read files
- Read syslog buffer on the CPU
- Read process data
- Read process data of watch tables
- Restore the CPU using a backup file
- Write/delete files
- Write process data
- Write process data via automation webpage programming (AWP) command
- Write process data of watch tables

[1] Available for Failsafe CPUs only.

Note that If you have set a user-defined Web page to be the entry page (Page 812) for the Web server, the user must have the "Open user-defined web pages" privilege.

See below an example of user roles and rights configured for a Web server user in the STEP 7 project for an S7-1200 V4.7 Failsafe CPU:



WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server or OPC UA users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

- Enable Access control (Page 147) under "Protection & Security > Access contro.
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Enable the setting "Only allow secure PG/PC and HMI communication" under "Protection & Security > Connection mechanisms".
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC from a location outside your protected network.
- Enable access to the Web server only with the HTTPS protocol.
- Perform error-checking and range-checking on your variables in your program logic because Web server or OPC UA users can change PLC variables to invalid values.
- For the OPC UA server: In your STEP 7 Device configuration, navigate to "Properties > OPC UA > Server > Security" and deselect "No security" in "Security policies available on the server for the secure channel".

Disruption of process operations can result in death, severe personal injury, and/or property damage.

NOTE

Update password encryption for device exchange to V4.x

After a device exchange to V4.x, you must update the Web server user password encryption. From the CPU's device configuration in the TIA Portal, click the "Upgrade password encryption" button in the Web server user management.

13.2.2 Assigning Web server user privileges for CPU project configurations earlier than V4.7

User Management & Access Control (UMAC) is only available when the configured firmware version of the CPU in the project is V4.7 or later.

If you have a CPU configured in your STEP 7 project to use a firmware version earlier than V4.7, you assign Web server users with various privilege levels under "Properties > Web server > User management". Enter user names, access levels, and passwords for the user logins that you want to provide.

After you download the configuration to the CPU, only authorized users can access Web server functions for which they have privileges.

Web server access levels

STEP 7 provides a default user named "Everybody" with no password. By default, this user has no additional privileges and can only view the Start (Page 773) and Introduction (Page 772)

standard Web pages. You can, however, configure additional privileges for the "Everybody" user as well as other users:

- Query diagnostics
- Read tags
- Write tags
- Read tag status
- Write tag status
- Open user-defined web pages
- Write in user-defined web pages
- Read files
- Write/delete files
- Change operating mode
- Flash LEDs
- Perform a firmware update
- Backup CPU
- Restore CPU
- Change system parameter
- Change application parameter

If you have set a user-defined Web page to be the entry page (Page 812) for the Web server, the Everybody user must have the "Open user-defined web pages" privilege.

WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server or OPC UA users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

- Enable Access control (Page 147) under "Protection & Security > Access control".
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Enable the setting "Only allow secure PG/PC and HMI communication" under "Protection & Security > Connection mechanisms".
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC from a location outside your protected network.
- Enable access to the Web server only with the HTTPS protocol.
- Perform error-checking and range-checking on your variables in your program logic because Web server or OPC UA users can change PLC variables to invalid values.
- For the OPC UA server: In your STEP 7 Device configuration, navigate to "Properties > OPC UA > Server > Security" and deselect "No security" in "Security policies available on the server for the secure channel".

Disruption of process operations can result in death, severe personal injury, and/or property damage.

NOTE

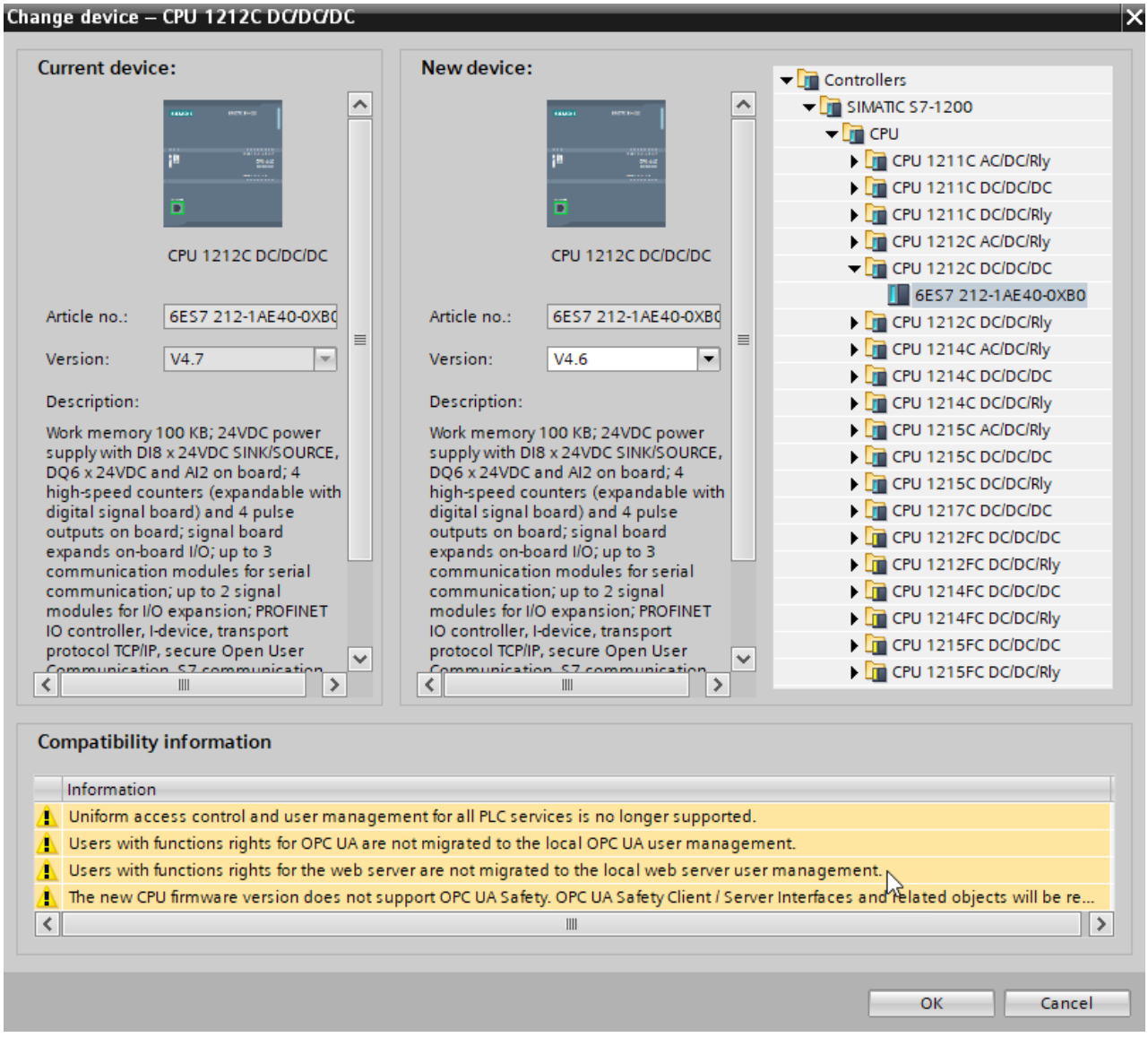
Update password encryption for device exchange to V4.x

After a device exchange (Page 1285) to V4.x, you must update the Web server user password encryption. From the CPU's device configuration in the TIA Portal, click the "Upgrade password encryption" button in the Web server user management.

13.2.3 User configuration compatibility

Upgrading configured firmware from an earlier version to V4.7

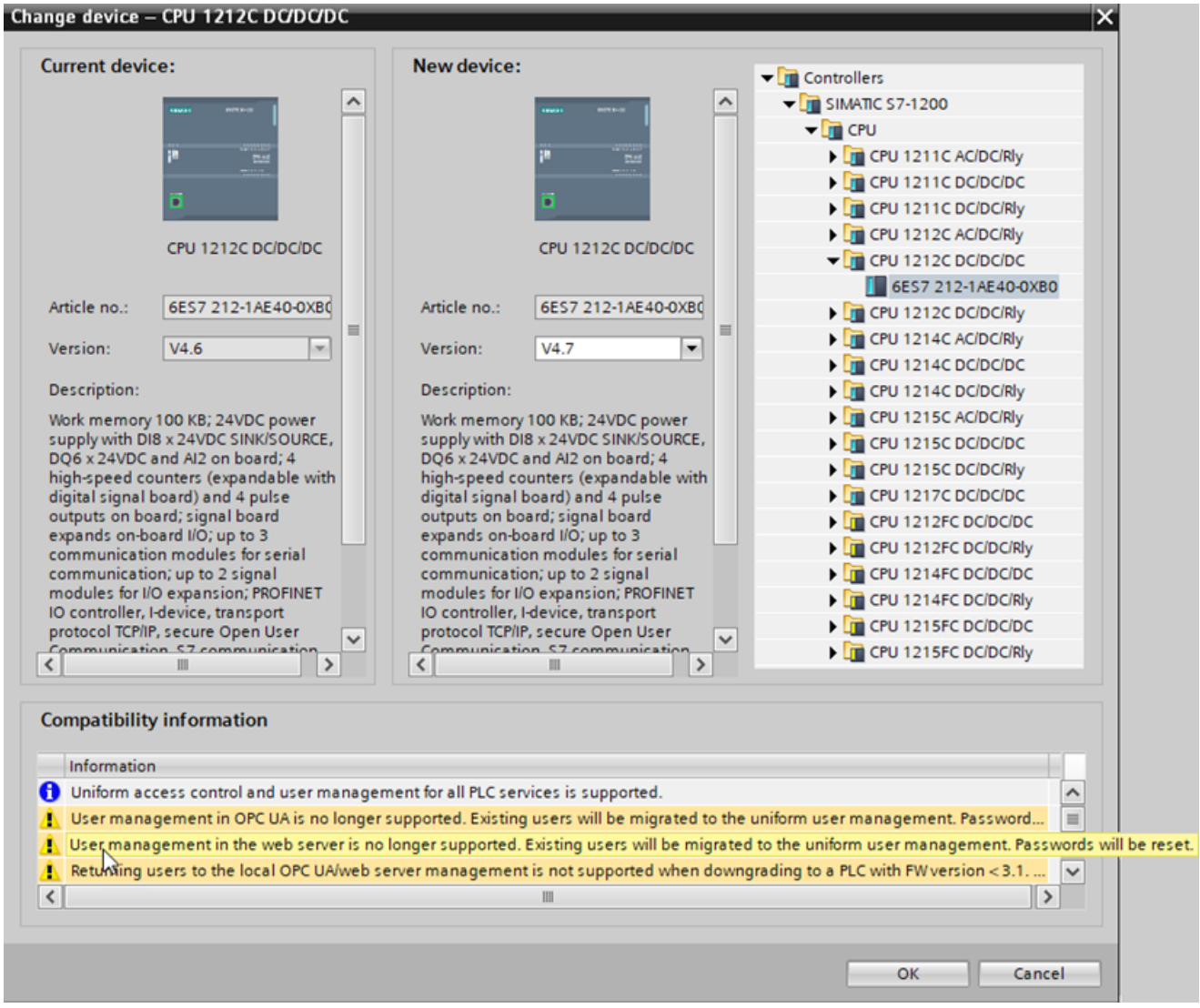
When you upgrade the configured firmware version in your STEP 7 project to V4.7, STEP 7 migrates users that you previously configured in "User management" to "Users and Roles". You reassign user passwords in the Project tree under "Security settings > Users and roles > Users."



For more information about Web server user privileges when upgrading firmware in the STEP 7 project, see "Editing devices and networks > Configuring devices and networks > Creating configurations > Configuring automation systems > Functional description of S7-1200 CPUs > Setting the operating behavior > Protection and Security > Settings for users and roles > Information about compatibility" in the TIA Portal Information System.

Downgrading configured firmware from V4.7 to an earlier version

When you downgrade the configured firmware version in your STEP 7 project from V4.7 to an earlier version, users configured in the Project tree under "Security settings > Users and roles > Users" will not be migrated. Users must be reconfigured in device "Properties > User management".



For more information about Web server user privileges when downgrading firmware in the STEP 7 project, see "Editing devices and networks > Configuring devices and networks > Creating configurations > Configuring automation systems > Functional description of

S7-1200 CPUs > Setting the operating behavior > Protection and Security > Settings for users and roles > Information about compatibility" in the TIA Portal Information System.

13.3 Accessing the Web pages from a PC

You can access the S7-1200 standard Web pages from a PC or from a mobile device through the IP address of the S7-1200 CPU or the IP address of any Web server-enabled CP (Page 766) in the local rack.

To access the S7-1200 standard Web pages from a PC, follow these steps:

1. Ensure that the S7-1200 and the PC are on a common Ethernet network or are connected directly to each other with a standard Ethernet cable.
2. Open a Web browser and enter the URL "https://ww.xx.yy.zz", where "ww.xx.yy.zz" corresponds to the IP address of the S7-1200 CPU or the IP address of a CP in the local rack.

The Web browser opens the Introduction standard Web page (Page 772) or the Default HTML page of your user-defined Web pages if you configured it to be the entry page (Page 812).

NOTE

Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC Web server from a location outside your protected network. Be aware also of any constraints (Page 834) that your Web environment or operating system might impose.

Accessing standard Web pages by entering the page URL

You can access a specific standard Web page from the URL of the page. To do so, enter the URL in the form "https://ww.xx.yy.zz/<page>.html", where "ww.xx.yy.zz" corresponds to the IP address of the S7-1200 CPU or the IP address of a CP in the local rack:

- https://ww.xx.yy.zz/login.html - page to log in (Page 769) if no user is currently logged in; otherwise, the page is blank
- https://ww.xx.yy.zz/start.html - start (Page 773) page with general information about the CPU
- https://ww.xx.yy.zz/identification.html - identifying information (Page 773) about the CPU including serial, order, and version numbers, now called the Diagnostics page
- https://ww.xx.yy.zz/diagnostic.html - the diagnostics buffer (Page 776)
- https://ww.xx.yy.zz/module.html - information about the modules in the local rack and the ability to update firmware (Page 777)
- https://ww.xx.yy.zz/communication.html - communication information (Page 781) about the network addresses, physical properties of the communication interfaces, and communication statistics
- https://ww.xx.yy.zz/variable.html - CPU variables (tags) and I/O (Page 784), accessible by address, PLC tag name, or data block tag name
- https://ww.xx.yy.zz/watch.html - watch tables (Page 786)
- https://ww.xx.yy.zz/datalogs.html - download, delete, or retrieve and clear Data Logs (Page 789)
- https://ww.xx.yy.zz/userfiles.html - User Files (Page 792) provides access to files on the SIMATIC memory card (external load memory)

- https://ww.xx.yy.zz/filebrowser.html - browser for accessing data log files or recipe files (Page 794) stored internally in the CPU or on a memory card
- https://ww.xx.yy.zz/index.html - introduction page (Page 772) to enter the standard Web pages

For example, if you enter "https://ww.xx.yy.zz/communication.html", the browser displays the communication page.

NOTE

Note that any standard Web page that is not listed specifically above (for example, the Online backup page (Page 787)) does not have a direct access URL.

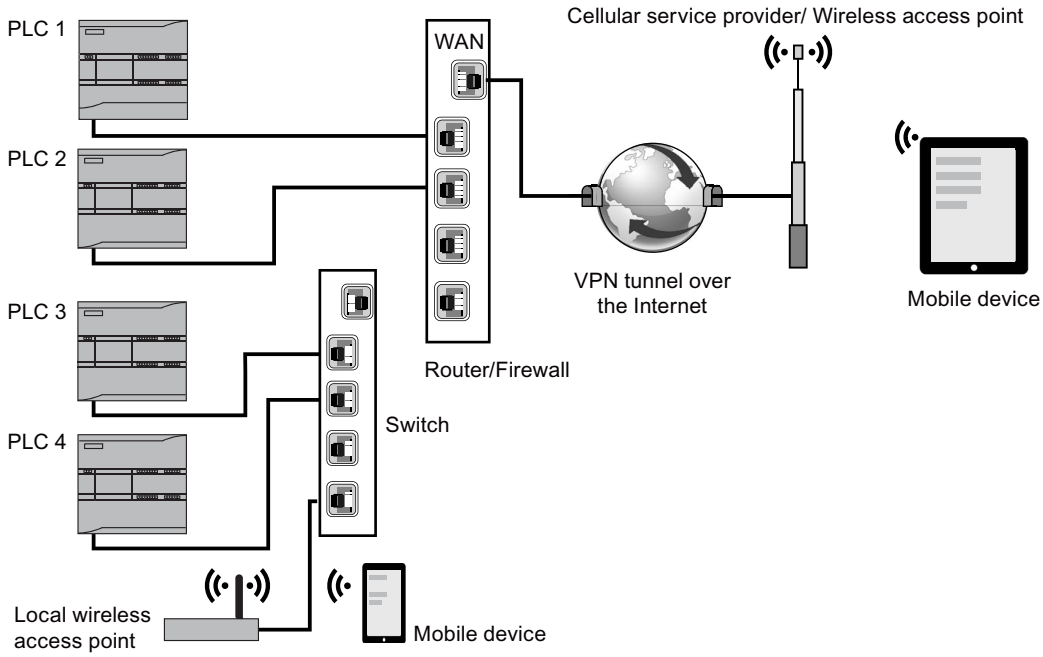
Secure access

Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC Web server from a location outside your protected network. Require and use https:// instead of http:// for secure access (Page 755) to the standard Web pages. When you connect to the S7-1200 with https://, the Web site encrypts the session with a digital certificate. The Web server transmits the data securely and it is not accessible for anyone to view. You typically get a security warning that you can confirm with "Yes" to proceed to the standard Web pages. To avoid the security warning with each secure access, you can import the Siemens software certificate to your Web browser (Page 767).

13.4 Accessing the Web pages from a mobile device

To access an S7-1200 from a mobile device, you must connect your PLC to a network that connects to the Internet or to a local wireless access point. Use a secure Virtual Private Network (VPN) to connect a mobile device to the S7-1200 PLC Web server. You can use port forwarding in the wireless router to map the IP address of the PLC to an address by which a mobile device can access it from the Internet. To configure port forwarding, follow the instructions for the software configuration of your router. You can connect as many PLCs and switching devices as your router supports.

Without port forwarding, you can connect to a PLC, but only locally within range of the wireless signal.



In this example, a mobile device that is within range of the local wireless access point can connect to PLC 3 and PLC 4 by their IP addresses. From the Internet outside the local wireless range, a mobile device can connect to PLC 1 and PLC 2 using the port forwarded address for each PLC.

To access the standard Web pages, you must have access to a cellular service or wireless access point. To access a PLC from the Internet, enter the port forwarded address in the Web browser of your mobile device to access the PLC, for example http://ww.xx.yy.zz:pppp or https://ww.xx.yy.zz:pppp, where ww.xx.yy.zz is the address of the router and pppp is the port assignment for a specific PLC.

For local access through a local wireless access point, enter the IP address of the S7-1200 CPU or a Web server-enabled CP (Page 766) in the local rack:

- http://ww.xx.yy.zz or https://ww.xx.yy.zz to access the standard Web pages (Page 768)
- http://ww.xx.yy.zz/basic or https://ww.xx.yy.zz/basic to access the basic Web pages (Page 769)

For increased security, configure the Web server to be accessible only by secure access (HTTPS) (Page 755).

13.5 Using a CP module to access Web pages

Regardless of whether you access the Web server from a PC or a mobile device, you can connect to standard Web pages through one of the following CP modules when you have configured it in STEP 7 and installed it in the local rack with the S7-1200 CPU:

- CP 1243-1
- CP 1243-7 LTE-EU
- CP 1243-7 LTE-US
- CP 1243-8 IRC

You use the Start standard Web page (Page 773) to access the Web pages through these CP modules. The Start page displays all configured and installed CP modules that you have in your local rack, but you can only access Web pages from the ones listed above.

NOTE

Access to standard Web pages when Web server-enabled CPs are in the local rack

You might observe delays up to one or two minutes when connecting to the S7-1200 standard Web pages when Web server-enabled CPs are in the local rack. If the pages do not appear to be available, or you get errors, just wait one or two minutes and refresh the page.

13.6 Web server security certificates

You can create certificates for the CPU in the device configuration of an S7-1200 CPU. This feature is available under the "Protection & Security > Certificate manager" general setting for the device.

You can create certificates for the Web server from "Web server > Security" in the device configuration for the CPU. Web server certificates are software downloaded, which enables you to use your own custom certificate.

Refer to the STEP 7 Information System for more information about certificates and also the topic Supported certificates (Page 529) in this document.

NOTE

S7-1200 certificate limit

The S7-1200 has a system certificate limit of 64.

All certificates count against this number (for example, Web server certificates, OPC UA certificates, and OUC certificates).

If the Web server certificate has been signed by a Certificate authority (CA) certificate and present in the TIA Portal, then 2 certificates are used by the Web server (one for the Web server certificate and one for its downloaded CA certificate).

If you have more than 64 certificates, the TIA Portal displays an error that states that you have exceeded the maximum number of 64 certificates. You must remove some certificates from the PLC configuration.

Working with certificates that are not self-signed

If you are not using self-signed certificates, use the "download certificate" link from the Introduction page (Page 772) to download the Siemens security certificate to your PC. The procedure for downloading and importing varies according to which Web browser you use. The "download certificate" link is not active when using self-signed certificates.

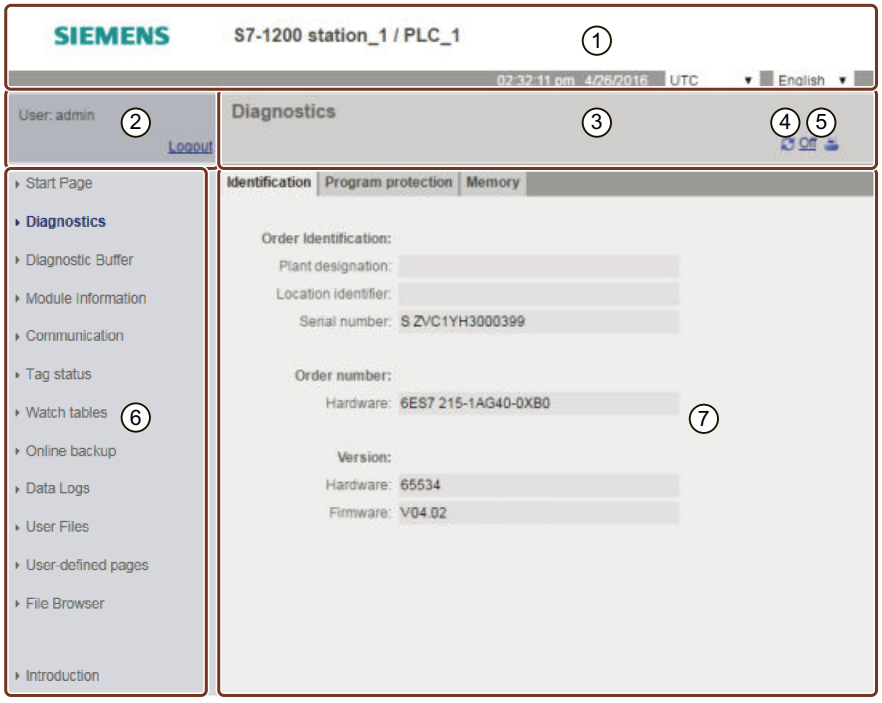
To import and install the Siemens certificate, follow the conventions of your Web browser.

After you install the Siemens security certificate "S7-1200 Controller Family" in the Internet options for your Web browser content, you do not have to verify a security prompt when you access the Web server with https:// ww.xx.yy.zz.

13.7 Standard Web pages

13.7.1 Layout of the standard Web pages

Each of the S7-1200 standard Web pages has a common layout with navigational links and page controls. Regardless of whether you are viewing the page on a PC or on a mobile device, each page has the same content area, but the layout and navigation controls vary based on the screen size and resolution of the device. On a standard PC or large mobile device the layout of a standard Web page appears as follows:



① Web server header with selector to display PLC Local time or UTC time, and a selector for the display language (Page 136)

② Log in or log out

③ Standard Web page header with name of the page that you are viewing. This example is the CPU Diagnostics > Identification page. Some of the standard Web pages, such as module information, also display a navigation path here if multiple screens of that type can be accessed.

④ Refresh icon: for pages with automatic refresh, enables or disables the automatic refresh function; for pages without automatic refresh, causes the page to update with current data

⑤ Print icon: prepares and displays a printable version of the information available from the displayed page

⑥ Navigation area to switch to another page

⑦ Content area for specific standard Web page that you are viewing. This example is the Diagnostics page.

NOTE

CP module standard Web pages

Certain CP modules (Page 766) provide standard Web pages that are similar in appearance and functionality to the S7-1200 CPU standard Web pages. Refer to your CP documentation for descriptions of the CP standard Web pages.

13.7.2 Basic pages

The Web server provides basic pages intended for use on mobile devices. You access the basic pages using the IP address of the device and appending "basic" to the URL: http://ww.xx.yy.zz/basic or https://ww.xx.yy.zz/basic

The basic pages look similar to the standard pages, but with some differences. The page omits the navigation area, login area, and the header area, and includes buttons for advancing backward and forward through the Web pages. Basic pages also include a Home page button that takes you to a Navigation page. You can also use the navigation controls provided with your mobile device for navigation. For example, the basic Diagnostics page appears as follows in the vertical orientation:

The minimum resolution for displaying a basic page is 240 x 240 pixels.

Note that the standard Web page illustrations in this chapter represent the standard PC Web page appearance. Most of the standard Web pages have equivalent basic pages.

13.7.3 Logging in and user privileges

Each of the PC standard Web pages provides a login window above the navigation pane. Due to space considerations, the basic Web pages provide a separate Login page. You assign the following user privileges under Security settings > Users and roles in the project tree:

- Change operating mode
- Change web server default page
- Read diagnostics
- Read syslog buffer on the CPU
- Flash LEDs
- Perform a firmware update
- Change time settings
- Create a backup of the CPU

- Restore the CPU using a backup file
- Download service data
- Change parameters of the F-System (F-Admin)[1]
- Read process data
- Read process data of the watch tables
- Write process data
- Write process data of the watch tables
- Open user-defined web pages
- Write process data through commands of the automation web page programming (AWP)
- Read files
- Write/delete files

[1] Available for Failsafe CPUs only.

Logging in

To perform certain actions such as changing the operating mode of the controller, writing values to memory, and updating the CPU firmware you must have the required privileges.

Note that if you have set the protection level of the CPU (Page 151) to "Complete protection (no access)", then the "Anonymous" user does not have permission to access the Web server, regardless of the Web server user permission settings.

⚠ WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server or OPC UA users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

- Enable Access control (Page 147) under "Protection & Security > Access control".
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Enable the setting "Only allow secure PG/PC and HMI communication" under "Protection & Security > Connection mechanisms".
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 PLC from a location outside your protected network.
- Enable access to the Web server only with the HTTPS protocol.
- Perform error-checking and range-checking on your variables in your program logic because Web server or OPC UA users can change PLC variables to invalid values.
- For the OPC UA server: In your STEP 7 Device configuration, navigate to "Properties > OPC UA > Server > Security" and deselect "No security" in "Security policies available on the server for the secure channel".

Disruption of process operations can result in death, severe personal injury, and/or property damage.

The log in frame is near the upper left corner on each standard Web page when displayed from a PC or a wide mobile device.

The Log In page is a separate page on small mobile devices that display the basic pages. It is selectable from the Home page.

The Log In screen might also display in the main frame, for example, during a Restore operation.

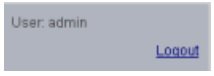
Your login session expires after thirty minutes of inactivity. If the currently-loaded page is continually refreshing, the login session timeout resets, preventing the session from expiring.

NOTE

If you encounter any problems logging in, download the Siemens security certificate (Page 767) from the Introduction page (Page 772). You can then log in with no errors.

Logging out

To log out, simply click the "Logout" link from any page when viewing from a PC or wide mobile device.



From the basic pages, navigate to the Login/Logout page from the Home page and tap the "Logout" button.

After you log out, you can only access and view standard Web pages according to the privileges of the "Anonymous" user. Each of the standard Web page descriptions defines the required privileges for that page.

NOTE

Log off prior to closing Web server

If you have logged in to the Web server, be sure to log off prior to closing your Web browser. The Web server supports a maximum of seven concurrent logins.

13.7.4 Introduction

The Introduction page is the welcome screen for entry into the S7-1200 standard Web pages.

Figure

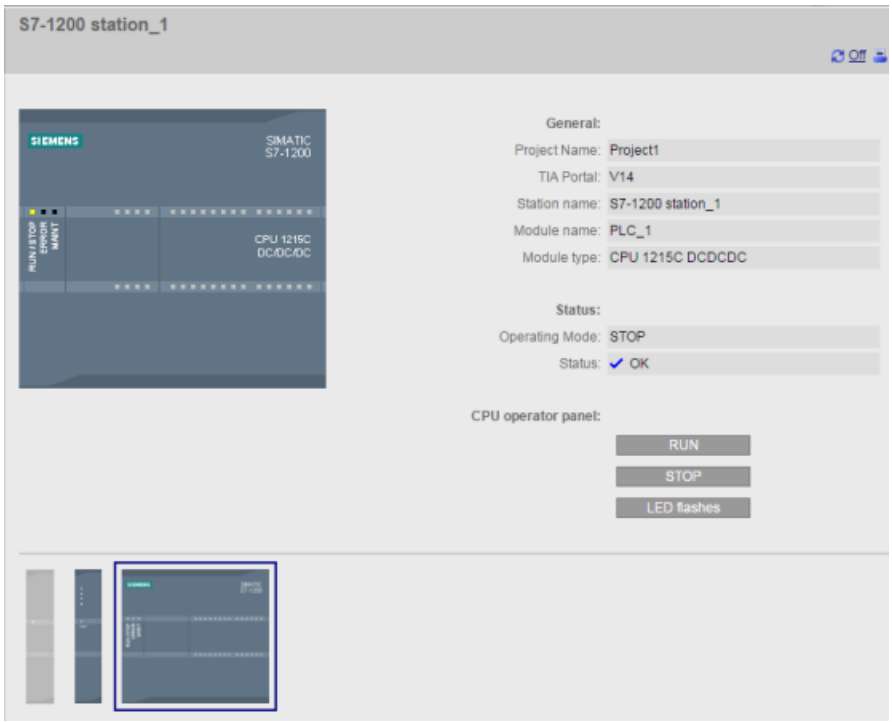
From this page, you click "Enter" to access the S7-1200 standard Web pages. At the top of the screen are links to useful Siemens Web sites, as well as a link to download the Siemens security certificate (Page 767). You can also choose to skip the introduction page on future accesses to the Web server.

13.7.5 Start

The Start page displays a representation of the CPU or CP to which you are connected and lists general information about the device and the TIA Portal version you used to download the project to the CPU. For the CPU, you can use the buttons to change the operating mode and flash the LEDs, if you have logged in (Page 769) with the "Change operating mode" privilege (Page 757).

The bottom portion of the screen is visible if you have configured and installed Web server-enabled CP modules (Page 766) in the local rack with the S7-1200 CPU. You can hover over and click a Web server-enabled CP module to access the standard Web pages. Refer to the documentation for your CP module for information about the CP module Web pages. You see the name of the CP module when you hover over it.

The Web server also displays any other CM and CP modules in the local rack, but you cannot click them as they do not contain Web pages. The module appearance for these CMs and CPs are light gray (desensitized) to indicate that they are display-only and not clickable modules.



Note that the S7-1200 fail-safe CPUs display additional data on this page related to functional safety.

13.7.6 Diagnostics

The Diagnostics page displays the following information:

- Identification: identifying characteristics of the module and plant and location information from STEP 7
- Program protection: status of know-how protection and CPU binding, which can be useful in planning for spare parts as well as STEP 7 configuration setting for allowing or preventing the copy of internal load memory to external load memory (SIMATIC memory card).
- Memory: load, work, and retentive memory usage

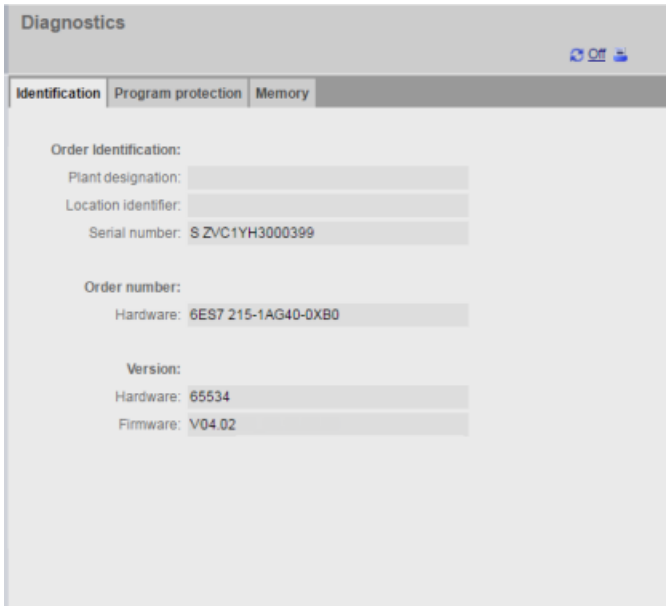
F-CPUs display an additional Fail-safe tab.

Viewing the Identification page requires the "Read out diagnostics" privilege (Page 757).

Identification tab

The Identification tab includes the following information:

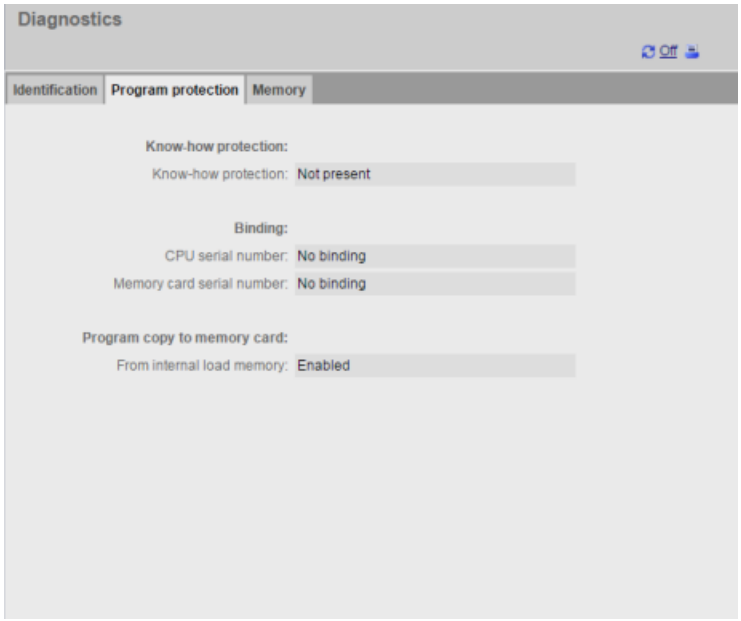
- Order Identification: Displays Plant designation, Location identifier, and Serial number
- Order Number: Displays the order number for the PLC
- Version: Displays version identification for both the PLC and the firmware



Program protection tab

The program protection tab includes the following information:

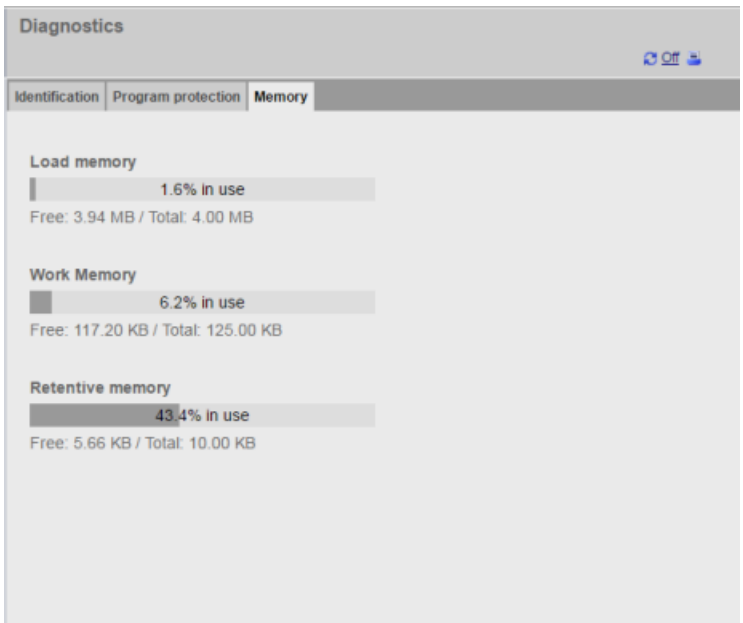
- Know-how protection (Page 159): Displays whether you have configured know-how protection for any of the program blocks in STEP 7
- Binding (Page 160): Displays whether you have bound the program to either the CPU or to the SIMATIC memory card
- Program copy to memory card (Page 159): Displays whether you have enabled the ability to copy the program from internal load memory to external load memory (SIMATIC memory card)



Memory tab

The Memory (Page 83) tab includes the following information:

- Load memory: Displays usage as a percentage and Free/Total available in MB
- Work memory: Displays usage as a percentage and Free/Total available in KB
- Retentive memory: Displays usage as a percentage and Free/Total available in KB



Fail-safe tab

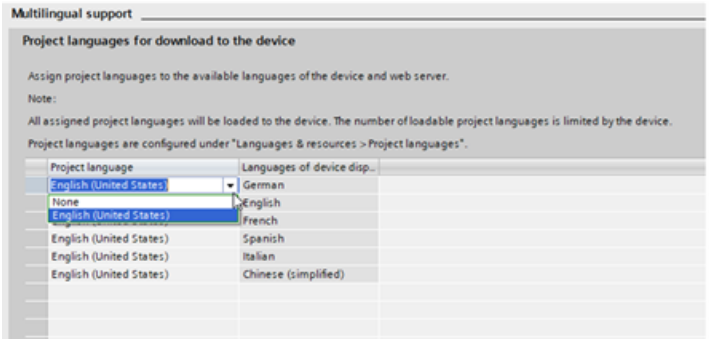
Refer to the S7-1200 Functional Safety Manual (https://support.industry.siemens.com/cs/ww/en/view/104547552) for information about the Diagnostics page Fail-safe tab.

13.7.7 Diagnostics Buffer

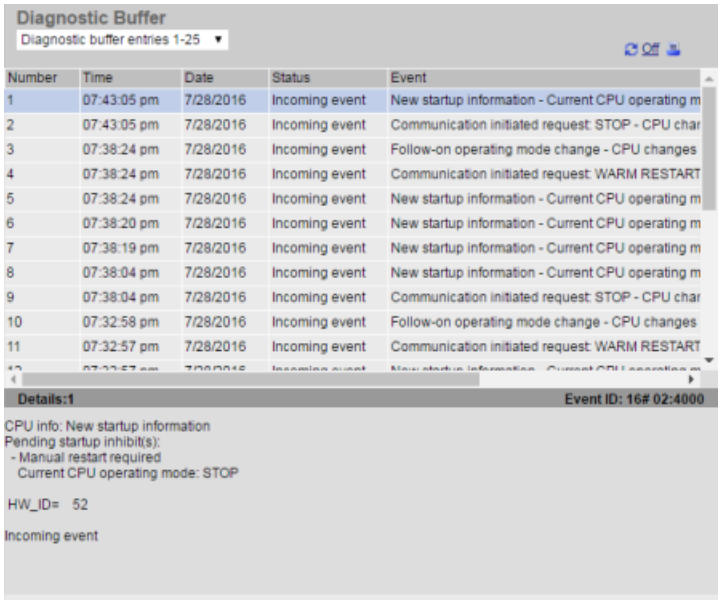
The diagnostics buffer page displays diagnostic events. The newest event is Number 1 at the top. The oldest event is Number 50. From the selector on the left, you can choose what range of diagnostics buffer entries to display, either 1 to 25 or 26 to 50. From the selector on the right, you can choose whether to display the times in UTC times or PLC local times. The top part of the page displays the diagnostic entries with the time and date of when the event occurred.

You can select any individual diagnostic entry to show detailed information about that entry in the bottom part of the page. Note that the display language of the diagnostics buffer entries depends upon your device configuration setting for multilingual support (Page 142).

You must configure the languages used for diagnostic text in the TIA Portal project downloaded to the PLC. This configuration is available in the PLC properties under "Multilingual support". Each language downloaded must be associated with a supported webserver language. The PLC is limited to 2 downloaded languages.



The Diagnostics Buffer page also includes a button to save the diagnostics buffer to a CSV file. By default, the Web server saves the comma-separated file to ASLog.csv in your Downloads folder. The file contains the complete diagnostics buffer at the time of the save operation. You can save the file as many times as you choose and keep multiple files. You can open the diagnostics buffer file with Microsoft Excel or any text editor.



Viewing the Diagnostics Buffer page requires the "Read out diagnostics" privilege (Page 757).

13.7.8 Module Information

The module information page provides the following:

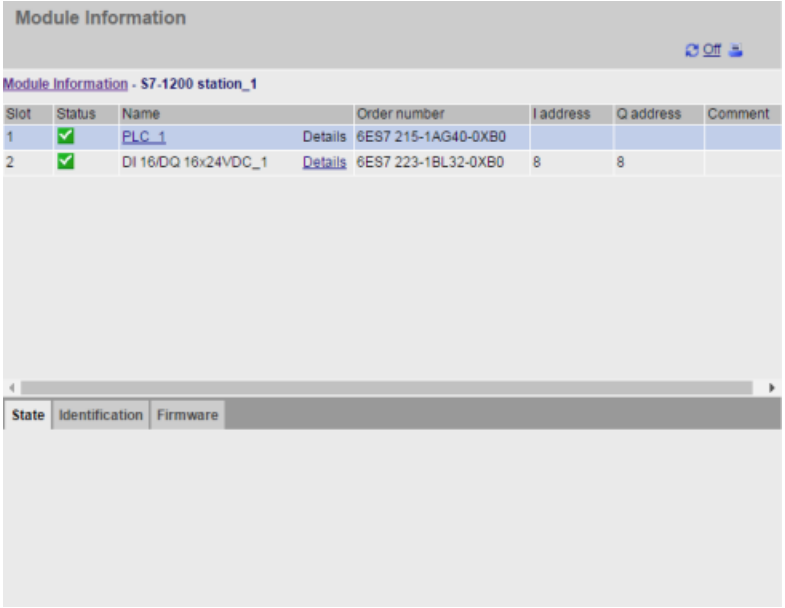
- Information about all the modules in the local rack
- The capability to perform a firmware update
- Information about distributed I/O systems

The top section of the screen shows a summary of the modules based on the device configuration in STEP 7, and the bottom section shows status, identification and firmware information for the selected module based on the corresponding connected module.

Viewing the Module Information page requires the "Read process data" privilege (Page 757).

Module information: State tab

The state tab in the bottom section of the module information page displays a description of the current state of the module that is selected in the top section. If the section is empty, then the module has no pending diagnostic state.



Status icons for the modules

For each module, the status column of the top section displays an icon that indicates the status of that module:

Icon	Meaning
	No fault
	Deactivated
	Maintenance required
	Maintenance demanded
	Error
	The CPU cannot reach the module or device (for devices other than the CPU)
	The CPU has established a connection to the device, but the module status is unknown (for devices other than the CPU)
	Input and output data are unavailable because the submodule has blocked its I/O channels (for devices other than the CPU)

Navigating

You can select a link in the top section to navigate to the module information for that particular module. Modules with submodules have links for each submodule. The type of information that is displayed varies with the module selected. For example, the module

information dialog initially displays the name of the S7-1200 station, a status indicator, and a comment. If you click the CPU name, the module information displays the following:

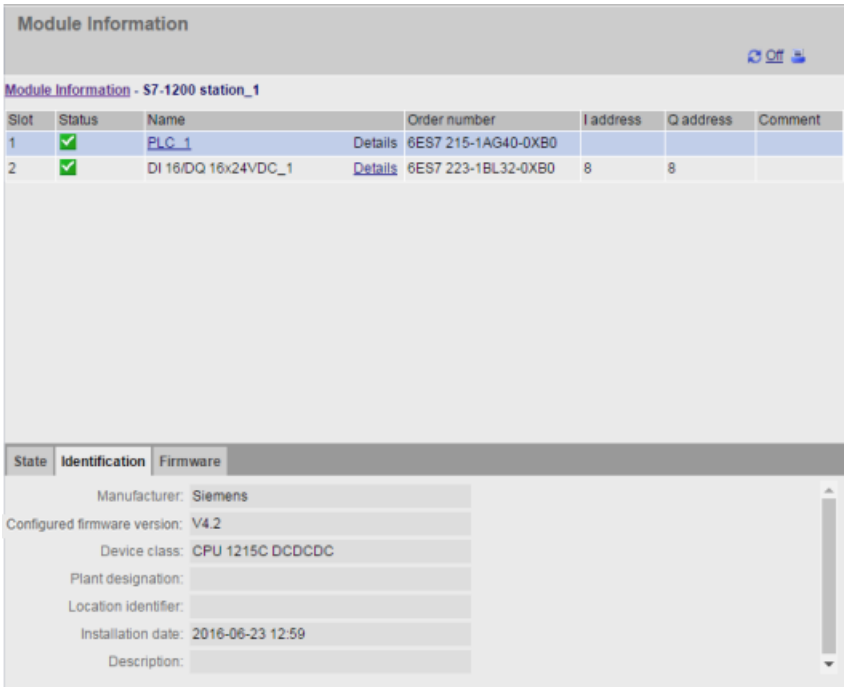
- Name of the digital and analog inputs and outputs that the CPU model provides,
- Addressing information for the I/O
- Status indicators
- Slot numbers
- Comments

Slot	Status	Name		Order number	I address	Q address	Comment
1	✓	DI 14/DQ 10_1	Details		0	0	
2	✓	AI 2_1	Details		64		
16	✓	HSC_1	Details		1000		
17	✓	HSC_2	Details		1004		
18	✓	HSC_3	Details		1008		
19	✓	HSC_4	Details		1012		
20	✓	HSC_5	Details		1016		
21	✓	HSC_6	Details		1020		
32	✓	Pulse_1	Details			1000	

The module information page shows the path you have followed. You can click any link in this path to return to a higher level.

Module information: Identification tab

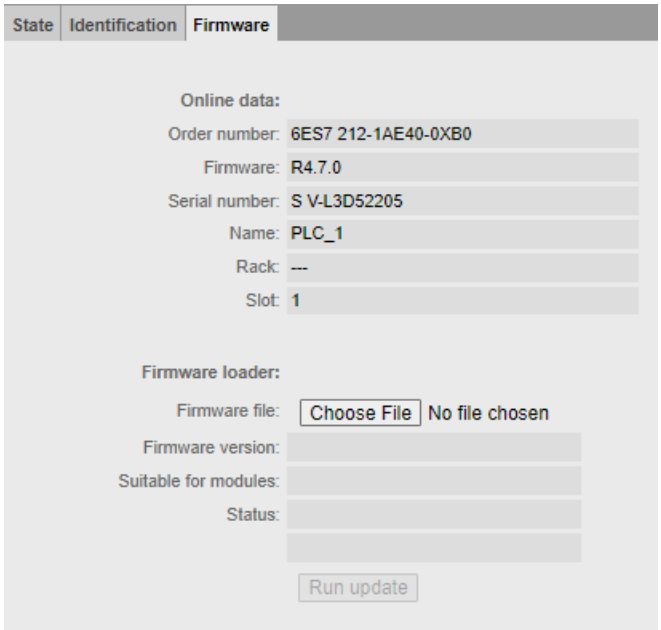
The identification tab displays the Identification and Maintenance (I&M) information of the selected module.



Note that if you click an F-I/O module in the top section, then the bottom section has a Safety tab. On this tab, you can see specific data related to the selected module as described in the S7-1200 Functional Safety Manual (https://support.industry.siemens.com/cs/ww/en/view/104547552).

Module information: Firmware tab

The firmware tab of the module information page displays information about the firmware of the selected module. If you have the "Update firmware" privilege (Page 757), you can also perform a firmware update of the CPU or other modules in the local rack that support firmware update or PROFINET I/O modules. For remote modules, you can view the firmware information, but not perform a firmware update.



Performing a firmware update

The CPU must be in STOP mode to perform a firmware update. When the CPU is in STOP mode, click the Browse button to navigate to and select a firmware file. Firmware updates are available on the Siemens Industry Online Support Web site (http://support.industry.siemens.com).

During the update, the page displays a message showing that the update is in progress. After the update completes, the page displays the article number and version number of the updated firmware. If you updated the firmware for the CPU or a signal board, the Web server restarts the CPU.

You can also perform a firmware update by one of these methods:

- Using the online and diagnostic tools of STEP 7 (Page 1055)
- Using a SIMATIC memory card (Page 117)
- Using the SIMATIC Automation Tool (https://support.industry.siemens.com/cs/ww/en/view/98161300)

NOTE

The firmware update process discards any additional data appended to the firmware update file. Appending data to a firmware update file has no effect on the firmware update or the S7-1200 CPU. You cannot append data, for example, to add components.

NOTE

Potential problems with performing a firmware update from the Web server

In the event of a communications disruption during a firmware update from the Web server, your Web browser could display a message asking whether you want to leave or stay on the current page. To avoid potential problems, select the option to stay on the current page.

If you close the Web browser while in the process of performing a firmware update from the Web server, you will be unable to change the operating mode of the CPU to RUN mode. If this situation happens, you must cycle power to the CPU to be able to change the CPU to RUN mode.

13.7.9 Communication

The communication page displays the following:

- Parameters of the connected CPU
- Communications statistics
- Connection resources
- Information about connections

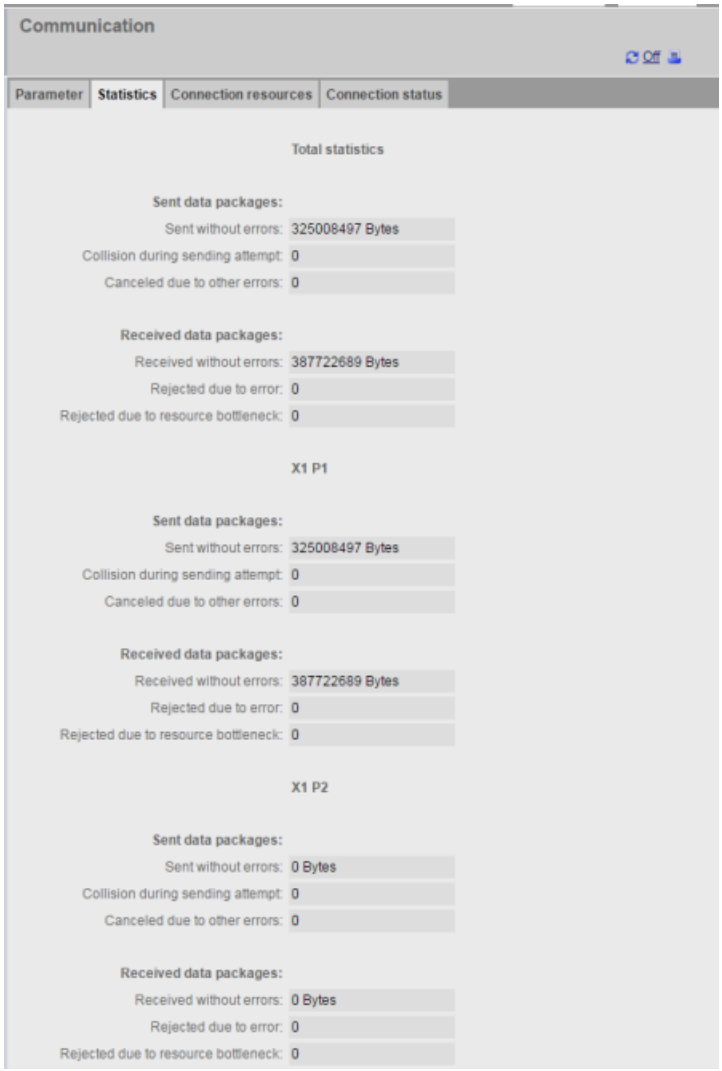
Viewing the Communication page requires the "Read process data" privilege (Page 757).

Parameter tab

The Parameter tab shows the following information:

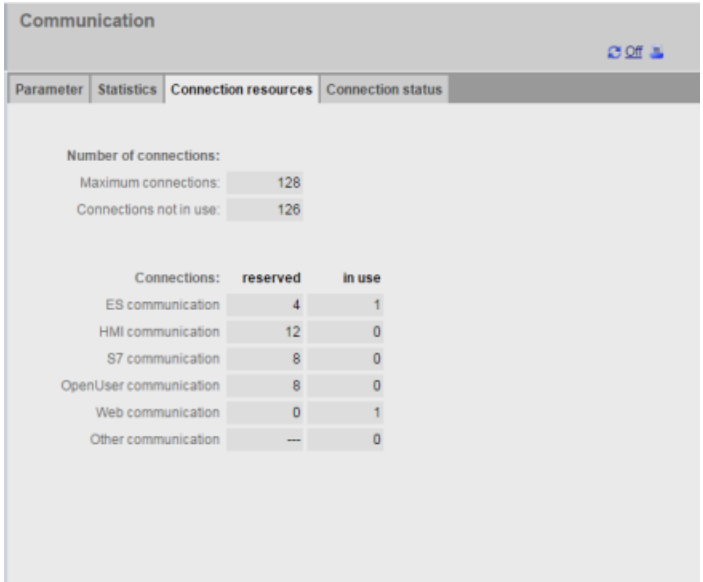
Statistics tab

The Statistics tab shows send and receive communication statistics:



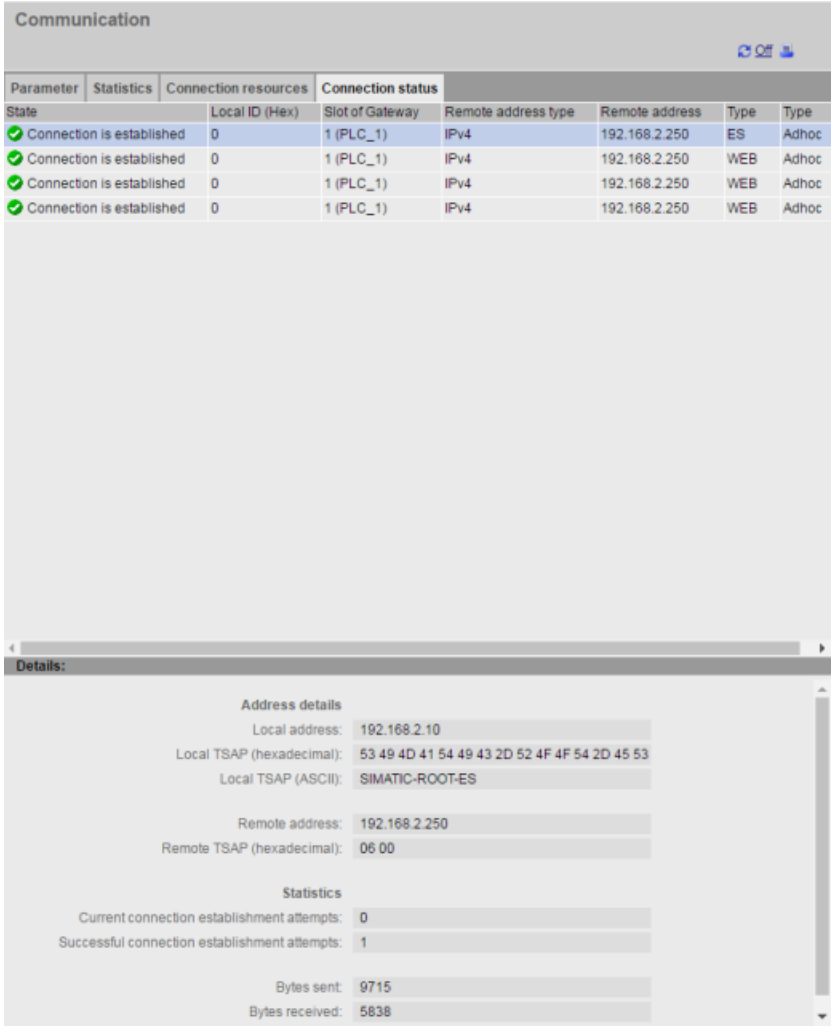
Connection resources tab

The Connection resources tab shows information about the total number of connection resources and how they are allocated for different types of communication:



Connection status tab

The Connections status tab shows the connections for the CPU, and connection details for the selected connection.



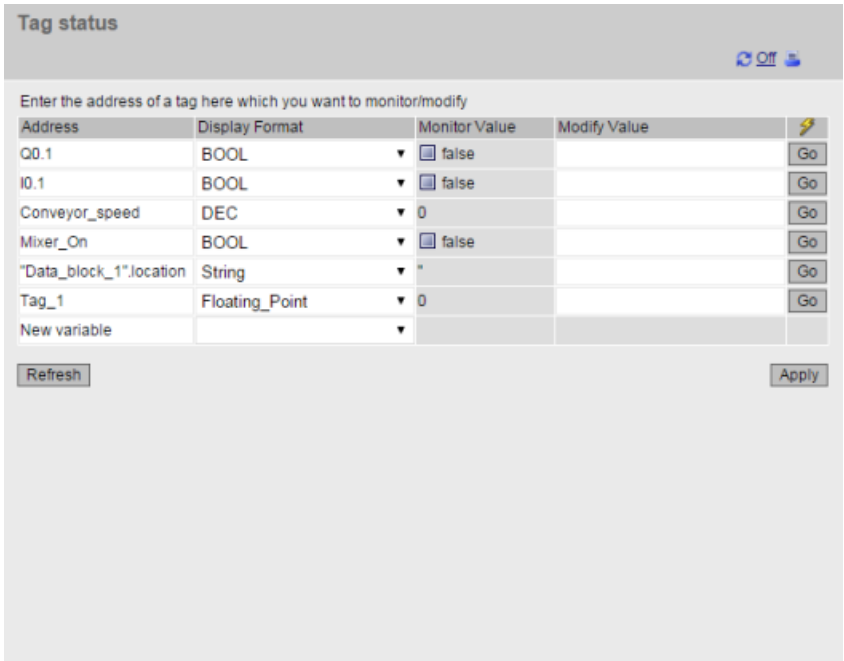
13.7.10 Tag status

The Tag status page allows you to view any of the I/O or memory data in your CPU. You can enter a direct address (such as %I0.0), a PLC tag name, or a tag from a specific data block. For data block tags, you enclose the data block name in double quotation marks. For each monitor value you can select a display format for the data. You can continue entering and specifying values until you have as many as you want within the limitations for the page. The monitor values show up automatically. You can click the "Refresh" button at any time to refresh all of the monitor values. If you have enabled automatic update in STEP 7 (Page 755), you can click the "Off" icon in the upper right area of the page to disable it. When automatic update is disabled, you can click "On" to re-enable it.

You can view the Tag status page if you have the "Read process data" privilege (Page 757).

If you log in (Page 769) as a user with the "Write process data" privilege, you can also modify data values. Enter any values that you wish to set in the appropriate "Modify Value" field. Click the "Go" button beside a value to write that value to the CPU. You can also enter multiple

values and click "Apply" to write all of the values to the CPU. The buttons and column labels for modifying only appear if you have the necessary privilege.



If you leave the Tag status page and return, the Tag status page does not retain your entries. You can bookmark the page and return to the bookmark to see the same entries. If you do not bookmark the page, you must re-enter the variables.

For values you frequently monitor or modify, consider using a Watch table (Page 786) instead.

NOTE

Be aware of the following information when using the standard Tag status page:

- Enclose all string modifications in single quotes.
- The Tag status page can monitor and modify tags that contain any of the following characters: &, <, (, +, ,(comma), ., [,], $, or %, providing you enclose the tag name in double quotation marks, for example, "Clock_2.5Hz".
- To monitor or modify just one field of a DTL tag, include the field in the Address, for example, "Data_block_1".DTL_tag.Year. Enter an integer value for the modify value according to the data type of the specific field of the DTL. For example, the Year field is a UInt.
- The maximum number of variable entries per page is 50.
- If a tag name displays special characters such that it is rejected as an entry on the Tag status page, you can enclose the tag name in double quotation marks. In most cases, the page will then recognize the tag name.

See also

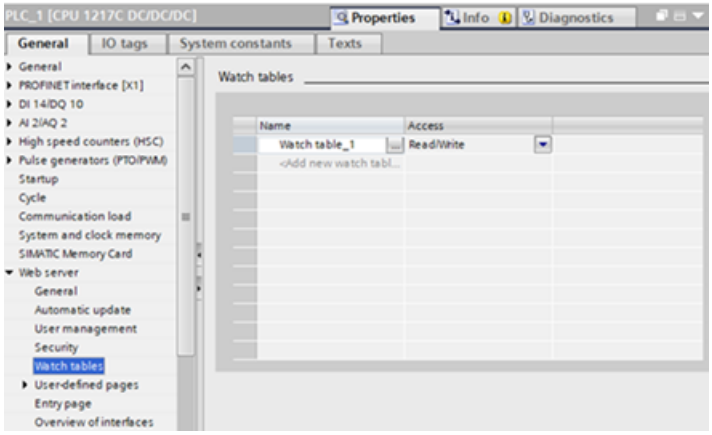
Rules for entering tag names and values (Page 835)

13.7.11 Watch tables

The Web server allows you to access watch tables that you have configured in STEP 7 and downloaded to the CPU. Watch tables with 50 or fewer entries offer the best performance in the Web server. Exceeding 50 entries might degrade system performance or cause watch table access errors.

STEP 7 configuration to select watch tables for the Web server

From the Device configuration of the CPU in STEP 7, you can add the watch tables that you want the Web server to be able to display. For each watch table that you select from the list of existing watch tables, you select Read or Read/Write privileges for it in STEP 7. When downloaded to the CPU, you can only view the watch tables that have the Read privilege but you can view and modify watch table tags when you select the Read/Write privilege.



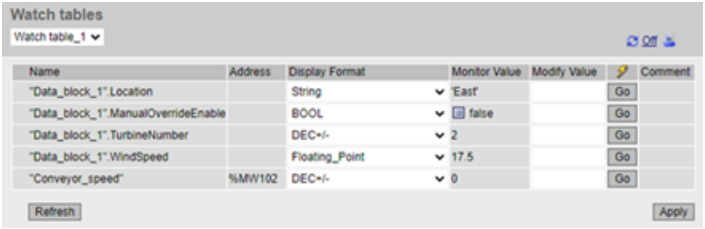
After you complete the watch table configuration in the Web server section of the device configuration, download your hardware configuration to the CPU.

Viewing watch tables from the Web server

From the Web server, if you have the "Read process data of the watch tables" privilege (Page 757), you can select "Watch tables" from the navigation menu to access the watch tables that you have configured and downloaded to the CPU. If you have downloaded more than one watch table, you can select the one you want to display from the drop-down list. The Web server displays the watch table that you created in STEP 7 and the current values according to the display format. You can change the display format if you choose, but when you return to the watch table page the Web server defaults to the display formats in the STEP 7 watch table.

Modifying watch table tags from the Web server

If you downloaded a watch table with the "Read/Write" access level, you must log in to the Web server as a user with "Write process data of the watch tables" privilege (Page 757) to modify tag values just like you do in a watch table in STEP 7. You can modify individual tag values and click "Go" to modify only the one value, or you can enter several values and click "Apply" to modify them all at once.



NOTE

Advantages of watch tables for modifying tags

For a user to modify tags and data block tags in the CPU from a watch table, you must configure the watch table in the Web server properties in the STEP 7 device configuration, and you must configure it for Read/Write access. By so doing, you can restrict the tags to which a user with the "Write process data of the watch tables" privilege can modify to only those tags in the configured Web server watch tables.

The Tag Status (Page 784) page, on the other hand, allows any user with the "write tag status" privilege to write to any tag or data block tag in the CPU.

By careful configuration of the Web server user management privileges (Page 757), you can help safeguard access to your PLC data.

See also

Rules for entering tag names and values (Page 835)

13.7.12 Online backup

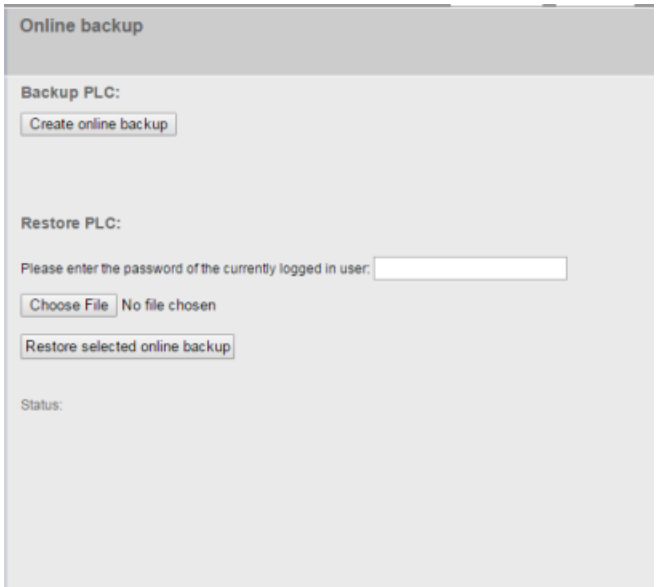
The Online backup standard Web page allows you to make a backup of the STEP 7 project for the online PLC as well as to restore a previously-made backup of the PLC. Before creating a backup or restoring a backup, place the PLC in STOP mode and cease all communication with the PLC such as HMI access and Web server access. If your CPU is not in STOP mode, the backup and restore functions prompt for confirmation to place the CPU in STOP mode before continuing.

If you have accessed the Online backup page through one of the Web-enabled CP modules, you can perform a backup but you cannot restore.

NOTE

You can also perform backup and restore operations from STEP 7 (Page 1085). Refer to these topics for a full description of what data you can back up and restore. The SIMATIC Automation Tool also provides backup and restore capability.

When you back files up from the Web server, your PC or device saves the backup files in the default folder for downloads. When you back files up from STEP 7, STEP 7 stores the files within the STEP 7 project. You cannot restore STEP 7 backup files from the Web server and you cannot restore Web server backup files from STEP 7. You can, however, save STEP 7 backup files directly to the download folder of your PC or device. If you do so, then you can restore these files from the Web server.



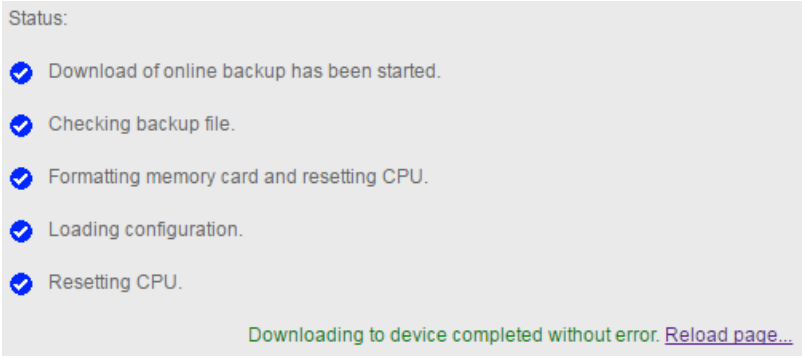
Backup PLC

From the Backup PLC section of the page, click the "Create online backup" button to make a backup of the project that is currently stored in the PLC. This function requires the "Create a backup of the CPU" user privilege (Page 757). If the CPU is in RUN mode and you have to change it to STOP mode, you also need the "Change operating mode" privilege. The PC or device will store the backup file at the default location for downloads. Depending on your browser and device settings, you might be prompted about saving the file.

Restore PLC

From the Restore PLC section of the page, enter the Web server user password and click the "Browse" or "Choose File" button (depending on your browser) to select a previously saved backup file. Click the "Load online backup" button and confirm the prompt to load this file in the connected PLC. This page requires the "Restore the CPU using a backup file" user privilege (Page 757). If the CPU is in RUN mode and you have to change it to STOP mode, you also need the "Change operating mode" privilege.

As the restore operation proceeds, you see a series of progress messages and you must reenter your user login and password. After each step of the process completes successfully, you see the following completion indicators and a link to reload the page:



WARNING

Restoring backups with unknown content

If you restore a backup with unknown content, you can cause malfunctions or program errors. In addition, if you restore a backup that does not have the Web server enabled in the device configuration of the CPU, you will not be able to access the CPU from the Web server.

Make sure that the backup consists of a configuration with known content.

Malfunctions or program errors can cause death, severe personal injury and/or property damage.

NOTE

Restoring a backup where the CPU IP address is different

If you attempt to restore a backup where the CPU IP address in the backup is different from the IP address of the current CPU, the Web server cannot display the message that the restore is complete. After you see the "Reset CPU" message for greater than five minutes, enter the new IP address that corresponds to the address in the backup file. The CPU now has this address, and you can resume Web server access.

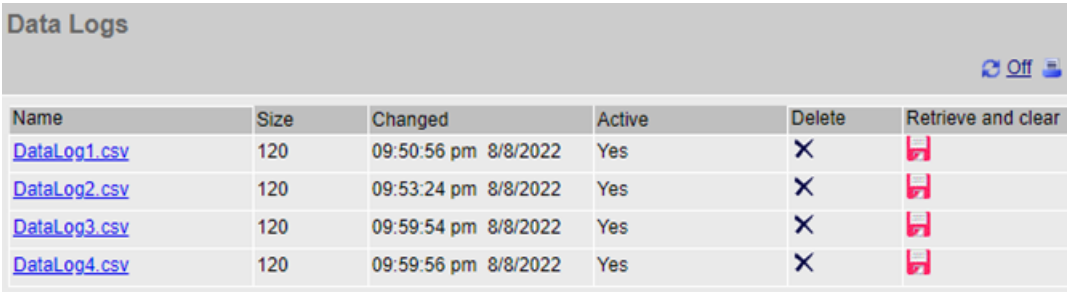
13.7.13 Data Logs

The Data Logs page allows you to access data logs.

The type of operations you can perform depends on your user privileges (Page 757). Any user with the "Read files" privilege can view the files. If you have the "Write/delete files" privilege, you can also:

- Download a data log from your PLC to your computer
- Delete a data log from your PLC
- Retrieve and clear a data log

Data logs are displayed in ascending, case-insensitive, alphabetical order. The data log list is paginated in increments of 50 data logs.



Name	Size	Changed	Active	Delete	Retrieve and clear
DataLog1.csv	120	09:50:56 pm 8/8/2022	Yes	✕	
DataLog2.csv	120	09:53:24 pm 8/8/2022	Yes	✕	
DataLog3.csv	120	09:59:54 pm 8/8/2022	Yes	✕	
DataLog4.csv	120	09:59:56 pm 8/8/2022	Yes	✕	

NOTE

Data log management

Keep no more than 1000 data logs in a file system. Exceeding this number can prevent the Web server from having enough CPU resources to display the data logs.

If you find that the Data Logs Web page is not able to display the data logs, then you must place the CPU in STOP mode in order to display and delete data logs.

Manage your data logs to ensure that you only keep the number that you need to maintain, and do not exceed 1000 data logs.

Working with a data log in Excel

The data log file is in USA/UK comma-separated values format (CSV). To open it in Excel on non-USA/UK systems, you must Importing CSV format data logs to non-USA/UK versions of Microsoft Excel (Page 836).

Active state

The "Active" column on the Data Logs page shows "Yes" when there is a data log control block on the CPU associated with that file, and "No" when one does not exist. The active state can not be manually altered by the user.

If the STEP 7 program has a data log open or is writing to a data log, the Web server is unable to delete, download, or retrieve and clear the data log file. In addition, while the Web server is performing a download of a data log either through a download or a Retrieve and Clear, you can perform no other data log operation until the download is completed or canceled. The Web server displays an "Application Busy" error message.

Download a data log file

You can download a data log file by clicking the file name. The Web server displays an error message if the file no longer exists or when another download is in progress. The error message remains on the page until you initiate an operation to reload the Data Logs page. The following operations cause the Web server to reload the Data Logs page:

- Refreshing the Data Logs page or navigating away and returning to the Data Logs page
- Changing the current Data Logs pagination selection
- Successfully deleting a data log
- Successfully retrieving and clearing a data log

NOTE

Data logs error message

The Web server 's auto-refresh functionality does not remove the error message from the page.

The following scenarios generate error messages on the Data Logs page:

Operation	Failure condition	Error message
Download Retrieve/Clear	• File does not exist • Invalid file name • Invalid HTTP request method • SMC is write-protected (Retrieve/Clear only)	Error while downloading the file
Delete	• Invalid HTTP request method • Invalid file name • File does not exist	Error while deleting the file
Delete	• SMC is write-protected	Error while deleting the file: memory card is write-protected
Delete	• User program is holding the data log file open	Application busy
Download Delete Retrieve/Clear	• Do not have required permission • HTTP request method is not POST or GET • Invalid ACTION parameter in URL	File operation not permitted
Download Delete Retrieve/Clear	• Invalid or missing HTTP referrer field	File operation not permitted: no referrer
Download Delete Retrieve/Clear	• User program is holding the data log file open • Currently downloading a data log	Application busy
Download Delete Retrieve/Clear	• Unexpected internal PLC error	Internal error

Deleting a data log

A data log cannot be deleted if it is open in the STEP 7 program. You must first close the data log before you can delete it. You can delete a data log by clicking the ✕ icon in the Delete column for a specific data log. To delete the data log file, confirm the delete operation from the Delete dialog.

Retrieve and Clear a data log

To open a data log and remove all entries, click the Retrieve and Clear icon. To retrieve the data log file and empty the contents, confirm the operation from the Retrieve and Clear dialog.

After you confirm the operation, the Web server allows you to download the contents of the data log file. The Save File dialog lets you choose whether to save the data log. After your selection, the Web server empties the contents of the data log file without deleting the file. You cannot cancel the clearing of the data log from the Save File dialog. You can only cancel the operation from the initial confirmation of the Retrieve and Clear dialog.

You can only retrieve and clear a data log when "No" is listed in the "Active" column.

If an error message displays, or the Retrieve and Clear icon is not visible, you must then click the ✕ icon in the Delete column to manually delete the file.

13.7.14 User Files

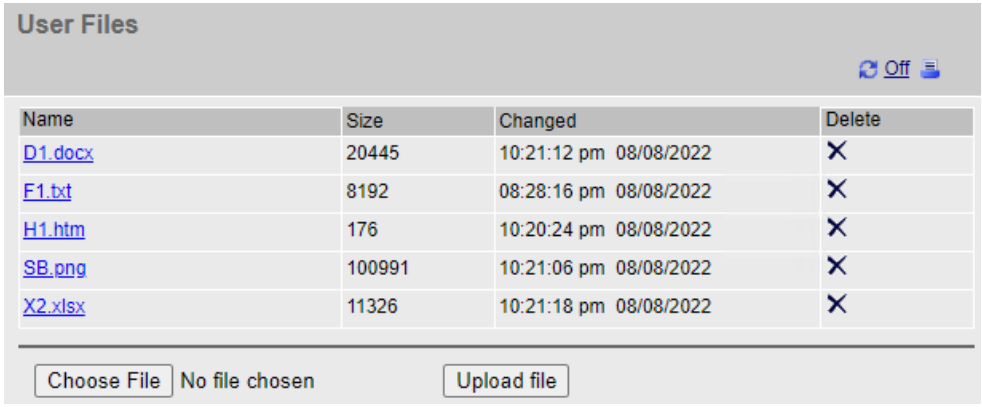
The User Files page provides access to files on the SIMATIC memory card (external load memory).

The type of user file access you have depends on your user privileges (Page 757). Any user with the "Read files" privilege can view the files and folders with the User Files page. If you have the "Write/delete files" privilege, you can also:

- Download a user file from your PLC to your computer
- Upload a user file from your computer to your PLC
- Delete a user file from your PLC

Viewing user files

To view user files, click User Files from the main navigation page



The file list includes the file's current size and the date of last modification. The list of files is populated from the "User Files" directory in the root of the SIMATIC memory card.

NOTE

User file management

Keep no more than 1,000 user files on the SIMATIC memory card. If more files are present, the Web server only allows you to view the first 1,000 files. Files are displayed in ascending, case-insensitive, alphabetical order.

User file list pagination

The user file list is paginated in increments of 50 items. A dropdown box lets you select the range of item you wish to see.

Downloading a user file

To download a user file, click a file in the list. Use Windows File Explorer to save the file to a folder you select.

Deleting a user file

To delete a user file, click the X icon for the file and confirm the prompt.

Uploading a user file

To upload a file from your programming device to the user files on your memory card, follow these steps:

1. Click Choose File.
2. From Windows File Explorer, select a file.
   The file must be less than 2 GB in size.
   The filename must consist only of these characters a-z A-Z 0-9 ._- (){}[]$!=~ (space)
3. Click Upload file.

Printing the User File list

You can print the list of the user files on your SIMATIC memory card by clicking the "Print" icon on your User Files Web page.

Errors with user files

The User Files page displays an error message if an operation fails to complete successfully:

The error message remains on the page until you refresh the User Files page.

NOTE
User files error message
The Web server's auto-refresh functionality does not remove an error message from the User Files page.

The following conditions generate error messages on the User Files page:

Operation	Failure condition	Error message
Download user file	• File does not exist • Internal PLC error	Error while downloading the file
Download user file Upload user file Delete user file	• Insufficient permissions for requested operation • Invalid HTTP request method or action parameter	File operation not permitted
Download user file Upload user file Delete user file	• Invalid or missing HTTP referrer field	File operation not permitted - no referrer
Delete user file	• Memory card is write-protected	File operation not permitted
Download Delete Retrieve/Clear	• File does not exist • Internal PLC error	Error while deleting the file - memory card is write-protected
Upload user file	• File name missing or invalid • Internal PLC error	Error when uploading the file
Upload user file	• File name already exists on PLC	Error while uploading the file - name already exists
Upload user file	• SMC is full	Error while uploading the file - memory card is full
Upload user file	• Invalid file name	Error while uploading the file - invalid character in file name
Upload user file	• File is too large for SM file system	Error while uploading the file - file too big
Upload user file	• SMC is write-protected	Error while uploading the file - memory card is write-protected

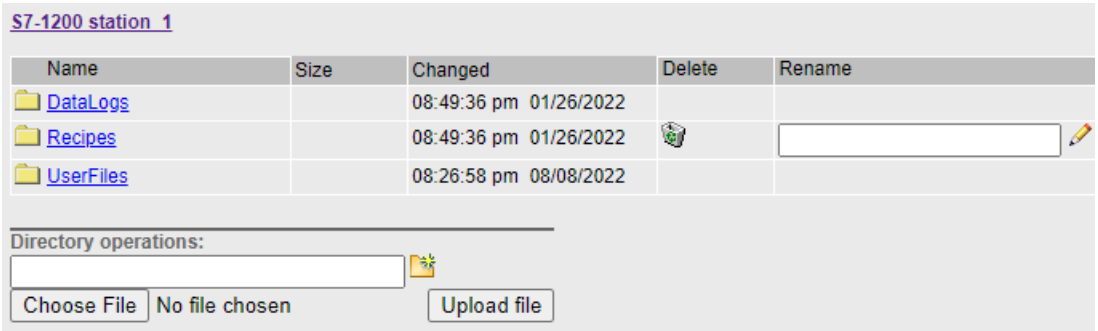
13.7.15 Data Log UserFiles API

A Data Log User Files API feature is available for S7-1200 User Files and Data Logs. Refer to the *S7-1500, ET200SP, ET200pro Web server manual* (https://support.industry.siemens.com/cs/us/en/view/59193560) for more information.

13.7.16 File Browser

The File Browser page provides access to files in the internal load memory of the CPU or on the SIMATIC memory card (external load memory). The file browser page initially displays the root folder of the load memory, which contains the "Recipes" and "DataLogs" folders, but also displays any other folders that you might have created, if using a memory card.
The type of file access you have to the files and folders depends on your user privileges (Page 757). Any user with "Read files" privileges can view the files and folders with the file browser. You cannot delete the Recipes or DataLogs folder regardless of your login privileges, but if

you had made custom folders on the memory card, you can delete those folders if you have logged in as a user with "Write/delete files" privileges.
Click a folder to access the individual files in the folder.



Recipe files

The recipe folder displays any recipe files that are present in load memory. Recipe files are also in CSV format, and you can open them in Microsoft Excel, or another program. You must have Write/delete privileges (Page 757) in order to delete, modify and save, rename or upload recipe files.

Uploading files and automatic page refresh

If you begin a file upload, the upload operation continues as long as you remain on the File Browser Web page. If you enabled automatic update to refresh the Web server pages every ten seconds, then whenever a page refresh occurs you see the incremental progress of the file upload operation. For example, if you are uploading a 2 MB file, you might see updates that show the file size in bytes at 2500, 5000, 10000, 15000, and 20000 as the file upload progresses.
If you navigate away from the File Browser page before the upload completes, the Web server deletes the incomplete file.

Additional information

NOTE
File name conventions
For the Web server to work with data log and recipe files, the characters in the file names must be from the ASCII character set with the exception of the characters \ / : * ? " < > | and the space character.
If your files are not compliant with this naming convention, the Web server can have errors in operations such as file upload or deletion. In this case, you might need to use a card reader and the Windows File Explorer to rename files that were on external load memory.

For information on programming with the data log instructions, and importing (Page 431) and exporting (Page 429) recipes, see the Recipes and Data logs (Page 425) chapter.

13.8 User-defined Web pages

The S7-1200 Web server also provides the means for you to create your own application-specific HTML pages that incorporate data from the PLC.

WARNING

Unauthorized access to the CPU through user-defined Web pages

Unauthorized access to the CPU through user-defined Web pages can disrupt process operation. Coding of user-defined Web pages that is not secure introduces security vulnerabilities such as cross-site scripting (XSS), code injection, and others.

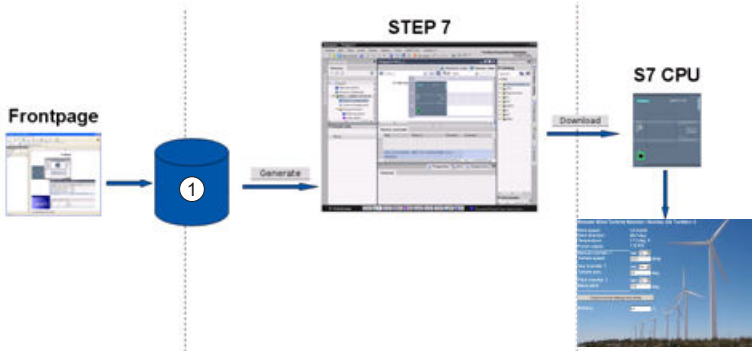
Protect your S7-1200 CPU from unauthorized access by installing it in a secure fashion as outlined in the "Operational Guidelines" white paper found on the Siemens Industrial Cybersecurity Web site (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

Disruption of process operations can cause death, severe personal injury and/or property damage.

You create user-defined Web pages using the HTML editor of your choice and download them to the CPU where they are accessible from the standard Web page menu. This process involves several tasks:

- Creating HTML pages with an HTML editor (Page 797)
- Including AWP commands in HTML comments in the HTML code (Page 798):The AWP commands are a fixed set of commands that Siemens provides for accessing CPU information.
- Configuring STEP 7 to read and process the HTML pages (Page 811)
- Generating blocks from the HTML pages (Page 811)
- Programming STEP 7 to control the use of the HTML pages (Page 812)
- Compiling and downloading the blocks to the CPU (Page 814)
- Accessing the user-defined Web pages from your PC (Page 814)

This process is illustrated below:



① HTML files with embedded AWP commands

13.8.1 Creating HTML pages

You can use the software package of your choice to create your own HTML pages for use with the Web server. Be sure that your HTML code is compliant to the HTML standards of the W3C (World Wide Web Consortium). STEP 7 does not perform any verification of your HTML syntax.

You can use a software package that lets you design in WYSIWYG or design layout mode, but you need to be able to edit your HTML code in pure HTML form. Most Web authoring tools provide this type of editing; otherwise, you can always use a simple text editor to edit the HTML code. Include the following line in your HTML page to set the charset for the page to UTF-8:

```
<meta http-equiv="content-type" content="text/html; charset=utf-8">
```

Also be sure to save the file from the editor in UTF-8 character encoding.

You use STEP 7 to compile everything in your HTML pages into STEP 7 data blocks. These data blocks consist of one control data block that directs the display of the Web pages and one or more fragment data blocks that contain the compiled Web pages. Be aware that extensive sets of HTML pages, particularly those with lots of images, require a significant amount of load memory space (Page 814) for the fragment DBs. If the internal load memory of your CPU is not sufficient for your user-defined Web pages, use a memory card (Page 106) to provide external load memory.

To program your HTML code to use data from the S7-1200, you include AWP commands (Page 798) as HTML comments. When finished, save your HTML pages to your PC and note the folder path where you save them.

NOTE

The file size limit for HTML files containing AWP commands is 64 kilobytes. You must keep your file size below this limit for STEP 7 to be able to successfully compile your pages.

Siemens recommends that all Web resource files (.ccc files, images, JavaScript files, and html files) are created with a size not exceeding 512 KB; otherwise, problems can occur when sending the file from the Web server to the browser. You can view the size of the respective Web resource file in the file explorer of the directory.

Refreshing user-defined Web pages

User-defined Web pages do not automatically refresh. It is your choice whether to program the HTML to refresh the page or not. For pages that display PLC data, refreshing periodically keeps the data current. For HTML pages that serve as forms for data entry, refreshing can interfere with the user entering data. If you want your entire page to automatically refresh, you can add this line to your HTML header, where "10" is the number of seconds between refreshes:

```
<meta http-equiv="Refresh" content="10">
```

You can also use JavaScript or other HTML techniques to control page or data refreshing. For this, refer to documentation on HTML and JavaScript.

13.8.2 AWP commands supported by the S7-1200 Web server

The S7-1200 Web server provides AWP commands that you embed in your user-defined Web pages as HTML comments for the following purposes:

- Reading variables (Page 799)
- Writing variables (Page 800)
- Reading special variables (Page 802)
- Writing special variables (Page 803)
- Defining enum types (Page 805)
- Assigning variables to enum types (Page 806)
- Creating fragment data blocks (Page 807)

General syntax

Except for the command to read a variable, the AWP commands are of the following syntax:

```
<!-- AWP_ <command name and parameters> -->
```

You use the AWP commands in conjunction with typical HTML form commands to write to variables in the CPU.

The descriptions of the AWP commands in the following pages use the following conventions:

- Items enclosed in brackets [ ] are optional.
- Items enclosed in angle brackets < > are parameter values to be specified.
- Quotation marks are a literal part of the command. They must be present as indicated.
- Special characters in tag or data block names, depending on usage, must be escaped or enclosed in quotation marks (Page 809).

Use a text editor or HTML editing mode to insert AWP commands into your pages.

NOTE

Expected syntax of AWP commands

The space after "<!--" and the space before "-->" in the formulation of an AWP command are essential to proper compiling of the command. Omission of the space characters can cause the compiler to be unable to generate the proper code. The compiler does not display an error in this case.

AWP command summary

The details for using each AWP command are in the topics to follow, but here is a brief summary of the commands:

Reading variables

```
:=<Varname>:
```

Writing variables

```
<!-- AWP_In_Variable Name='<Varname1>' [Use='<Varname2>'] ... -->
```

This AWP command merely declares the variable in the Name clause to be writable. Your HTML code performs writes to the variable by name from <input>, <select>, or other HTML statements within an HTML form.

Reading special variables

```
<!-- AWP_Out_Variable Name='<Type>:<Name>' [Use='<Varname>'] -->
```

Writing special variables

```
<!-- AWP_In_Variable Name='<Type>:<Name>' [Use='<Varname>']-->
```

Defining enum types

```
<!-- AWP_Enum_Def Name='<Enum type name>' Values='<Value>, <Value>,
... ' -->
```

Referencing enum types

```
<!-- AWP_In_Variable Name='<Varname>' Enum="<Enum type name>" -->
<!-- AWP_Out_Variable Name='<Varname>' Enum="<Enum type name>" -->
```

Creating fragments

```
<!-- AWP_Start_Fragment Name='<Name>' [Type=<Type>][ID=<id>] -->
```

Importing fragments

```
<!-- AWP_Import_Fragment Name='<Name>' -->
```

13.8.2.1 Reading variables

User-defined Web pages can read variables (PLC tags) and data block tags from the CPU, provided that you have configured the tags to be accessible from an HMI.

Syntax

```
:=<Varname>:
```

Parameters

<Varname>	The variable to be read, which can be a PLC tag name from your STEP 7 program, a data block tag, I/O, or addressable memory. For memory or I/O addresses or alias names (Page 809), do not use quotation marks around the tag name. For PLC tags, use double quotation marks around the tag name. For data block tags, enclose the block name only in double quotation marks. The tag name is outside of the quotation marks. Note that you use the data block name and not a data block number. Reference array elements using array element syntax.

Examples

```
:="Conveyor_speed":
:="My_Data_Block".flag1:
:=I0.0:
:=MW100:
:="My_Data_Block".Array_Dim1[0]:
:="My_Data_Block".Array_Dim2[0,0]:
```

Example reading an aliased variable

```
<!-- AWP_Out_Variable Name='flag1' Use='"My_Data_Block".flag1' -->
:=flag1:
```

NOTE

Defining alias names for PLC tags and data block tags is described in the topic Using an alias for a variable reference (Page 804).

If a tag name or data block name includes special characters, you must use additional quotation marks or escape characters as described in the topic Handling tag names that contain special characters (Page 809).

13.8.2.2 Writing variables

User-defined pages can write data to the CPU. This is accomplished by using an AWP command to identify a variable in the CPU to be writable from the HTML page. The variable must be specified by PLC tag name or data block tag name. You can declare multiple variable names in one statement. To write the data to the CPU, you use standard HTTP POST commands.

A typical usage is to design a form in your HTML page with text input fields or select list choices that correspond to writable CPU variables. As with all user-defined pages, you then generate the blocks from STEP 7 such that they are included in your STEP 7 program. When a user with privileges to modify variables subsequently accesses this page and types data into the input fields or selects a choice from a select list, the Web server converts the input to the appropriate data type for the variable, and writes the value to the variable in the CPU. Note that the name clause for HTML input fields and HTML select lists uses syntax typical for the name clause of the AWP_In_Variable command. Typically enclose the name in single quotation marks and if you reference a data block, enclose the data block name in double quotation marks.

For form management details, refer to documentation for HTML.

Syntax

```
<!-- AWP_In_Variable Name='<Varname1>' [Use='<Varname2>'] ... -->
```

Parameters

<Varname1>	If no Use clause is provided, Varname1 is the variable to be written. It can be a PLC tag name from your STEP 7 program, a tag from a specific data block, or a data block name. If a Use clause is provided, Varname1 is an alternate name for the variable referenced in <Varname2> (Page 804). It is a local name within the HTML page.
<Varname2>	If a Use clause is provided, Varname2 is the variable to be written. It can be a PLC tag name from your STEP 7 program or a tag from a specific data block.

For both Name clauses and Use clauses, the complete name must be enclosed in single quotation marks. Within the single quotes, use double quotation marks around a PLC tag and double quotation marks around a data block name. The data block name is within the double quotes but not the data block tag name. Note that for data block tags, you use the name of the block and not a data block number. Reference array elements using array element syntax.

If you use an AWP_In_Variable command to make a data block writable, then every tag in the data block is writable.

Examples using HTML input field

```
<!-- AWP_In_Variable Name='"Target_Level"' -->
<form method="post">
<p>Input Target Level: <input name='"Target_Level"' type="text" />
</p>
</form>

<!-- AWP_In_Variable Name='"Data_block_1".Braking' -->
<form method="post">
<p>Braking: <input name='"Data_block_1".Braking' type="text" />
%</p>
</form>

<!-- AWP_In_Variable Name='"Data_block_1".Array_Dim2' -->
<form method="post">
<p>Two-dimensional array value [2,1]: <input
name='"Data_block_1".Array_Dim2[2,1]' type="text" /> %</p>
</form>
```

Example using Use clause

```
<!-- AWP_In_Variable Name='"Braking"' Use='"Data_block_1".Braking'
-->
<form method="post">
<p>Braking: <input name='"Braking"' type="text" /> %</p>
</form>
```

Example using writable data block

```
<!-- AWP_In_Variable Name='"Data_block_1"' -->
<form method="post">
<p>Braking: <input name='"Data_block_1".Braking' type="text" /> %
</p>
<p>Turbine Speed: <input name='"Data_block_1".TurbineSpeed'
size="10" value='"Data_block_1".TurbineSpeed' type="text" />
</p>
</form>
```

Example using HTML select list

```
<!-- AWP_In_Variable Name='"Data_block_1".ManualOverrideEnable'-->
<form method="post">
<select name='"Data_block_1".ManualOverrideEnable'>
<option value=:"Data_block_1".ManualOverrideEnable:> </option>
<option value=1>Yes</option>
<option value=0>No</option>
```

```
</select><input type="submit" value="Submit setting" /></form>
```

NOTE

Only a user with the "Write process data through commands of the automation web page programming (AWP)" privilege (Page 757) can write data to the CPU. The Web server ignores the commands if the user does not have these privileges.

If a tag name or data block name includes special characters, you must use additional quotation marks or escape characters as described in the topic "Handling tag names that contain special characters (Page 809)".

13.8.2.3 Reading special variables

The Web server provides the ability to read values from the PLC to store in special variables in the HTTP response header. You might, for example, want to read a pathname from a PLC tag to redirect the URL to another location using the HEADER:Location special variable.

Syntax

```
<!-- AWP_Out_Variable Name='<Type>:<Name>' [Use='<Varname>'] -->
```

Parameters

<Type>	The type of special variable, which is one of the following: HEADER COOKIE_VALUE COOKIE_EXPIRES
<Name>	Refer to HTTP documentation for a list of all the names of HEADER variables. A few examples are listed below: Status: response code Location: path for redirection Retry-After: how long service is expected to be unavailable to the requesting client For types COOKIE_VALUE and COOKIE_EXPIRES, <Name> is the name of a specific cookie. COOKIE_VALUE:name: value of the named cookie COOKIE_EXPIRES:name: expiration time in seconds of named cookie The Name clause must be enclosed in single or double quotation marks. If no Use clause is specified, the special variable name corresponds to a PLC tag name. Enclose the complete Name clause within single quotation marks and the PLC tag in double quotation marks. The special variable name and PLC tag name must match exactly.
<Varname>	Name of the PLC tag or data block tag into which the variable is to be read The Varname must be enclosed in single quotation marks. Within the single quotes, use double quotation marks around a PLC tag or data block name. The data block name is within the double quotes but not the data block tag name. Note that for data block tags, you use the name of the block and not a data block number.

If a tag name or data block name includes special characters, you must use additional quotation marks or escape characters as described in the topic Handling tag names that contain special characters (Page 809).

Example: Reading a special variable with no Use clause

```
<!-- AWP_Out_Variable Name='"HEADER:Status"' -->
```

In this example, the HTTP special variable "HEADER:Status" receives the value of the PLC tag "HEADER:Status". The name in the PLC tag table must match the name of the special variable exactly if no Use clause is specified.

Example: Reading a special variable with a Use clause

```
<!-- AWP_Out_Variable Name='HEADER:Status' Use='"Status"' -->
```

In this example, the special variable "HEADER:Status" receives the value of the PLC tag "Status".

13.8.2.4 Writing special variables

The Web server provides the ability to write values to the CPU from special variables in the HTTP request header. For example, you can store information in STEP 7 about the cookie associated with a user-defined Web page, the user that is accessing a page, or header information. The Web server provides access to specific special variables that you can write to the CPU when logged in as a user with privileges to modify variables.

Syntax

```
<!-- AWP_In_Variable Name='<Type>:<Name>' [Use='<Varname>']-->
```

Parameters

<Type>	The type of special variable and is one of the following: HEADER SERVER COOKIE_VALUE
<Name>	Specific variable within the types defined above, as shown in these examples: HEADER:Accept: content types that are acceptable HEADER:User-Agent: information about the user agent originating the request. SERVER:current_user_id: id of the current user; 0 if no user logged in SERVER:current_user_name: name of the current user COOKIE_VALUE:<name>: value of the named cookie Enclose the Name clause in single quotation marks. If no Use clause is specified, the special variable name corresponds to a PLC variable name. Enclose the complete Name clause within single quotation marks and the PLC tag in double quotation marks. The special variable name must match the PLC tag name exactly. Refer to HTTP documentation for a list of all the names of HEADER variables.
<Varname>	The variable name in your STEP 7 program into which you want to write the special variable, which can be a PLC tag name, or a data block tag. The Varname must be enclosed in single quotation marks. Within the single quotes, use double quotation marks around a PLC tag or data block name. The data block name is within the double quotes but not the data block tag name. Note that for data block tags, you use the name of the block and not a data block number.

Examples

```
<!-- AWP_In_Variable Name='"SERVER:current_user_id"' -->
```

In this example, the Web page writes the value of the HTTP special variable "SERVER:current_user_id" to the PLC tag named "SERVER:current_user_id ".

```
<!-- AWP_In_Variable Name=SERVER:current_user_id' Use='"my_userid"'
-->
```

In this example, the Web page writes the value of the HTTP special variable "SERVER:current_user_id" to the PLC tag named "my_userid".

NOTE

Only a user with the "Write process data through commands of the automation web page programming (AWP)" privilege (Page 757) can write data to the CPU. The Web server ignores the commands if the user does not have these privileges.

If a tag name or data block name includes special characters, you must use additional quotation marks or escape characters as described in the topic "Handling tag names that contain special characters (Page 809)".

13.8.2.5 Using an alias for a variable reference

You can use an alias in your user-defined Web page for an In_Variable or an Out_Variable. For example, you can use a different symbolic name in your HTML page than the one used in the CPU, or you can equate a variable in the CPU with a special variable. The AWP Use clause provides this capability.

Syntax

```
<-- AWP_In_Variable Name='<Varname1>' Use='<Varname2>' -->
<-- AWP_Out_Variable Name='<Varname1>' Use='<Varname2>' -->
```

Parameters

<Varname1>	The alias name or special variable name Varname1 must be enclosed in single or double quotation marks.
<Varname2>	Name of the PLC variable for which you want to assign an alias name. The variable can be a PLC tag, a data block tag, or a special variable. Varname2 must be enclosed in single quotation marks. Within the single quotes, use double quotation marks around a PLC tag, special variable, or data block name. The data block name is within the double quotes but not the data block tag name. Note that for data block tags, you use the name of the block and not a data block number.

Examples

```
<-- AWP_In_Variable Name='SERVER:current_user_id'
Use='"Data_Block_10".server_user' -->
```

In this example, the special variable SERVER:current_user_id is written to the tag "server_user" in data block "Data_Block_10".

```
<-- AWP_Out_Variable Name='Weight'
Use='"Data_Block_10".Tank_data.Weight' -->
```

In this example, the value in data block structure member Data_Block_10.Tank_data.Weight can be referenced simply by "Weight" throughout the rest of the user-defined Web page.

```
<-- AWP_Out_Variable Name='Weight' Use='"Raw_Milk_Tank_Weight"' -->
```

In this example, the value in the PLC tag "Raw_Milk_Tank_Weight" can be referenced simply by "Weight" throughout the rest of the user-defined Web page.

If a tag name or data block name includes special characters, you must use additional quotation marks or escape characters as described in the topic Handling tag names that contain special characters (Page 809).

13.8.2.6 Defining enum types

You can define enum types in your user-defined pages and assign the elements in an AWP command.

Syntax

```
<!-- AWP_Enum_Def Name='<Enum type name>' Values='<Value>,
<Value>,... ' -->
```

Parameters

<Enum type name>	Name of the enumerated type, enclosed in single or double quotation marks.
<Value>	<constant>:<name> The constant indicates the numerical value for the enum type assignment. The total number is unbounded. The name is the value assigned to the enum element.

Note that the entire string of enum value assignments is enclosed in single quotation marks, and each individual enum type element assignment is enclosed in double quotation marks. The scope of an enum type definition is global for the user-defined Web pages. If you have set up your user-defined Web pages in language folders (Page 826), the enum type definition is global for all pages in the language folder.

Example

```
<!-- AWP_Enum_Def Name='AlarmEnum' Values='0:"No alarms", 1:"Tank is
full", 2:"Tank is empty"' -->
```

13.8.2.7 Referencing CPU variables with an enum type

You can assign a variable in the CPU to an enum type. This variable can be used elsewhere in your user-defined Web page in a read operation (Page 799) or a write operation (Page 800). On a read operation, the Web server will replace the numerical value that is read from the CPU with the corresponding enum text value. On a write operation, the Web server will replace the text value with the integer value of the enumeration that corresponds to the text before writing the value to the CPU.

Syntax

```
<!-- AWP_In_Variable Name='<Varname>' Enum="<EnumType>" -->
<!-- AWP_Out_Variable Name='<Varname>' Enum="<EnumType>" -->
```

Parameters

<Varname>	Name of PLC tag or data block tag to associate with the enum type, or the name of the alias name for a PLC tag (Page 804) if declared. Varname must be enclosed in single quotation marks. Within the single quotes, use double quotation marks around a PLC tag or data block name. Note that for data block tags, you use the name of the block and not a data block number. The data block name is within the double quotes but not the data block tag name.
<EnumType>	Name of the enumerated type, which must be enclosed in single or double quotation marks

The scope of an enum type reference is the current fragment.

Example usage in a variable read

```
<!-- AWP_Out_Variable Name='"Alarm"' Enum="AlarmEnum" -->...
<p>The current value of "Alarm" is :="Alarm":</p>
```

If the value of "Alarm" in the CPU is 2, the HTML page displays 'The current value of "Alarm" is Tank is empty' because the enum type definition (Page 805) assigns the text string "Tank is empty" to the numerical value 2.

Example usage in a variable write

```
<!-- AWP_Enum_Def Name='AlarmEnum' Values='0:"No alarms", 1:"Tank is
full", 2:"Tank is empty"' -->
<!-- AWP_In_Variable Name='"Alarm"' Enum='AlarmEnum' -->...
<form method="POST">
<p><input type="hidden" name='"Alarm"' value="Tank is full" /></p>
<p><input type="submit" value='Set Tank is full' /><p>
</form>
```

Because the enum type definition (Page 805) assigns "Tank is full" to the numerical value 1, the value 1 is written to the PLC tag named "Alarm" in the CPU.

Note that the Enum clause in the AWP_In_Variable declaration must correspond exactly to the Name clause in the AWP_Enum_Def declaration.

Example usage in a variable write with use of an alias

```
<!-- AWP_Enum_Def Name='AlarmEnum' Values='0:"No alarms", 1:"Tank is
full", 2:"Tank is empty"' -->
<!-- AWP_In_Variable Name='"Alarm"' Enum='AlarmEnum'
Use='"Data_block_4".Motor1.Alarm'-->...
<form method="POST">
<p><input type="hidden" name='"Alarm"' value="Tank is full" /></p>
<p><input type="submit" value='Set Tank is full' /><p>
</form>
```

Because the enum type definition (Page 805) assigns "Tank is full" to the numerical value 1, the value 1 is written to the alias "Alarm" which corresponds to the PLC tag named "Motor1.Alarm" in data block "Data_Block_4" in the CPU.

If a tag name or data block name includes special characters, you must use additional quotation marks or escape characters as described in the topic Handling tag names that contain special characters (Page 809).

NOTE

Previous releases required a separate AWP_Enum_Ref declaration to associate a variable with a defined enum type. STEP 7 and the S7-1200 support existing code with AWP_Enum_Ref declarations; however, this command is no longer needed.

13.8.2.8 Creating fragments

STEP 7 converts and stores user-defined Web pages as a control DB and fragment DBs when you click "Generate blocks" in the CPU Properties for the Web server. You can set up specific fragments for specific pages or for sections of specific pages. You can identify these fragments by a name and number with the "Start_Fragment" AWP command. Everything in the page following the AWP_Start_Fragment command belongs to that fragment until another AWP_Start_Command is issued or until end of file is reached.

Syntax

```
<!-- AWP_Start_Fragment Name='<Name>'
[Type=<Type>][ID=<id>][Mode=<Mode>] -->
```

Parameters

<Name>	Text string: name of fragment DB Fragment names must begin with a letter or underscore and be comprised of letters, numeric digits, and underscores. The fragment name is a regular expression of the form: [a-zA-Z_][a-zA-Z_0-9]*
<Type>	"manual" or "automatic" manual: The STEP 7 program must request this fragment and can respond accordingly. Operation of the fragment must be controlled with STEP 7 and the control DB variables. automatic: The Web server processes the fragment automatically. If you do not specify the type parameter, the default is "automatic".

<id>	Integer identification number. If you do not specify the ID parameter, the Web server assigns a number by default. For manual fragments, set the ID to a low number. The ID is the means by which the STEP 7 program controls a manual fragment.
<Mode>	"visible" or "hidden" visible: Contents of the fragment will display on the user-defined Web page. hidden: Contents of the fragment will not display on the user-defined Web page. If you do not specify the type parameter, the default is "visible".

Manual fragments

If you create a manual fragment for a user-defined Web page or portion of a page, then your STEP 7 program must control when the fragment is sent. The STEP 7 program must set appropriate parameters in the control DB for a user-defined page under manual control and then call the WWW instruction with the control DB as modified. For understanding the structure of the control DB and how to manipulate individual pages and fragments, see the topic Advanced user-defined Web page control (Page 829).

13.8.2.9 Importing fragments

You can create a named fragment from a portion of your HTML code and then import that fragment elsewhere in your set of user-defined Web pages. For example, consider a set of user-defined Web pages that has a start page and then several other HTML pages accessible from links on the start page. Suppose each of the separate pages is to display the company logo on the page. You could implement this by creating a fragment (Page 807) that loads the image of the company logo. Each individual HTML page could then import this fragment to display the company logo. You use the AWP Import_Fragment command for this purpose. The HTML code for the fragment only exists in one fragment, but you can import this fragment DB as many times as necessary in as many Web pages as you choose.

Syntax

```
<!-- AWP_Import_Fragment Name='<Name>' -->
```

Parameters

<Name>	Text string: name of the fragment DB to be imported

Example

Excerpt from HTML code that creates a fragment to display an image:

```
<!-- AWP_Start_Fragment Name='My_company_logo' --><p><img
src="company_logo.jpg"></p>
```

Excerpt from HTML code in another .html file that imports the fragment that displays the logo image:

```
<!-- AWP_Import_Fragment Name='My_company_logo' -->
```

Both .html files (the one that creates the fragment and the one that imports it) are in the folder structure that you define when you configure the user-defined pages in STEP 7 (Page 811).

13.8.2.10 Combining definitions

When declaring variables for use in your user-defined Web pages, you can combine a variable declaration and an alias for the variable (Page 804). You can also declare multiple In_Variables in one statement and multiple Out_Variables in one statement.

Examples

```
<!-- AWP_In_Variable Name='"Level"' Name='"Weight"' Name='"Temp"'
-->
<!-- AWP_Out_Variable Name='HEADER:Status' Use='"Status"'
        Name='HEADER:Location' Use="Location"
        Name='COOKIE_VALUE:name' Use="my_cookie" -->
<!-- AWP_In_Variable Name='Alarm' Use='"Data_block_10".Alarm' -->
```

13.8.2.11 Handling tag names that contain special characters

When specifying variable names in user-defined Web pages, you must take special care if tag names contain characters that have special meanings.

Reading variables

You use the following syntax to read a variable (Page 799):

:=<Varname>:

The following rules apply to reading variables:

- For variable names from the PLC tag table, enclose the tag name in double quotation marks.
- For variable names that are data block tags, enclose the data block name in double quotation marks. The tag is outside of the quotation marks.
- For variable names that are direct I/O addresses, memory addresses, or alias names, do not use quotation marks around the read variable.
- For tag names or data block tag names that contain a backslash, precede the backslash with another backslash.
- If a tag name or data block tag name contains a colon, less than sign, greater than sign, or ampersand define an alias that has no special characters for the read variable, and read the variable using the alias. Precede colons in tag names in a Use clause with a backslash.

Table 13-1 Examples of Read variables

Data block name	Tag name	Read command
n/a	ABC:DEF	`<!--AWP_Out_Variable Name='special_tag' Use='"ABC:DEF"' --> :=special_tag:`
n/a	T\	`:="T\\":`
n/a	A \B 'C :D	`<!--AWP_Out_Variable Name='another_special_tag' Use='"A \\B \'C :D"' --> :=another_special_tag:`
n/a	a<b	`<!--AWP_Out_Variable Name='a_less_than_b' Use='"a<b"' --> :=a_less_than_b:`
Data_block_1	Tag_1	`:="Data_block_1".Tag_1:`
Data_block_1	ABC:DEF	`<!-- AWP_Out_Variable Name='special_tag' Use='"Data_block_1".ABC\:DEF'--> :=special_tag:`
DB A' B C D$ E	Tag	`:="DB A' B C D$ E".Tag:`
DB:DB	Tag:Tag	`<!--AWP_Out_Variable Name='my_tag' Use='"DB:DB".Tag\:Tag' --> :=my_tag:`

Name and Use clauses

The AWP commands AWP_In_Variable, AWP_Out_Variable, AWP_Enum_Def, AWP_Enum_Ref, AWP_Start_Fragment and AWP_Import_Fragment have Name clauses. HTML form commands such as <input> and <select> also have name clauses. AWP_In_Variable and AWP_Out_Variable can additionally have Use clauses. Regardless of the command, the syntax for Name and Use clauses regarding the handling of special characters is the same:

- The text you provide for a Name or Use clause must be enclosed within single quotation marks. If the enclosed name is a PLC tag or Data block name, use single quotation marks for the full clause.
- Within a Name or Use clause, data block names and PLC tag names must be enclosed within double quotation marks.
- If a tag name or Data block name includes a single quote character or backslash, escape that character with a backslash. The backslash is the escape character in the AWP command compiler.

Table 13-2 Examples of Name clauses

Data block name	Tag name	Name clause options
n/a	ABC'DEF	`Name='"ABC\'DEF"'`
n/a	A \B 'C :D	`Name='"A \\B \'C :D"'`
Data_block_1	Tag_1	`Name='"Data_block_1".Tag_1'`
Data_block_1	ABC'DEF	`Name='"Data_block_1".ABC\'DEF'`
Data_block_1	A \B 'C :D	`Name='"Data_block_1".A \\B \'C :D'`
DB A' B C D$ E	Tag	`Name='"DB A\' B C D$ E".Tag'`

Use clauses follow the same conventions as Name clauses.

NOTE

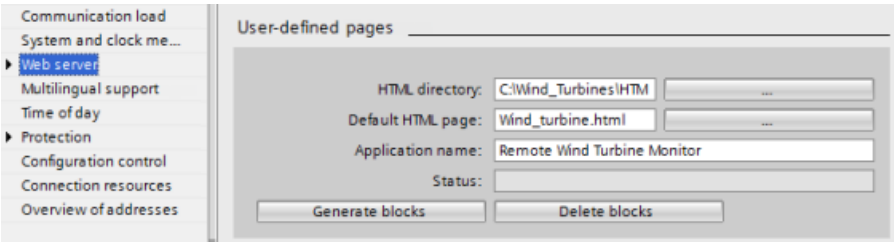
Regardless of what characters you use in your HTML page, set the charset of the HTML page to UTF-8 and save it from the editor with UTF-8 character encoding.

13.8.3 Configuring use of user-defined Web pages

To configure user-defined Web pages from STEP 7, follow these steps:

1. Select the CPU in the Device Configuration view.
2. Display the "Web server" properties in the inspector window for the CPU.
3. If not already selected, select the check box for "Activate Web server on this module".
4. Select "Permit access only with HTTPS" to ensure that the Web server uses encrypted communication and to increase the security of your Web-accessible CPU.
5. Enter or browse to the folder name on your PC where you saved the HTML default page (start page).
6. Enter the name of the default page.
7. Provide a name for your application (optional). The Web server uses the application name to further subcategorize or group web pages. When you provide an application name, the Web server creates an URL for your user-defined page in the following format: http[s]://ww.xx.yy.zz/awp/<application name>/<pagename>.html. If you do not provide an application name, the URL is http[s]://ww.xx.yy.zz/awp/<pagename>.html.

   Avoid special characters in the application name. Some characters can cause the Web server to be unable to display the user-defined pages.



8. In the Advanced section, enter filename extensions of files that include AWP commands. By default, STEP 7 analyzes files with .htm, .html, or .js extensions. If you have additional file extensions, append them. To save processing resources, do not enter file extensions if no files of that type include AWP commands.
9. Keep the default for the Web DB number, or enter a number of your choice. This is the DB number of the control DB that controls display of the Web pages.
10. Keep the default for the fragment DB start number, or enter a number of your choice. This is the first of the fragment DBs that contains the Web pages.

Generating program blocks

When you click the "Generate blocks" button, STEP 7 generates data blocks from the HTML pages in the HTML source directory that you specified and a control data block for the operation of your Web pages. You can set these attributes as needed for your application (Page 812). STEP 7 also generates a set of fragment data blocks to hold the representation of all of your HTML pages. When you generate the data blocks, STEP 7 updates the properties to display the control data block number, and the number of the first of the fragment data blocks. After you generate the data blocks, your user-defined Web pages are a part of your

STEP 7 program. The blocks corresponding to these pages appear in the Web server folder, which is in the System blocks folder under Program blocks in the project navigation tree.

Deleting program blocks

To delete data blocks that you have previously generated, click the "Delete data blocks" button. STEP 7 deletes the control data block and all of the fragment data blocks from your project that correspond to user-defined Web pages.

13.8.4 Configuring the entry page

In the Device configuration of the CPU, you have the opportunity to designate a user-defined Web page to be the entry page when you access the Web server from either a PC or a mobile device. Otherwise, the entry page is the Introduction (Page 772) standard Web page.

To select a user-defined Web page to be the entry page, follow these steps:

1. Select the CPU in the Device configuration view.
2. In the inspector window, select "Web server" from the CPU properties and enable the Web server (Page 755).
3. Select "Entry page" in the Web server properties.
4. Select "AWP1" from the drop-down list to configure the Web server to display a user-defined page upon access. (The other selection, "Start page", sets the Web server to display the standard Introduction Web page upon access.)

Users must have the "Open user-defined web pages" privilege (Page 757). The STEP 7 program must include a call to the WWW instruction (Page 812).

After you have completed configuration and downloaded the project to the CPU, the Web server can use the "Default HTML page" that you selected when you configured your user-defined Web pages (Page 811) as the entry page.

NOTE

The CPU must be in RUN mode to display a user-defined entry page.

13.8.5 Programming the WWW instruction for user-defined web pages

Your STEP 7 user program must include and execute the WWW instruction in order for the user-defined Web pages to be accessible from the standard Web pages. The control data block is the input parameter to the WWW instruction and specifies the content of the pages as represented in the fragment data blocks, as well as state and control information. STEP 7 creates the control data block when you click the "Create blocks" button in the configuration of user-defined Web pages (Page 811).

Programming the WWW instruction

The STEP 7 program must execute the WWW instruction for the user-defined Web pages to be accessible from the standard Web pages. You might want the user-defined Web pages available only under certain circumstances as dictated by your application requirements and preferences. In this case, your program logic can control when to call the WWW instruction.

Table 13-3 WWW instruction

LAD / FBD	SCL	Description
	ret_val := WWW(ctrl_db:=_uint_in_);	Provides access to user-defined Web pages from standard Web pages

You must provide the control data block input parameter (CTRL_DB) which corresponds to the integer DB number of the control DB. You can find this control DB block number (called Web DB Number) in the Web Server properties of the CPU after you create the blocks for the user-defined Web pages. Enter the integer DB number as the CTRL_DB parameter of the WWW instruction. The return value (RET_VAL) contains the function result. Note that the WWW instruction executes asynchronously and that the RET_VAL output might have an initial value of 0 although an error can occur later. The program can check the state of the control DB to ensure that the application started successfully, or check RET_VAL with a subsequent call to WWW.

Table 13-4 Return value

RET_VAL	Description
0	No error
16#00yx	x: The request represented by the respective bit is in the waiting state: x=1: request 0 x=2: request 1 x=4: request 2 x=8: request 3 The x values can be logically OR-ed to represent waiting states of multiple requests. If x = 6, for example, requests 1 and 2 are waiting. y: 0: no error; 1: error exists and "last_error" has been set in the control DB (Page 829)
16#803a	The control DB is not loaded.
16#8081	The control DB is of the wrong type, format, or version.
16#80C1	No resources are available to initialize the web application.

Usage of the Control DB

STEP 7 creates the control data block when you click "Generate blocks" and displays the control DB number in the User-defined Web pages properties. You can find the control DB as well in the Program blocks folder in the project navigation tree.

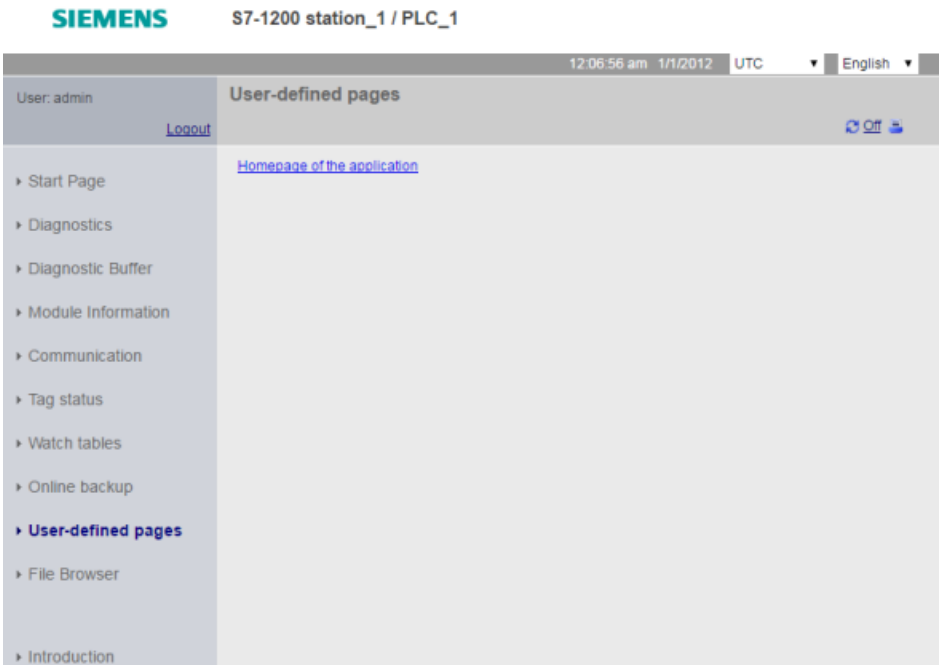
Typically, your STEP 7 program uses the control DB directly as created by the "Generate blocks" process with no additional manipulation. However, the STEP 7 user program can set global commands in the control DB to deactivate the web server or to subsequently re-enable it. Also, for user-defined pages that you create as manual fragment DBs (Page 811), the STEP 7 user program must control the behavior of these pages through a request table in the control DB. For information on these advanced tasks, see the topic Advanced user-defined Web page control (Page 829).

13.8.6 Downloading the program blocks to the CPU

After you have generated the blocks for user-defined Web pages, they are part of your STEP 7 program just like any other program blocks. You follow the normal process to download the program blocks to the CPU. Note that you can only download user-defined Web page program blocks when the CPU is in STOP mode.

13.8.7 Accessing the user-defined Web pages

You access your user-defined Web pages from the standard Web pages (Page 764). The standard Web pages display a link for "User-defined pages" on the left side navigation menu. The basic page navigation also provides a link to "User-defined pages". When you click the "User-defined pages" link, your Web browser goes to the page that provides a link to your default page. From within the user-defined pages, navigation is according to how you designed your specific pages.



NOTE

You can also define a user-defined page as the entry page (Page 812) for the Web server.

13.8.8 Constraints specific to user-defined Web pages

The constraints for standard Web pages (Page 834) also apply to user-defined Web pages. In addition, user-defined Web pages have some specific considerations.

Load memory space

Your user-defined Web pages become data blocks when you click "Generate blocks", which require load memory space. If you have a memory card installed, you have up to the capacity of your memory card as external load memory space for the user-defined Web pages.

If you do not have a memory card installed, these blocks take up internal load memory space, which is limited according to your CPU model.

You can check the amount of load memory space that is used and the amount that is available from the Online and Diagnostic tools in STEP 7. You can also look at the properties for the individual blocks that STEP 7 generates from your user-defined Web pages and see the load memory consumption.

NOTE

If you need to reduce the space required for your user-defined Web pages, reduce your use of images if applicable.

Quotation marks in text strings

Avoid using text strings that contain embedded single or double quotation marks in data block tags that you use for any purpose in user-defined Web pages. Because HTML syntax often uses single quotes or double quotes as delimiters, quotation marks within text strings can break the display of user-defined Web pages.

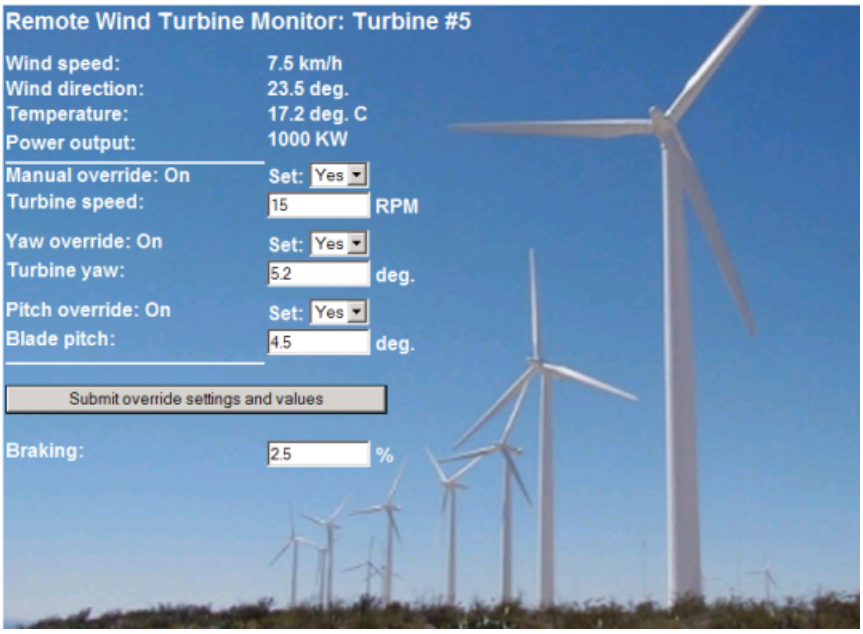
For data block tags of type String that you use in user-defined Web pages, observe the following rules:

- Do not enter single or double quotation marks in the data block tag string value in STEP 7.
- Do not let the user program make assignments of strings containing quotes to these data block tags.

13.8.9 Example of a user-defined web page

13.8.9.1 Web page for monitoring and controlling a wind turbine

As an example of a user-defined Web page, consider a Web page that is used to remotely monitor and control a wind turbine:



Description

In this application, each wind turbine in a wind turbine farm is equipped with an S7-1200 for control of the turbine. Within the STEP 7 program, each wind turbine has a data block with data specific to that wind turbine.

The user-defined Web page provides remote turbine access from a PC. A user can connect to standard web pages of the CPU of a particular wind turbine and access the user-defined "Remote Wind Turbine Monitor" Web page to see the data for that turbine. A user with the "Write process data" privilege can also put the turbine in manual mode and control the variables for turbine speed, yaw, and pitch from the Web page.

A user with these privileges can also set a braking value regardless of whether the turbine is under manual or automatic control.

The STEP 7 program would check the Boolean values for overriding automatic control, and if set, would use the user-entered values for turbine speed, yaw, and pitch. Otherwise, the program would ignore these values.

Files used

This user-defined Web page example consists of three files:

- **Wind_turbine.html**: This is the HTML page that implements the display shown above, using AWP commands to access controller data.
- **Wind_turbine.css**: This is the cascading style sheet that contains formatting styles for the HTML page. Use of a cascading style sheet is optional, but it can simplify the HTML page development.
- **Wind_turbine.jpg**: This is the background image that the HTML page uses. Use of images in user-defined Web pages is, of course, optional, and does require additional space in the CPU.

These files are not provided with your installation, but are described as an example.

Implementation

The HTML page uses AWP commands to read values from the PLC (Page 799) for the display fields and to write values to the PLC (Page 800) for data coming from user input. This page also uses AWP commands for enum type definition (Page 805) and reference (Page 806) for handling ON/OFF settings.

The first part of the page displays a header line that includes the wind turbine number.

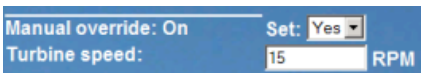
The next part of the page displays atmospheric conditions at the wind turbine. I/O at the turbine site provide the wind speed, wind direction, and current temperature.

Figure

Next, the page displays the power output of the turbine as read from the S7-1200.

The following sections allow for manual control of the turbine, overriding the normal automatic control by the S7-1200. These types are as follows:

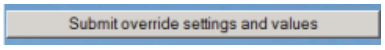
- Manual override: enables manual override of the turbine. The STEP 7 user program requires that the manual override setting be true before enabling the use of any of the manual settings for turbine speed, or yaw or pitch.



- Yaw override: enables manual override of the yaw setting, and a manual setting for the yaw. The STEP 7 user program requires that both manual override and yaw override be true in order to apply the yaw setting.

- Pitch override: enables manual override of the pitch of the blades. The STEP 7 user program requires that both manual override and pitch override be true in order to apply the blade pitch setting.

The HTML page includes a submit button to post the override settings to the controller.



The braking user input field provides a manual setting for a braking percentage. The STEP 7 user program does not require manual override to accept a braking value.

In addition, the HTML page uses an AWP command to write the special variable (Page 803) that contains the user ID of the user that is accessing the page to a tag in the PLC tag table.

13.8.9.2 Reading and displaying controller data

The "Remote Wind Turbine Monitor" HTML page uses numerous AWP commands for reading data from the controller (Page 799) and displaying it on the page. For example, consider the HTML code for displaying the power output as shown in this portion of the example Web page:

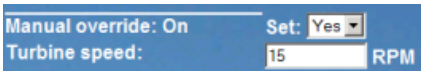
Example HTML code

The following excerpt from the "Remote Wind Turbine Monitor" HTML page displays the text "Power Output:" in the left cell of a table row and reads the variable for the power output and displays it in the right cell of the table row along with the text abbreviation for kilowatts, kW. The AWP command :="Data_block_1".PowerOutput: performs the read operation. Note that data blocks are referenced by name, not by data block number (that is, "Data_block_1" and not "DB1").

```
<tr style="height:2%;">
<td>
<p>Power output:</p>
</td>
<td>
<p style="margin-bottom:5px;"> :="Data_block_1".PowerOutput: kW</p>
</td>
</tr>
```

13.8.9.3 Using an enum type

The "Remote Wind Turbine Monitor" HTML page uses enum types for the three instances where HTML page displays "ON" or "OFF" for a Boolean value, and for where the user sets a Boolean value. The enum type for "ON" results in a value of 1, and the enum type for "OFF" results in a value of 0. For example, consider the HTML code for reading and writing the Manual Override Enable setting in "Data_block_1".ManualOverrideEnable value using an enum type:



Example HTML code

The following excerpts from the "Remote Wind Turbine Monitor" HTML page show how to declare an enum type called "OverrideStatus" with values of "Off" and "On" for 0 and 1, and then setting an enum type reference to OverrideStatus for the ManualOverrideEnable Boolean tag in the data block named "Data_block_1".

```
<!-- AWP_In_Variable Name='"Data_block_1".ManualOverrideEnable'
Enum="OverrideStatus" -->
<!-- AWP_Enum_Def Name="OverrideStatus" Values='0:"Off",1:"On"' -->
```

Where the HTML page includes a display field in a table cell for the current state of ManualOverrideEnable, it uses just a normal read variable command, but with the use of the previously declared and referenced enum type, the page displays "Off" or "On" rather than 0 or 1.

```
<td style="width:24%; border-top-style: Solid; border-top-width:
2px; border-top-color: #ffffff;">
<p>Manual override: :="Data_block_1".ManualOverrideEnable:</p>
</td>
```

The HTML page includes a drop-down select list for the user to change the value of ManualOverrideEnable. The select list uses the text "Yes" and "No" to display in the select lists. With the use of the enum type, "Yes" is correlated to the value "On" of the enum type, and "No" is correlated to the value "Off". The empty selection leaves the value of ManualOverrideEnable as it is.

```
<select name='"Data_block_1".ManualOverrideEnable'>
<option value=':"Data_block_1".ManualOverrideEnable:'> </option>
<option value="On">Yes</option>
<option selected value="Off">No</option>
</select>
```

The select list is included within a form on the HTML page. When the user clicks the submit button, the page posts the form, which writes a value of "1" to the Boolean ManualOverrideEnable in Data_block_1 if the user had selected "Yes", or "0" if the user had selected "No".

13.8.9.4 Writing user input to the controller

The "Remote Wind Turbine Monitor" HTML page includes several AWP commands for writing data to the controller (Page 800). The HTML page declares AWP_In_Variables for Boolean variables so that a user with the "Write process data" privilege can put the wind turbine under manual control and enable manual override for the turbine speed, yaw override, and/or blade pitch override. The page also uses AWP_In_Variables to allow a user with these privileges to subsequently set floating-point values for the turbine speed, yaw, pitch, and braking percentage. The page uses an HTTP form post command to write the AWP_In_Variables to the controller.

For example, consider the HTML code for manually setting the braking value:

Example HTML code

The following excerpt from the "Remote Wind Turbine Monitor" HTML page first declares an AWP_In_Variable for "Data_block_1" that enables the HTML page to write to any tags in the data block "Data_block_1". The page displays the text "Braking:" in the left cell of a table row. In the right cell of the table row is the field that accepts user input for the "Braking" tag of "Data_block_1". This user input value is within an HTML form that uses the HTTP method

"POST" to post the entered text data to the CPU. The page then reads the actual braking value from the controller and displays it in the data entry field.

A user with the "Write process data" privilege can use this page to write a braking value to the data block in the CPU that controls braking.

```
<!-- AWP_In_Variable Name='"Data_block_1"' -->
...
<tr style="vertical-align: top; height: 2%;">
<td style="width: 22%;"><p>Braking:</p></td>
<td>
<form method="POST">
<p><input name='"Data_block_1".Braking' size="10" type="text"> %</p>
</form>
</td>
</tr>
```

NOTE

Note that if a user-defined page has a data entry field for a writable data block tag that is a string data type, the user must enclose the string in single quotation marks when entering the string value in the field.

NOTE

Note that if you declare an entire data block in an AWP_In_Variable declaration such as <!-- AWP_In_Variable Name='"Data_block_1"' -->, then every tag within that data block can be written from the user-defined Web page. Use this when you intend for all of the tags in a data block to be writable. Otherwise, if you only want specific data block tags to be writable from the user-defined Web page, declare it specifically with a declaration such as <!-- AWP_In_Variable Name='"Data_block_1".Braking' -->

13.8.9.5 Writing a special variable

The "Remote Wind Turbine Monitor" Web page writes the special variable SERVER:current_user_id to a PLC tag in the CPU, providing that the user has the "Write process data" privilege. In this case, the PLC tag value contains the user ID of the user who is accessing the "Remote Wind Turbine Monitor" Web page.

The Web page writes the special variable to the PLC and requires no user interface.

Example HTML code

```
<!-- AWP_In_Variable Name="SERVER:current_user_id" Use="User_ID"-->
```

13.8.9.6 Reference: HTML listing of remote wind turbine monitor Web page

Wind_turbine.html

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<!--
This test program simulates a Web page to monitor and control a Wind
Turbine
Required PLC tags and Data Block Tags in STEP 7:
```

```
PLC Tag:
User_ID: Int

Data Blocks:
Data_block_1

Tags in Data_Block_1:

TurbineNumber: Int
WindSpeed: Real
WindDirection: Real
Temperature: Real
PowerOutput: Real
ManualOverrideEnable: Bool
TurbineSpeed: Real
YawOverride: Bool
Yaw: Real
PitchOverride: Bool
Pitch: Real
Braking: Real
The user-defined Web page displays current values for the PLC data,
and provides a select list to set the three Booleans using an
enumerated type assignment. The "Submit" button posts the selected
Boolean values as well as the data entry fields for TurbineSpeed,
Yaw, and Pitch. The value for Braking can be set without use of the
"Submit" button.

No actual STEP 7 program is required to use this page.
Theoretically, the STEP 7 program would only act on the values of
TurbineSpeed, Yaw, and Pitch, if the associated Booleans were set.
The only STEP 7 requirement is to call the WWW instruction with the
DB number of the generated data blocks for this page.
-->
<!-- AWP_In_Variable Name='"Data_block_1"' -->
<!-- AWP_In_Variable Name='"Data_block_1".ManualOverrideEnable'
Enum="OverrideStatus" -->
<!-- AWP_In_Variable Name='"Data_block_1".PitchOverride'
Enum="OverrideStatus" -->
<!-- AWP_In_Variable Name='"Data_block_1".YawOverride'
Enum="OverrideStatus" -->
<!-- AWP_In_Variable Name="SERVER:current_user_id" Use="User_ID"-->
<!-- AWP_Enum_Def Name="OverrideStatus" Values='0:"Off",1:"On"' -->

<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<link rel="stylesheet" href="Wind_turbine.css">
<title>Remote Wind Turbine Monitor</title>
</head>
<body>
<table cellpadding="0" cellspacing="2">
<tr style="height: 2%;">
<td colspan="2">
<h2>Remote Wind Turbine Monitor: Turbine
#:="Data_block_1".TurbineNumber:</h2>
</td>
```

```
<tr style="height: 2%;"><td style="width: 25%;"><p>Wind
speed:</p></td>
<td><p> :="Data_block_1".WindSpeed: km/h</p></td>
</tr>

<tr style="height: 2%;">
<td style="width: 25%;"><p>Wind direction:</p></td>

<td><p> :="Data_block_1".WindDirection: deg.</p></td>
</tr>

<tr style="height: 2%;"><td style="width:
25%;"><p>Temperature:</p></td>
<td><p> :="Data_block_1".Temperature: deg. C</p></td>
</tr>

<tr style="height: 2%;">
<td style="width: 25%;"><p>Power output:</p></td>
<td><p style="margin-bottom:5px;"> :="Data_block_1".PowerOutput:
kW</p>
</td>
</tr>

<form method="POST" action="">
<tr style="height: 2%;" >
<td style="width=25%; border-top-style: Solid; border-top-width:
2px; border-top-color: #ffffff;">
<p>Manual override: :="Data_block_1".ManualOverrideEnable:</p>
</td>
<td class="Text">Set:

<select name='"Data_block_1".ManualOverrideEnable'>
<option value=':="Data_block_1".ManualOverrideEnable:'> </option>
<option value="On">Yes</option>
<option value="Off">No</option>
</select>

</td>
</tr>

<tr style="vertical-align: top; height: 2%;"><td style="width:
25%;"><p>Turbine speed:</p></td>
<td>
<p style="margin-bottom:5px;"><input
name='"Data_block_1".TurbineSpeed' size="10"
value=':="Data_block_1".TurbineSpeed:' type="text"> RPM</p>
</td>
</tr>

<tr style="vertical-align: top; height: 2%;">
<td style="width: 25%;">
<p>Yaw override: :="Data_block_1".YawOverride: </p>
</td>
<td class="Text">Set:
```

```
<select name='"Data_block_1".YawOverride'>
<option value=':="Data_block_1".YawOverride:'> </option>
<option value="On">Yes</option>
<option value="Off">No</option>
</select>

</td>
</tr>

<tr style="vertical-align: top; height: 2%;">
<td style="width: 25%;">
<p>Turbine yaw:</p>
</td>
<td>
<p style="margin-bottom:5px;"><input name='"Data_block_1".Yaw'
size="10" value=':="Data_block_1".Yaw:' type="text"> deg.</p>
</td>
</tr>

<tr style="vertical-align: top; height: 2%;">
<td style="width: 25%;">
<p>Pitch override: :="Data_block_1".PitchOverride: </p>
</td>
<td class="Text">Set:

<select name='"Data_block_1".PitchOverride'>
<option value=':="Data_block_1".PitchOverride:'> </option>
<option value="On">Yes</option>
<option value="Off">No</option>
</select>

</td>
</tr>

<tr style="vertical-align: top; height: 2%;">
<td style="width=25%; border-bottom-style: Solid; border-bottom-
width: 2px; border-bottom-color: #ffffff;">
<p>Blade pitch:</p>
</td>
<td>
<p style="margin-bottom:5px;"><input name='"Data_block_1".Pitch'
size="10" value=':="Data_block_1".Pitch:' type="text"> deg.</p>
</td>

</tr>
<tr style="height: 2%;">
<td colspan="2">
<input type="submit" value="Submit override settings and values">
</td>
</tr>
</form>

<tr style="vertical-align: top; height: 2%;">
<td style="width: 25%;"><p>Braking:</p></td>
```

```
<td>
<form method="POST" action="">
<p> <input name='"Data_block_1".Braking' size="10"
value=':="Data_block_1".Braking:' type="text"> %</p>
</form>
</td>
</tr>
<tr><td></td></tr>

</table>
</body>
</html>
```

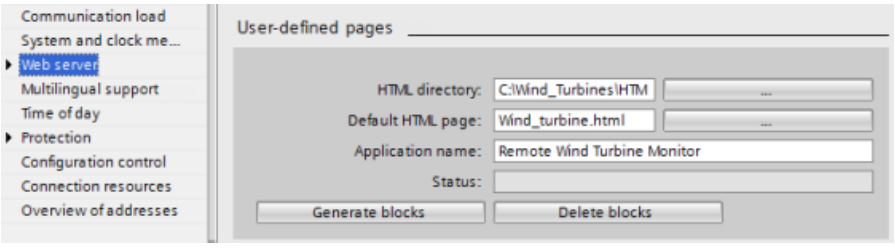
Wind_turbine.css

```
BODY {
    background-image: url('./Wind_turbine.jpg');
    background-position: 0% 0%;
    background-repeat: no-repeat;
    background-size: cover;
}
H2 {
    font-family: Arial;
    font-weight: bold;
    font-size: 14.0pt;
    color: #FFFFFF;
    margin-top:0px;
    margin-bottom:10px;
}
P {
    font-family: Arial;
    font-weight: bold;
    color: #FFFFFF;
    font-size: 12.0pt;
    margin-top:0px;
    margin-bottom:0px;
}
TD.Text {
    font-family: Arial;
    font-weight: bold;
    color: #FFFFFF;
    font-size: 12.0pt;
    margin-top:0px;
    margin-bottom:0px;
}
```

13.8.9.7 Configuration in STEP 7 of the example Web page

To include the "Remote Wind Turbine Monitor" HTML page as a user-defined Web page for the S7-1200, you configure the data about the HTML page in STEP 7 and create data blocks from the HTML page.

Access the CPU Properties for the S7-1200 that controls the wind turbine, and enter the configuration information in the User-defined pages properties of the Web Server:



Configuration fields

- HTML directory: This field specifies the fully-qualified pathname to the folder where the default page (home page or start page) is located on the computer. The "..." button allows you to browse to the folder that you need.
- Default HTML page: This field specifies the filename of the default page or home page of the HTML application. The "..." button allows you to select the file that you need. For this example, WindTurbine.html is the default HTML page. The Remote Wind Turbine Monitor example only consists of a single page, but in other user-defined applications the default page can call up additional pages from links on the default page. Within the HTML code, the default page must reference other pages relative to the HTML source folder.
- Application name: This optional field contains the name that the Web browser includes in the address field when displaying the page. For this example, it is "Remote Wind Turbine Monitor", but you can use any name.

No other fields require configuration.

Final steps

To use the Remote Wind Turbine Monitor as configured, generate the blocks, program the WWW instruction (Page 812) with the number of the generated control DB as an input parameter, download the program blocks, and put the CPU in run mode.

When an operator subsequently accesses the standard Web pages for the S7-1200 that controls the wind turbine, the "Remote Wind Turbine Monitor" Web page is accessible from the "User-defined pages" link on the navigation bar. This page now provides the means to monitor and control the wind turbine.

13.8.10 Setting up user-defined Web pages in multiple languages

The Web server provides the means for you to provide user-defined Web pages in the following languages:

- German (de)
- English (en)
- Spanish (es)
- French (fr)
- Italian (it)
- Simplified Chinese (zh)

You do this by setting up your HTML pages in a folder structure (Page 826) that corresponds to the languages and by setting a specific cookie named "siemens_automation_language" from your pages (Page 826). The Web server responds to this cookie, and switches to the default page in the corresponding language folder.

13.8.10.1 Creating the folder structure

To provide user-defined Web pages in multiple languages, you set up a folder structure under your HTML directory. The two-letter folder names are specific and must be named as shown below:

de: German
en: English
es: Spanish
fr: French
it: Italian
zh: Simplified Chinese

At the same level, you can also include any other folders that your pages need, for example, folders for images or scripts.

You can include any subset of the language folders. You do not have to include all six languages. Within the language folders, you create and program your HTML pages in the appropriate language.

13.8.10.2 Programming the language switch

The Web server performs switching between languages through the use of a cookie named "siemens_automation_language". This is a cookie defined and set in the HTML pages, and interpreted by the Web server to display a page in the appropriate language from the language folder of the same name. The HTML page must include a JavaScript to set this cookie to one of the pre-defined language identifiers: "de", "en", "es", "fr", "it', or "zh".

For example, if the HTML page sets the cookie to "de", the Web server switches to the "de" folder and displays the page with the default HTML page name as defined in the STEP 7 configuration (Page 829).

Example

The following example uses a default HTML page named "langswitch.html" in each of the language folders. Also in the HTML directory is a folder named "script". The script folder

includes a JavaScript file named "lang.js". Each langswitch.html page uses this JavaScript to set the language cookie, "siemens_automation_language".

HTML for "langswitch.html" in "en" folder

The header of the HTML page sets the language to English, sets the character set to UTF-8, and sets the path to the JavaScript file lang.js.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Language" content="en">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Language switching english page</title>
<script type="text/javascript" src="script/lang.js" ></script>
```

The body of the file uses a select list for the user to select between German and English. English ("en") is pre-selected for the language. When the user changes the language, the page calls the DoLocalLanguageChange() JavaScript function with the value of the selected option.

```
<!-- Language Selection -->
<table>
   <tr>
      <td align="right" valign="top" nowrap>
       <!-- change language immediately on selection change -->
          <select name="Language"
                   onchange="DoLocalLanguageChange(this)"
                   size="1">
            <option value="de" >German</option>
            <option value="en" selected >English</option>
           </select>
      </td>
   </tr>
</table><!-- Language Selection End-->
```

HTML for "langswitch.html" in "de" folder

The header for the German langswitch.html page is the same as English, except the language is set to German.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Language" content="de"><meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
<title>Sprachumschaltung Deutsche Seite</title>
<script type="text/javascript" src="script/lang.js" ></script>
</head>
```

The HTML in the German page is identical to that of the English page, except that the default value of the selected language is German ("de").

```
<!-- Language Selection -->
<table>
   <tr>
     <td align="right" valign="top" nowrap>
       <!-- change language immediately on change of the selection
-->
       <select name="Language"
               onchange="DoLocalLanguageChange(this)"
               <size="1">
```

```
                <option value="de" selected >Deutsch</option>
                <option value="en" >Englisch</option>
            </select>
           </td>
       </tr>
</table><!-- Language Selection End-->
```

JavaScript "lang.js" in "script" folder

The function "DoLocalLanguageChange()" is in the lang.js file. This function calls the "SetLangCookie()" function and then reloads the window that is displaying the HTML page.

The function "SetLangCookie()" constructs an assignment that assigns the value from the select list to the "siemens_automation_language" cookie of the document. It also sets the path to the application so that the switched page, and not the requesting page, receives the value of the cookie.

Optionally, in the commented section, the page could set an expiration value for the cookie.

```
function DoLocalLanguageChange(oSelect) {
        SetLangCookie(oSelect.value);
        top.window.location.reload();
    }
function SetLangCookie(value) {
        var strval = "siemens_automation_language=";
        // This is the cookie by which the Web server
        // detects the desired language
        // This name is required by the Web server.
        strval = strval + value;
        strval = strval + "; path=/ ;";
        // Set path to the application, since otherwise
        // path would be set to the requesting page
        // and this page would not get the cookie.
        /* OPTIONAL
           use expiration if this cookie should live longer
           than the current browser session:
           var now = new Date();
           var endttime = new Date(now.getTime() + expiration);
           strval = strval + "; expires=" +
                    endttime.toGMTString() + ";";
        */
        document.cookie = strval;
    }
```

NOTE

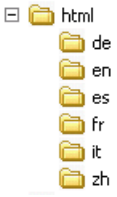
If your user-defined Web page implementation includes HTML files within language-specific folders (en, de, for example) and also HTML files that are not in the language-specific folders, note that you cannot define enum types with the AWP_Enum_Def command in files in both locations. If you use enums, you must define them either within files in the language -specific folders or within files outside of the language-specific folders. You cannot make enum declarations in files in both places.

13.8.10.3 Configuring STEP 7 to use a multi-language page structure

The procedure for configuring multi-language user-defined Web pages is similar to the general process for configuring user-defined Web pages (Page 811). When you have folders set up for languages, however, you set your HTML directory setting to the folder that contains the individual language folders. You do not set the HTML directory to be one of the language folders.

When you select the default HTML page, you navigate into the language folder and select the HTML page that is to be the start page. When you subsequently generate blocks and download the blocks to the CPU, the Web server displays the start page in the language folder that you configured.

For example, if the folder structure shown here was at C:\, the setting for HTML directory would be C:\html, and if English were to be the initial page display, you would navigate to en\langswitch.html for the default HTML page setting.



13.8.11 Advanced user-defined Web page control

When you generate data blocks for your user-defined Web pages, STEP 7 creates a control DB that it uses to control display of and interaction with the user-defined pages. STEP 7 also creates a set of fragment DBs that represent the individual pages. Under normal circumstances, you do not need to know the structure of the control DB or how to manipulate it.

If you want to turn a web application on and off, for example, or manipulate individual manual fragments, you use the control DB tags and the WWW instruction to do so.

Structure of the control DB

The control DB is an extensive data structure, and is accessible when programming your STEP 7 user program. Only some of the control data block tags are described here.

NOTE

Do not make changes in the control DB structure other than changes similar to those described below. Modifications to the control DB structure can prevent the Web server from operating correctly.

Commandstate structure

"Commandstate" is a structure that contains global commands and global states for the Web server.
The global commands in the "Commandstate" structure apply to the Web server in general. You can deactivate the Web server or restart it from the control DB parameters.

Block tag	Data type	Description
init	BOOL	Evaluate the control DB and initialize the Web application
deactivate	BOOL	Deactivate the Web application

Global states in the Commandstate structure

The global states apply to the Web server in general and contain status information about the Web application.

Block tag	Data type	Description
initializing	BOOL	Web application is reading control DB
error	BOOL	Web application could not be initialized
deactivating	BOOL	Web application is terminating
deactivated	BOOL	Web application is terminated
initialized	BOOL	Web application is initialized
last_error	INT	Last error returned from a WWW instruction call (Page 812) when the return code of WWW is 16#0010: 16#0001: fragment DB structure is inconsistent 16#0002: the application name already exists 16#0003: no resources (memory) 16#0004: control DB structure is inconsistent 16#0005: fragment DB not available 16#0006: fragment DB not for AWP 16#0007: enumeration data is inconsistent 16#000D: conflicting size of the control DB

Request table

Request table

The request table is an array of structures containing commands and states that apply to individual fragment DBs. If you created fragments with the AWP_Start_Fragment (Page 807) command of type "manual", the STEP 7 user program must control these pages through the control DB. The request states are read-only and provide information about the current fragment. You use the request commands to control the current fragment.

Block tag	Data type	Description
requesttab	ARRAY [1 .. 4] OF STRUCT	Array of structures for individual fragment DB control. The Web server can process up to four fragments at a time. The array index for a particular fragment is arbitrary when the Web server is processing multiple fragments or fragments from multiple browser sessions.

Struct members of requesttab struct

Block tag	Data type	Description
page_index	UINT	Number of the current web page
fragment_index	UINT	Number of the current fragment - can be set to a different fragment
// Request Commands		
continue	BOOL	Enables current page/fragment for sending and continues with the next fragment
repeat	BOOL	Enables current page/fragment for resending and continues with the same fragment
abort	BOOL	Close http connection without sending
finish	BOOL	Send this fragment; page is complete - do not process any additional fragments
// Request states		The request states are read-only
idle	BOOL	Nothing to do, but active
waiting	BOOL	Fragment is waiting to be enabled
sending	BOOL	Fragment is sending
aborting	BOOL	User has aborted current request

Operation

Whenever your program makes changes to the control DB, it must call the WWW instruction with the number of the modified control DB as its parameter. The global commands and request commands take effect when the STEP 7 user program executes the WWW instruction (Page 812).
The STEP 7 user program can set the fragment_index explicitly, thus causing the Web server to process the specified fragment with a request command. Otherwise, the Web server processes the current fragment for the current page when the WWW instruction executes.

Possible techniques for using the fragment_index include:

- Processing the current fragment: Leave fragment_index unchanged and set the continue command.
- Skip the current fragment: Set fragment_index to 0 and set the continue command.
- Replace current fragment with a different fragment: Set the fragment_index to the new fragment ID and set the continue command.

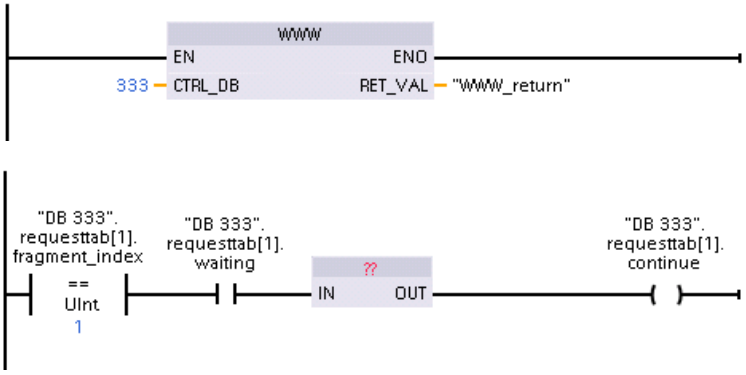
To check global states or request states that might be changing, the STEP 7 user program must call the WWW instruction to evaluate the current values of these states. A typical usage might be to call the WWW instruction periodically until a specific state occurs.

NOTE

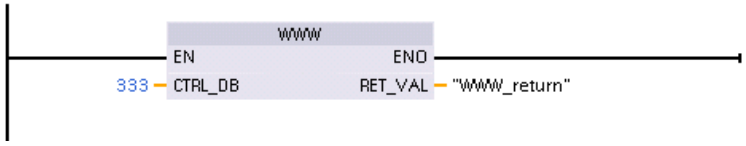
If the STEP 7 user program sets more than one request command, the WWW instruction processes only one in this order of precedence: abort, finish, repeat, continue. The WWW instruction clears all of the request commands after processing.

Examples

The following example shows a STEP 7 user program that is checking for a fragment with an ID of 1 to be in the waiting state, following a prior call to the WWW instruction. It might also wait for other application-specific conditions to occur. Then it performs whatever processing is necessary for the fragment, such as setting data block tags, performing calculations, or other application-specific tasks. Afterwards, it sets the continue flag so that the Web server will execute this fragment.



When the program calls the WWW instruction with this modified control DB, the user-defined Web page with this fragment can be displayed from the Web browser.



Note that this is a simplified example; the fragment to check could be in any one of the four requesttab structs in the array. Your program must handle all four requesttab structs.

13.8.12 Web API

The S7-1200 CPU provides a Web API that is an interface for you to read and write process data. The S7-1200 Web API implements some of the functionality of the S7-1500 Web API, which is documented below in "Supported Web API methods".

Note that the S7-1200 CPU limits the number of concurrent API sessions to 50.

Unsupported Web API data types

The S7-1200 Web API supports the S7-1500 Web API supported data types with the exception of the following:

- LWord
- LInt
- LTime_Of_Day
- S5Time
- LDT

You can find the S7-1500 Web API supported data types in this S7-1500 Web server document (https://support.industry.siemens.com/cs/us/en/view/59193560) at the following location: Application Programming Interface (API) > Read and write process data > Supported data types.

Supported Web API methods

The S7-1200 supports the following Web API methods:

- Api.Ping
- Api.Version
- Api.GetCertificateUrl
- Api.ChangePassword
- Api.GetPasswordPolicy
- Api.GetAuthenticationMode
- Api.Browse
- Api.Login
- Api.Logout
- Api.GetPermissions
- PlcProgram.Browse
- PlcProgram.Write
- PlcProgram.Read
- Syslog.Browse

13.9 Constraints

The following IT considerations can affect your use of the Web server:

- Typically, you must use the IP address of the CPU to access the standard Web pages or user-defined Web pages, or the IP address of a wireless router with a port number. If your Web browser does not allow connecting directly to an IP address, see your IT administrator. If your local policies support DNS, you can connect to the IP address through a DNS entry to that address.
- Firewalls, proxy settings, and other site-specific restrictions can also restrict access to the CPU. See your IT administrator to resolve these issues.
- The standard Web pages use JavaScript and cookies. If your Web browser settings disable JavaScript or cookies, enable them. If you cannot enable them, some features are restricted (Page 835). Use of JavaScript and cookies in user-defined Web pages is optional. If used, you must enable them in your browser.
- The Web server supports Transport Layer Security (TLS). You can access the standard Web pages and user-defined Web pages with an URL of either http://ww.xx.yy.zz or https://ww.xx.yy.zz, where "ww.xx.yy.zz" represents the IP address of the CPU.
- Siemens provides a security certificate for secure access to the Web server. From the Introduction standard Web page (Page 772), you can download and import the certificate into the Internet options of your Web browser (Page 767). If you choose to not import the certificate, you will get a security verification prompt every time you access the Web server with https://.

Number of connections

The Web server supports a maximum of 30 active connections. Various actions consume the 30 connections, depending on the Web browser that you use and the number of different objects per page (.css files, images, JavaScript files, additional .html files). Some connections persist while the Web server is displaying a page; other connections do not persist after the initial connection.

If, for example, you are using certain versions of Mozilla Firefox, which support a maximum of six persistent connections, you could use five browser or browser tab instances before the Web server starts dropping connections. In the case where a page is not using all six connections, you could have additional browser or browser tab instances.

Also be aware that the number of active connections can affect page performance. For this reason, the Web pages may not load fully.

NOTE

Log off prior to closing Web server

If you have logged in to the Web server, be sure to log off prior to closing your Web browser. The Web server supports a maximum of seven concurrent logins.

Failure to log off can leave multiple connections open, depending on your browser. By opening and closing Web server browser windows multiple times without logging off, you could consume all of the 30 connections. If you consume all of the connections, you would then receive an "Invalid login" message when you attempt to log in. You would have to wait up to 30 minutes before the Web server frees up enough connections for you to log in again. To avoid this problem, always log off before closing the Web server if you have logged in.

13.9.1 Use of JavaScript

The standard Web pages use HTML, JavaScript, and cookies. If your site restricts the use of JavaScript and cookies, then enable them for the pages to function properly. If you cannot enable JavaScript for your Web browser, the standard Web pages cannot run. Consider using the basic pages, which do not use JavaScript.

See also

Layout of the standard Web pages (Page 768)

13.9.2 Feature restrictions when the Internet options do not allow cookies

If you disable cookies in your Web browser, the following restrictions apply:

- You cannot log in.
- You cannot change the language setting.
- You cannot switch from UTC time to PLC time. Without cookies, all times are in UTC time.

13.9.3 Rules for entering tag names and values

Be aware of the following conventions when using the Tag status (Page 784) and Watch tables (Page 786) standard pages:

- If modifying the entire value of a DTL tag, for example, "Data_block_1_.DTL_tag, use the following DTL syntax for the modify value: DTL#YYYY-MM-DD-HH-MM-SS[.sssssssss]
- When using exponential notation to enter a value for a Real or LReal data type:
  - To enter a real-number value (Real or LReal) with a positive exponent (such as +3.402823e+25), enter the value in either of the following formats:
    +3.402823e25
    +3.402823e+25
  - To enter real-number value (Real or LReal) with a negative exponent (such as +3.402823e-25), enter the value as follows:
    +3.402823e-25
  - Be sure that the mantissa portion of the real value in exponential notation includes a decimal point. Failure to include a decimal point results in the modification of the value to an unexpected integer value. For example, enter -1.0e8 rather than -1e8.
- LReal values can be only 15 digits (regardless of the location of the decimal point). Entering more than 15 digits creates a rounding error.

Limitations on the Tag status and Watch Table page:

- The maximum number of characters for the URL is 2083. You can see the URL that represents your current page in the address bar of your browser.
- For the character display format, if the actual CPU values are not valid ASCII characters as interpreted by the browser then the page displays the character preceded by a dollar sign: $.

13.9.4 Importing CSV format data logs to non-USA/UK versions of Microsoft Excel

Data log files are in the comma-separated values (CSV) file format. You can open these files directly in Excel from the Data Logs page when your system is running the USA or UK version of Excel. In other countries, however, this format is not widely used because commas occur frequently in numerical notation.

To open a data log file that you have saved, follow these steps for non USA/UK versions of Excel:

1. Open Excel and create an empty workbook.
2. From the "Data > Import External Data" menu, select the "Import Data" command.
3. Navigate to and select the data log file you want to open. The Text Import Wizard starts.
4. From the Text Import Wizard, change the default option for "Original data type" from "Fixed width" to "Delimited".
5. Click the Next button.
6. From the Step 2 dialog, select the "Comma" check box to change the delimiter type from "Tab" to "Comma".
7. Click the Next button.
8. From the Step 3 dialog, you can optionally change the Date format from MDY (month/day/year) to another format.
9. Complete the remaining steps of the Text Import Wizard to import the file.

Communication processor and Modbus TCP 14

14.1 Using the serial communication interfaces

Two communication modules (CMs) and one communication board (CB) provide the interface for PtP communications:

- CM 1241 RS232 (Page 1261)
- CM 1241 RS422/485 (Page 1262)
- CB 1241 RS485 (Page 1259)

You can connect up to three CMs (of any type) plus a CB for a total of four communication interfaces. Install the CM to the left of the CPU or another CM. Install the CB on the front of the CPU. Refer to the installation guidelines (Page 51)for information on module installation and removal.

The serial communication interfaces have the following characteristics:

- Have an isolated port
- Support Point-to-Point protocols
- Are configured and programmed through the point-to-point communication processor instructions
- Display transmit and receive activity by means of LEDs
- Display a diagnostic LED (CMs only)
- Are powered by the CPU: No external power connection is needed.

Refer to the technical specifications for communication interfaces (Page 1250).

LED indicators

The communication modules have three LED indicators:

- Diagnostic LED (DIAG): This LED flashes red until it is addressed by the CPU. After the CPU powers up, it checks for CMs and addresses them. The diagnostic LED begins to flash green. This means that the CPU has addressed the CM, but has not yet provided the configuration to it. The CPU downloads the configuration to the configured CMs when the program is downloaded to the CPU. After a download to the CPU, the diagnostic LED on the communication module should be a steady green.
- Transmit LED (Tx): The transmit LED illuminates when data is being transmitted out the communication port.
- Receive LED (Rx): This LED illuminates when data is being received by the communication port.

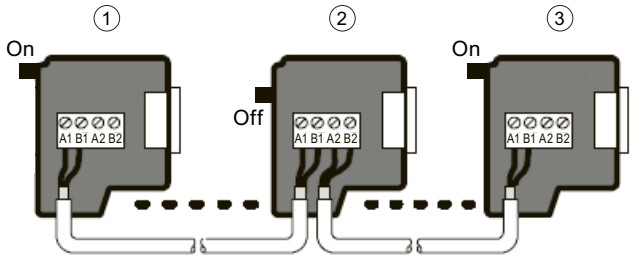
The communication board provides transmit (TxD) and receive (RxD) LEDs. It has no diagnostic LED.

14.2 Biasing and terminating an RS485 network connector

Siemens provides an RS485 network connector (Page 1276) that you can use to easily connect multiple devices to an RS485 network. The connector has two sets of terminals that allow you to attach the incoming and outgoing network cables. The connector also includes switches for selectively biasing and terminating the network.

NOTE

You terminate and bias only the two ends of the RS485 network. The devices in between the two end devices are not terminated or biased. Bare cable shielding: Approximately 12 mm (1/2 in) must contact the metal guides of all locations.

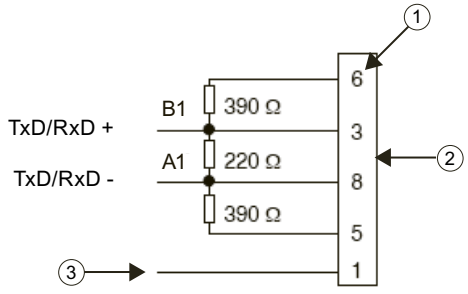
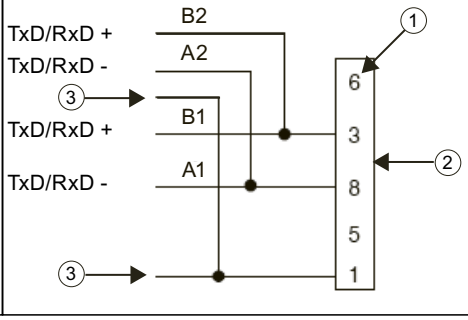


① Switch position = On: Terminated and biased

② Switch position = Off: No termination or bias

③ Switch position = On: Terminated and biased

Table 14-1 Termination and bias for the RS485 connector

Terminating device (bias ON)	Non-terminating device (bias OFF)
	

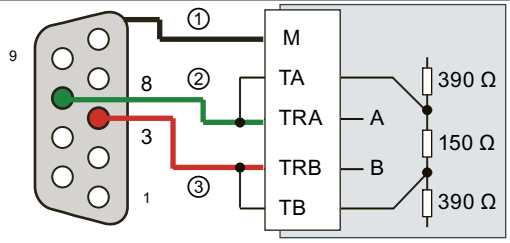
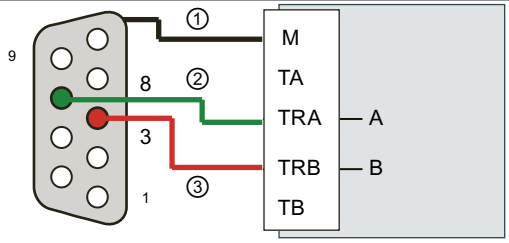
① Pin number

② Network connector

③ Cable shield

The CB 1241 provides internal resistors for terminating and biasing the network. To terminate and bias the connection, connect TRA to TA and connect TRB to TB to include the internal resistors to the circuit. CB 1241 does not have a 9-pin connector. The following table shows the connections to a 9-pin connector on the communications partner.

Table 14-2 Termination and bias for the CB 1241

Terminating device (bias ON)	Non-terminating device (bias OFF)
	

① Connect M to the cable shield

② A = TxD/RxD - (Green wire / Pin 8)

③ B = TxD/RxD + (Red wire / Pin 3)

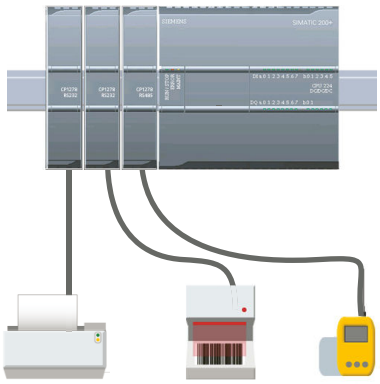
14.3 Point-to-point (PtP) communication

The CPU supports the following Point-to-Point communication (PtP) for character-based serial protocols:

- PtP, Freeport (Page 840)
- PtP, 3964(R) (Page 841)
- USS (Page 889)
- Modbus (Page 902)

14.3.1 PtP, Freeport communication

PtP with a Freeport, or freely constructed, protocol provides maximum freedom and flexibility, but requires extensive implementation in the user program.



PtP enables a wide variety of possibilities:

- The ability to send information directly to an external device such as a printer
- The ability to receive information from other devices such as barcode readers, RFID readers, third-party camera or vision systems, and many other types of devices
- The ability to exchange information, sending and receiving data, with other devices such as GPS devices, third-party camera or vision systems, radio modems, and many more

This type of PtP communication is serial communication that uses standard UARTs to support a variety of baud rates and parity options. The RS232 and RS422/485 communication modules (CM 1241) and the RS485 communication board (CB 1241) provide the electrical interfaces for performing the PtP communications.

PtP Freeport over PROFIBUS or PROFINET

PtP enables you to use a PROFINET or PROFIBUS distributed I/O rack to communicate to various devices (RFID readers, GPS device, and others):

- PROFINET (Page 530): You connect the Ethernet interface of the S7-1200 CPU to a PROFINET interface module. PtP communication modules in the rack with the interface module can then provide serial communications to the PtP devices.
- PROFIBUS (Page 691): You insert a PROFIBUS communication module in the left side of the rack with the S7-1200 CPU. You connect the PROFIBUS communication module to a rack containing a PROFIBUS interface module. PtP communication modules in the rack with the interface module can then provide serial communications to the PtP devices.

For this reason, the S7-1200 supports two sets of PtP instructions:

- Legacy point-to-point instructions (Page 990): These instructions existed prior to version V4.0 of the S7-1200 and only work with serial communications using a CM 1241 communication module or CB 1241 communication board.
- Point-to-point instructions (Page 857): These instructions provide all of the functionality of the legacy instructions, plus the ability to support PtP communication modules over PROFINET and PROFIBUS distributed I/O. The point-to-point instructions allow you to access the communication modules over the distributed I/O rack.

  The S7-1200 CM 1241 modules must have a minimum firmware version of V2.1 to use the point-to-point instructions. These modules are limited to the local rack to the left side of the S7-1200 CPU. You can also use the point-to-point instructions with a CB 1241.

Communications over distributed I/O use the following modules:

Station	Module	Article number	Interface
ET 200MP	CM PtP RS232 BA	6ES7540-1AD00-0AA0	RS232
	CM PtP RS232 HF	6ES7541-1AD00-0AB0	RS232
	CM PtP RS422/485 BA	6ES7540-1AB00-0AA0	RS422/RS485
	CM PtP RS422/485 HF	6ES7541-1AB00-0AB0	RS422/RS485
ET 200SP	CM PtP	6ES7137-6AA01-0BA0	RS232 and RS422/RS485

NOTE

You can use the point-to-point instructions to access a communication board, local (or left side) serial modules, serial modules over PROFINET, and serial modules over PROFIBUS. STEP 7 provides the legacy point-to-point instructions only to support existing programs. The legacy instructions still function, however, with the current S7-1200 CPUs. You do not have to convert prior programs from one set of instructions to the other.

NOTE

CM module firmware version requirement for Time synchronization and PtP communication

If you have enabled "CPU synchronizes the modules of the device" in the Time synchronization (Page 165) properties for the PROFINET interface in the device configuration, update the firmware versions of the connected communication modules to the latest available versions. Enabling module time synchronization for communication modules with old firmware versions can cause communication issues or errors.

14.3.2 3964(R) communication

The S7-1200 CPU supports the 3964(R) protocol to enable communication between a CM 1241, RS232 module or a CM 1241, RS422/485 module and a communication partner that uses the 3964(R) protocol. Unlike the PtP communication described above where you define specific send (transmit) and receive characteristics for the messages, the 3964(R) protocol proscribes a strict protocol using the following control characters:

- STX Start of text
  Start of character string to be transmitted
- DLE Data Link Escape
  Data transmission switchover
- ETX End of Text
  End of character string to be transmitted
- BCC Block check character
- NAK Negative Acknowledge

Refer to the chapter describing serial data transmission principles in the S7-300 CP 341 Point-to-Point Communication, Installation, and Parameter Assignment Manual. (https://support.industry.siemens.com/cs/us/en/view/1117397) manual for a complete description of the protocol.

Configuring the communication module

To communicate to a partner using the 3964(R) protocol, you must include one of the following communication modules in your device configuration in STEP 7:

- CM 1241, RS232
- CM 1241, RS422/485

The firmware version of the CM module must be V2.2.0 or later.

For the communication module, you then configure the communication ports (Page 842), priority, and protocol parameters (Page 855).

Communication to a partner with the 3964(R) protocol

When you configure a CM for 3964(R) protocol, you use the standard point-to-point send and receive instructions to transfer data between the CPU and its communication partner.

The CM embeds your data from the BUFFER parameter of the send instruction into the 3964(R) protocol and sends the data to the communication partner.

The CM receives data from the communication partner by means of the 3964(R) protocol, removes the protocol information, and returns the data in the BUFFER parameter of the receive instruction.

Refer to the following point-to-point instructions:

- Send_P2P (Transmit send buffer data) (Page 870)
- Receive_P2P (Enable receive messages) (Page 873)

You can also use the legacy point-to-point send and receive instructions:

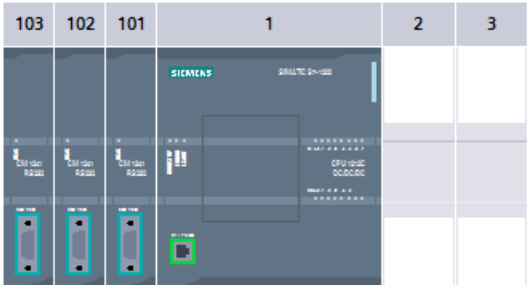
- SEND_PTP (Transmit send buffer data) (Page 997)
- RCV_PTP (Enable receive messages) (Page 999)

14.3.3 Configuring the PtP Freeport communication

You can use either of the following methods to configure the communication interfaces for PtP Freeport communication:

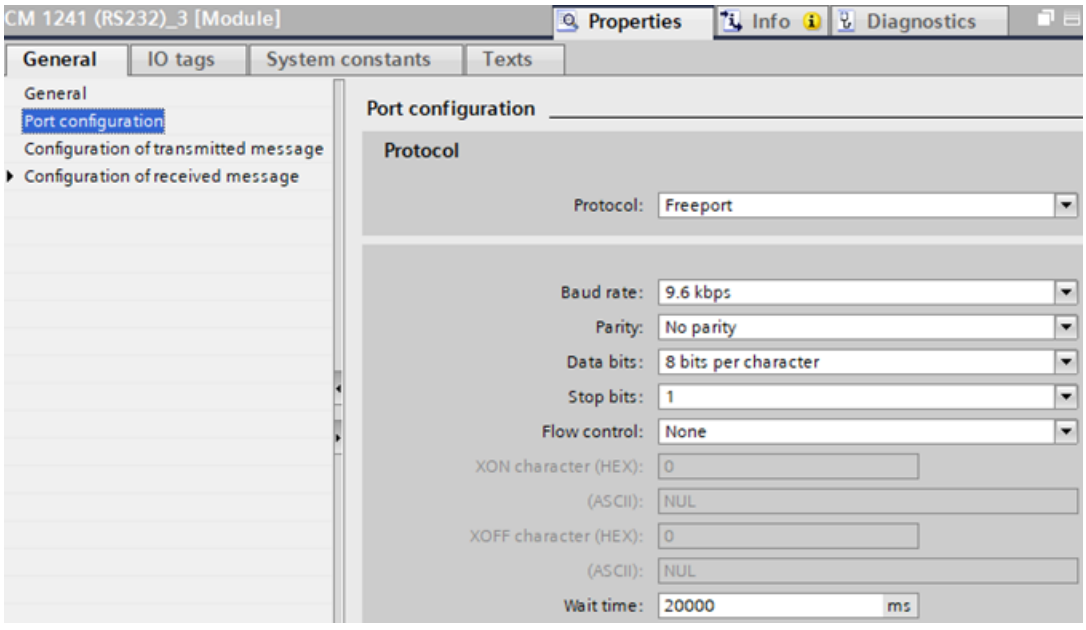
- Use the device configuration in STEP 7 to configure the port parameters (baud and parity), the send parameters and the receive parameters. The CPU stores the device configuration settings and applies the settings after a power cycle and a RUN to STOP transition.
- Use the Port_Config (Page 859), Send_Config (Page 861), and Receive_Config (Page 863) instructions to set the parameters. The port settings set by the instructions are valid while the CPU is in RUN mode. The port settings revert to the device configuration settings after a STOP transition or power cycle.

After configuring the hardware devices (Page 121), you configure parameters for the communication interfaces by selecting one of the CMs in your rack or the CB, if configured.



The "Properties" tab of the inspector window displays the parameters of the selected CM or CB. Select "Port configuration" to edit the following parameters:

- Protocol
- Baud rate
- Parity
- Data bits
- Stop bits
- Flow control (RS232 only)
- Wait time

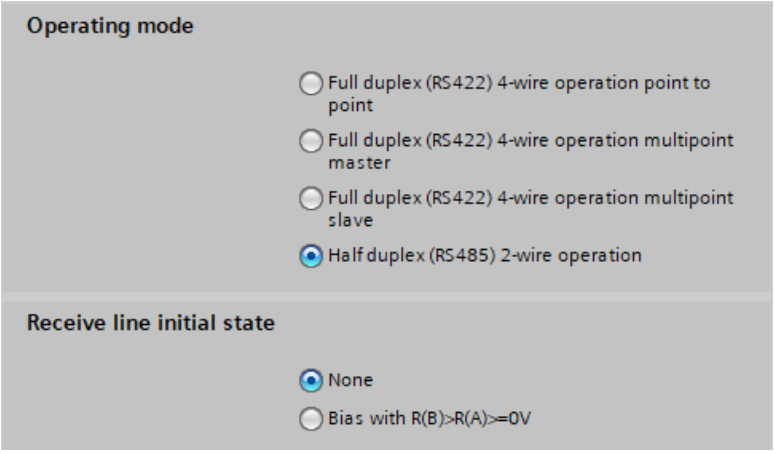


For the CM 1241 RS232 and CB RS485 (except for flow control (Page 844), which only the CM 1241 RS232 supports), the port configuration parameters are the same regardless of whether you are configuring an RS232 or an RS485 communication module or the RS485 communication board. The parameter values can differ.

For the CM 1241 RS422/485, you have additional options for port configuration as shown below. The 422 mode of the CM 1241 RS422/485 module also supports software flow control.

Select "Port configuration" to edit the following RS422/485 parameters:

- Operating mode
- Receive line initial state



Your STEP 7 program can also configure the port or change the existing configuration with the Port_Config instruction (Page 859). The instruction topic provides more detail about the operational mode and initial line state as well as other parameters.

Parameter	Definition
Baud rate	The default value for the baud rate is 9.6 Kbits per second. Valid choices are: 300 baud, 600 baud, 1.2 Kbits, 2.4 Kbits, 4.8 Kbits, 9.6 Kbits, 19.2 Kbits, 38.4 Kbits, 57.6 Kbits, 76.8 Kbits, and 115.2 Kbits.
Parity	The default value for parity is no parity. Valid choices are: No parity, even, odd, mark (parity bit always set to 1), and space (parity bit always set to 0).
Data bits per character	The number of data bits in a character. Valid choices are 7 or 8.
Number of stop bits	The number of stop bits can be either one or two. The default is one.
Flow control	For the RS232 communication module, you can select either hardware or software flow control (Page 844). If you select hardware flow control, you can select whether the RTS signal is always on, or RTS is switched. If you select software flow control, you can define the XON and XOFF characters. The RS485 communication interfaces do not support flow control. The 422 mode of the CM 1241 RS422/485 module supports software flow control.
Wait time	Wait time specifies the time that the CM or CB waits to receive CTS after asserting RTS, or for receiving an XON after receiving an XOFF, depending on the type of flow control. If the wait time expires before the communication interface receives an expected CTS or XON, the CM or CB aborts the transmit operation and returns an error to the user program. You specify the wait time in milliseconds. The range is 0 to 65535 milliseconds.
Operating mode	This selects the operating mode RS422 or RS485 and network configurations.
Receive line initial state	This selects the bias options. Valid values are none, forward bias and reverse bias. Reverse bias is used to allow cable break detection.

14.3.3.1 Managing flow control

Flow control refers to a mechanism for balancing the sending and receiving of data transmissions so that no data is lost. Flow control ensures that a transmitting device is not sending more information than a receiving device can handle. Flow control can be accomplished through either hardware or software. The RS232 CM supports both hardware and software flow control. The RS485 CM and CB do not support flow control. The 422 mode of the CM 1241 RS422/485 module supports software flow control. You specify the type of flow control either when you configure the port (Page 842) or with the PORT_CFG instruction (Page 990).

Hardware flow control works through the Request-to-send (RTS) and Clear-to-send (CTS) communication signals. With the RS232 CM, the RTS signal is output from pin 7 and the CTS signal is received through pin 8. The RS232 CM is a DTE (Data Terminal Equipment) device which asserts RTS as an output and monitors CTS as an input.

Hardware flow control: RTS switched

If you enable RTS switched hardware flow control for an RS232 CM, the module sets the RTS signal active to send data. It monitors the CTS signal to determine whether the receiving device can accept data. When the CTS signal is active, the module can transmit data as long as the CTS signal remains active. If the CTS signal goes inactive, then the transmission must stop.

Transmission resumes when the CTS signal becomes active. If the CTS signal does not become active within the configured wait time, the module aborts the transmission and returns an error to the user program. You specify the wait time in the port configuration (Page 842).

The RTS switched flow control is useful for devices that require a signal that the transmit is active. An example would be a radio modem that uses RTS as a "Key" signal to energize the radio transmitter. The RTS switched flow control will not function with standard telephone modems. Use the RTS always on selection for telephone modems.

Hardware flow control: RTS always on

In RTS always on mode, the CM 1241 sets RTS active by default. A device such as a telephone modem monitors the RTS signal from the CM and utilizes this signal as a clear-to-send. The modem only transmits to the CM when RTS is active, that is, when the telephone modem sees an active CTS. If RTS is inactive, the telephone module does not transmit to the CM.

To allow the modem to send data to the CM at any time, configure "RTS always on" hardware flow control. The CM thus sets the RTS signal active all the time. The CM will not set RTS inactive even if the module cannot accept characters. The transmitting device must ensure that it does not overrun the receive buffer of the CM.

Data Terminal Ready (DTR) and Data Set Ready (DSR) signal utilization

The CM sets DTR active for either type of hardware flow control. The module transmits only when the DSR signal becomes active. The state of DSR is only evaluated at the start of the send operation. If DSR becomes inactive after transmission has started, the transmission will not be paused.

Software flow control

Software flow control uses special characters in the messages to provide flow control. You configure Hex characters that represent XON and XOFF.

XOFF indicates that a transmission must stop. XON indicates that a transmission can resume. XOFF and XON must not be the same character.

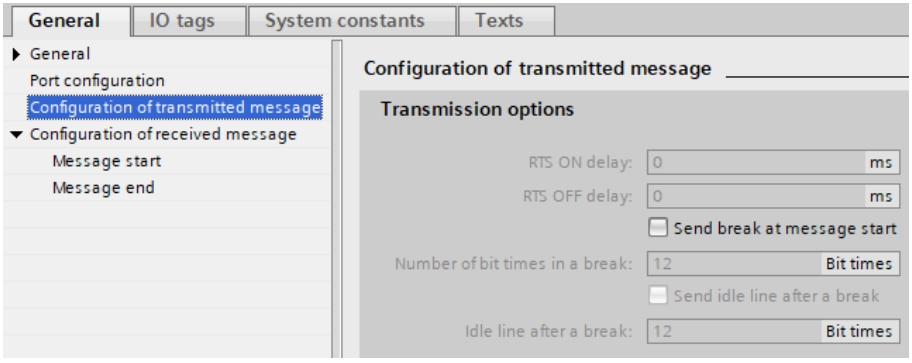
When the transmitting device receives an XOFF character from the receiving device, it stops transmitting. Transmitting resumes when the transmitting device receives an XON character. If it does not receive an XON character within the wait time that is specified in the port

configuration (Page 842), the CM aborts the transmission and returns an error to the user program.
Software flow control requires full-duplex communication, as the receiving partner must be able to send XOFF to the transmitting partner while a transmission is in progress. Software flow control is only possible with messages that contain only ASCII characters. Binary protocols cannot utilize software flow control.

Before the CPU can engage in PtP Freeport communications, you must configure parameters for transmitting (or sending) messages and receiving messages. These parameters dictate how communications operate when messages are being transmitted to or received from a target device.

14.3.3.2 Configuring transmit (send) parameters

From the device configuration of the CPU, you configure how a communication interface transmits data by setting the "Transmit message configuration" properties for the selected interface.



You can also dynamically configure or change the transmit message parameters from the user program by using the Send_Config (Page 861) instruction.

NOTE

Parameter values set from the Send_Config instruction in the user program override the "Transmit message configuration" properties. Note that the CPU does not retain parameters set from the Send_Config instruction in the event of power down.

Parameter	Definition
RTS On delay	Specifies the amount of time to wait after activating RTS before transmission is initiated. The range is 0 to 65535 ms, with a default value of 0. This parameter is valid only when the port configuration (Page 842) specifies hardware flow control. CTS is evaluated after the RTS On delay time has expired. This parameter is applicable for RS232 modules only.
RTS Off delay	Specifies the amount of time to wait before de-activating RTS after completion of transmission. The range is 0 to 65535 ms, with a default value of 0. This parameter is valid only when the port configuration (Page 842) specifies hardware flow control. This parameter is applicable for RS232 modules only.
Send break at message start Number of bit times in a break	Specifies that upon the start of each message, a break will be sent after the RTS On delay (if configured) has expired and CTS is active. You specify how many bit times constitute a break where the line is held in a spacing condition. The default is 12 and the maximum is 65535, up to a limit of eight seconds.

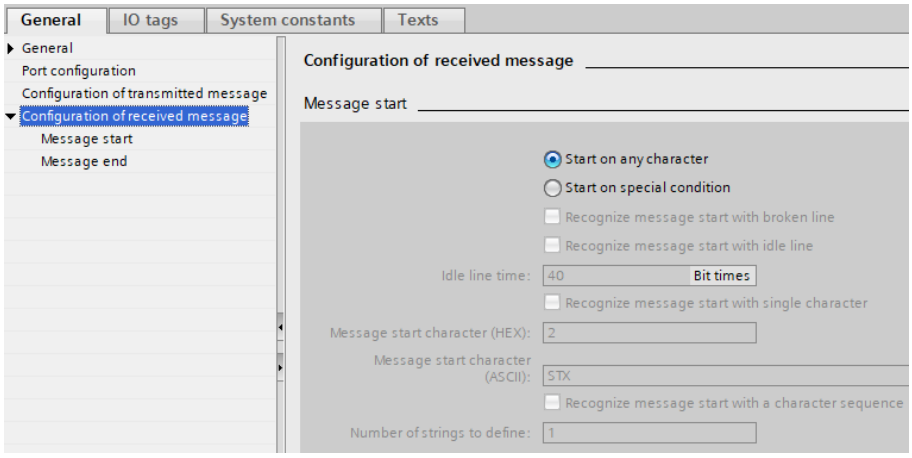
Parameter	Definition
Send idle line after a break Idle line after a break	Specifies that an idle line will be sent before message start. It is sent after the break, if a break is configured. The "Idle line after a break" parameter specifies how many bit times constitute an idle line where the line is held in a marking condition. The default is 12 and the maximum is 65535, up to a limit of eight seconds.

14.3.3.3 Configuring receive parameters

You can configure how a communication interface:

- Receives data
- Recognizes the start of a message
- Recognizes the end of a message

Set these parameters in the "Configuration of received message" properties for the selected interface.



You can also dynamically configure or change the receive message parameters from the user program by using the Receive_Config instruction (Page 863).

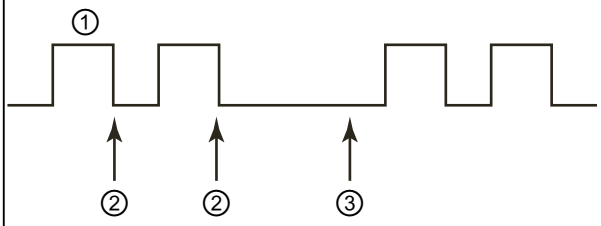
NOTE

Parameter values set from the Receive_Config instruction in the user program override the "Receive message configuration" properties. Note that the CPU does not retain parameters set from the RCV_CFG instruction in the event of power down or transition to STOP.

Message start conditions

You can determine how the communication interface recognizes the start of a message. The start characters and the characters comprising the message go into the receive buffer until a configured end condition is met.

You can specify multiple start conditions. If you specify more than one start condition, all of the start conditions must be met before the message is considered started. For example, if you configure an idle line time and a specific start character, the CM or CB will first look for the idle line time requirement to be met and then the CM will look for the specified start character. If some other character is received (not the specified start character), the CM or CB will restart the start of message search by again looking for an idle line time.

Parameter	Definition
Start on Any Character	The Any Character condition specifies that any successfully received character indicates the start of a message. This character is the first character within a message.
Line Break	The Line Break condition specifies that a message receive operation starts after a break character is received.
Idle Line	The Idle Line condition specifies that a message reception starts once the receive line has been idle or quiet for the number of specified bit times. Once this condition occurs, the start of a message begins.  ① Characters ② Restarts the idle line timer ③ Idle line is detected and message receive is started
Special condition: Recognize message start with single character	Specifies that a particular character indicates the start of a message. This character is then the first character within a message. Any character that is received before this specific character is discarded. The default character is STX.
Special condition: Recognize message start with a character sequence	Specifies that a particular character sequence from up to four configured sequences indicates the start of a message. For each sequence, you can specify up to five characters. For each character position, you specify either a specific hex character, or that the character is ignored in sequence matching (wild-card character). The last specific character of a character sequence terminates that start condition sequence. Incoming sequences are evaluated against the configured start conditions until a start condition has been satisfied. Once the start sequence has been satisfied, evaluation of end conditions begins. You can configure up to four specific character sequences. You use a multiple-sequence start condition when different sequences of characters can indicate the start of a message. If any one of the character sequences is matched, the message is started.

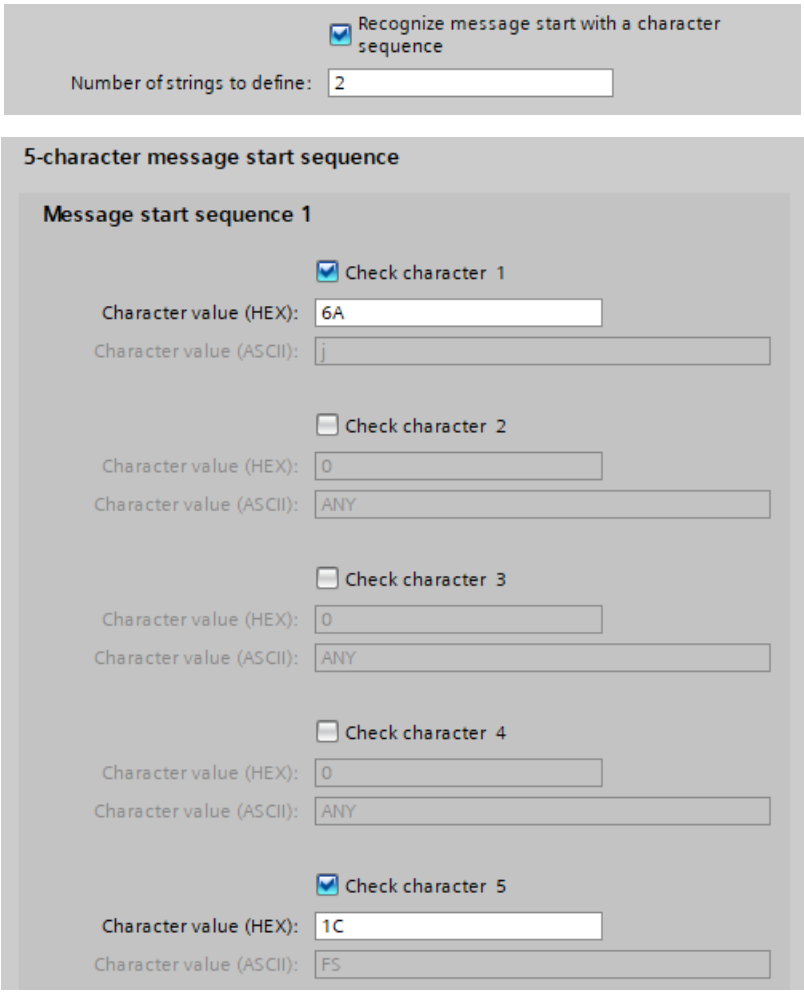
The order of checking start conditions is:

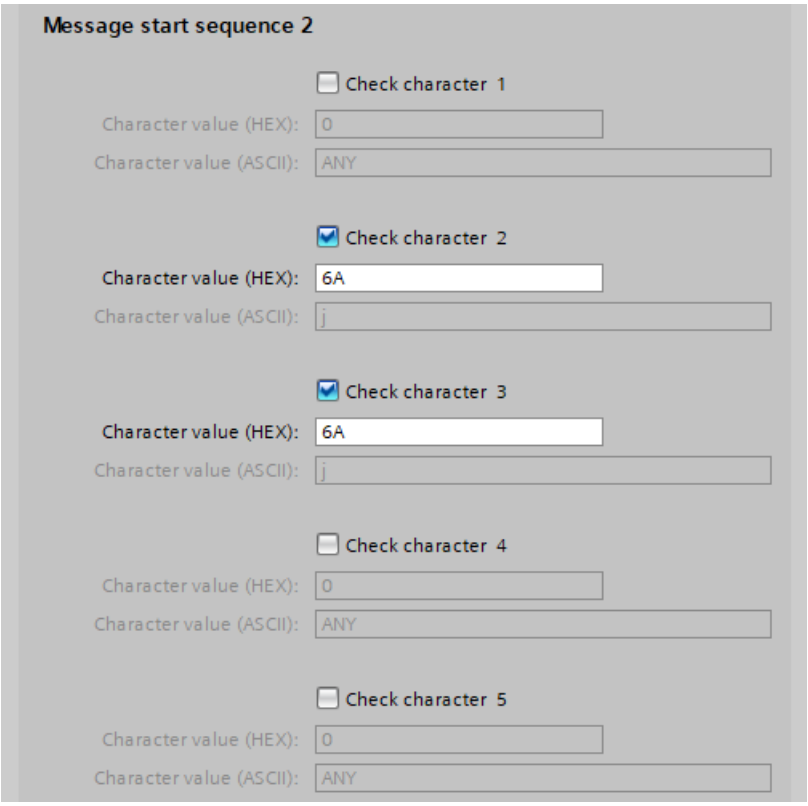
- Idle line
- Line break
- Characters or character sequences

While checking for multiple start conditions, if one of the conditions is not met, the CM or CB will restart the checking with the first required condition. After the CM or CB establishes that the start conditions have been met, it begins evaluating end conditions.

Example configuration: Start message on one of two character sequences

Consider the following start message condition configuration:





With this configuration, the start condition is satisfied when either pattern occurs:

- When a five-character sequence is received where the first character is 0x6A and the fifth character is 0x1C. The characters at positions 2, 3, and 4 can be any character with this configuration. After the fifth character is received, evaluation of end conditions begins.
- When two consecutive 0x6A characters are received, preceded by any character. In this case, evaluation of end conditions begins after the second 0x6A is received (3 characters). The character preceding the first 0x6A is included in the start condition.

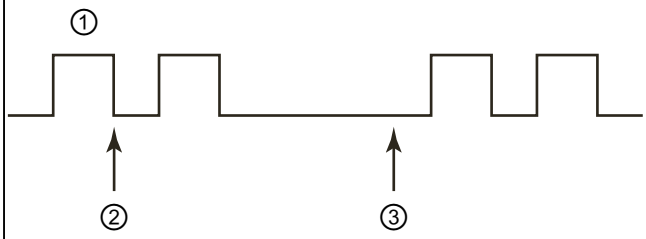
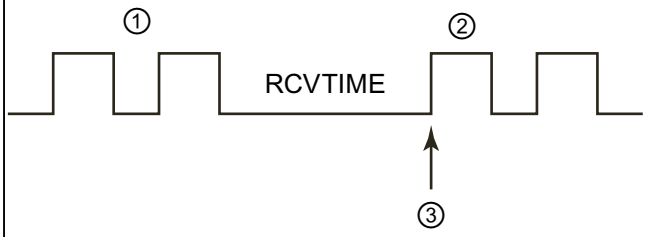
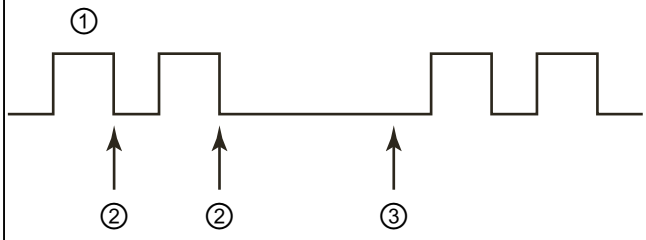
Example sequences that would satisfy this start condition are:

- <any character> 6A 6A
- 6A 12 14 18 1C
- 6A 44 A5 D2 1C

Message end conditions

You also configure how the communication interface recognizes the end of a message. You can configure multiple message end conditions. If any one of the configured conditions occurs, the message ends.

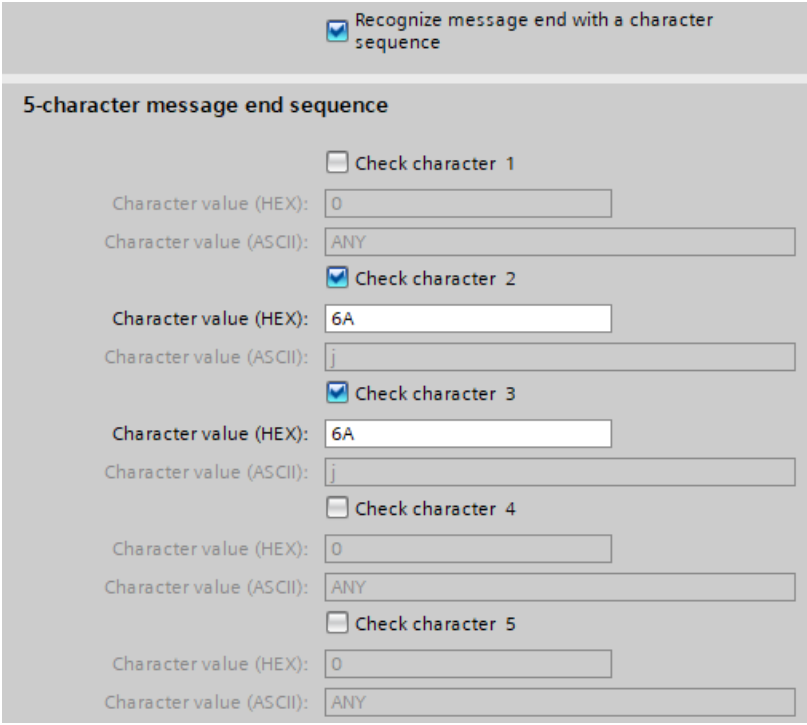
For example, you could specify an end condition with an end of message timeout of 300 milliseconds, an inter-character timeout of 40 bit times, and a maximum length of 50 bytes. The message will end if the message takes longer than 300 milliseconds to receive, or if the gap between any two characters exceeds 40 bit times, or if 50 bytes are received.

Parameter	Definition
Recognize message end by message timeout	The message end occurs when the configured amount of time to wait for the message end has expired. The message timeout period begins when a start condition has been satisfied. The default is 200 ms and the range is 0 to 65535 ms.  ① Received characters ② Start Message condition satisfied: message timer starts ③ Message timer expires and terminates the message
Recognize message end by response timeout	The message end occurs when the configured amount of time to wait for a response expires before a valid start sequence is received. The response timeout period begins when a transmission ends and the CM or CB begins the receive operation. The default response timeout is 200 ms and the range is 0 to 65535 ms. If a character is not received within the response time period, RCVTIME, then an error is returned to the corresponding RCV_PTP instruction. The response timeout does not define a specific end condition. It only specifies that a character must be successfully received within the specified time. You must configure another end condition to indicate the actual end of a message.  ① Transmitted characters ② Received characters ③ First character must be successfully received by this time.
Recognize message end by inter-character gap	The message end occurs when the maximum configured timeout between any two consecutive characters of a message has expired. The default value for the inter-character gap is 12 bit times and the maximum number is 65535 bit times, up to a maximum of eight seconds. 

Parameter	Definition
	① Received characters ② Restarts the intercharacter timer ③ The intercharacter timer expires and terminates the message.
Recognize message end by receiving a fixed number of characters	The message end occurs when the specified number of characters has been received. The valid range for the fixed length is 1 to 4096. Note that for the S7-1200, this end condition is only valid for V4.0 CPUs or higher.
Recognize message end by max length	The message end occurs when the configured maximum number of characters has been received. The valid range for maximum length is 1 to 1024. This condition can be used to prevent a message buffer overrun error. When this end condition is combined with timeout end conditions and the timeout condition occurs, any valid received characters are provided even if the maximum length is not reached. This allows support for varying length protocols when only the maximum length is known.
Read message length from message	The message itself specifies the length of the message. The message end occurs when a message of the specified length has been received. The method for specifying and interpreting the message length is described below.
Recognize message end with a character	The message end occurs when a specified character is received.
Recognize message end with a character sequence	The message end occurs when a specified character sequence is received. You can specify a sequence of up to five characters. For each character position, you specify either a specific hex character, or that the character is ignored in sequence matching. Leading characters that are ignored characters are not part of the end condition. Trailing characters that are ignored characters are part of the end condition.

Example configuration: End message with a character sequence

Consider the following end message condition configuration:



In this case, the end condition is satisfied when two consecutive 0x6A characters are received, followed by any two characters. The character preceding the 0x6A 0x6A pattern is not part of the end character sequence. Two characters following the 0x6A 0x6A pattern are required to terminate the end character sequence. The values received at character positions 4 and 5 are irrelevant, but they must be received to satisfy the end condition.

NOTE

If you want your character sequence to indicate the end of the message, put the sequence in the last character positions. In the example above, if you wanted 0x6A 0x6A to end the message with no trailing characters, you would configure 0x6A in character positions 4 and 5.

Specification of message length within the message

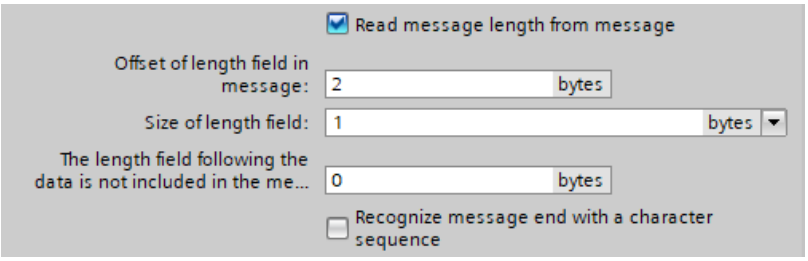
When you select the special condition where the message length is included in the message, you must provide three parameters that define information about the message length.

The actual message structure varies according to the protocol in use. The three parameters are as follows:

- n: the character position (1-based) within the message that starts the length specifier
- Length size: The number of bytes (one, two, or four) of the length specifier
- Length m: the number of characters following the length specifier that are not included in the length count

The ending characters do not need to be contiguous. The "Length m" value can be used to specify the length of a checksum field whose size is not included in the length field.

These fields appear in Configuration of received message under device properties:



Example 1: Consider a message structured according to the following protocol:

STX	Len (n)	Characters 3 to 14 counted by the length											
		ADR	PKE		INDEX		PWD		STW		HSW		BCC
1	2	3	4	5	6	7	8	9	10	11	12	13	14
STX	0x0C	xx	xxxx		xxxx		xxxx		xxxx		xxxx		xx

Configure the receive message length parameters for this message as follows:

- n = 2 (The message length starts with byte 2.)
- Length size = 1 (The message length is defined in one byte.)
- Length m = 0 (There are no additional characters following the length specifier that are not counted in the length count. Twelve characters follow the length specifier.)

In this example, the characters from 3 to 14 inclusive are the characters counted by Len (n).

Example 2: Consider another message structured according to the following protocol:

SD1	Len (n)	Len (n)	SD2	Characters 5 to 10 counted by length						FCS	ED
				DA	SA	FA	Data unit=3 bytes				
1	2	3	4	5	6	7	8	9	10	11	12
xx	0x06	0x06	xx	xx	xx	xx	xx	xx	xx	xx	xx

Configure the receive message length parameters for this message as follows:

- n = 3 (The message length starts at byte 3.)
- Length size = 1 (The message length is defined in one byte.)
- Length m = 3 (There are three characters following the length specifier that are not counted in the length. In the protocol of this example, the characters SD2, FCS, and ED are not counted in the length count. The other six characters are counted in the length count; therefore the total number of characters following the length specifier is nine.)

In this example, the characters from 5 to 10 inclusive are the characters counted by Len (n).

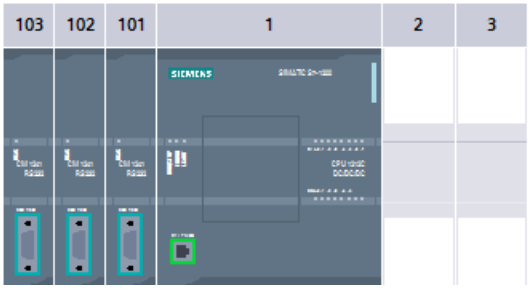
14.3.4 Configuring 3964(R) communication

14.3.4.1 Configuring the 3964(R) communication ports

You can use either of the following methods to configure the communication interfaces for 3964(R) communication:

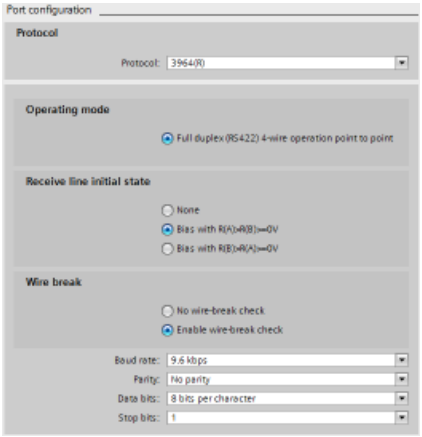
- Use the device configuration in STEP 7 to configure the port parameters. The CPU stores the device configuration settings and applies the settings after a power cycle.
- Use the Port_Config (Page 859) instruction to set the port parameters. The port settings set by the instructions are valid while the CPU is in RUN mode. The port settings revert to the device configuration settings after a power cycle.

After adding the communication interfaces to the device configuration (Page 126), you configure parameters for the communication interfaces by selecting one of the CMs in your rack.



The "Properties" tab of the inspector window displays the parameters of the selected CM. Select "Port configuration" to edit the following parameters:

- Protocol: 3964(R)
- Operating mode
  (CM 1241 (RS422/485) module only)
- Receive line initial state
  (CM 1241 (RS422/485) module only)
- Wire break
  (CM 1241 (RS422/485) module only)
- Baud rate
- Parity
- Data bits
- Stop bits



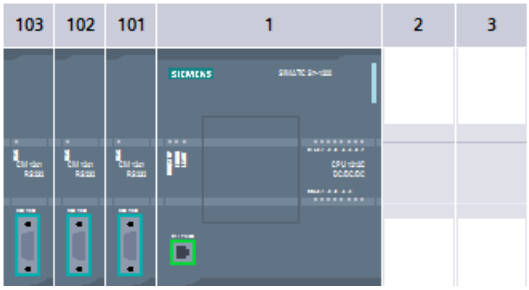
Parameter	Definition
Protocol	3964R or Freeport. Select 3964R to configure port for 3964(R) communication
Operating mode*	Full duplex (RS422) four-wire operation point-to-point. (Enabled)
Receive line initial state*	Enable one of the following choices: • None • Bias with R(A)>R(B)>=0V • Bias with R(B)>R(A)>=0V
Wire break*	Enable one of the following choices: • No wire-break check • Enable wire-break check
Baud rate	The default value for the baud rate is 9.6 Kbits per second. Valid choices are: 300 baud, 600 baud, 1.2 Kbits, 2.4 Kbits, 4.8 Kbits, 9.6 Kbits, 19.2 Kbits, 38.4 Kbits, 57.6 Kbits, 76.8 Kbits, and 115.2 Kbits.
Parity	The default value for parity is no parity. Valid choices are: No parity, even, odd, mark (parity bit always set to 1), space (parity bit always set to 0), and any parity (set parity bit to 0 for transmission; ignore parity error when receiving).
Data bits per character	The number of data bits in a character. Valid choices are 7 or 8.
Number of stop bits	The number of stop bits can be either one or two. The default is one.

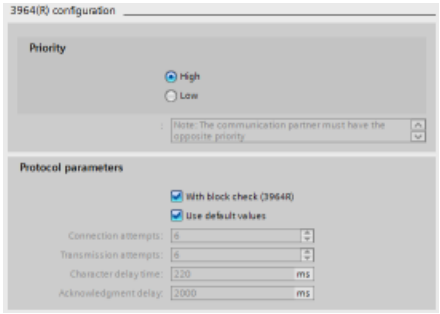
* CM 1241 (RS422/485) module only

14.3.4.2 Configuring the 3964(R) priority and protocol parameters

You can use either of the following methods to configure the communication interfaces for 3964(R) communication:

- In the device configuration of the communication interface, click "3964(R) configuration" to set the priority and configure the protocol parameters. The CPU stores the device configuration settings and applies the settings after a power cycle.
- Use the P3964_Config (Page 868) instruction to set the priority and protocol configuration parameters. The values set by the instructions are valid while the CPU is in RUN mode. The values revert to the device configuration settings after a power cycle.





The "Properties" tab of the inspector window displays the parameters of the selected CM. Select "3964(R) configuration" to edit the following parameters:

- Priority (high or low)
- Protocol parameters
  - With block check (3964R)
  - Use default values
    Connection attempts
    Transmission attempts
    Character delay time
    Acknowledgement delay

Parameter	Definition
Priority	High or low: The CM will be either high or low and the communication partner must be the opposite.
With block check (3964)	If selected, 3964(R) communication employs transmission security by including a block check character (BCC). If not selected transmission security does not include a block check character.
Use default values	If selected, 3964(R) uses default values for the following protocol parameters: • Connection attempts • Transmission attempts • Character delay time • Acknowledgement delay If not selected, you can configure values for each of these parameters.
Connection attempts	Number of connection attempts (default value: 6 connection attempts) 1 to 255
Transmission attempts	Number of transmission attempts (default value: 6 connection attempts) 1 to 255
Character delay time	Character delay time setting (depending on the set data transmission rate) (default value: 220 ms) 1 ms to 65535 ms
Acknowledgement delay	Acknowledgment delay time setting (depending on the set data transmission rate) (default value: 2000 ms when block check is enabled; 550 ms when block check is not enabled) 1 ms to 65535 ms

NOTE

With the exception of Priority, the protocol settings must be the same for the CM module and the communication partner.

14.3.5 Point-to-point instructions

14.3.5.1 Common parameters for Point-to-Point instructions

Table 14-3 Common input parameters for the PTP instructions

Parameter	Description
REQ	Many of the PtP instructions use the REQ input to initiate the operation on a low to high transition. The REQ input must be high (TRUE) for one execution of an instruction, but the REQ input can remain TRUE for as long as desired. The instruction does not initiate another operation until it has been called with the REQ input FALSE so that the instruction can reset the history state of the REQ input. This is required so that the instruction can detect the low to high transition to initiate the next operation. When you place a PtP instruction in your program, STEP 7 prompts you to identify the instance DB. Use a unique DB for each PtP instruction call. This ensures that each instruction properly handles inputs such as REQ.
PORT	A port address is assigned during communication device configuration. After configuration, a default port symbolic name can be selected from the parameter assistant drop-list. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "Constants" tab of the PLC tag table.
Bit time resolution	Several parameters are specified in a number of bit times at the configured baud rate. Specifying the parameter in bit times allows the parameter to be independent of baud rate. All parameters that are in units of bit times can be specified to a maximum number of 65535. However, the maximum amount of time that a CM or CB can measure is eight seconds.

The DONE, NDR, ERROR, and STATUS output parameters of the PtP instructions provide execution completion status for the PtP operations.

Table 14-4 DONE, NDR, ERROR, and STATUS output parameters

Parameter	Data type	Default	Description
DONE	Bool	FALSE	Set TRUE for one execution to indicate that the last request completed without errors; otherwise, FALSE.
NDR	Bool	FALSE	Set TRUE for one execution to indicate that the requested action has completed without error and that the new data has been received; otherwise, FALSE.
ERROR	Bool	FALSE	Set TRUE for one execution to indicate that the last request completed with errors, with the applicable error code in STATUS; otherwise, FALSE.
STATUS	Word	0	Result status: • If the DONE or NDR bit is set, then STATUS is set to 0 or to an informational code. • If the ERROR bit is set, then STATUS is set to an error code. • If none of the above bits are set, then the instruction returns status results that describe the current state of the function. STATUS retains its value for the duration of the execution of the function.

NOTE

The DONE, NDR, and ERROR parameters are set for one execution only. Your program logic must save temporary output state values in data latches, so you can detect state changes in subsequent program scans.

Table 14-5 Common condition codes

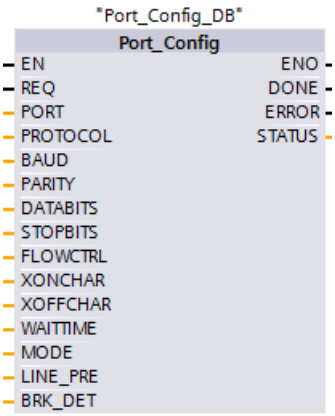
STATUS (W#16#....)	Description
0000	No error
7000	Function is not busy
7001	Function is busy with the first call.
7002	Function is busy with subsequent calls (polls after the first call).
8x3A	Illegal pointer in parameter x
8070	All internal instance memory in use, too many concurrent instructions in progress
8080	Port number is illegal.
8081	Timeout, module error, or other internal error
8082	Parameterization failed because parameterization is in progress in background.
8083	Buffer overflow: The CM or CB returned a received message with a length greater than the length parameter allowed.
8090	Internal error: Wrong message length, wrong sub-module, or illegal message Contact customer support.
8091	Internal error: Wrong version in parameterization message Contact customer support.
8092	Internal error: Wrong record length in parameterization message Contact customer support.

Table 14-6 Common error classes

Class description	Error classes	Description
Port configuration	16#81Ax	Used to define common port configuration errors
Transmit configuration	16#81Bx	Used to define common transmit configuration errors
Receive configuration	16#81Cx 16#82Cx	Used to define common receive configuration errors
Transmission runtime	16#81Dx	Used to define common transmission runtime errors
Reception runtime	16#81Ex	Used to define common reception runtime errors
Signal handling	16#81Fx	Used to define common errors associated with all signal handling
Pointer errors	16#8p01 to 16#8p51	Used for ANY pointer errors where "p" is the parameter number of the instruction
Embedded protocol errors	16#848x 16#858x	Used for embedded protocol errors

14.3.5.2 Port_Config (Configure communication parameters dynamically)

Table 14-7 Port_Config (Port Configuration) instruction

LAD / FBD	SCL	Description
	**"Port_Config_DB"(REQ:=_bool_in_, PORT:=_word_in_, PROTOCOL:=_uint_in_, BAUD:=_uint_in_, PARITY:=_uint_in_, DATABITS:=_uint_in_, STOPBITS:=_uint_in_, FLOWCTRL:=_uint_in_, XONCHAR:=_char_in_, XOFFCHAR:=_char_in_, WAITTIME:=_uint_in_, MODE:=_uint_in_, LINE_PRE:=_uint_in_, BRK_DET:=_uint_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	Port_Config allows you to change port parameters such as baud rate from your program. You can set up the initial static configuration of the port in the device configuration properties, or just use the default values. You can execute the Port_Config instruction in your program to change the configuration.

[1] STEP 7 automatically creates the DB when you insert the instruction.

The CPU does not permanently store the values you set with the Port_Config instruction. The CPU restores the parameters configured in the device configuration when the CPU transitions from RUN to STOP mode and after a power cycle. See Configuring the communication ports (Page 842) and Managing flow control (Page 844) for more information.

Table 14-8 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activate the configuration change on rising edge of this input. (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
PROTOCOL	IN	UInt	0 - Freeport protocol (Default value) 1. 3964(R) protocol
BAUD	IN	UInt	Port baud rate (Default value: 6): 1 = 300 baud, 2 = 600 baud, 3 = 1200 baud, 4 = 2400 baud, 5 = 4800 baud, 6 = 9600 baud, 7 = 19200 baud, 8 = 38400 baud, 9 = 57600 baud, 10 = 76800 baud, 11 = 115200 baud
PARITY	IN	UInt	Port parity (Default value: 1): 1 = No parity, 2 = Even parity, 3 = Odd parity, 4 = Mark parity, 5 = Space parity
DATABITS	IN	UInt	Bits per character (Default value: 1): 1 = 8 data bits, 2 = 7 data bits
STOPBITS	IN	UInt	Stop bits (Default value: 1): 1 = 1 stop bit, 2 = 2 stop bits

[1] Not applicable when Protocol=1 (3964(R) protocol)

[2] Only modes 0 and 1 are valid when Protocol=1 (3964(R) protocol) depending on whether your CM module is an RS232 module or RS422 module.

Parameter and type		Data type	Description
FLOWCTRL*	IN	UInt	Flow control (Default value: 1): 1 = No flow control, 2 = XON/XOFF, 3 = Hardware RTS always ON, 4 = Hardware RTS switched
XONCHAR[1]	IN	Char	Specifies the character that is used as the XON character. This is typically a DC1 character (16#11). This parameter is only evaluated if flow control is enabled. (Default value: 16#11)
XOFFCHAR[1]	IN	Char	Specifies the character that is used as the XOFF character. This is typically a DC3 character (16#13). This parameter is only evaluated if flow control is enabled. (Default value: 16#13)
WAITTIME[1]	IN	UInt	Specifies how long to wait for a XON character after receiving a XOFF character, or how long to wait for the CTS signal after enabling RTS (0 to 65535 ms). This parameter is only evaluated if flow control is enabled. (Default value: 2000)
MODE[2]	IN	UInt	Specifies the selection of the module's operating mode. • 0 = Full duplex (RS232) • 1 = Full duplex (RS422) four-wire mode (point-to-point), transmitter always enabled • 2 = Full duplex (RS422) four-wire mode (multipoint master), transmitter always enabled • 3 = Full duplex (RS422) four-wire mode (multipoint slave), transmitter enabled while sending • 4 = Half duplex (RS485) two-wire mode
LINE_PRE	IN	UInt	Specifies the inactive (idle) line condition. For RS422 and RS485 modules the idle line condition is established by applying a bias voltage to the R(A) and R(B) signals. The following selections are possible: • 0 = Not biased (No Presetting) (default) • 1 = Biased with R(A) > R(B) ≥ 0V; RS422 only • 2 = Biased with R(B) > R(A) ≥ 0V; RS422 and RS485
BRK_DET	IN	UInt	Enables/disables communications cable break detection. Enabling cable break detection causes the module to indicate a fault when the communications cable is not connected to the module. In RS422 Point-to-Point mode cable break detection is only possible when Receive Line Presetting is used with bias applied so that R(A) > R(B) ≥ 0V. • 0 -= No Cable Break Detection (default) • 1 = Cable Break Detection enabled
DONE	OUT	Bool	TRUE for one execution after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one execution after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

[1] Not applicable when Protocol=1 (3964(R) protocol)

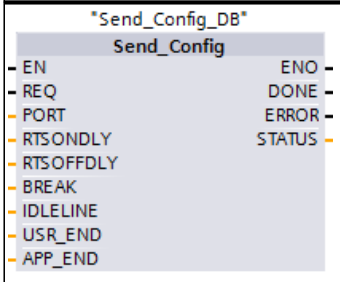
[2] Only modes 0 and 1 are valid when Protocol=1 (3964(R) protocol) depending on whether your CM module is an RS232 module or RS422 module.

Table 14-9 Condition codes

STATUS (W#16#....)	Description
81A0	Specific protocol does not exist.
81A1	Specific baud rate does not exist.
81A2	Specific parity option does not exist.
81A3	Specific number of data bits does not exist.
81A4	Specific number of stop bits does not exist.
80A5	Specific type of flow control does not exist.
81A6	Wait time is 0 and flow control enabled
81A7	XON and XOFF are illegal values (for example, the same value)
81A8	Error in the block header (for example, wrong block type or wrong block length)
81A9	Reconfiguration rejected because a configuration is in progress
81AA	Invalid RS422/RS485 mode of operation
81AB	Invalid presetting of the receive line for break detection
81AC	Invalid RS232 break handling
8280	Negative acknowledgement while reading the module
8281	Negative acknowledgement while writing the module
8282	DP slave or module not available

14.3.5.3 Send_Config (Configure serial transmission parameters dynamically)

Table 14-10 Send_Config (Send Configuration) instruction

LAD / FBD	SCL	Description
	**"Send_Config_DB"(REQ:=_bool_in_, PORT:=_word_in_, RTSONDLY:=_uint_in_, RTSOFFDLY:=_uint_in_, BREAK:=_uint_in_, IDLELINE:=_uint_in_, USR_END:=_string_in_, APP_END:=_string_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	Send_Config allows the dynamic configuration of serial transmission parameters for a PtP communication port. Any queued messages within a CM or CB are discarded when Send_Config is executed.

[1] STEP 7 automatically creates the DB when you insert the instruction.

You can set up the initial static configuration of the port in the device configuration properties, or just use the default values. You can execute the Send_Config instruction in your program to change the configuration.

The CPU does not permanently store the values you set with the Send_Config instruction. The CPU restores the parameters (Page 846) configured in the device configuration when the CPU transitions from RUN to STOP mode and after a power cycle.

Table 14-11 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activate the configuration change on the rising edge of this input. (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
RTSONDLY	IN	UInt	Number of milliseconds to wait after enabling RTS before any Tx data transmission occurs. This parameter is only valid when hardware flow control is enabled. The valid range is 0 - 65535 ms. A value of 0 disables the feature. (Default value: 0)
RTSOFFDLY	IN	UInt	Number of milliseconds to wait after the Tx data transmission occurs before RTS is disabled: This parameter is only valid when hardware flow control is enabled. The valid range is 0 - 65535 ms. A value of 0 disables the feature. (Default value: 0)
BREAK	IN	UInt	This parameter specifies that a break will be sent upon the start of each message for the specified number of bit times. The maximum is 65535 bit times up to an eight second maximum. A value of 0 disables the feature. (Default value: 12)
IDLELINE	IN	UInt	This parameter specifies that the line will remain idle for the specified number of bit times before the start of each message. The maximum is 65535 bit times up to an eight second maximum. A value of 0 disables the feature. (Default value: 0)
USR_END*	IN	STRING[2]	Specifies the number and the characters in the end delimiter. The end delimiter is embedded in the transmit buffer (characters only) and marks the end of the transmitted message (characters are transmitted until the end delimiter is encountered). The end delimiter is appended to the end of the message. • STRING[2,0,xx,yy] – End delimiter is not used (default) • STRING[2,1,xx,yy] – End delimiter is a single character • STRING[2,2,xx,yy] – End delimiter is two characters Either USR_END or APP_END must have a length of zero.
APP_END*	IN	STRING[5]	Specifies the number and the characters to be appended to the transmitted message (only the characters are appended). STRING[5,0,aa,bb,cc,dd,ee] – End char is not used (default) • STRING[5,1,aa,bb,cc,dd,ee] – Transmit one end character • STRING[5,2,aa,bb,cc,dd,ee] – Transmit two end characters • STRING[5,3,aa,bb,cc,dd,ee]– Transmit three end characters • STRING[5,4,aa,bb,cc,dd,ee] – Transmit four end characters • STRING[5,5,aa,bb,cc,dd,ee] – Transmit five end characters
DONE	OUT	Bool	TRUE for one execution after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one execution after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

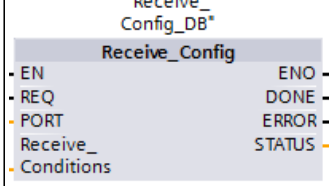
* Not supported for the CM and CB 1241s; you must use an empty string ("") for the parameter.

Table 14-12 Condition codes

STATUS (W#16#....)	Description
81B0	Transmit interrupt configuration is not allowed. Contact customer support.
81B1	Break time is greater than the maximum allowed value.
81B2	Idle time is greater than the maximum allowed value.
81B3	Error in the block header, for example, wrong block type or wrong block length
81B4	Reconfiguration rejected because a configuration is in progress
81B5	The number of end delimiters specified is greater than two or the number of end characters is greater than five
81B6	Send configuration rejected when configured for firmware embedded protocols
8280	Negative acknowledgement while reading the module
8281	Negative acknowledgement while writing the module
8282	DP slave or module not available

14.3.5.4 Receive_Config (Configure serial receive parameters dynamically)

Table 14-13 Receive_Config (Receive Configuration) instruction

LAD / FBD	SCL	Description
	**"Receive_Config_DB"(REQ:=_bool_in_, PORT:=_uint_in_, Receive_Conditions:=_struct_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	Receive_Config performs dynamic configuration of serial receiver parameters for a PtP communication port. This instruction configures the conditions that signal the start and end of a received message. Any queued messages within a CM or CB are discarded when Receive_Config is executed.

[1] STEP 7 automatically creates the DB when you insert the instruction.

You can set up the initial static configuration of the communication port in the device configuration properties, or just use the default values. You can execute the Receive_Config instruction in your program to change the configuration.

The CPU does not permanently store the values you set with the Receive_Config instruction. The CPU restores the parameters configured in the device configuration when the CPU transitions from RUN to STOP mode and after a power cycle. See the topic "Configuring receive parameters (Page 847)" for more information.

Table 14-14 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activate the configuration change on the rising edge of this input. (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)

Parameter and type		Data type	Description
CONDITIONS	IN	CONDITIONS	The Conditions data structure specifies the starting and ending message conditions as described below.
DONE	OUT	Bool	TRUE for one scan, after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one scan, after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

Start conditions for the Receive_P2P instruction

The Receive_P2P instruction uses the configuration specified by the Receive_Config instruction to determine the beginning and ending of point-to-point communication messages. The start of a message is determined by the start conditions. The start of a message can be determined by one or a combination of start conditions. If more than one start condition is specified, all the conditions must be satisfied before the message is started. See the topic "Configuring receive parameters (Page 847)" for a description of the message start conditions.

Parameter CONDITIONS data type structure part 1 (start conditions)

Table 14-15 CONDITIONS structure for start conditions

Parameter and type		Data type	Description
STARTCOND	IN	UInt	Specifies the start condition (Default value: 1) • 01H - Start Char • 02H - Any Char • 04H - Line Break • 08H - Idle Line • 10H - Sequence 1 • 20H - Sequence 2 • 40H - Sequence 3 • 80H - Sequence 4
IDLETIME	IN	UInt	The number of bit times required for idle line timeout. (Default value: 40). Only used with an idle line condition. 0 to 65535
STARTCHAR	IN	Byte	The start character used with the start character condition. (Default value: B#16#2)
STRSEQ1CTL	IN	Byte	Sequence 1 ignore/compare control for each character: (Default value: B#16#0) These are the enabling bits for each character in start sequence • 01H - Character 1 • 02H - Character 2 • 04H - Character 3 • 08H - Character 4 • 10H - Character 5 Disabling the bit associated with a character means any character will match, in this sequence position.
STRSEQ1	IN	Char[5]	Sequence 1 start characters (5 characters). Default value: 0
STRSEQ2CTL	IN	Byte	Sequence 2 ignore/compare control for each character. Default value: B#16#0)
STRSEQ2	IN	Char[5]	Sequence 2 start characters (5 characters). Default value: 0

Parameter and type		Data type	Description
STRSEQ3CTL	IN	Byte	Sequence 3 ignore/compare control for each character. Default value: B#16#0
STRSEQ3	IN	Char[5]	Sequence 3 start characters (5 characters). Default value: 0
STRSEQ4CTL	IN	Byte	Sequence 4 ignore/compare control for each character. Default value: B#16#0
STRSEQ4	IN	Char[5]	Sequence 4 start characters (5 characters), Default value: 0

Example

Consider the following received hexadecimal coded message: "**68** 10 aa **68** bb 10 aa 16" and the configured start sequences shown in the table below. Start sequences begin to be evaluated when the first 68H character is successfully received. Upon successfully receiving the fourth character (the second 68H), then start condition 1 is satisfied. Once the start conditions are satisfied, the evaluation of the end conditions begins.

The start sequence processing can be terminated due to various parity, framing, or inter-character timing errors. These errors result in no received message, because the start condition was not satisfied.

Table 14-16 Start conditions

Start condition	First Character	First Character +1	First Character +2	First Character +3	First Character +4
1	**68**H	xx	xx	**68**H	xx
2	10H	aaH	xx	xx	xx
3	dcH	aaH	xx	xx	xx
4	e5H	xx	xx	xx	xx

End conditions for the Receive_P2P instruction

The end of a message is determined by the specification of end conditions. The end of a message is determined by the first occurrence of one or more configured end conditions. The section "Message end conditions" in the topic "Configuring receive parameters (Page 847)" describes the end conditions that you can configure in the Receive_Config instruction.

You can configure the end conditions in either the properties of the communication interface in the device configuration, or from the Receive_Config instruction. Whenever the CPU transitions from STOP to RUN, the receive parameters (both start and end conditions) return to the device configuration settings. If the STEP 7 user program executes Receive_Config, then the settings are changed to the Receive_Config conditions.

Parameter CONDITIONS data type structure part 2 (end conditions)

Table 14-17 CONDITIONS structure for end conditions

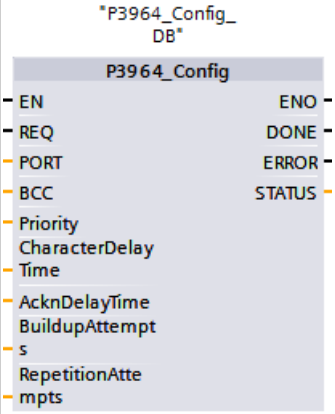
Parameter	Parameter type	Data type	Description
ENDCOND	IN	UInt 0	This parameter specifies message end condition: • 01H - Response time • 02H - Message time • 04H - Inter-character gap • 08H - Maximum length • 10H - N + LEN + M • 20H - Sequence
MAXLEN	IN	UInt 1	Maximum message length: Only used when the maximum length end condition is selected. 1 to 1024 bytes
N	IN	UInt 0	Byte position within the message of the length field. Only used with the N + LEN + M end condition. 1 to 1022 bytes
LENGTHSIZE	IN	UInt 0	Size of the byte field (1, 2, or 4 bytes). Only used with the N + LEN + M end condition.
LENGTHM	IN	UInt 0	Specify the number of characters following the length field that are not included in the value of the length field. This is only used with the N + LEN + M end condition. 0 to 255 bytes
RCVTIME	IN	UInt 200	Specify how long to wait for the first character to be received. The receive operation will be terminated with an error if a character is not successfully received within the specified time. This is only used with the response time condition. (0 to 65535 bit times with an 8 second maximum) This parameter is not a message end condition since evaluation terminates when the first character of a response is received. It is an end condition only in the sense that it terminates a receiver operation because no response is received when a response is expected. You must select a separate end condition.
MSGTIME	IN	UInt 200	Specify how long to wait for the entire message to be completely received once the first character has been received. This parameter is only used when the message timeout condition is selected. (0 to 65535 milliseconds)
CHARGAP	IN	UInt 12	Specify the number of bit times between characters. If the number of bit times between characters exceeds the specified value, then the end condition will be satisfied. This is only used with the inter-character gap condition. (0 to 65535 bit times up to 8 second maximum)
ENDSEQ1CTL	IN	Byte B#16#0	Sequence 1 ignore/compare control for each character: These are the enabling bits for each character for the end sequence. Character 1 is bit 0, character 2 is bit 1, ..., character 5 is bit 4. Disabling the bit associated with a character means any character will match, in this sequence position.
ENDSEQ1	IN	Char[5] 0	Sequence 1 start characters (5 characters)

Table 14-18 Condition codes

STATUS (W#16#....)	Description
81C0	Illegal start condition selected
81C1	Illegal end condition selected, no end condition selected
81C2	Receive interrupt enabled and this is not possible.
81C3	Maximum length end condition is enabled and max length is 0 or > 1024.
81C4	Calculated length is enabled and N is >= 1023.
81C5	Calculated length is enabled and length is not 1, 2 or 4.
81C6	Calculated length is enabled and M value is > 255.
81C7	Calculated length is enabled and calculated length is > 1024.
81C8	Response timeout is enabled and response timeout is zero.
81C9	Inter-character gap timeout is enabled and it is zero.
81CA	Idle line timeout is enabled and it is zero.
81CB	End sequence is enabled but all chars are "don't care".
81CC	Start sequence (any one of 4) is enabled but all characters are "don't care".
81CD	Invalid receive message overwrite protection selection error
81CE	Invalid receive message buffer handling on STOP to RUN transition selection error
81CF	Error in the block header, for example, wrong block type or wrong block length
8281	Negative acknowledgement while writing the module
8282	DP slave or module not available
82C0	Reconfiguration rejected because a configuration is in progress
82C1	The specified value for the number of messages that the module can buffer is greater than the maximum permitted value.
82C2	Receive configuration rejected when configured for firmware embedded protocols
8351	Data type not allowed at this Variant pointer

14.3.5.5 P3964_Config (Configuring the 3964(R) protocol)

Table 14-19 P3964_Config (Configuring the 3964(R) protocol) instruction

LAD / FBD	SCL	Description
	**"P3964_Config_DB"(REQ:=_bool_in_, PORT:=_uint_in_, BCC:=_usint_in, Priority:= _usint_in, CharacterDelayTime:=_uint_in, AcknDelayTime:= _uint_in, BuildupAttempts:=_usint_in_, RepetitionAttempts:=_usint_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	P3964_Config allows you to change priority and protocol parameters during runtime. You can set up the initial static configuration of the port in the device configuration properties, or just use the default values. You can execute the P3964_Config instruction in your program to change the configuration.

[1] STEP 7 automatically creates the DB when you insert the instruction.

The CPU does not permanently store the values you set with the P3964_Config instruction. The CPU restores the parameters configured in the device configuration after a power cycle of the CPU. See Configuring the 3964(R) communication priority and protocol parameters (Page 855) for more information.

Table 14-20 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activate the configuration change on rising edge of this input. (Default value: False)
PORT	IN	UInt	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
BCC	IN	USInt	Activates/deactivates the use of the block check • 0 = without block check • 1 = with block check
Priority	IN	UInt	Selection of the priority • 0 = low priority • 1 = high priority The priority of the CM must be the opposite of the priority of the communication partner.
CharacterDelay-Time	IN	UInt	Character delay time setting (depending on the set data transmission rate) (default value: 220 ms) 1 ms to 65535 ms
AcknDelayTime	IN	UInt	Acknowledgment delay time setting (depending on the set data transmission rate) (default value: 2000 ms) 1 ms to 65535 ms
BuildupAttempts	IN	UInt	Number of connection attempts (default value: 6 connection attempts) 1 to 255
RepetitionAt-tempts	IN	UInt	Number of transmission attempts (default value: 6 connection attempts) 1 to 255

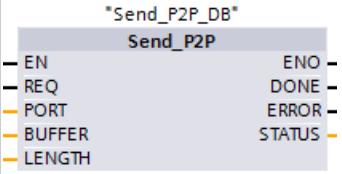
Parameter and type		Data type	Description
DONE	OUT	Bool	TRUE for one execution after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one execution after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

Table 14-21 Condition codes

STATUS (W#16#....)	Description
16#8380	Parameter assignment error: Invalid value for "Character delay time".
16#8381	Parameter assignment error: Invalid value for "Response timeout".
16#8382	Parameter assignment error: Invalid value for "Priority".
16#8383	Parameter assignment error: Invalid value for "Block check"
16#8384	Parameter assignment error: Invalid value for "Connection attempts".
16#8385	Parameter assignment error: Invalid value for "Transmission attempts".
16#8386	Runtime error: Number of connection attempts exceeded
16#8387	Runtime error: Number of transmission attempts exceeded
16#8388	Runtime error: Error at the "Block check character" The internally calculated value of the block check character does not correspond to the block check character received by the partner at the connection end.
16#8389	Runtime error: Invalid character received while waiting for free receive buffer
16#838A	Runtime error: Logical error during receiving. After DLE was received, a further random character (other than DLE or ETX) was received.
16#838B	Runtime error: Character delay time exceeded
16#838C	Runtime error: Wait time for free receive buffer has started
16#838D	Runtime error: frame repetition does not start within 4 s after NAK
16#838E	Runtime error: In idle mode, one or several characters (other than NAK or STX) were received.
16#838F	Runtime error: Initialization conflict - Both partners have set high priority
16#8391	Parameter assignment error: 3964 configuration data rejected because Freeport is set

14.3.5.6 Send_P2P (Transmit send buffer data)

Table 14-22 Send_P2P (Send Point-to-Point data) instruction

LAD / FBD	SCL	Description
	**"Send_P2P_DB"(REQ:=_bool_in_, PORT:=_word_in_, BUFFER:=_variant_in_, LENGTH:=_uint_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	Send_P2P initiates the transmission of the data and transfers the assigned buffer to the communication interface. The CPU program continues while the CM or CB sends the data at the assigned baud rate. Only one send operation can be pending at a given time. The CM or CB returns an error if a second Send_P2P is executed while the CM or CB is already transmitting a message.

[1] STEP 7 automatically creates the DB when you insert the instruction.

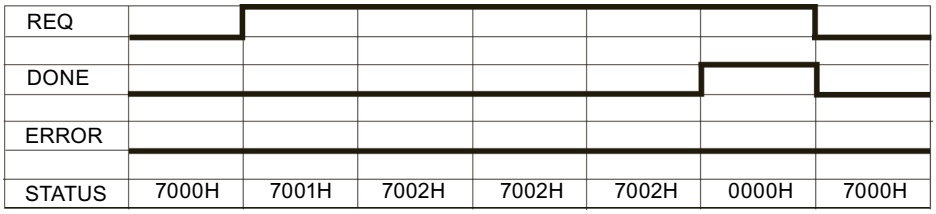
Table 14-23 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activates the requested transmission on the rising edge of this transmission enable input. This initiates transfer of the contents of the buffer to the Point-to-Point communication interface. (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
BUFFER	IN	Variant	This parameter points to the starting location of the transmit buffer. (Default value: 0) **Note:** Boolean data or Boolean arrays are not supported.
LENGTH	IN	UInt	Transmitted frame length in bytes (Default value: 0) When transmitting a complex structure, always use a length of 0. When the length is 0, the instruction transmits the entire frame.
DONE	OUT	Bool	TRUE for one scan, after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one scan, after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

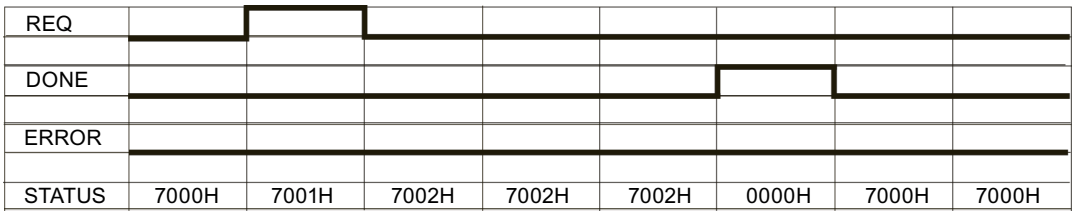
While a transmit operation is in progress, the DONE and ERROR outputs are FALSE. When a transmit operation is complete, either the DONE or the ERROR output will be set TRUE to show the status of the transmit operation. While DONE or ERROR is TRUE, the STATUS output is valid.

The instruction returns a status of 16#7001 if the communication interface accepts the transmit data. Subsequent Send_P2P executions return 16#7002, if the CM or CB is still busy transmitting. When the transmit operation is complete, the CM or CB returns the status of the transmit operation as 16#0000 (if no errors occurred). Subsequent executions of Send_P2P with REQ low return a status of 16#7000 (not busy).

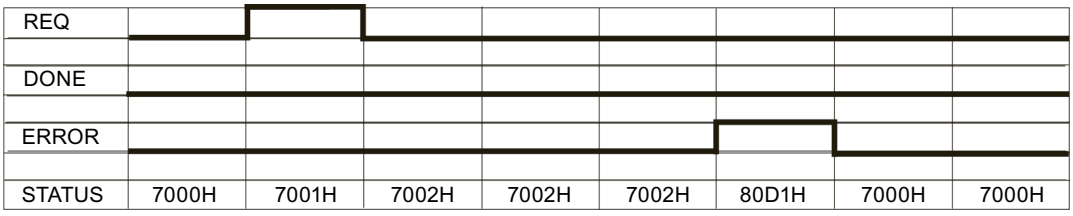
The following diagrams show the relationship of the output values to REQ. This assumes that the instruction is called periodically to check for the status of the transmission process. In the diagram below, it is assumed that the instruction is called every scan (represented by the STATUS values).



The following diagram shows how the DONE and STATUS parameters are valid for only one scan if the REQ line is pulsed (for one scan) to initiate the transmit operation.



The following diagram shows the relationship of DONE, ERROR and STATUS parameters when there is an error.



The DONE, ERROR and STATUS values are only valid until Send_P2P executes again with the same instance DB.

Table 14-24 Condition codes

STATUS (W#16#....)	Description
81D0	New request while transmitter active
81D1	Transmit aborted because of no CTS within wait time
81D2	Transmit aborted because of no DSR from the DCE device
81D3	Transmit aborted because of queue overflow (transmit more than 1024 bytes)
81D5	Reverse bias signal (wire break condition)
81D6	Transmission request rejected because end delimiter was not found in the transmit buffer
81D7	Internal error / error in synchronization between FB and CM
81D8	Transmission attempt rejected because the port has not been configured
81DF	CM has reset the interface to the FB due to one of the following reasons • The module has restarted (Power cycle) • The CPU has reached a breakpoint • The module has been reparameterized In each case the module indicates this code in the Status parameter. The module resets Status and Error to zero after the first received record for SEND_P2P.
8281	Negative acknowledgement while writing the module

STATUS (W#16#....)	Description
8282	DP slave or module not available
8301	Illegal syntax ID at an ANY pointer
8322	Range length error when reading a parameter
8324	Range error when reading a parameter
8328	Alignment error when reading a parameter
8332	The parameter contains a DB number that is higher than the highest permitted number (DB number error).
833A	The DB for the BUFFER parameter does not exist.

NOTE

Setting the maximum record length for Profibus communication

When using a CM1243-5 Profibus Master module to control an ET 200SP or ET 200MP Profibus device that uses an RS232, RS422, or RS485 point-to-point module, you need to explicitly set the "max_record_len" data block tag to 240 as defined below:

Set "max_record_len" in the instance DB (for example, "Send_P2P_DB".max_record_len) to 240 after running any configuration instruction such as Port_Config, Send_Config, or Receive_Config.

Explicitly assigning max_record_len is only necessary with Profibus communication; Profinet communication already uses a valid max_record_len value.

Interaction of the LENGTH and BUFFER parameters

The minimum size of data that can be transmitted by the SEND_P2P instruction is one byte. The BUFFER parameter determines the size of the data to be transmitted. You cannot use the data type Bool or arrays of Bool for the BUFFER parameter.

You can always set the LENGTH parameter to 0 and ensure that SEND_P2P sends the entire data structure represented by the BUFFER parameter. If you only want to send part of a data structure in the BUFFER parameter, you can set LENGTH as follows:

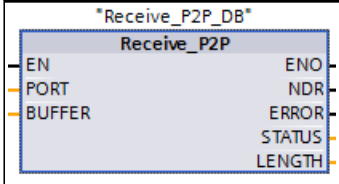
Table 14-25 LENGTH and BUFFER parameters

LENGTH	BUFFER	Description
= 0	Not used	The complete data is sent as defined at the BUFFER parameter. You do not need to specify the number of transmitted bytes when LENGTH = 0.
> 0	Elementary data type	The LENGTH value must contain the byte count of this data type. For example, for a Word value, the LENGTH must be two. For a Dword or Real, the LENGTH must be four. Otherwise, nothing is transferred and the error 8088H is returned.
	Structure	The LENGTH value can contain a byte count less than the complete byte length of the structure, in which case the instruction sends only the first n bytes of the structure from the BUFFER, where n = LENGTH. Since the internal byte organization of a structure cannot always be determined, you might get unexpected results. In this case, use a LENGTH of 0 to send the complete structure.

LENGTH	BUFFER	Description
> 0	Array	The LENGTH value must contain a byte count that is less than or equal to the complete byte length of the array and which must be a multiple of the data element byte count. For example, the LENGTH parameter for an array of Words must be a multiple of two and for an array of Reals, a multiple of four. When LENGTH is specified, the instruction transfers the number of array elements that correspond to the LENGTH value in bytes. If your BUFFER, for example, contains an array of 15 Dwords (60 total bytes), and you specify a LENGTH of 20, then the first five Dwords in the array are transferred. The LENGTH value must be a multiple of the data element byte count. Otherwise, STATUS = 8088H, ERROR = 1, and no transmission occurs.
	String	The LENGTH parameter contains the number of characters to be transmitted. Only the characters of the String are transmitted. The maximum and actual length bytes of the String are not transmitted.

14.3.5.7 Receive_P2P (Enable receive messages)

Table 14-26 Receive_P2P (Receive Point-to-Point) instruction

LAD / FBD	SCL	Description
	**"Receive_P2P_DB"(PORT:=_word_in_, BUFFER:=_variant_in_, NDR=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, LENGTH=>_uint_out_);**	Receive_P2P checks for messages that have been received in the CM or CB. If a message is available, it will be transferred from the CM or CB to the CPU. An error returns the appropriate STATUS value.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 14-27 Data types for the parameters

Parameter and type		Data type	Description
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
BUFFER	IN	Variant	This parameter points to the starting location of the receive buffer. This buffer should be large enough to receive the maximum length message. Boolean data or Boolean arrays are not supported. (Default value: 0)
NDR	OUT	Bool	TRUE for one execution when new data is ready and operation is complete with no errors.
ERROR	OUT	Bool	TRUE for one execution after the operation was completed with an error.
STATUS	OUT	Word	Execution condition code (Default value: 0)
LENGTH	OUT	UInt	Length of the returned message in bytes (Default value: 0)

The STATUS value is valid when either NDR or ERROR is TRUE. The STATUS value provides the reason for termination of the receive operation in the CM or CB. This is typically a positive value, indicating that the receive operation was successful and that the receive process terminated normally. If the STATUS value is negative (the Most Significant Bit of the hexadecimal value is set), the receive operation was terminated for an error condition such as parity, framing, or overrun errors.

Each PtP communication interface can buffer up to a maximum of 1024 bytes. This could be one large message or several smaller messages. If more than one message is available in the CM or CB, the Receive_P2P instruction returns the oldest message available. A subsequent Receive_P2P instruction execution returns the next oldest message available.

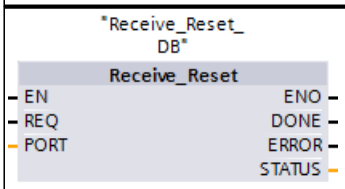
Table 14-28 Condition codes

STATUS (W#16#...)	Description
0000	No buffer present
0094	Message terminated due to received maximum character length
0095	Message terminated because of message timeout
0096	Message terminated because of inter-character timeout
0097	Message terminated because of response timeout
0098	Message terminated because the "N+LEN+M" length condition was satisfied
0099	Message terminated because of end sequence was satisfied
8085	LENGTH parameter has a value of 0 or is greater than 1KB.
8088	The LENGTH parameter or the received length is longer than the area specified in BUFFER or the received length is longer than the area specified in BUFFER.
8090	Incorrect configuration message, wrong message length, wrong submodule, illegal message
81E0	Message terminated because the receive buffer is full
81E1	Message terminated due to parity error
81E2	Message terminated due to framing error
81E3	Message terminated due to overrun error
81E4	Message terminated because calculated length exceeds buffer size
81E5	Reverse bias signal (wire break condition)
81E6	The message queue is full. This error is reported without data. If it occurs, the module toggles between an error free data transfer and this error.
81E7	Internal error, error in synchronization between instruction and CM: set when a sequence error is detected
81E8	Message terminated, inter-character timeout expired before the end of message criteria was satisfied
81E9	Modbus CRC error detected (Only used by modules that support CRC generation/checking for the Modbus protocol)
81EA	Modbus telegram is too short (Only used by modules that support CRC generation/checking for the Modbus protocol)
81EB	Message terminated, because maximum message size exceeded
8201	Illegal syntax ID at an ANY pointer
8223	Range length error when writing a parameter. The parameter is located either entirely or partly outside the range of an address or that the length of a bit range is not a multiple of 8 with an ANY pointer.
8225	Range error when writing a parameter. The parameter is located in a range that is illegal for the system function.
8229	Alignment error when writing a parameter. The referenced parameter is located at bit address that is not equal to 0.
8230	Parameter is located in a read-only global DB
8231	Parameter is located in a read-only instance DB.

STATUS (W#16#...)	Description
8232	Parameter contains a DB number that is higher than the highest block number allowed (DB number error).
823A	The DB for the BUFFER parameter does not exist.
8280	Negative acknowledgement while reading the module
8282	DP slave or module not available

14.3.5.8 Receive_Reset (Delete receive buffer)

Table 14-29 Receive_Reset (Receiver Reset) instruction

LAD / FBD	SCL	Description
	**"Receive_Reset_DB"(REQ:=_bool_in_, PORT:=_word_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	Receive_Reset clears the receive buffers in the CM or CB.

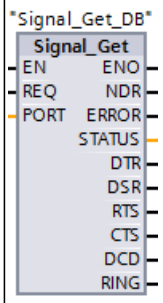
[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 14-30 Data types for parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activates the receiver reset on the rising edge of this enable input (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
DONE	OUT	Bool	When TRUE for one scan, indicates that the last request was completed without errors.
ERROR	OUT	Bool	When TRUE, shows that the last request was completed with errors. Also, when this output is TRUE, the STATUS output will contain related error codes.
STATUS	OUT	Word	Error code (Default value: 0)

14.3.5.9 Signal_Get (Query RS-232 signals)

Table 14-31 Signal_Get (Get RS232 signals) instruction

LAD / FBD	SCL	Description
	**"Signal_Get_DB"(REQ:=_bool_in_, PORT:=_uint_in_, NDR=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, DTR=>_bool_out_, DSR=>_bool_out_, RTS=>_bool_out_, CTS=>_bool_out_, DCD=>_bool_out_, RING=>_bool_out_);**	Signal_Get reads the current states of RS232 communication signals. This function is valid only for the RS232 CM.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 14-32 Data types for the parameters

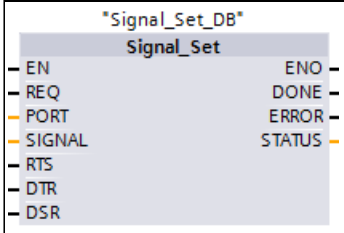
Parameter and type		Data type	Description
REQ	IN	Bool	Get RS232 signal state values on the rising edge of this input (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table.
NDR	OUT	Bool	TRUE for one scan, when new data is ready and the operation is complete with no errors
ERROR	OUT	Bool	TRUE for one scan, after the operation was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)
DTR	OUT	Bool	Data terminal ready, module ready (output). Default value: False
DSR	OUT	Bool	Data set ready, communication partner ready (input). Default value: False
RTS	OUT	Bool	Request to send, module ready to send (output). Default value: False
CTS	OUT	Bool	Clear to send, communication partner can receive data (input). Default value: False
DCD	OUT	Bool	Data carrier detect, receive signal level (always False, not supported)
RING	OUT	Bool	Ring indicator, indication of incoming call (always False, not supported)

Table 14-33 Condition codes

STATUS (W#16#....)	Description
81F0	CM or CB is RS485 and no signals are available
81F4	Error in the block header, for example, wrong block type or wrong block length
8280	Negative acknowledgement while reading the module
8282	DP slave or module not available

14.3.5.10 Signal_Set (Set RS-232 signals)

Table 14-34 Signal_Set (Set RS232 signals) instruction

LAD / FBD	SCL	Description
	**"Signal_Set_DB"(REQ:=_bool_in_, PORT:=_word_in_, SIGNAL:=_byte_in_, RTS:=_bool_in_, DTR:=_bool_in_, DSR:=_bool_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	Signal_Set sets the states of RS232 communication signals. This function is valid only for the RS232 CM.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 14-35 Data types for parameters

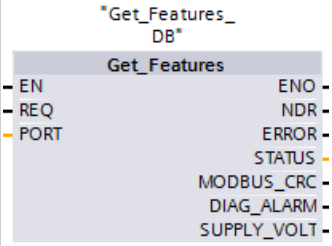
Parameter and type		Data type	Description
REQ	IN	Bool	Start the set RS232 signals operation, on the rising edge of this input (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
SIGNAL	IN	Byte	Selects which signal to set: (multiple allowed). Default value: 0 • 01H = Set RTS • 02H = Set DTR • 04H = Set DSR
RTS	IN	Bool	Request to send, module ready to send value to set (true or false), Default value: False
DTR	IN	Bool	Data terminal ready, module ready to send value to set (true or false). Default value: False
DSR	IN	Bool	Data set ready (only applies to DCE type interfaces), not used.
DONE	OUT	Bool	TRUE for one execution after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one execution after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

Table 14-36 Condition codes

STATUS (W#16#....)	Description
81F0	CM or CB is RS485 and no signals can be set
81F1	Signals cannot be set because of Hardware flow control
81F2	Cannot set DSR because module is DTE
81F3	Cannot set DTR because module is DCE
81F4	Error in the block header, for example, wrong block type or wrong block length
8280	Negative acknowledgement while reading the module
8281	Negative acknowledgement while writing the module
8282	DP slave or module not available

14.3.5.11 Get_Features

Table 14-37 Get_Features (Get advanced features) instruction

LAD / FBD	SCL	Description
	**"Get_Features_DB"(REQ:=_bool_in_, PORT:=_word_in_, NDR:=_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, MODBUS_CRC=>_bool_out_, DIAG_ALARM=>_bool_out_, SUPPLY_VOLT=>_bool_out);**	Get_Features reads the advanced feature capabilities of a module.

[1] STEP 7 automatically creates the DB when you insert the instruction.

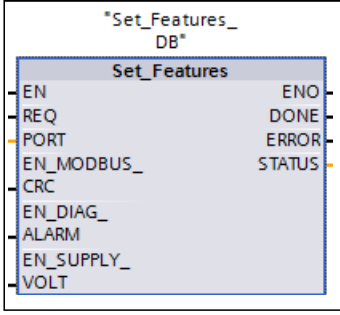
Table 14-38 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activate the configuration change on the rising edge of this input. (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
NDR	OUT	Bool	Indicates that new data is ready.
ERROR	OUT	Bool	TRUE for one scan, after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)
MODBUS_CRC*	OUT	Bool	MODBUS CRC generation and checking
DIAG_ALARM*	OUT	Bool	Diagnostic alarm generation
SUPPLY_VOLT*	OUT	Bool	Diagnostics for missing supply voltage L+ is available

*Get_Features returns TRUE (1) if the feature is available, FALSE (0) if the feature is not available

14.3.5.12 Set_Features

Table 14-39 Set_Features (Set advanced features) instruction

LAD / FBD	SCL	Description
	**"Set_Features_DB"(REQ:=_bool_in_, PORT:=_word_in_, EN_MODBUS_CRC:=_bool_in_, EN_DIAG_ALARM:=_bool_in_, EN_SUPPLY_VOLT:=_bool_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	Set_Features sets the advanced features that a module supports.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 14-40 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activate the configuration change on the rising edge of this input. (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
EN_MODBUS_CRC	IN	Bool	Enable MODBUS CRC generation and checking: • 0: CRC calculation tuned OFF (default) • 1: CRC calculation turned ON Note: Only V2.1 CMs, V4.x CPUs with CBs, and CM PtP modules for distributed I/O support this parameter.
EN_DIAG_ALARM	IN	Bool	Enable diagnostic alarm generation: • 0: Diagnostic alarm turned OFF • 1: Diagnostic alarm turned ON (default)
EN_SUPPLY_VOLT	IN	Bool	Enable diagnostics for missing supply voltage L+: • 0: Supply voltage diagnostic disabled (default) • 1: Supply voltage diagnostic enabled
DONE	OUT	Bool	Indicates that set features is done
ERROR	OUT	Bool	TRUE for one scan, after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

14.3.6 Programming the PtP communications

STEP 7 provides extended instructions that enable the user program to perform Point-to-Point communications with a protocol designed and implemented in the user program. These instructions fall into two categories:

- Configuration instructions
- Communication instructions

Configuration instructions

Before your user program can engage in PtP communication, you must configure the communication interface port and the parameters for sending data and receiving data.

You can perform the port configuration and message configuration for each CM or CB through the device configuration or through these instructions in your user program:

- Port_Config (Page 859)
- Send_Config (Page 861)
- Receive_Config (Page 863)

Communication instructions

The PtP communication instructions enable the user program to send messages to and receive messages from the communication interfaces. For information about transferring data with these instructions, see the section on data consistency (Page 178).

All of the PtP functions operate asynchronously. The user program can use a polling architecture to determine the status of transmissions and receptions. Send_P2P and Receive_P2P can execute concurrently. The communication modules and communication board buffer the transmit and receive messages as necessary up to a maximum buffer size of 1024 bytes.

The CMs and CB send messages to and receive messages from the actual point-to-point devices. The message protocol is in a buffer that is either received from or sent to a specific communication port. The buffer and port are parameters of the send and receive instructions:

- Send_P2P (Page 870)
- Receive_P2P (Page 873)

Additional instructions provide the capability to reset the receive buffer, and to get and set specific RS232 signals:

- Receive_Reset (Page 875)
- Signal_Get (Page 876)
- Signal_Set (Page 877)

14.3.6.1 Polling architecture

The STEP 7 user program must call the S7-1200 point-to-point instructions cyclically/periodically to check for received messages. Polling the send tells the user program when the transmit has completed.

Polling architecture: master

The typical sequence for a master is as follows:

1. A Send_P2P (Page 870) instruction initiates a transmission to the CM or CB.
2. The Send_P2P instruction executes on subsequent scans to poll for the transmit complete status.
3. When the Send_P2P instruction indicates that the transmission is complete, the user code can prepare to receive the response.
4. The Receive_P2P (Page 873) instruction executes repeatedly to check for a response. When the CM or CB has collected a response message, the Receive_P2P instruction copies the response to the CPU and indicates that new data has been received.
5. The user program can process the response.
6. Go to step 1 and repeat the cycle.

Polling architecture: slave

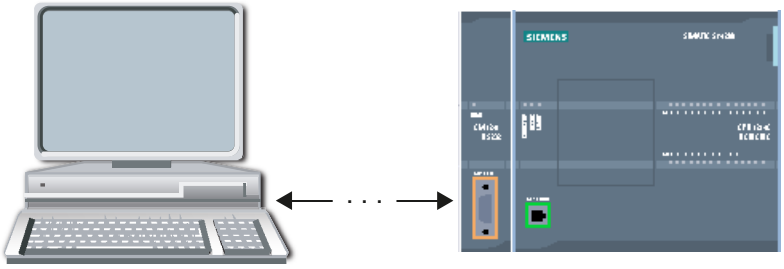
The typical sequence for a slave is as follows:

1. The user program executes the Receive_P2P instruction every scan.
2. When the CM or CB has received a request, the Receive_P2P instruction indicates that new data is ready and the request is copied into the CPU.
3. The user program services the request and generates a response.
4. Use a Send_P2P instruction to send the response back to the master.
5. Repeatedly execute Send_P2P to be sure the transmit occurs.
6. Go to step 1 and repeat the cycle.

The slave must be responsible for calling Receive_P2P frequently enough to receive a transmission from the master before the master times out while waiting for a response. To accomplish this task, the user program can call RCV_PTP from a cyclic OB, where the cycle time is sufficient to receive a transmission from the master before the timeout period expires. If you set the cycle time for the OB to provide for two executions within the timeout period of the master, the user program can receive transmissions without missing any.

14.3.7 Example: Point-to-Point communication

In this example, an S7-1200 CPU communicates to a PC with a terminal emulator through a CM 1241 RS232 module. The point-to-point configuration and STEP 7 program in this example illustrate how the CPU can receive a message from the PC and echo the message back to the PC.



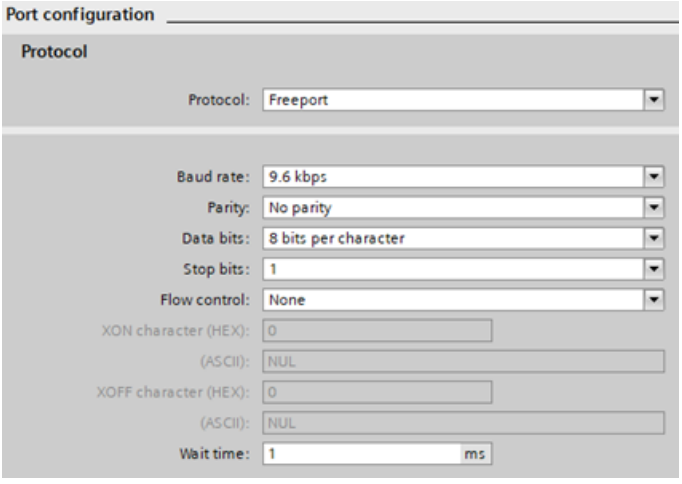
You must connect the communication interface of the CM 1241 RS232 module to the RS232 interface of the PC, which is normally COM1. Because both of these ports are Data Terminal Equipment (DTE), you must switch the receive and transmit pins (2 and 3) when connecting the two ports, which you can accomplish by either of the following methods:

- Use a NULL modem adapter to swap pins 2 and 3 together with a standard RS232 cable.
- Use a NULL modem cable, which already has pins 2 and 3 swapped. You can usually identify a NULL modem cable as one with two female 9-pin D connector ends.

14.3.7.1 Configuring the communication module

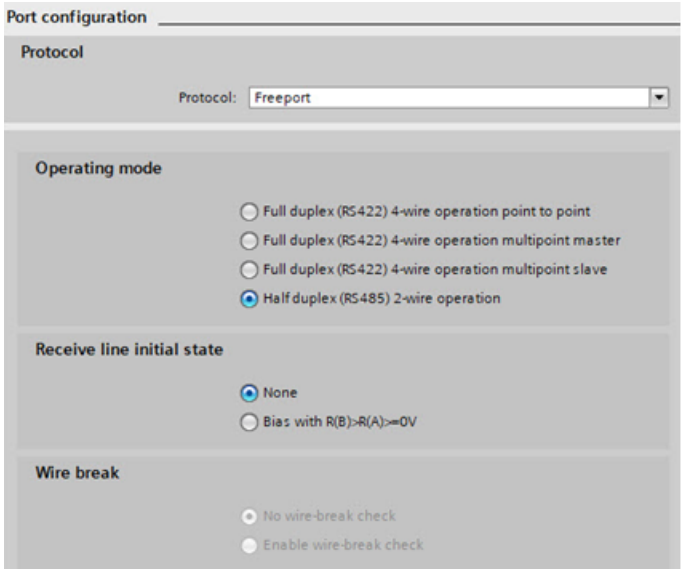
You can configure the CM 1241 from the Device configuration in STEP 7 or with user program instructions. This example uses the Device configuration method.

- Port configuration: Click the communication port of the CM module from the Device configuration, and configure the port as shown:

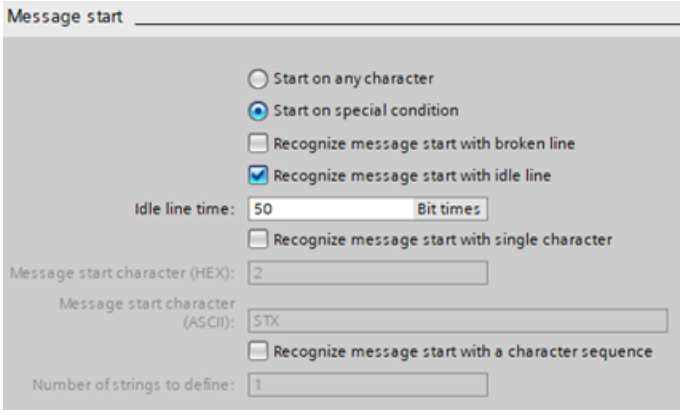


NOTE

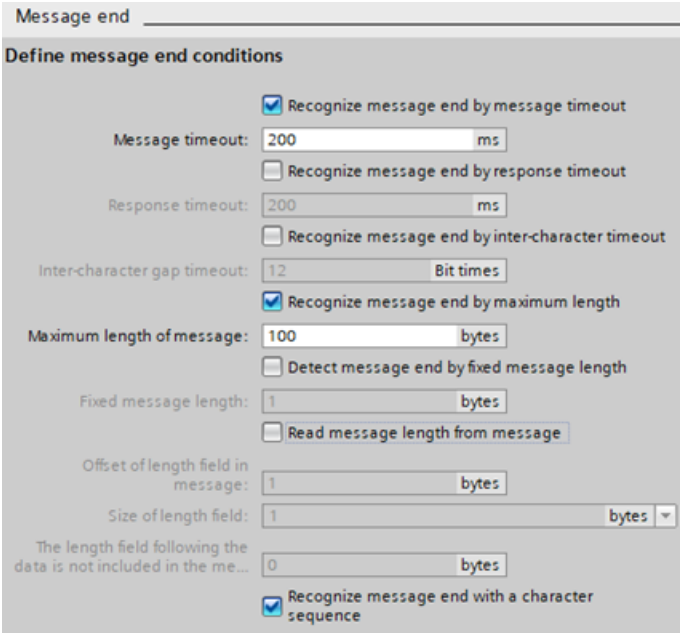
The configuration settings for the CM 1241 (RS422/RS485) module include "Operating mode", "Receive line initial state", and "Wire break" as shown below. Refer to Configuring the RS422 and RS485 (Page 885).

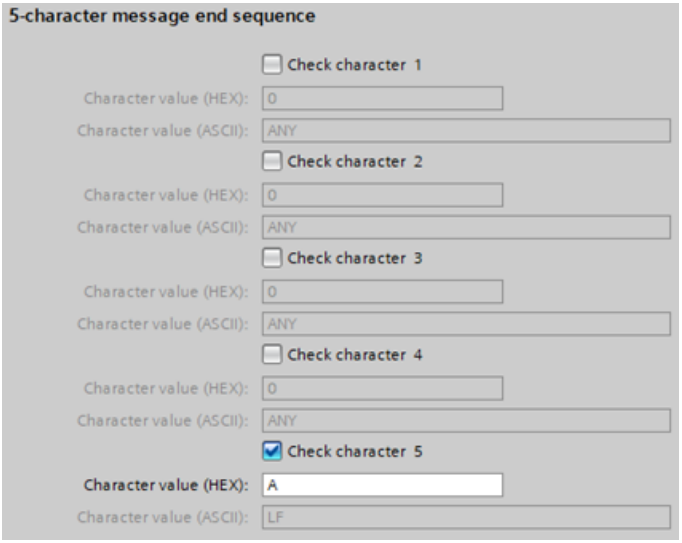


- Transmit message configuration: Accept the default for transmit message configuration. No break is to be sent at message start.
- Receive message start configuration: Configure the CM 1241 to start receiving a message when the communication line is inactive for at least 50 bit times (about 5 milliseconds at 9600 baud = 50 * 1/9600):



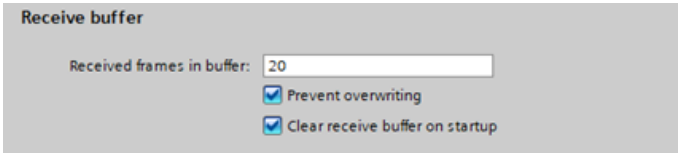
- Receive message end configuration: Configure the CM 1241 to end a message when it receives a maximum of 100 bytes or a linefeed character (10 decimal or a hexadecimal). The end sequence allows up to five end characters in sequence. The fifth character in the sequence is the linefeed character. The preceding four end sequence characters are "don't care" or unselected characters. The CM 1241 does not evaluate the "don't care" characters but looks for a linefeed character preceded by zero or more "don't care" characters to indicate the message end.





Receive buffer: Configure the number of received messages that the module will queue, stop the module from receiving more messages once the queue is full, and clear all previously received messages on a stop to run (startup) transition.

NOTE
Receive buffer settings
The receive buffer settings are only available for CM 1241 (RS232) and CM 1241 (RS422/485) with V2.1.



14.3.7.2 RS422 and RS485 operating modes

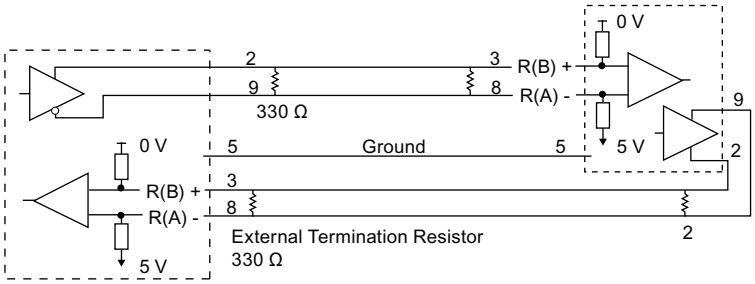
Configuring the RS422

For RS422 mode, there are three operating modes depending on your network configuration. Select one of these operating modes based on the devices in your network. The different selections for Receive line initial state reference the cases shown below for more details.

- Full duplex (RS422) four wire mode (point-to-point connection): select this option when there are two devices on your network. In the Receive line initial state:
  - Select none when you supply the bias and termination (Case 3).
  - Select forward bias to use internal bias and termination (Case 2).
  - Select reverse bias to use internal bias and termination, and enable cable break detection for both devices (Case 1).
- Full duplex (RS422) four wire mode (multipoint master): select this option for the master device when you have a network with one master and multiple slaves. In the Receive line initial state:
  - Select none when you supply the bias and termination (Case 3).
  - Select forward bias to use internal bias and termination (Case 2).
  - Cable break detection is not possible in this mode.
- Full duplex (RS422) four wire mode (multipoint slave): Select this option for all the slave devices when you have a network with one master and multiple slaves. In the Receive line initial state:
  - Select none when you supply the bias and termination (Case 3).
  - Select forward bias to use internal bias and termination (Case 2).
  - Select reverse bias to use internal bias and termination, and enable cable break detection for the slaves (Case 1).

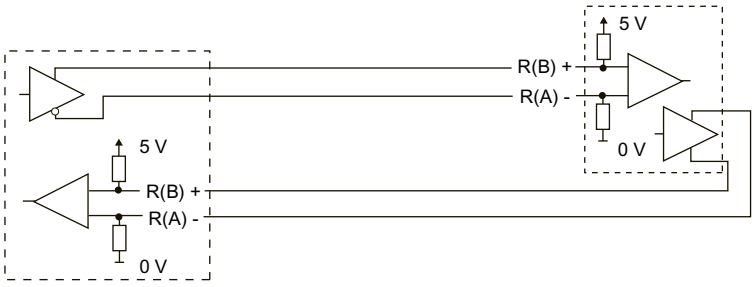
Case 1: RS422 with cable break detection

- Mode of operation: RS422
- Receive line initial state: Reverse bias (biased with R(A) > R(B) > 0V)
- Cable break: Cable break detection enabled (transmitter always active)



Case 2: RS422 No cable break detection, forward bias

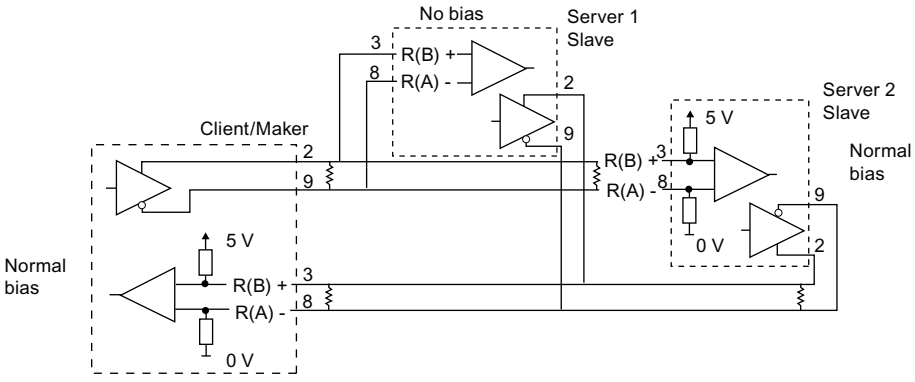
- Mode of operation: RS422
- Receive line initial state: Forward bias (biased with R(B) > R(A) > 0 V)
- Cable break: No cable break detection (transmitter enabled only while transmitting)



Case 3: RS422: No cable break detection, no bias

- Mode of operation: RS422
- Receive line initial state: no bias
- Cable break: No cable break detection (transmitter enabled only while transmitting)

Bias and termination are added by the user at the end nodes of the network.



Configuring the RS485

For RS485 mode, there is only one operating mode. The different selections for Receive line initial state reference the cases shown below for more details.

- Half duplex (RS485) two wire mode. In the Receive line initial state:
  - Select none when you supply the bias and termination (Case 5).
  - Select forward bias to use internal bias and termination (Case 4).

Case 4: RS485: Forward bias

- Mode of operation: RS485
- Receive line initial state: Forward bias (biased with R(B) > R(A) > 0 V)

Case 5: RS485: No bias (external bias)

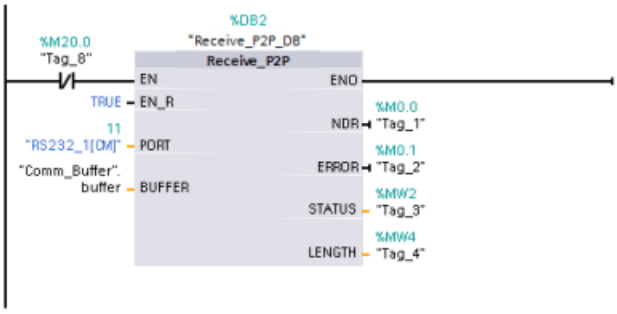
- Mode of operation: RS485
- Receive line initial state: No bias (external bias required)

14.3.7.3 Programming the STEP 7 program

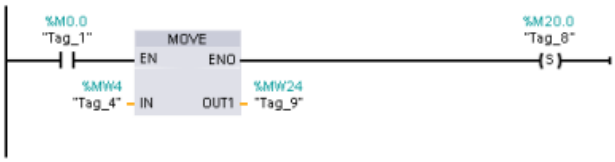
The example program uses a global data block for the communication buffer, a RCV_PTP instruction (Page 999) to receive data from the terminal emulator, and a SEND_PTP instruction (Page 997) to echo the buffer back to the terminal emulator. To program the example, add the data block configuration and Main program block OB 1 as described below.

Global data block "Comm_Buffer": Create a global data block (DB) and name it "Comm_Buffer". Create one value in the data block called "buffer" with a data type of "array [0 .. 99] of byte".

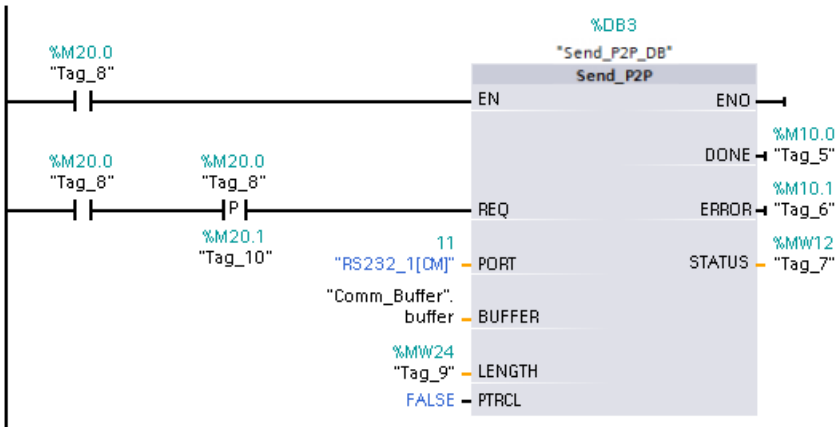
Network 1: Enable the RCV_PTP instruction whenever SEND_PTP is not active. Tag_8 at MW20.0 indicates when sending is complete in Network 4, and when the communication module is thus ready to receive a message.



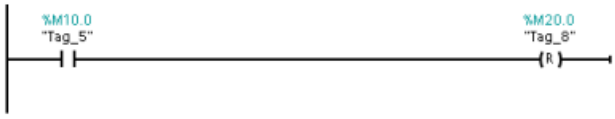
Network 2: Use the NDR value (Tag_1 at M0.0) set by the RCV_PTP instruction to make a copy of the number of bytes received and to set a flag (Tag_8 at M20.0) to trigger the SEND_PTP instruction.



Network 3: Enable the SEND_PTP instruction when the M20.0 flag is set. Also use this flag to set the REQ input to TRUE for one scan. The REQ input tells the SEND_PTP instruction that a new request is to be transmitted. The REQ input must only be set to TRUE for one execution of SEND_PTP. The SEND_PTP instruction is executed every scan until the transmit completes. The transmit is complete when the last byte of the message has been transmitted from the CM 1241. When the transmit is complete, the DONE output (Tag_5 at M10.0) is set TRUE for one execution of SEND_PTP.



Network 4: monitor the DONE output of SEND_PTP and reset the transmit flag (Tag_8 at M20.0) when the transmit operation is complete. When the transmit flag is reset, the RCV_PTP instruction in Network 1 is enabled to receive the next message.



14.3.7.4 Configuring the terminal emulator

You must set up the terminal emulator to support the example program. You can use most any terminal emulator on your PC, such as HyperTerminal. Make sure that the terminal emulator is in the disconnected mode before editing the settings as follows:

1. Set the terminal emulator to use the RS232 port on the PC (normally COM1).
2. Configure the port for 9600 baud, 8 data bits, no parity (none), 1 stop bit and no flow control.
3. Change the settings of the terminal emulator to emulate an ANSI terminal.
4. Configure the terminal emulator ASCII setup to send a line feed after every line (after the user presses the Enter key).
5. Echo the characters locally so that the terminal emulator displays what is typed.

14.3.7.5 Running the example program

To exercise the example program, follow these steps:

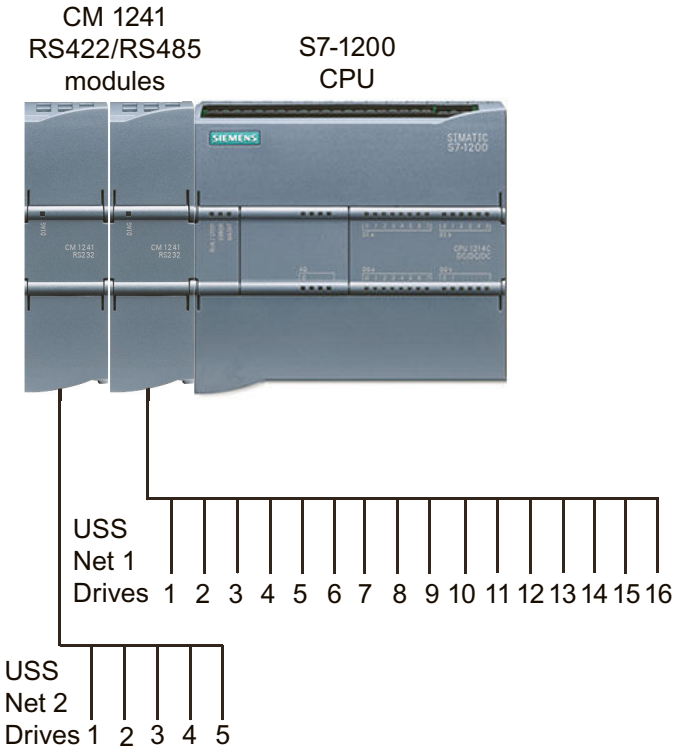
1. Download the STEP 7 program to the CPU and ensure that it is in RUN mode.
2. Click the "connect" button on the terminal emulator to apply the configuration changes and open a terminal session to the CM 1241.
3. Type characters at the PC and press Enter.

The terminal emulator sends the characters to the CM 1241 and to the CPU. The CPU program then echoes the characters back to the terminal emulator.

14.4 Universal serial interface (USS) communication

The USS instructions control the operation of motor drives which support the universal serial interface (USS) protocol. You can use the USS instructions to communicate with multiple drives through RS485 connections to CM 1241 RS485 communication modules or a CB 1241 RS485 communication board. Up to three CM 1241 RS422/RS485 modules and one CB 1241 RS485 board can be installed in a S7-1200 CPU. Each RS485 port can operate up to sixteen drives.

The USS protocol uses a master-slave network for communications over a serial bus. The master uses an address parameter to send a message to a selected slave. A slave itself can never transmit without first receiving a request to do so. Direct message transfer between the individual slaves is not possible. USS communication operates in half-duplex mode. The following USS illustration shows a network diagram for an example drive application.



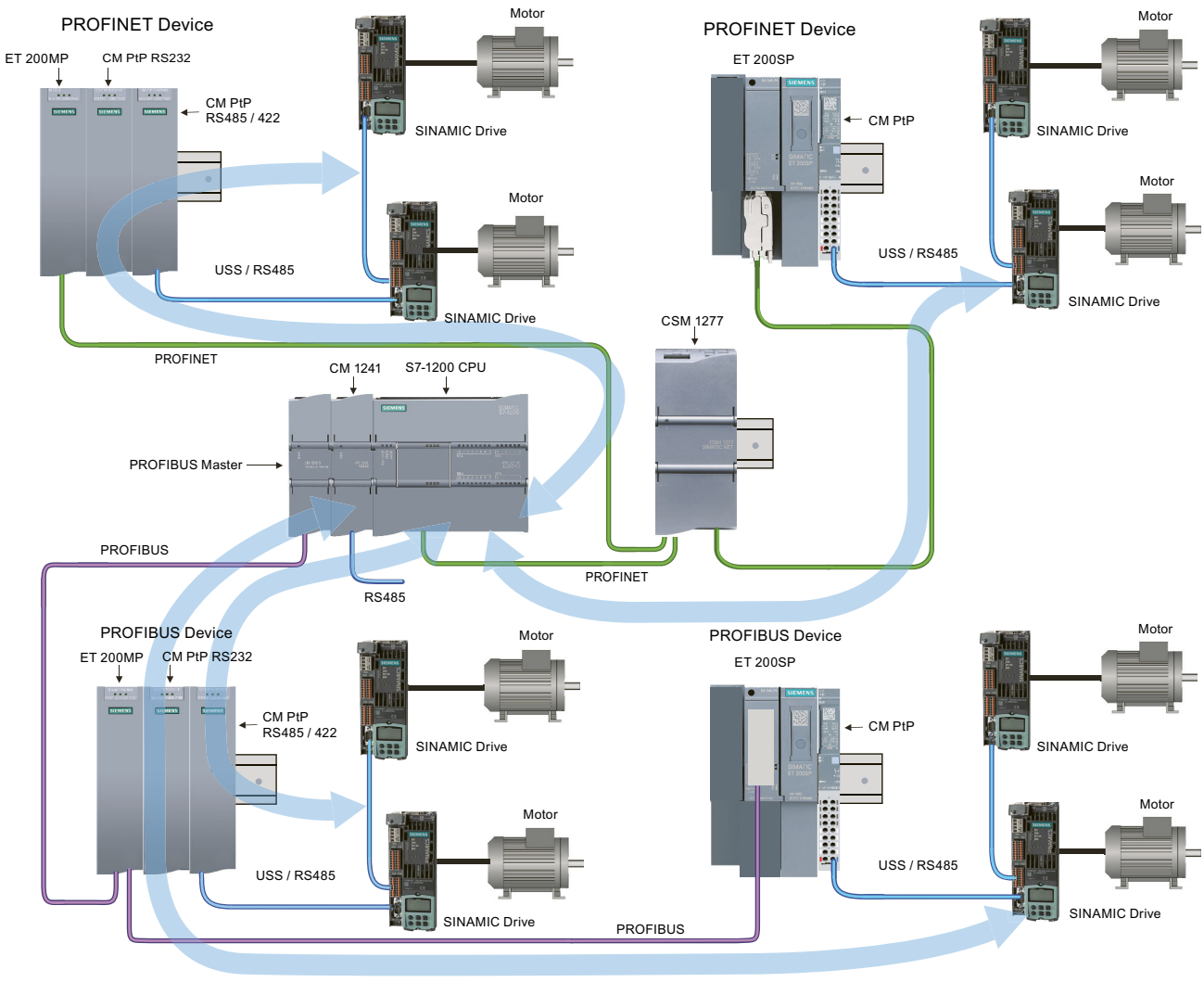
USS communications through PROFIBUS or PROFINET

USS communication enables you to use a PROFINET or PROFIBUS distributed I/O rack to communicate to various devices (RFID readers, GPS device, and others):

- PROFINET (Page 530): You connect the Ethernet interface of the S7-1200 CPU to a PROFINET interface module. PtP communication modules in the rack with the interface module can then provide serial communications to USS drives.
- PROFIBUS (Page 691): You insert a PROFIBUS communication module in the left side of the rack with the S7-1200 CPU. You connect the PROFIBUS communication module to a rack containing a PROFIBUS interface module. PtP communication modules in the rack with the interface module can then provide serial communications to USS drives.

The S7-1200 supports two sets of USS instructions:

- USS instructions (Page 892): These USS instructions provide all of the functionality of the legacy instructions, plus the ability to connect to PROFINET and PROFIBUS distributed I/O. These USS instructions allow you to configure the communications between the PtP communication modules in the distributed I/O rack and the USS drives. S7-1200 CM 1241 modules must have a minimum firmware version of V2.1 to use these USS instructions.
- Legacy USS instructions (Page 1005): These USS instructions existed prior to version V4.0 of the S7-1200 and only work with serial communications using a CM 1241 communication module or CB 1241 communication board.



The blue arrows indicate the flow of bidirectional communication between devices.

Note that STEP 7 provides different versions of the USS instructions. For information on instruction versions, refer to Use Instruction versions (https://support.industry.siemens.com/cs/ww/en/view/109798671/113722878475) in the STEP 7 Information System.

Requirements for using the USS protocol

The four USS instructions use two FBs and two FCs to support the USS protocol. For each USS network, one instance data block (DB) is used for USS_Port_Scan and one instance data block for all calls of USS_Drive_Control. For further requirements, refer to the topic "Requirements for using the USS protocol (https://support.industry.siemens.com/cs/ww/en/view/109798671/140076559243)" in the STEP 7 Information System.

14.4.1 USS instructions

14.4.1.1 USS_Port_Scan (Edit communication using USS network)

Table 14-41 USS_Port_Scan instruction

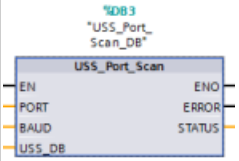
LAD / FBD	SCL	Description
	**USS_Port_Scan(PORT:=_uint_in_, BAUD:=_dint_in_, ERROR=>_bool_out_, STATUS=>_word_out_, USS_DB:=_fbtref_inout_);**	The USS_Port_Scan instruction handles communication over a USS network.

Table 14-42 Data types for the parameters

Parameter and type		Data type	Description
PORT	IN	Port	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table.
BAUD	IN	DInt	The baud rate used for USS communication.
USS_DB	INOUT	USS_BASE	The name of the instance DB that is created and initialized when a USS_Drive_Control instruction is placed in your program.
ERROR	OUT	Bool	When true, this output indicates that an error has occurred and the STATUS output is valid.
STATUS	OUT	Word	The status value of the request indicates the result of the scan or initialization. Additional information is available in the "USS_Extended_Error" variable for some status codes.

Typically, there is only one USS_Port_Scan instruction per PtP communication port in the program, and each call of this Function Block (FB) handles a transmission to or from a single drive. All USS functions associated with one USS network and PtP communication port must use the same instance DB.

Your program must execute the USS_Port_Scan instruction often enough to prevent drive timeouts. USS_Port_Scan is usually called from a cyclic interrupt OB to prevent drive timeouts and keep the most recent USS data updates available for USS_Drive_Control calls.

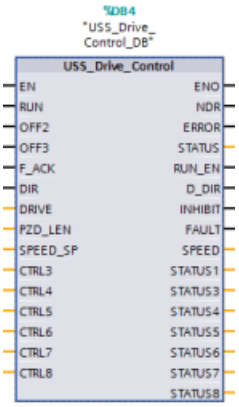
NOTE

When using the USS protocol library and the USS_Port_Scan instruction with a CB 1241, you must set the LINE_PRE data block tag to a value of 0 (No initial state). The default value of 2 for the LINE_PRE data block tag results in an error value of 16#81AB being returned by the USS_Port_Scan instruction. The LINE_PRE data block tag is found in the data block associated with the USS_Port_Scan instruction (usually named USS_Port_Scan_DB).

Ensure the start value of LINE_PRE is changed to a 0 (zero).

14.4.1.2 USS_Drive_Control (Swap data with drive)

Table 14-43 USS_Drive_Control instruction

LAD / FBD	SCL	Description
	**"USS_Drive_Control_DB"(RUN:=_bool_in_, OFF2:=_bool_in_, OFF3:=_bool_in_, F_ACK:=_bool_in_, DIR:=_bool_in_, DRIVE:=_usint_in_, PZD_LEN:=_usint_in_, SPEED_SP:=_real_in_, CTRL3:=_word_in_, CTRL4:=_word_in_, CTRL5:=_word_in_, CTRL6:=_word_in_, CTRL7:=_word_in_, CTRL8:=_word_in_, NDR=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, RUN_EN=>_bool_out_, D_DIR=>_bool_out_, INHIBIT=>_bool_out_, FAULT=>_bool_out_, SPEED=>_real_out_, STATUS1=>_word_out_, STATUS3=>_word_out_, STATUS4=>_word_out_, STATUS5=>_word_out_, STATUS6=>_word_out_, STATUS7=>_word_out_, STATUS8=>_word_out_);**	The USS_Drive_Control instruction exchanges data with a drive by creating request messages and interpreting the drive response messages. A separate function block should be used for each drive, but all USS functions associated with one USS network and PtP communication port must use the same instance data block. You must create the DB name when you place the first USS_Drive_Control instruction and then reference the DB that was created by the initial instruction usage. STEP 7 automatically creates the DB when you insert the instruction.

[1] LAD and FBD: Expand the box to reveal all the parameters by clicking the bottom of the box. The parameter pins that are grayed are optional and parameter assignment is not required.

Table 14-44 Data types for the parameters

Parameter and type		Data type	Description
RUN	IN	Bool	Drive start bit: When true, this input enables the drive to run at the preset speed. When RUN goes to false while a drive is running, the motor will be ramped down to a stop. This behavior differs from the dropping power (OFF2) or braking the motor (OFF3).
OFF2	IN	Bool	Electrical stop bit: When false, this bit causes the drive to coast to a stop with no braking.
OFF3	IN	Bool	Fast stop bit: When false, this bit causes a fast stop by braking the drive rather than just allowing the drive to coast to a stop.
F_ACK	IN	Bool	Fault acknowledge bit: This bit is set to reset the fault bit on a drive. The bit is set after the fault is cleared to indicate to the drive it no longer needs to indicate the previous fault.
DIR	IN	Bool	Drive direction control: This bit is set to indicate that the direction is forward (for positive SPEED_SP).
DRIVE	IN	USInt	Drive address: This input is the address of the USS drive. The valid range is drive 1 to drive 16.

Parameter and type		Data type	Description
PZD_LEN	IN	USInt	Word length: This is the number of words of PZD data. The valid values are 2, 4, 6, or 8 words. The default value is 2.
SPEED_SP	IN	Real	Speed set point: This is the speed of the drive as a percentage of configured frequency. A positive value specifies forward direction (when DIR is true). Valid range is 200.00 to -200.00.
CTRL3	IN	Word	Control word 3: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
CTRL4	IN	Word	Control word 4: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
CTRL5	IN	Word	Control word 5: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
CTRL6	IN	Word	Control word 6: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
CTRL7	IN	Word	Control word 7: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
CTRL8	IN	Word	Control word 8: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
NDR	OUT	Bool	New data ready: When true, the bit indicates that the outputs contain data from a new communication request.
ERROR	OUT	Bool	Error occurred: When true, this indicates that an error has occurred and the STATUS output is valid. All other outputs are set to zero on an error. Communication errors are only reported on the USS_Port_Scan instruction ERROR and STATUS outputs.
STATUS	OUT	Word	The status value of the request indicates the result of the scan. This is not a status word returned from the drive.
RUN_EN	OUT	Bool	Run enabled: This bit indicates whether the drive is running.
D_DIR	OUT	Bool	Drive direction: This bit indicates whether the drive is running forward.
INHIBIT	OUT	Bool	Drive inhibited: This bit indicates the state of the inhibit bit on the drive.
FAULT	OUT	Bool	Drive fault: This bit indicates that the drive has registered a fault. You must fix the problem and then set the F_ACK bit to clear this bit when set.
SPEED	OUT	Real	Drive Current Speed (scaled value of drive status word 2): The value of the speed of the drive as a percentage of configured speed.
STATUS1	OUT	Word	Drive Status Word 1: This value contains fixed status bits of a drive.
STATUS3	OUT	Word	Drive Status Word 3: This value contains a user-configurable status word on the drive.
STATUS4	OUT	Word	Drive Status Word 4: This value contains a user-configurable status word on the drive.
STATUS5	OUT	Word	Drive Status Word 5: This value contains a user-configurable status word on the drive.
STATUS6	OUT	Word	Drive Status Word 6: This value contains a user-configurable status word on the drive.
STATUS7	OUT	Word	Drive Status Word 7: This value contains a user-configurable status word on the drive.
STATUS8	OUT	Word	Drive Status Word 8: This value contains a user-configurable status word on the drive.

When the initial USS_Drive_Control execution occurs, the drive indicated by the USS address (parameter DRIVE) is initialized in the Instance DB. After this initialization, subsequent executions of USS_Port_Scan can begin communication to the drive at this drive number.

Changing the drive number requires a CPU STOP-to-RUN mode transition that initializes the instance DB. Input parameters are configured into the USS TX message buffer and outputs are read from a "previous" valid response buffer if any exists. There is no data transmission during USS_Drive_Control execution. Drives communicate when USS_Port_Scan is executed. USS_Drive_Control only configures the messages to be sent and interprets data that might have been received from a previous request.

You can control the drive direction of rotation using either the DIR input (Bool) or using the sign (positive or negative) with the SPEED_SP input (Real). The following table indicates how these inputs work together to determine the drive direction, assuming the motor is wired for forward rotation.

Table 14-45 Interaction of the SPEED_SP and DIR parameters

SPEED_SP	DIR	Drive rotation direction
Value > 0	0	Reverse
Value > 0	1	Forward
Value < 0	0	Forward
Value < 0	1	Reverse

14.4.1.3 USS_Read_Param (Readout parameters from the drive)

Table 14-46 USS_Read_Param instruction

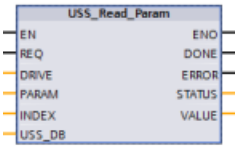
LAD / FBD	SCL	Description
	**USS_Read_Param(REQ:=_bool_in_, DRIVE:=_usint_in_, PARAM:=_uint_in_, INDEX:=_uint_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, VALUE=>_variant_out_, USS_DB:=_fbtref_inout_);**	The USS_Read_Param instruction reads a parameter from a drive. All USS functions associated with one USS network and PtP communication port must use the same data block. USS_Read_Param must be called from a main program cycle OB.

Table 14-47 Data types for the parameters

Parameter type		Data type	Description
REQ	IN	Bool	Send request: When true, REQ indicates that a new read request is desired. This is ignored if the request for this parameter is already pending.
DRIVE	IN	USInt	Drive address: DRIVE is the address of the USS drive. The valid range is drive 1 to drive 16.
PARAM	IN	UInt	Parameter number: PARAM designates which drive parameter is written. The range of this parameter is 0 to 2047. On some drives, the most significant byte can access PARAM values greater than 2047. See your drive manual for details on how to access an extended range.
INDEX	IN	UInt	Parameter index: INDEX designates which Drive Parameter index is to be written. A 16-bit value where the Least Significant Byte is the actual index value with a range of (0 to 255). The Most Significant Byte may also be used by the drive and is drive-specific. See your drive manual for details.
USS_DB	INOUT	USS_BASE	The name of the instance DB that is created and initialized when a USS_Drive_Control instruction is placed in your program.
VALUE	IN	Word, Int, UInt, DWord, DInt, UDInt, Real	This is the value of the parameter that was read and is valid only when the DONE bit is true.
DONE[1]	OUT	Bool	When true, indicates that the VALUE output holds the previously requested read parameter value. This bit is set when USS_Drive_Control sees the read response data from the drive. This bit is reset when either: you request the response data using another USS_Read_Param poll, or on the second of the next two calls to USS_Drive_Control.
ERROR	OUT	Bool	Error occurred: When true, ERROR indicates that an error has occurred and the STATUS output is valid. All other outputs are set to zero on an error. Communication errors are only reported on the USS_Port_Scan instruction ERROR and STATUS outputs.
STATUS	OUT	Word	STATUS indicates the result of the read request. Additional information is available in the "USS_Extended_Error" variable for some status codes.

[1] The DONE bit indicates that valid data has been read from the referenced motor drive and delivered to the CPU. It does not indicate that the USS library is capable of immediately reading another parameter. A blank PKW request must be sent to the motor drive and must also be acknowledged by the instruction before the parameter channel for the specific drive becomes available for use. Immediately calling a USS_Read_Param or USS_Write_Param FC for the specified motor drive will result in a "0x818A" error.

14.4.1.4 USS_Write_Param (Change parameters in the drive)

NOTE

EEPROM write operations (for the EEPROM inside a USS drive)

Do not overuse the EEPROM permanent write operation. Minimize the number of EEPROM write operations to extend the EEPROM life.

Table 14-48 USS_Write_Param instruction

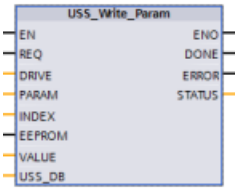
LAD / FBD	SCL	Description
	**USS_Write_Param(REQ:=_bool_in_, DRIVE:=_usint_in_, PARAM:=_uint_in_, INDEX:=_uint_in_, EEPROM:=_bool_in_, VALUE:=_variant_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, USS_DB:=_fbtref_inout_);**	The USS_Write_Param instruction modifies a parameter in the drive. All USS functions associated with one USS network and PtP communication port must use the same data block. USS_Write_Param must be called from a main program cycle OB.

Table 14-49 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Send request: When true, REQ indicates that a new write request is desired. This is ignored if the request for this parameter is already pending.
DRIVE	IN	USInt	Drive address: DRIVE is the address of the USS drive. The valid range is drive 1 to drive 16.
PARAM	IN	UInt	Parameter number: PARAM designates which drive parameter is written. The range of this parameter is 0 to 2047. On some drives, the most significant byte can access PARAM values greater than 2047. See your drive manual for details on how to access an extended range.
INDEX	IN	UInt	Parameter index: INDEX designates which Drive Parameter index is to be written. A 16-bit value where the least significant byte is the actual index value with a range of (0 to 255). The most significant byte may also be used by the drive and is drive-specific. See your drive manual for details.
EEPROM	IN	Bool	Store To Drive EEPROM: When true, a write drive parameter transaction will be stored in the drive EEPROM. If false, the write is temporary and will not be retained if the drive is power cycled.
VALUE	IN	Word, Int, UInt, DWord, DInt, UDInt, Real	The value of the parameter that is to be written. It must be valid on the transition of REQ.
USS_DB	INOUT	USS_BASE	The name of the instance DB that is created and initialized when a USS_Drive_Control instruction is placed in your program.
DONE[1]	OUT	Bool	When true, DONE indicates that the input VALUE has been written to the drive. This bit is set when USS_Drive_Control sees the write response data from the drive. This bit is reset when either you request the response data using another USS_Drive_Control poll, or on the second of the next two calls to USS_Drive_Control.
ERROR	OUT	Bool	When true, ERROR indicates that an error has occurred and the STATUS output is valid. All other outputs are set to zero on an error. Communication errors are only reported on the USS_Port_Scan instruction ERROR and STATUS outputs.
STATUS	OUT	Word	STATUS indicates the result of the write request. Additional information is available in the "USS_Extended_Error" variable for some status codes.

[1] The DONE bit indicates that valid data has been read from the referenced motor drive and delivered to the CPU. It does not indicate that the USS library is capable of immediately reading another parameter. A blank PKW request must be sent to the motor drive and must also be acknowledged by the instruction before the parameter channel for the specific drive becomes available for use. Immediately calling a USS_Read_Param or USS_Write_Param FC for the specified motor drive will result in a "0x818A" error.

14.4.2 USS status codes

USS instruction status codes are returned at the STATUS output of the USS functions.

Table 14-50 STATUS codes [1]

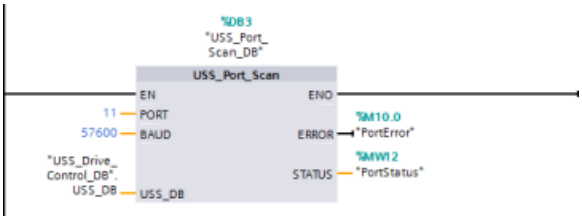
STATUS (W#16#....)	Description
0000	No error
8180	The length of the drive response did not match the characters received from the drive. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
8181	VALUE parameter was not a Word, Real or DWord data type.
8182	The user supplied a Word for a parameter value and received a DWord or Real from the drive in the response.
8183	The user supplied a DWord or Real for a parameter value and received a Word from the drive in the response.
8184	The response telegram from drive had a bad checksum. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
8185	Illegal drive address (valid drive address range: 1 to16)
8186	The speed set point is out of the valid range (valid speed SP range: -200% to 200%).
8187	The wrong drive number responded to the request sent. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
8188	Illegal PZD word length specified (valid range = 2, 4, 6 or 8 words)
8189	Illegal Baud Rate was specified.
818A	The parameter request channel is in use by another request for this drive.
818B	The drive has not responded to requests and retries. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
818C	The drive returned an extended error on a parameter request operation. See the extended error description below this table.
818D	The drive returned an illegal access error on a parameter request operation. See your drive manual for information of why parameter access may be limited.
818E	The drive has not been initialized. This error code is returned to USS_Read_Param or USS_Write_Param when USS_Drive_Control, for that drive, has not been called at least once. This keeps the initialization on first scan of USS_Drive_Control from overwriting a pending parameter read or write request, since it initializes the drive as a new entry. To fix this error, call USS_Drive_Control for this drive number.
80Ax-80Fx	Specific errors returned from PtP communication FBs called by the USS Library - These error code values are not modified by the USS library and are defined in the PtP instruction descriptions.

[1] In addition to the USS instruction errors listed above, errors can be returned from the underlying PtP communication instructions (Page 857).

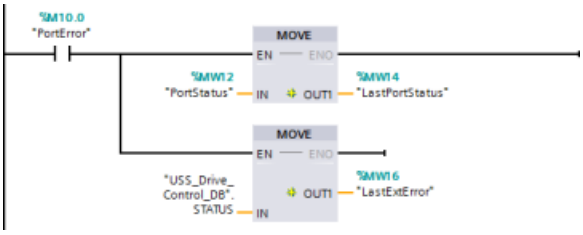
For several STATUS codes, additional information is provided in the "USS_Extended_Error" variable of the USS_Drive_Control Instance DB. For STATUS codes hexadecimal 8180, 8184, 8187, and 818B, USS_Extended_Error contains the drive number where the communication error occurred. For STATUS code hexadecimal 818C, USS_Extended_Error contains a drive error code returned from the drive when using a USS_Read_Param or USS_Write_Param instruction.

Example: Communication errors reporting

Communication errors (STATUS = 16#818B) are only reported on the USS_Port_Scan instruction and not on the USS_Drive_Control instruction. For example, if the network is not properly terminated, then it is possible for a drive to go to RUN but the USS_Drive_Control instruction will show all "0's' for the output parameters. In this case, you can only detect the communication error on the USS_Port_Scan instruction. Since this error is only visible for one scan, you will need to add some capture logic as illustrated in the following example. In this example, when the error bit of the USS_Port_Scan instruction is TRUE, then the STATUS and the USS_Extended_Error values are saved into M memory. The drive number is placed in the USS_Extended_Error variable when the STATUS code value is hexadecimal 8180, 8184, 8187, or 818B.



Network 1: "PortStatus"port status and"USS_Drive_Control_DB".USS_Extended_Error
extended error code values are only valid for
one program scan. The values must be
captured for later processing.



Network 2: The "PortError" contact triggers the storage of the "PortStatus" value in "LastPortStatus" and
the"USS_Drive_Control_DB".USS_Extended_Error
value in "LastExtError".

Read and write access to a drive's internal parameters

USS drives support read and write access to a drive's internal parameters. This feature allows remote control and configuration of the drive. Drive parameter access operations can fail due to errors such as values out of range or illegal requests for a drive's current mode. The drive generates an error code value that is returned in the "USS_Extended_Error" variable. This error code value is only valid for the last execution of a USS_Read_Param or USS_Write_Param instruction. The drive error code is put into USS_Extended_Error variable when the STATUS code value is hexadecimal 818C. The error code value of USS_Extended_Error depends on the drive model. See the drive's manual for a description of the extended error codes for read and write parameter operations.

14.4.3 USS general drive setup requirements

USS general drive setup requirements consist of the following points:

- The drives must be set to use 4 PKW words.
- The drives can be configured for 2, 4, 6, or 8 PZD words.
- The number of PZD word's in the drive must match PZD_LEN input on the USS_Drive_Control instruction for that drive.
- The baud rate in all the drives must match the BAUD input on the USS_Port_Scan instruction.

- The drive must be set for remote control.
- The drive must be set for frequency set-point to USS on COM Link.
- The drive address must be set to 1 to 16 and match the DRIVE input on the USS_Drive_Control block for that drive.
- The drive direction control must be set to use the polarity of the drive set-point.
- The RS485 network must be terminated properly.

14.4.4 Example: USS general drive connection and setup

Connecting a MicroMaster drive

This information about SIEMENS MicroMaster drives is provided as an example. For other drives, refer to the drive's manual for setup instructions.

To make the connection to a MicroMaster Series 4 (MM4) drive, insert the ends of the RS485 cable into the two caged-clamp, screw-less terminals provided for USS operation. Standard PROFIBUS cable and connectors can be used to connect the S7-1200.

CAUTION

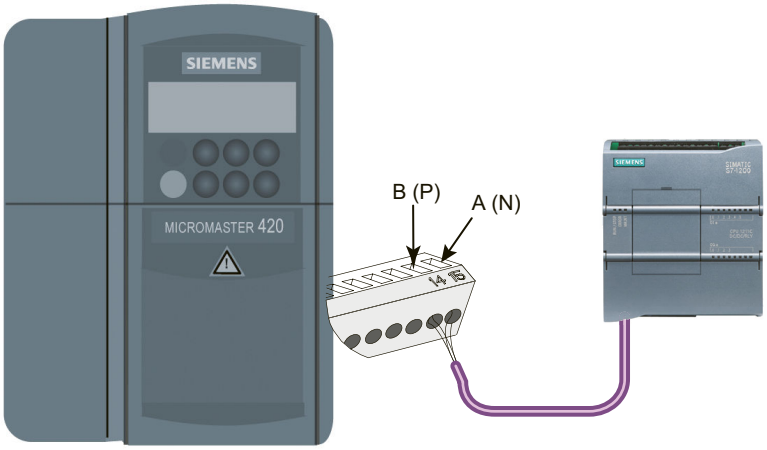
Risks when interconnecting equipment with different reference potentials

Interconnecting equipment with different reference potentials can cause unwanted currents to flow through the interconnecting cable. These unwanted currents can cause communications errors or damage equipment.

Be sure all equipment that you connect with a communications cable either shares a common circuit reference or is isolated to prevent unwanted current flows. The shield must be tied to the chassis ground or to pin 1 on the 9-pin connector. Tie the wiring terminal 2-0 V on the MicroMaster drive to the chassis ground.

Communications errors or damaged equipment can cause injury.

The two wires at the opposite end of the RS485 cable must be inserted into the MM4 drive terminal blocks. To make the cable connection on a MM4 drive, remove the drive cover(s) to access the terminal blocks. See the MM4 user manual for details about how to remove the covers(s) of your specific drive.



The terminal block connections are labeled numerically. Using a PROFIBUS connector on the S7-1200 side, connect the A terminal of the cable to the drive terminal 15 (for an MM420) or terminal 30 (MM440). Connect the B terminal of B (P) A (N) the cable connector to terminal 14 (MM420) or terminal 29 (MM440).

If the S7-1200 is a terminating node in the network, or if the connection is point-to-point, it is necessary to use terminals A1 and B1 (not A2 and B2) of the connector since they allow the termination settings to be set (for example, with DP connector type 6ES7972-0BA40-0X40).

⚠ WARNING

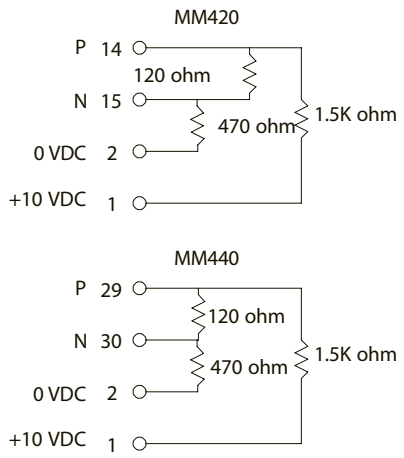
Risk of electric shock or electrocution

Some drives have high voltages. Failure to replace drive covers properly can result in electric shock or electrocution.

Make sure the drive covers are replaced properly before supplying power to the unit.

Electric shock or electrocution can result in severe personal injury or death.

If the drive is configured as the terminating node in the network, then termination and bias resistors must also be wired to the appropriate terminal connections. This diagram shows examples of the MM4 drive connections necessary for termination and bias.



Setting up the MM4 drive

Before you connect a drive to the S7-1200, you must ensure that the drive has the following system parameters. Use the keypad on the drive to set the parameters:

1. Reset the drive to factory settings (optional).	P0010=30 P0970=1
If you skip step 1, then ensure that these parameters are set to the indicated values.	USS PZD length = P2012 Index 0=(2, 4, 6, or 8) USS PKW length = P2013 Index 0=4
2. Enable the read/write access to all parameters (Expert mode).	P0003=3
3. Check the motor settings for your drive. The settings will vary according to the motor(s) being used. To set the parameters P304, P305, P307, P310, and P311, you must first set parameter P010 to 1 (quick commissioning mode). When you are finished setting the parameters, set parameter P010 to 0. Parameters P304, P305, P307, P310, and P311 can only be changed in the quick commissioning mode.	P0304 = Rated motor voltage (V) P0305 = Rated motor current (A) P0307 = Rated motor power (W) P0310 = Rated motor frequency (Hz) P0311 = Rated motor speed

4. Set the local/remote control mode.	P0700 Index 0=5
5. Set selection of frequency set-point to USS on COM link.	P1000 Index 0=5
6. Ramp up time (optional) This is the time in seconds that it takes the motor to accelerate to maximum frequency.	P1120=(0 to 650.00)
7. Ramp down time (optional) This the time in seconds that it takes the motor to decelerate to a complete stop.	P1121=(0 to 650.00)
8. Set the serial link reference frequency:	P2000=(1 to 650 Hz)
9. Set the USS normalization:	P2009 Index 0=0
10. Set the baud rate of the RS485 serial interface:	P2010 Index 0= 4 (2400 baud) 5 (4800 baud) 6 (9600 baud) 7 (19200 baud 8 (38400 baud) 9 (57600 baud) 12 (115200 baud)
11. Enter the Slave address. Each drive (a maximum of 31) can be operated over the bus.	P2011 Index 0=(0 to 31)
12. Set the serial link timeout. This is the maximum permissible period between two incoming data telegrams. This feature is used to turn off the inverter in the event of a communications failure. Timing starts after a valid data telegram has been received. If a further data telegram is not received within the specified time period, the inverter will trip and display fault code F0070. Setting the value to zero switches off the control.	P2014 Index 0=(0 to 65,535 ms) 0=timeout disabled
13. Transfer the data from RAM to EEPROM:	P0971=1 (Start transfer) Save the changes to the parameter settings to EEPROM

14.5 Modbus communication

14.5.1 Overview of Modbus TCP and Modbus RTU communication

Modbus function codes

- A CPU operating as a Modbus TCP client or Modbus RTU master can read/write both data and I/O states in a remote Modbus TCP server or Modbus RTU slave. Remote data can be read and then processed in your program logic.
- A CPU operating as a Modbus TCP server or Modbus RTU slave allows a supervisory device to read/write both data and I/O states in CPU memory. A Modbus TCP client or Modbus RTU master can write new values into slave/server CPU memory that is available to your program logic.

WARNING

Avoiding security risks from physical network attacks

If an attacker can physically access your networks, the attacker can possibly read and write data.

For example, I/O exchange through PROFIBUS, PROFINET, AS-i, or other I/O bus, GET/PUT, T-Block, and communication modules (CMs) have no security features. You must protect these forms of communication by limiting physical access. If an attacker can physically access your networks using these forms of communication, the attacker can possibly read and write data.

If you fail to protect these forms of communication, death or severe personal injury can result.

For security information and recommendations, see the "Operational Guidelines" white paper on the Siemens Industrial Cybersecurity Web site (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

Table 14-51 Read data functions: Read remote I/O and program data

Modbus function code	Read slave (server) functions - standard addressing
01	Read output bits: 1 to 2000 bits per request
02	Read input bits: 1 to 2000 bits per request
03	Read Holding registers: 1 to 125 words per request
04	Read input words: 1 to 125 words per request

Table 14-52 Write data functions: Write remote I/O and modify program data

Modbus function code	Write slave (server) functions - standard addressing
05	Write one output bit: 1 bit per request
06	Write one holding register: 1 word per request
15	Write one or more output bits: 1 to 1968 bits per request
16	Write one or more holding registers: 1 to 123 words per request

- Modbus function codes 08 and 11 provide slave device communication diagnostic information.
- Modbus function code 0 broadcasts a message to all slaves (with no slave response). The broadcast function is not available for Modbus TCP, because communication is connection based.
- Modbus function code 23 can Write and Read one or more holding registers: 1 to 121/125 (Write/Read) words per request. This function code is only available for Modbus TCP.

Table 14-53 Modbus network station addresses

Station		Address
TCP station	Station address	IP address and port number
RTU station	Standard station address	1 to 247
	Extended station address	1 to 65535

Modbus memory addresses

The actual number of Modbus memory addresses available depends on the CPU model, how much work memory exists, and how much CPU memory is used by other program data. The table below gives the nominal value of the address range.

Table 14-54 Modbus memory addresses

Station		Address range
TCP station	Standard memory address	10K
RTU station	Standard memory address	10K
	Extended memory address	64K

14.5.2 Modbus TCP

14.5.2.1 Overview

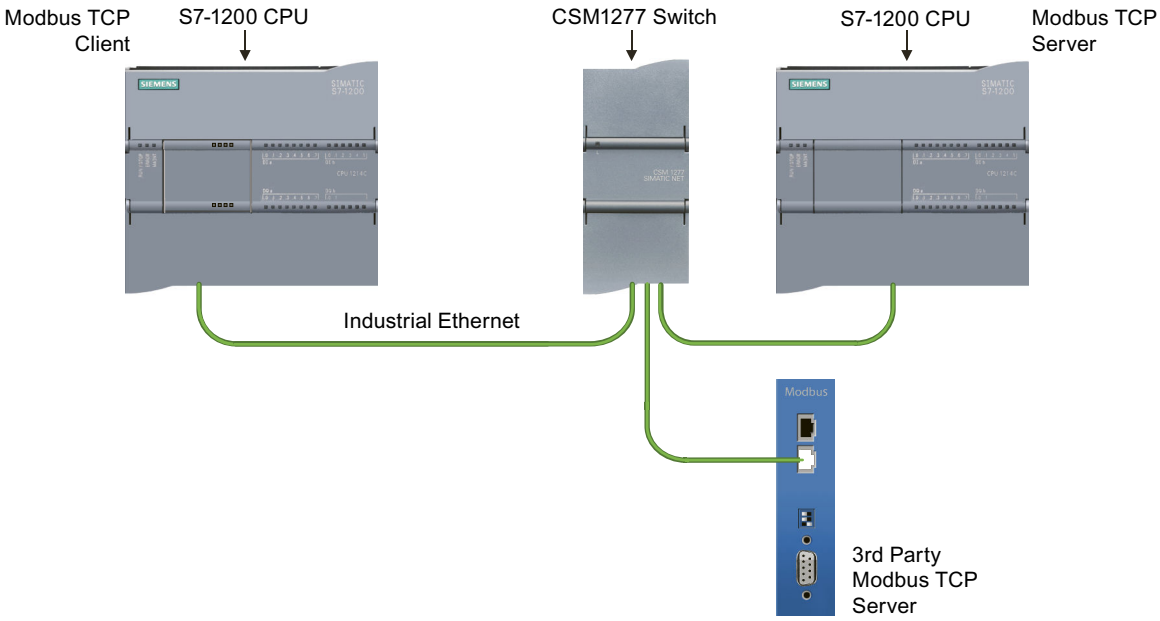
Modbus TCP (Transmission Control Protocol) is a standard network communication protocol that uses the PROFINET connector on the CPU for TCP/IP communication. No additional communication hardware module is required.

Modbus TCP uses Open User Communications (OUC) connections as a Modbus communication path. Multiple client-server connections may exist in addition to the connection between STEP 7 and the CPU. Mixed client and server connections are supported up to the maximum number of connections allowed by the CPU model (Page 526).

Each MB_SERVER connection must use a unique instance DB and IP port number. Only 1 connection per IP port is supported. Each MB_SERVER (with its unique instance DB and IP port) must be executed individually for each connection.

A Modbus TCP client (master) must control the client-server connection with the DISCONNECT parameter. The basic Modbus client actions are shown below:

1. Initiate a connection to a particular server (slave) IP address and IP port number
2. Initiate client transmission of a Modbus message and receive the server responses
3. When desired, initiate the disconnection of client and server to enable connection with a different server.



Modbus TCP instructions and versions

The Modbus TCP instructions (Page 906) provide the capability to communicate between Modbus TCP clients, Modbus TCP servers, and third-party Modbus TCP devices through a switch. Older S7-1200 programs might use Legacy Modbus TCP instructions. (Page 1013) STEP 7 provides different versions of the Modbus TCP instructions. For information on instruction versions, refer to Use Instruction versions (https://support.industry.siemens.com/cs/ww/en/view/109798671/113722878475) in the STEP 7 Information System.

14.5.2.2 Modbus TCP instructions

MB_CLIENT (Communicate using PROFINET as Modbus TCP client) instruction

Table 14-55 MB_CLIENT instruction

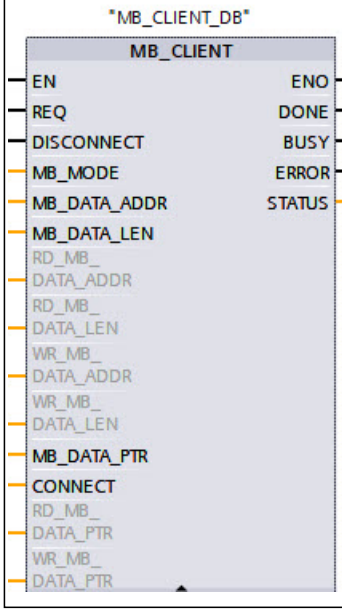
LAD / FBD	SCL	Description
	**"MB_CLIENT_DB"(REQ:=_bool_in_, DISCONNECT:=_bool_in_, MB_MODE:=_usint_in_, MB_DATA_ADDR:=_udint_in_, MB_DATA_LEN:=_uint_in_, RD_MB_DATA_ADDR:=_uint_in_, RD_MB_DATA_LEN:=_uint_in_, WR_MB_DATA_ADDR:=_uint_in_, WR_MB_DATA_LEN:=_uint_in_, DONE=>_bool_out_, BUSY=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, MB_DATA_PTR:=_variant_inout_, CONNECT:=_variant_inout_, RD_MB_DATA_PTR:=_variant_inout_, WR_MB_DATA_PTR: =_variant_inout_);**	MB_CLIENT communicates as a Modbus TCP client through the PROFINET port on the S7-1200 CPU. No additional communication hardware module is required.MB_CLIENT can make a client-server connection, send a Modbus function request, receive a response, and control the disconnection from a Modbus TCP server.

Table 14-56 Data types for the parameters

Parameter and type		Data type	Description
REQ	In	Bool	FALSE = No Modbus communication request TRUE = Request to communicate with a Modbus TCP server
DISCONNECT	IN	Bool	The DISCONNECT parameter allows your program to control connection and disconnection with a Modbus server device. If DISCONNECT = 0 and a connection does not exist, then MB_CLIENT attempts to make a connection to the assigned IP address and port number. If DISCONNECT = 1 and a connection exists, then a disconnect operation is attempted. Whenever this input is enabled, no other operation will be attempted.
MB_MODE	IN	USInt	Mode selection: Assigns the type of request (read, write, or diagnostic). See the Modbus functions table below for details.
MB_DATA_ADDR	IN	UDInt	Modbus starting Address: Assigns the starting address of the data to be accessed by MB_CLIENT. See the following Modbus functions table for valid addresses.
MB_DATA_LEN	IN	UInt	Modbus data Length: Assigns the number of bits or words to be accessed in this request. See the following Modbus functions table for valid lengths
MB_DATA_PTR	IN_OUT	Variant	Pointer to the Modbus data register: The register buffers data going to or coming from a Modbus server. The pointer must assign a non-optimized global DB or an M memory address.
CONNECT	IN_OUT	Variant	Reference to a Data block structure that contains connection parameters in the system data type "TCON_IP_v4". The following data types are also supported: TCON_IP_V4_SEC, TCON_QDN and TCON_QDN_SEC. See "Parameters for the PROFINET connection" (Page 551).

Parameter and type		Data type	Description
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error.
BUSY	OUT	Bool	• 0 - No MB_CLIENT operation in progress • 1 - MB_CLIENT operation in progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the MB_CLIENT execution ended with an error. The error code at the STATUS parameter is valid only during the single cycle where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code

Modbus function 23

Description

With the Modbus function 23, the following is carried out in a job:

1. Data is transferred from the CPU to the Modbus server and written into one or more holding registers.
2. Data is read from one or more holding registers of the Modbus server and transferred to the CPU.

The "MB_CLIENT" instruction supports the Modbus function 23 as of instruction version V6.0.

Parameters

When the Modbus function 23 is used, the MB_MODE parameter must have the value 123.

The parameters MB_DATA_ADDR, MB_DATA_LEN and MB_DATA_PTR are not used and must have their default values as values.

When Modbus function 23 is used, six new parameters are used, which are described in the table below. Each of these parameters starts with "RD_" or "WR_" to indicate that it belongs to the read or write task. The default is that these parameters are hidden. When using Modbus function 23, these six parameters must all be used. If you use another Modbus function, then these six parameters must have the value 0 or they must be empty. Otherwise, the STATUS value 16#818D is returned.

Table 14-57 Data types for the parameters

Parameter and type		Data type	Description
RD_MB_DATA_ADDR	IN	UInt	Start address on the remote device as of which data is to be read. Permitted values: 0 to 65535
RD_MB_DATA_LEN	IN	UInt	Number of registers to be read from the remote device. Permitted values: 1 to 125
WR_MB_DATA_ADDR	IN	UInt	Start address on the remote device as of which data is to be written. Permitted values: 0 to 65535
WR_MB_DATA_LEN	IN	UInt	Number of registers to be written to the remote device. Permitted values: 1 to 121
RD_MB_DATA_PTR	IN_OUT	Variant	Pointer to a data buffer for the data to be read from the Modbus server. The same data types as for MB_DATA_PTR are permitted as data types.
WR_MB_DATA_PTR	IN_OUT	Variant	Pointer to a data buffer for the data to be written to the Modbus server. The same data types as for MB_DATA_PTR are permitted as data types.

STATUS parameter

The meaning of the STATUS values 16#8383, 8189, 818A, 818B is expanded. The STATUS value 16#818D is added.

Upgrade project, upgrade instruction

When you upgrade an existing project with MB_CLIENT instructions (e.g. instruction version V5.2), the new instruction version is not automatically used in your program. To use Modbus function 23, you must upgrade the instruction version manually.

REQ parameter

FALSE = No Modbus communication request
TRUE = Request to communicate with a Modbus TCP server

If no instance of MB_CLIENT is active and parameter DISCONNECT=0, when REQ=1 a new Modbus request starts. If the connection is not already established, then a new connection is made.

If the same instance of MB_CLIENT is executed again with DISCONNECT=0 and REQ=1, before the completion of the current request, then no subsequent Modbus transmission will be made. However, as soon as the current request is completed, a new request can be processed if MB_CLIENT is executed with REQ=1.

When the current MB_CLIENT communication request is complete, the DONE bit is TRUE for one cycle. The DONE bit can be used as a time gate to sequence multiple MB_CLIENT requests.

NOTE

Input data consistency during MB_CLIENT processing

Once a Modbus client initiates a Modbus operation, all the input states are saved internally and are then compared on each successive call. The comparison is used to determine if this particular call was the originator of the active client request. More than one MB_CLIENT call can be performed using a common instance DB.

It is important that the inputs are not changed during the period of time that an MB_CLIENT operation is actively being processed. If this rule is not followed, then an MB_CLIENT cannot determine the active instance.

MB_MODE and MB_DATA_ADDR parameters select the Modbus communication function

The MB_CLIENT instruction uses an MB_MODE input rather than a function code. MB_DATA_ADDR assigns the starting Modbus address of the remote data.

The combination of MB_MODE and MB_DATA_ADDR determines the function code that is used in the actual Modbus message. The following table shows the correspondence between parameter MB_MODE, MB_DATA_ADDR, and Modbus function:

Table 14-58 Modbus functions

MB_MODE	Modbus function	Data length	Operation and data	MB_DATA_ADDR
0	01	1 to 2000	Read output bits: 1 to 2000 bits per request	1 to 9999
101	01	1 to 2000	Read output bits: 1 to 2000 bits per request	00000 to 65535
0	02	1 to 2000	Read input bits: 1 to 2000 bits per request	10001 to 19999
102	02	1 to 2000	Read input bits: 1 to 2000 bits per request	00000 to 65535
0	03	1 to 125	Read Holding registers: 1 to 125 words per request	40001 to 49999 or 400001 to 465535
103	03	1 to 125	Read Holding registers: 1 to 125 words per request	00000 to 65535
0	04	1 to 125	Read input words: 1 to 125 words per request	30001 to 39999
104	04	1 to 125	Read input words: 1 to 125 words per request	00000 to 65535
1	05	1	Write one output bit: One bit per request	1 to 9999
105	05	1	Write one output bit: One bit per request	00000 to 65535
1	06	1	Write one holding register: 1 word per request	40001 to 49999 or 400001 to 465535
106	06	1	Write one holding register: 1 word per request	00000 to 65535
1	15	2 to 1968	Write multiple output bits: 2 to 1968 bits per request	1 to 9999
1	16	2 to 123	Write multiple holding registers: 2 to 123 words per request	40001 to 49999 or 400001 to 465535
2	15	1 to 1968	Write one or more output bits: 1 to 1968 bits per request	1 to 9999
115	15	1 to 1968	Write one or more output bits: 1 to 1968 bits per request	00000 to 65535
2	16	1 to 123	Write one or more holding registers: 1 to 123 words per request	40001 to 49999 or 400001 to 465535
116	16	1 to 123	Write one or more holding registers: 1 to 123 words per request	00000 to 65535
11	11	0	Read the server communication status word and event counter. The status word indicates busy (0 = not busy, 0xFFFF = busy). The event counter is incremented for each successful completion of a message. Both the MB_DATA_ADDR and MB_DATA_LEN parameters of MB_CLIENT are ignored for this function.	

MB_MODE	Modbus function	Data length	Operation and data	MB_DATA_ADDR
80	08	1	Check server status with diagnostic code 0x0000 (Loopback test, server echoes the request) 1 word per request	
81	08	1	Reset server event counter with diagnostic code 0x000A 1 word per request	
123	23	1 to 121 (Write) 1 to 125 (Read)	Write holding registers of the remote device and read holding registers of the remote device in one job. Note: This Modbus function is supported by "MB_CLIENT" as of instruction version V6.0. The parameters RD_MB_DATA_ADDR, RD_MB_DATA_LEN, WR_MB_DATA_ADDR, WR_MB_DATA_LEN, RD_MB_DATA_PTR WR_MB_DATA_PTR are used for this purpose.	
3 to 10,12 to 79,82 to 100,107 to 114,117 to 255			Reserved	

NOTE

MB_DATA_PTR assigns a buffer to store data read/written to/from a Modbus TCP server

The data buffer can be located in a non-optimized global DB or M memory address.

For a buffer in M memory, use the Any Pointer format. This is in the format P#"Bit Address" "Data Type" "Length", an example would be P#M1000.0 WORD 500.

MB_DATA_PTR parameter assigns a communication buffer

- MB_CLIENT communication functions:
  - Read and write 1-bit data from Modbus server addresses (00001 to 09999)
  - Read 1-bit data from Modbus server addresses (10001 to 19999)
  - Read 16-bit word data from Modbus server addresses (30001 to 39999) and (40001 to 49999)
  - Write 16-bit word data to Modbus server addresses (40001 to 49999)
- Word or bit sized data is transferred to/from the DB or M memory buffer assigned by MB_DATA_PTR.
- If a DB is assigned as the buffer by MB_DATA_PTR, then you must assign data types to all DB data elements.
  - The 1-bit Bool data type represents one Modbus bit address
  - 16-bit single word data types like WORD, UInt, and Int represent one Modbus word address
  - 32-bit double word data types like DWORD, DInt, and Real represent two Modbus word addresses

- Complex DB elements can be assigned by MB_DATA_PTR, such as
  - Arrays
  - Named structures where each element is unique.
  - Named complex structures where each element has a unique name and a 16 or 32 bit data type.
- No requirement that the MB_DATA_PTR data areas be in the same global data block (or M memory area). You can assign one data block for Modbus reads, another data block for Modbus writes, or one data block for each MB_CLIENT.

CONNECT parameter assigns data used to establish a PROFINET connection

You must use a global data block and store the required connection data before you can reference this DB at the CONNECT parameter.

1. Create a new global DB or use an existing global DB to store the CONNECT data. You can use one DB to store multiple TCON_IP_v4 data structures. Each Modbus TCP client or server connection uses a TCON_IP_v4 data structure. You reference the connection data at the CONNECT parameter.
2. Name the DB and a static variable with a helpful name. For example, name the data block "Modbus connections" and a static variable "TCPactive_1" (for Modbus TCP client connection 1).
3. In the DB editor, assign the system data type "TCON_IP_v4" in the Data Type column, for the example static variable "TCPactive_1".
4. Expand the TCON_IP_v4 structure so you can modify the connection parameters, as shown in the following image.
5. Modify data in the TCON_IP_v4 structure for an MB_CLIENT connection.
6. Enter the DB structure reference for the CONNECT parameter of MB_CLIENT. For the example, this would be "Modbus connections".TCPactive_1.

Modbus connections

	Name	Data type	Start value	Comment
1	Static			
2	TCPactive_1	TCON_IP_v4		
3	InterfaceId	HW_ANY	64	HW-identifier of IE-interface submodule
4	ID	CONN_OUC	1	connection reference / identifier
5	ConnectionType	Byte	16#0B	type of connetion: 11=TCP/IP, 19=UDP (17=TC...
6	ActiveEstablished	Bool	True	active/passive connection establishment
7	RemoteAddress	IP_V4		remote IP address (IPv4)
8	ADDR	array [1..4] of Byte		IPv4 address
9	ADDR[1]	Byte	192	
10	ADDR[2]	Byte	168	
11	ADDR[3]	Byte	2	
12	ADDR[4]	Byte	241	
13	RemotePort	UInt	502	remote UDP/TCP port number
14	LocalPort	UInt	0	local UDP/TCP port number

Modify TCON_IP_V4 DB data for each MB_CLIENT connection

- **InterfaceID**: Using the Device configuration window, click on the CPU PROFINET port image. Then click on the General properties tab and use the Hardware identifier that you see there.
- **ID**: Enter a connection ID number between 1 and 4095. Modbus TCP communication is made using underlying TCON, TDISCON, TSEND, and TRCV instructions, for OUC (Open User Communication).
- **ConnectionType**: For TCP/IP, use the default 16#0B (decimal number = 11).

- **ActiveEstablished**: This value must be 1 or TRUE. The connection is active in that MB_CLIENT initiates Modbus communication.
- **RemoteAddress**: Enter the IP address of the target Modbus TCP server into the four ADDR array elements. For example, enter 192.168.2.241, as in the previous image.
- **RemotePort**: The default is 502. This number is the IP port number of the Modbus server that MB_CLIENT attempts to connect and communicate with. Some third-party Modbus servers require that you use another port number.
- **LocalPort**: This value must be 0, for an MB_CLIENT connection.

Multiple client connections

A Modbus TCP client can support concurrent connections up to the maximum number of Open User Communications connections allowed by the PLC. The total number of connections for a PLC, including Modbus TCP Clients and Servers, must not exceed the maximum number of supported Open User Communications connections (Page 526).

Individual concurrent client connections must follow these rules:

- Each MB_CLIENT connection must use a unique instance DB
- Each MB_CLIENT connection must assign a unique server IP address
- Each MB_CLIENT connection must assign a unique connection ID
- Unique IP port numbers may or may not be required depending upon the server configuration

A different connection ID must be used with each instance DB. In summary, the instance DB and the connection ID are paired together and must be unique for each connection.

Table 14-59 MB_CLIENT instance data block: User accessible static variables

Variable	Data type	Default	description
Blocked_Proc_Timeout	Real	3.0	Amount of time (in seconds) to wait upon a blocked Modbus client instance before removing this instance as being ACTIVE. This can occur, for example, when a client request has been issued and then application stops executing the client function before completely finishing the request. The maximum S7-1200 limit is 55 seconds.
MB_Unit_ID	Word	255	Modbus unit identifier: A Modbus TCP server is addressed using its IP address. As a result, the MB_UNIT_ID parameter is not used for Modbus TCP addressing. The MB_UNIT_ID parameter corresponds to the slave address in the Modbus RTU protocol. If a Modbus TCP server is used for a gateway to a Modbus RTU protocol, the MB_UNIT_ID can be used to identify the slave device connected on the serial network. The MB_UNIT_ID would be used to forward the request to the correct Modbus RTU slave address. Some Modbus TCP devices may require the MB_UNIT_ID parameter to be within a restricted range.
RCV_TIMEOUT	Real	2.0	Time in seconds that the MB_CLIENT waits for a server to respond to a request.
Connected	Bool	0	Indicates whether the connection to the assigned server is connected or disconnected: 1=connected, 0=disconnected

Table 14-60 MB_CLIENT protocol errors

STATUS* (W#16#)	Local and/or remote errors	Error code in the answer from MB_SERVER (B#16#)	Description
80C8	Local	-	No response of the server in the defined period. Check the connection to the Modbus server. This error is only reported on completion of the configured repeated attempts. If the "MB_CLIENT" instruction does not receive an answer with the originally transferred transaction ID (see static tag MB_TRANSACTION_ID) within the defined period, this error code is output.
8380	Local	-	Received Modbus frame has incorrect format or too few bytes were received.
8381	Remote	01	Function code is not supported.
8382	Local	-	• The length of the Modbus frame in the frame header does not match the number of received bytes. • The number of bytes does not match the number of actually transmitted bytes (only functions 1-4). For example, this is the case when "MB_CLIENT" requests an odd number of words, but "MB_SERVER" always sends an even number of words. • The start address in the received frame does not match the saved start address (functions 5, 6, 15, 16). • The number of words does not match the number of actually transmitted words (functions 15 and 16).
	Remote	03	Invalid length specification in received Modbus frame. Check the server side.
8383	Local	-	• Instruction version < V6.0: Error reading or writing data or access outside the address area of MB_DATA_PTR (Page 924). • Instruction version >= V6.0: Error reading or writing data or access outside the address area of MB_DATA_PTR, RD_MB_DATA_PTR or WR_MB_DATA_PTR.
	Remote	02	Error reading or writing data or access outside the address area of the server
8384	Local	-	• Invalid exception code received. • A different data value was received than was originally sent by the client (functions 5, 6 and 8). • Invalid status value received (function 11)
	Remote	03	Error in data value for function 5
8385	Local	-	• Diagnostics code not supported. • A different subfunction code was received than was originally sent by the client (function 8).
	Remote	03	Diagnostics code not supported
8386	Local	-	Received function code does not match the one sent originally.
8387	Local	-	The protocol ID of the Modbus TCP frame received by the server is not "0".
8388	Local	-	The Modbus server sent a different data length than was requested. This error occurs only when using the Modbus functions 5, 6, 15 or 16.
* The status codes can be displayed as integer or hexadecimal values in the program editor. For information on switching the display formats, refer to "See also".			

Table 14-61 MB_CLIENT execution condition codes [1]

STATUS (W#16#)	MB_CLIENT parameter errors
7001	MB_CLIENT is waiting for a Modbus server response to a connect or disconnect request, on the assigned TCP port. This code is only returned for the first execution of a connect or disconnect operation.
7002	MB_CLIENT is waiting for a Modbus server response to a connect or disconnect request, for the assigned TCP port. This will be returned for any subsequent executions, while waiting for completion of a connect or disconnect operation.
7003	A disconnect operation has successfully completed (Only valid for one PLC scan).
80C8	The server has not responded in the assigned time. MB_CLIENT must receive a response using the transaction ID that was originally transmitted within the assigned time or this error is returned. Check the connection to the Modbus server device. This error is only returned after retries (if applicable) have been attempted.
8188	The MB_MODE parameter has an invalid value.
8189	• Instruction version < V6.0: Invalid addressing of data at the MB_DATA_ADDR parameter. • Instruction version >= V6.0: Invalid addressing of data at the MB_DATA_ADDR, RD_MB_DATA_ADDR or WR_MB_DATA_ADDR parameter
818A	• Instruction version < V6.0: Invalid data length at the MB_DATA_LEN parameter. • Instruction version >= V6.0: Invalid data length at the MB_DATA_LEN, RD_MB_DATA_LEN or WR_MB_DATA_LEN parameter
818B	Invalid pointer to the DATA_PTR area. This can be the combination of MB_DATA_ADDRESS + MB_DATA_LEN.
818C	Pointer DATA_PTR points to an non-optimized DB area (must be a non-optimized DB area or M memory area)
818D	One or more parameters do not have their default value but are not used with the specified Modbus function. Example: If MB_MODE has the value 123, MB_DATA_ADDR and MB_DATA_LEN must have the value 0 and MB_DATA_PTR must be empty. If MB_MODE has a value other than 123, all parameters that begin with "RD_" or "WR_" must have the value 0 or be empty.
8200	The port is busy processing an existing Modbus request.
8380	Received Modbus frame is incorrect or too few bytes have been received.
8387	The assigned Connection ID parameter is different from the ID used for previous requests. There can only be a single Connection ID used within each MB_CLIENT instance DB. This code is also returned as an internal error if the Modbus TCP protocol ID received from a server is not 0.
8388	A Modbus server returned a quantity of data that is different than what was requested. This code applies to Modbus functions 15 or 16 only.

[1] In addition to the MB_CLIENT errors listed above, errors can be returned from the underlying T block communication instructions (TCON, TDISCON, TSEND, and TRCV).

MB_SERVER (Communicate using PROFINET as Modbus TCP server) instruction

Table 14-62 MB_SERVER instruction

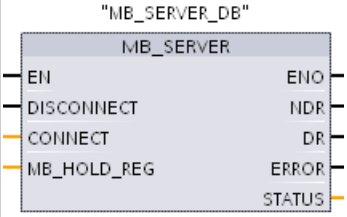
LAD / FBD	SCL	Description
	**"MB_SERVER_DB"(** **DISCONNECT:=_bool_in_,** **CONNECT:=_variant_in_,** **NDR=>_bool_out_,** **DR=>_bool_out_,** **ERROR=>_bool_out_,** **STATUS=>_word_out_,** **MB_HOLD_REG:=_variant_inout_);**	MB_SERVER communicates as a Modbus TCP server through the PROFINET port on the S7-1200 CPU. No additional communication hardware module is required. MB_SERVER can accept a request to connect with Modbus TCP client, receive a Modbus function request, and send a response message.

Table 14-63 Data types for the parameters

Parameter and type		Data type	Description
DISCONNECT	IN	Bool	MB_SERVER attempts to make a "passive" connection with a partner device. This means that the server is passively listening for a TCP connection request from any requesting IP address. If DISCONNECT = 0 and a connection does not exist, then a passive connection can be initiated. If DISCONNECT = 1 and a connection exists, then a disconnect operation is initiated. This parameter allows your program to control when a connection is accepted. Whenever this input is enabled, no other operation will be attempted.
CONNECT	IN	Variant	Reference to a Data block structure that contains connection parameters in the system data type "TCON_IP_v4". The following data types are also supported: TCON_IP_V4, TCON_QDN and TCON_QDN_SEC. See "Parameters for the PROFINET connection" (Page 551).
MB_HOLD_REG	IN_OUT	Variant	Pointer to the MB_SERVER Modbus holding register: The holding register must either be a non-optimized global DB or an M memory address. This memory area is used to hold the data a Modbus client is allowed to access using Modbus register functions 3 (read), 6 (write), 16 (write), and 23 (write/read).
NDR	OUT	Bool	New Data Ready: 0 = No new data, 1 = Indicates that new data has been written by a Modbus client
DR	OUT	Bool	Data Read: 0 = No data read, 1 = Indicates that data has been read by a Modbus client.
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after MB_SERVER execution ended with an error. The error code at the STATUS parameter is valid only during the single cycle where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code

CONNECT parameter assigns data used to establish a PROFINET connection

You must use a global data block and store the required connection data before you can reference this DB at the CONNECT parameter.

1. Create a new global DB or use an existing global DB to store the CONNECT data. You can use one DB to store multiple TCON_IP_v4 data structures. Each Modbus TCP client or server connection uses a TCON_IP_v4 data structure. You reference the connection data at the CONNECT parameter.
2. Name the DB and a static variable with a helpful name. For example, name the data block "Modbus connections" and a static variable "TCPpassive_1" (for Modbus TCP server connection 1).
3. In the DB editor, assign the system data type "TCON_IP_v4" in the Data Type column, for the example static variable "TCPactive_1".
4. Expand the TCON_IP_v4 structure so you can modify the connection parameters, as shown in the following image.
5. Modify data in the TCON_IP_v4 structure for an MB_SERVER connection.
6. Enter the DB structure reference for the CONNECT parameter of MB_SEVER. For the example, this would be "Modbus connections".TCPpassive_1.

Modbus connections

	Name	Data type	Start value	Comment
1	Static			
2	TCPpassive_1	TCON_IP_v4		
3	InterfaceId	HW_ANY	64	HW-identifier of IE-interface submodule
4	ID	CONN_OUC	1	connection reference / identifier
5	ConnectionType	Byte	16#0B	type of connetion: 11=TCP/IP, 19=UDP (17=TC...
6	ActiveEstablished	Bool	False	active/passive connection establishment
7	RemoteAddress	IP_V4		remote IP address (IPv4)
8	ADDR	array [1..4] of Byte		IPv4 address
9	ADDR[1]	Byte	192	
10	ADDR[2]	Byte	168	
11	ADDR[3]	Byte	2	
12	ADDR[4]	Byte	241	
13	RemotePort	UInt	0	remote UDP/TCP port number
14	LocalPort	UInt	502	local UDP/TCP port number

Modify TCON_IP_V4 DB data for each MB_SERVER connection

- **InterfaceID**: Using the Device configuration window, click on the CPU PROFINET port image. Then click on the General properties tab and use the Hardware identifier that you see there.
- **ID**: Enter a number between 1 and 4095 that is unique for this connection. Modbus TCP communication is made using underlying TCON, TDISCON, TSEND, and TRCV instructions, for OUC (Open User Communication). Up to eight simultaneous OUC connections are allowed.
- **ConnectionType**: For TCP/IP, use the default 16#0B (decimal value = 11).
- **ActiveEstablished**: This value must be 0 or FALSE. The connection is passive in that MB_SERVER is waiting for a communication request from a Modbus client.
- **RemoteAddress**: There are two options.
  - Use 0.0.0.0 and MB_CLIENT will respond to a Modbus request from any TCP client
  - Enter the IP address of a target Modbus TCP client and MB_CLIENT only responds to a request originating from this client's IP address. For example, enter 192.168.2.241, as in the previous image.
- **RemotePort**: This value must be 0, for an MB_SERVER connection.
- **LocalPort**: The default is 502. This number is the IP port number of the Modbus client that MB_SERVER attempts to connect and communicate with. Some third-party Modbus clients require another port number.

Modbus and process image addresses

MB_SERVER allows incoming Modbus function codes (1, 2, 4, 5, and 15) to read/write bits/words directly in the input/output process image. For data transfer function codes (3, 6, and 16), the MB_HOLD_REG parameter must be defined as a data type larger than a byte. The following table shows the mapping of Modbus addresses to the process image in the CPU.

Table 14-64 Mapping of Modbus addresses to the process image

Modbus functions						S7-1200	
Codes	Function	Data area	Address range			Data area	CPU address
01	Read bits	Output	1	To	8192	Output Process Image	Q0.0 to Q1023.7
02	Read bits	Input	10001	To	18192	Input Process Image	I0.0 to I1023.7
04	Read words	Input	30001	To	30512	Input Process Image	IW0 to IW1022
05	Write bit	Output	1	To	8192	Output Process Image	Q0.0 to Q1023.7
15	Write bits	Output	1	To	8192	Output Process Image	Q0.0 to Q1023.7

Incoming Modbus message function codes function codes (3, 6, and 16) read/write words in a Modbus holding register, which can be in M memory or a data block. The type of holding register is specified by the MB_HOLD_REG parameter.

NOTE

MB_HOLD_REG parameter assignment

Modbus holding registers defined as arrays of word, integer, wide character, unsigned integer, byte, short integer, unsigned short integer, character, double word, double integer, unsigned double integer, or real can be placed in any memory area.

You must place Modbus holding registers that you defined as structures in non-optimized DBs.

For a Modbus holding register in M memory, use the Any Pointer format. This is in the format P#"Bit Address" "Data Type" "Length". An example would be P#M1000.0 WORD 500.

The following table shows examples of Modbus addresses to holding register mapping used for Modbus function codes 03 (read words), 06 (write word), and 16 (write words). The actual upper limit of DB addresses is determined by the maximum work memory limit and M memory limit, for each CPU model.

WARNING

Risks with access to the process image

Each Modbus TCP client has read and write access to the process image inputs and outputs, and to the data block or bit memory area defined by the Modbus holding register. Unauthorized read and write operations can change PLC variables into invalid values and disrupt process operations.

To reduce the risk of unauthorized access, restrict access to an IP address of a specific Modbus client. For information on additional industrial security measures that can be implemented, please visit the Siemens Industrial Cybersecurity Web site (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

Disruption of process operations can result in death, severe injury and/or property damage.

Table 14-65 Mapping examples of Modbus address to CPU memory address

Modbus Address	MB_HOLD_REG parameter examples		
	P#M100.0 Word 5	**P#DB10.DBx0.0 Word 5**	**"Recipe".ingredient**
40001	MW100	DB10.DBW0	"Recipe".ingredient[1]
40002	MW102	DB10.DBW2	"Recipe".ingredient[2]
40003	MW104	DB10.DBW4	"Recipe".ingredient[3]
40004	MW106	DB10.DBW6	"Recipe".ingredient[4]
40005	MW108	DB10.DBW8	"Recipe".ingredient[5]

Modbus Application Protocol header

The Modbus Application Protocol header is the first seven bytes of every Modbus TCP message. This header contains the Transaction Identifier, Protocol Identifier, Length, and Unit Identifier. The MB_SERVER instruction response message contains the same values for the Transaction Identifier, Protocol Identifier, and Unit Identifier that were received in the Modbus request message. The Length field is calculated by the MB_SERVER instruction.

Multiple server connections

Multiple server connections may be created. A single PLC can establish concurrent connections to multiple Modbus TCP clients.

A Modbus TCP server can support concurrent connections up to the maximum number of Open User Communications connections allowed by the PLC. The total number of connections for a PLC, including Modbus TCP Clients and Servers, must not exceed the maximum number of supported Open User Communications connections (Page 526). The Modbus TCP connections may be shared between Client and Server type connections.

Individual concurrent server connection must follow these rules:

- Each MB_SERVER connection must use a unique instance DB.
- Each MB_SERVER connection must assign a unique IP port number. Only 1 connection per port is supported.
- Each MB_SERVER connection must assign a unique connection ID.
- The MB_SERVER must be called individually for each connection (with its respective instance DB).

The connection ID must be unique for each individual connection. A single, connection ID must be used with each individual instance DB. The instance DB and the connection ID are paired together and must be unique for every connection.

Table 14-66 Modbus diagnostic function codes

MB_SERVER Modbus diagnostic functions		
Codes	Sub-function	Description
08	0x0000	Return query data echo test: The MB_SERVER will echo back to a Modbus client a data word that is received.
08	0x000A	Clear communication event counter: The MB_SEVER will clear the communication event counter that is used for Modbus function 11.
11		Get communication event counter: The MB_SERVER uses an internal communication event counter for recording the number of successful Modbus read and write requests that are sent to the Modbus server. The counter does not increment on any request for Function 8, Function 11, or any request that results in a communication error. The broadcast function is not available for Modbus TCP, because only one client-server connection exists at any one time.

MB_SERVER instruction data block (DB) variables

This table shows the public static variables that are stored in the MB_SERVER instance data block and can be used in your program

Table 14-67 MB_SERVER public static variables

Variable	Data type	Default	Description
HR_Start_Offset	Word	0	Assigns the starting address of the Modbus Holding register
Request_Count	Word	0	The number of all requests received by this server.
Server_Message_Count	Word	0	The number of requests received for this specific server.
Xmt_Rcv_Count	Word	0	The number of transmissions or receptions that have encountered an error. Also, incremented if a message is received that is an invalid Modbus message.
Exception_Count	Word	0	Modbus specific errors that require a returned exception
Success_Count	Word	0	The number of requests received for this specific server that has no protocol errors.
Connected	Bool	0	Indicates whether the connection to the assigned client is connected or disconnected: 1=connected, 0=disconnected
QB_Start	UInt	0	The starting address of the output bytes to which the CPU can write (QB0 to QB65535)
QB_Count	UInt	65535	The number of bytes to which a remote device can write. If QB_Count = 0, a remote device cannot write to the outputs. Example: To allow only QB10 through QB17 to be writable, QB_Start = 10 and QB_Count = 8.
QB_Read_Start	UInt	0	The starting address of the output bytes to which the CPU can read (QB0 to QB65535)
QB_Read_Count	UInt	65535	The number of output bytes from which a remote device can read. If QB_Count = 0, a remote device cannot read from the outputs. Example: To allow only QB10 through QB17 to be readable, QB_Start = 10 and QB_Count = 8.

Variable	Data type	Default	Description
IB_Read_Start	UInt	0	The starting address of the input bytes to which the CPU can read (IB0 to IB65535)
IB_Read_Count	UInt	65535	The number of input bytes from which a remote device can read. If IB_Count = 0, a remote device cannot read from the inputs. Example: To allow only IB10 through IB17 to be readable, IB_Start = 10 and IB_Count = 8.
NDR_immediate	Bool	FALSE	Identical meaning as the parameter NDR (New Data Ready). The MB_SERVER updates the "NDR_immediate" in the same call that processes a Modbus TCP write request.
DR_immediate	Bool	FALSE	Identical meaning as the parameter DR (Data Read). The MB_SERVER updates the "DR_immediate" in the same call that processes a Modbus TCP write request.

Your program can write data to the control Modbus server operations and the following variables:

- HR_Start_Offset
- QB_Start
- QB_Count
- QB_Read_Start
- QB_Read_Count
- IB_Read_Start
- IB_Read_Count

Version requirements for MB_SERVER instruction data block (DB) variables availability are as follows:

Table 14-68 MB_SERVER instruction data block (DB) variables availability version requirements: Instruction, TIA Portal, and S7-1200 CPU

MB_SERVER instruction version	TIA Portal version	S7-1200 CPU firmware (FW) version	Data block variables
4.2	V14 SP1	CPU FW V4.0 or later	QB_Start
			QB_Count
5.0 or later	V15 or later	CPU FW V4.2 or later	QB_Start
			QB_Count
			QB_Read_Start
			QB_Read_Count
			IB_Read_Start
			IB_Read_Count
			NDR_immediate
			DR_immediate

HR_Start_Offset

Modbus holding register addresses begin at 40001. These addresses correspond to the beginning PLC memory address of the holding register. However, you can use the "HR_Start_Offset" variable to start the beginning Modbus holding register address at another number instead of 40001.

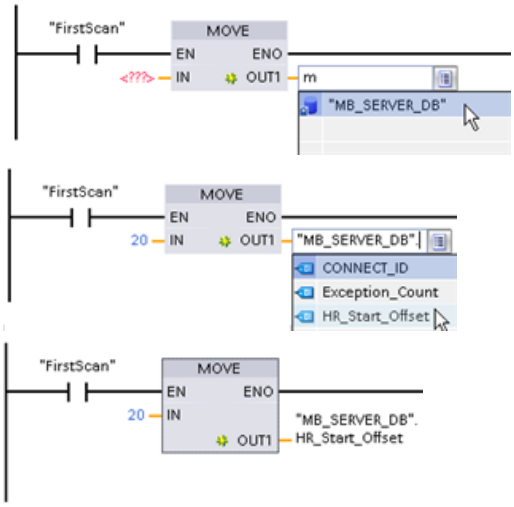
For example, if the holding register starts at MW100 and is 100 words long. An offset of 20 specifies a beginning holding register address of 40021 instead of 40001. Any address less than 40021 or greater than 40119 results in an addressing error.

Table 14-69 Example of Modbus holding register addressing

HR_Start_Offset	Address	Minimum	Maximum
0	Modbus address (Word)	40001	40099
	S7-1200 address	MW100	MW298
20	Modbus address (Word)	40021	40119
	S7-1200 address	MW100	MW298

HR_Start_Offset is word data in the MB_SERVER instance data block that assigns the starting address of the Modbus holding register. You can set this public static variable by using the parameter helper drop list, after MB_SERVER is placed in your program.

For example, after you place MB_SERVER in a LAD network, you can go to a previous network and assign HR_Start_Offset. The start address must be assigned prior to execution of MB_SERVER.



Entering a Modbus server variable using the default DB name:

1. Set the cursor in the parameter field and type an m character.
2. Select "MB_SERVER_DB" from the drop list of DB names.
3. Select "MB_SERVER_DB.HR_Start_Offset" from the drop list of DB variables.

Access to data areas in data blocks (DB) instead of direct access to Modbus addresses

You can access data areas in DBs. In the global DB "Attributes" Property page, you must deselect the "Only store in load memory" and "Optimized block access" check boxes.

If a Modbus request arrives and you did not define a data area for the Modbus data type of the corresponding function code, the MB_SERVER instruction treats the request as in previous instruction versions: You access process images and holding registers directly.

If you have defined a data area for the Modbus data type of the function code, the MB_SERVER instruction reads from or writes to that data area. Whether it reads or writes depends on the job type.

NOTE

If a data area is configured, the MB_SERVER instruction ignores the offsets or ranges configured by the static variables in the instance data block that corresponds to the data_type of the data area. Those offsets and ranges only apply to the process image or the memory referenced by MB_HOLD_REG. The data area start and length parameters provide its own way of defining offsets and ranges

For one individual Modbus request, you can only read from or write to one data area. If, for example, you want to read holding registers that extend over multiple data areas, you require multiple Modbus requests.

These are the rules for defining data areas:

- You can define up to eight data areas in different DBs; each DB must only contain one data area. An individual MODBUS request can only read from precisely one data area or write to precisely one data area. Each data area corresponds to one MODBUS address area. You define the data areas in the "Data_Area_Array" static tag of the instance DB.
- If you want to use less than eight data areas, you must place the required data areas one behind the other, without any gaps. The first blank entry in the data areas ends the data area search during processing. If, for example, you define the field elements 1, 2, 4, and 5, the "Data_Area_Array" only recognizes field elements 1 and 2. as field element 3 is empty.
- The Data_Area_Array field consists of eight elements: Data_Area_Array[1] to Data_Area_Array[8]
- Each field element Data_Area_Array[x], 1 <= x <= 8, is a UDT of the type MB_DataArea and is structured as follows:

Parameter	Data type	Meaning
data_ type	UInt	Identifier for the MODBUS data type that is mapped to this data area: – 0: Identifier for an empty field element or an unused data area. In this case, the values of db, start and length are irrelevant. – 1: Process image output (used with function codes 1, 5, and 15) – 2: Process image input (used with function code 2) – 3: Holding register (used with function codes 3, 6, and 16) – 4: Input register (used with function code 4) Note: If you have defined a data area for a MODBUS data type, the instruction MB_SERVER can no longer access this MODBUS data type directly. If the address of a MODBUS request for such a data type does not correspond to a defined data area, a value of W#16#8383 is returned in STATUS.
db	UInt	Number of the data block to which the MODBUS register or bits subsequently defined are mapped The DB number must be unique in the data areas. The same DB number must not be defined in multiple data areas. In the global DB "Attributes" Property page, you must deselect the "Only store in load memory" and "Optimized block access" check boxes. Data areas also start with the byte address 0 of the DB. Permitted values: 1 to 60999

Parameter	Data type	Meaning
start	UInt	First MODBUS address that is mapped to the data block starting from address 0.0 Permitted values: 0 to 65535
length	UInt	Number of bits (for the values 1 and 2 of data_type) or number of registers (for the values 3 and 4 of data_type) The MODBUS address areas of one and the same MODBUS data type must not overlap. Permitted values: 1 to 65535

Examples of the definition of data areas:

- First example: data_type = 3, db = 1, start = 10, length = 6
  The CPU maps the holding registers (data_type = 3) in data block 1 (db = 1), placing the Modbus address 10 (start = 10) at data word 0 and the last valid Modbus address 15 (length = 6) at data word 5.
- Second example: data_type = 2, db = 15, start = 1700, length = 112
  The CPU maps the inputs (data_type = 2) in data block 15 (db = 15), placing the Modbus address 1700 (start = 1700) at data word 0 and the last valid Modbus address 1811 (length = 112) at data word 111.

Condition codes

Table 14-70 MB_SERVER execution condition codes [1]

STATUS (W#16#)	Response code to Modbus server (B#16#)	Modbus protocol errors
7001		MB_SERVER is waiting for a Modbus client to connect to the assigned TCP port. This code is returned on the first execution of a connect or disconnect operation.
7002		MB_SERVER is waiting for a Modbus client to connect to the assigned TCP port. This code is returned for any subsequent executions, while waiting for completion of a connect or disconnect operation.
7003		A disconnect operation has successfully completed (Only valid for one PLC scan).
8187		MB_HOLD_REG is not valid, could be pointing into an optimized DB, or is pointing to an area of less than 2 bytes.
818C		Pointer MB_HOLD_REG points to a non-optimized DB area (must be a non-optimized global DB area or M memory area) or Blocked process timeout exceeds the limit of 55 seconds. (S7-1200 specific)
8381	01	Function code not supported
8382	03	Error in data length: • Invalid length specification in received Modbus frame. • The frame length entered in the header of the Modbus frame does not match the number of actually received bytes. • The number of bytes entered in the header of the Modbus frame does not match the number of actually received bytes (functions 15 and 16).
8383	02	Data address error or access outside the bounds of the MB_HOLD_REG address area

STATUS (W#16#)	Response code to Modbus server (B#16#)	Modbus protocol errors
8384	03	Data value error
8385	03	Data diagnostic code not supported (function code 08)
8389		Invalid data area definition: • Invalid data_type value • DB number invalid or does not exist: – Invalid db value – DB number does not exist – DB number is already used by another data area – DB with optimized access – DB is not located in the work memory • Invalid length value • Overlapping of MODBUS address ranges that belong to the same MODBUS data type

[1] In addition to the MB_SERVER errors listed above, errors can be returned from the underlying T block communication instructions (TCON, TDISCON, TSEND, and TRCV).

MB_RED_CLIENT (Redundant communication over PROFINET as a Modbus TCP client)

You can use this instruction to establish a connection between an S7-1200 CPU and a device that supports the Modbus TCP protocol.

Table 14-71 MB_RED_CLIENT instruction

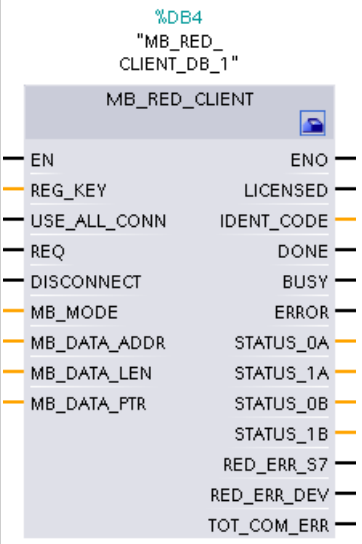
LAD / FBD	SCL	Description
	**"MB_RED_CLIENT_DB"(REG_KEY:=_string_in_, USE_ALL_CONN:=_bool_in_ REQ:=_bool_in_, DISCONNECT:=_bool_in_, MB_MODE:=_usint_in_, MB_DATA_ADDR:=_udint_in_, MB_DATA_LEN:=_uint_in_, LICENSED=>_bool_out_ IDENT_CODE=>_string_out_ DONE=>_bool_out_, BUSY=>_bool_out_, ERROR=>_bool_out_, STATUS_0A=>_word_out_, STATUS_1A=>_word_out_, STATUS_0B=>_word_out_, STATUS_1B=>_word_out_, RED_ERR_S7=>_bool_out_, RED_ERR_DEV=>_bool_out_, TOT_COM_ERR=>_bool_out_, MB_DATA_PTR:=_variant_inout_);**	The MB_RED_CLIENT instruction communicates as a Modbus TCP client over the PROFINET connection. You use the instruction MB_RED_CLIENT to establish a redundant connection between the client and the server, send Modbus requests, receive responses, and control connection termination by the Modbus TCP client.

Table 14-72 Data types for the parameters

Parameter and type		Data type	Description
REG_KEY [1]	IN	STRING[17]	Registration code for licensing The MB_RED_CLIENT instruction must be licensed on each CPU individually.
USE_ALL_CONN	IN	Bool	Specify the number of configured connections over which the frame is to be sent: • 0: Send frame over one connection, switch to next connection only in case of error • 1: Send frame over all configured connections
REQ	IN	Bool	Modbus query to the Modbus TCP server The REQ parameter is level-controlled. This means that as long as the input is set (REQ = TRUE), the instruction sends communication requests. If the connection has not been established yet, it is established now, and the Modbus frame is sent immediately thereafter. Changes to the input parameters will not become effective until the server has responded, or an error message has been output. If the parameter REQ is set again during an ongoing Modbus request, no additional transmission takes place afterwards.
DISCONNECT	IN	Bool	With this parameter, you control the establishment and termination of the connection to the Modbus server: • 0: Establish communication connection to the connection partner configured at the CONNECT parameter (see CONNECT parameter). • 1: Disconnect the communication connection. No other function is executed during connection termination. The value 0003 is output at the STATUS_x parameter after successful connection termination.
MB_MODE [2]	IN	USInt	Selects the mode of the Modbus request (read, write or diagnostics) or direct selection of a Modbus function
MB_DATA_ADDR [2]	IN	UDInt	Modbus address depending on MB_MODE
MB_DATA_LEN	IN	UInt	Data length: Number of bits or registers for the data access
MB_DATA_PTR [2]	IN_OUT	Variant	Pointer to a data buffer for the data to be received from the Modbus server or to be sent to the Modbus server.
LICENSED [1]	OUT	Bool	• 0: Instruction is not licensed • 1: Instruction is licensed
IDENT_CODE [1]	OUT	STRING[18]	Identification for licensing. Use this string to request the REG_KEY registration code.
DONE	OUT	Bool	The bit at the DONE output parameter is set to "1" as soon as the activated Modbus job is completed without errors on at least one connection.
BUSY	OUT	Bool	• 0: No Modbus request in progress • 1: Modbus request being processed The BUSY output parameter is not set during connection establishment and termination.

1 Refer to the "Licensing" section below for further information.

2 Refer to the "Input parameters: MB_MODE, MB_DATA_ADDR, MB_DATA_LEN, and MB_DATA_PTR" section below for further information.

3 Refer to the "Output parameters: STATUS_x, RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR" section below for further information.

Parameter and type		Data type	Description
ERROR	OUT	Bool	• 0: No error • 1: The activated Modbus job could not be transmitted successfully on any of the configured connections. The cause of error is indicated by the STATUS_x parameter.
STATUS_0A [3]	OUT	Word	Detailed status information of the instruction on connection 0A.
STATUS_1A [3]	OUT	Word	Detailed status information of the instruction on connection 1A.
STATUS_0B [3]	OUT	Word	Detailed status information of the instruction on connection 0B.
STATUS_1B [3]	OUT	Word	Detailed status information of the instruction on connection 1B.
RED_ERR_S7 [3]	OUT	Bool	• 0: No redundancy error in SIMATIC • 1: Redundancy error in SIMATIC
RED_ERR_S7 [3]	OUT	Bool	• 0: No redundancy error on side of link partner • 1: Redundancy error on side of link partner
RED_ERR_S7 [3]	OUT	Bool	• 0: At least 1 configured connection is established • 1: Complete loss of communication, all configured connections are terminated

[1] Refer to the "Licensing" section below for further information.

[2] Refer to the "Input parameters: MB_MODE, MB_DATA_ADDR, MB_DATA_LEN, and MB_DATA_PTR" section below for further information.

[3] Refer to the "Output parameters: STATUS_x, RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR" section below for further information.

NOTE

Consistent input data during an MB_RED_CLIENT call

When a Modbus client instruction is called, the values of the input parameters are stored internally. The values must not be changed while the frame is being processed.

Multiple client connections

The CPUs can process multiple Modbus TCP client connections. The maximum number of connections depends on the CPU being used and can be found in the technical specifications of the CPU. The total number of connections of one CPU, including those of the Modbus TCP clients and server must not exceed the maximum number of supported connections.

With individual client connections, remember the following rules:

- Each MB_RED_CLIENT connection must use a unique instance DB.
- For each MB_RED_CLIENT connection, a unique server IP address must be specified.
- Each MB_RED_CLIENT connection requires a unique connection ID. The connection IDs must be unique throughout the CPU.

Operation and redundancy

The communication nodes can be designed as standalone or redundant. If one of the partners is designed as standalone, we refer to it as single-sided redundancy. If both partners are designed redundantly, we refer to it as double-sided redundancy:

- Single-sided redundancy:
  - Description: One connection each must be configured for each connection between the communication partners. The connection points of the **SIMATIC S7** are referred to as **0** and **1**; the connection points of the **communication partner** are referred to as **A** and **B**. The R-CPU or H-CPU 1 refers to the connection point 0, the R-CPU or H-CPU 2 refers to the connection point 1.
  - Configuration: If the S7 is designed redundantly, one connection is created from the S7 connection point 0 to junction A of the link partner (Connection from the S7 connection point **0** to the partner/node **A** => connection **0A**), and one connection from the S7 connection point 1 to junction A of the link partner (Connection from the S7 connection point **1** to the partner/node **A** => connection **1A**). The figure illustrates the connection designations:

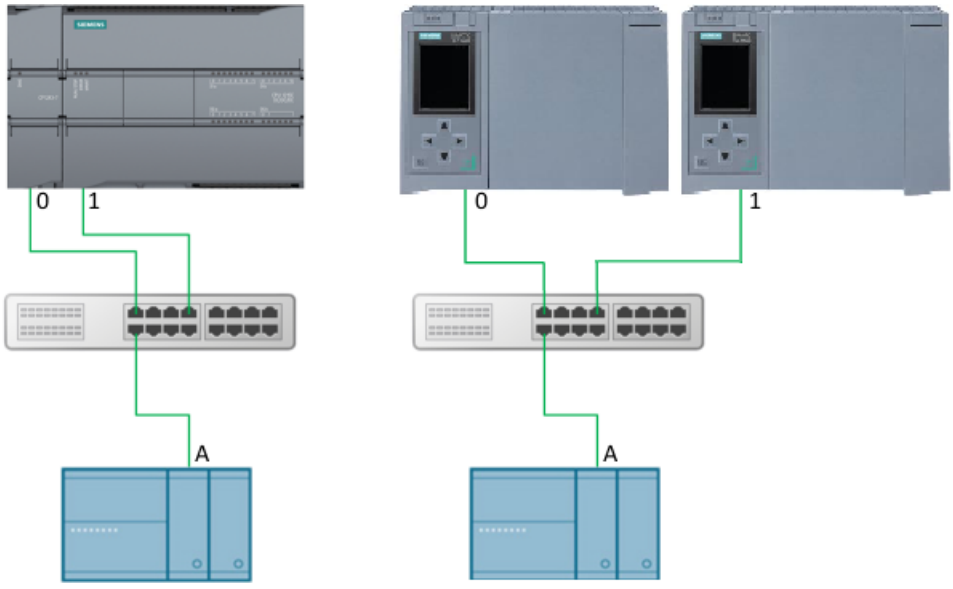


Figure 14-1 Single-sided redundancy S7

– If the S7 is designed as standalone and the link partner is designed redundantly, one connection is created from the S7 connection point 0 to junction A of the link partner (connection from the S7 connection point **0** to the partner/node **A** => connection **0A**), and one connection from the S7 connection point 0 to junction B of the link partner (connection from the S7 connection point **0** to the partner/node **B** => connection **0B**). The figure illustrates the connection designations:

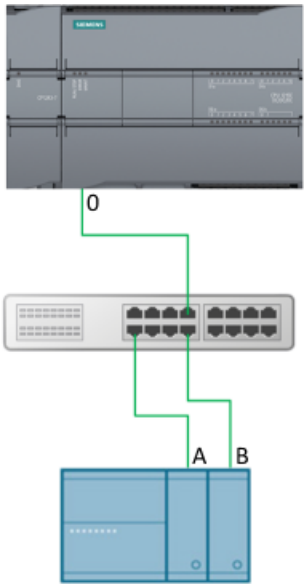


Figure 14-2 Single-sided redundancy partner

- Double-sided redundancy:
  - Description: One connection each must be configured for each connection between the communication partners. The connection points of the SIMATIC S7 are referred to as **0** and **1**; the connection points of the **communication partner** are referred to as **A** and **B**.

    The R-CPU or H-CPU 1 refers to the connection point 0 the R-CPU or H-CPU 2 refers to the connection point 1.
  - Configuration: In the case of double-sided redundancy, two connections are created from connection point 0 (connection from the S7 connection point **0** to the partner/node **A** => connection **0A** and connection from the S7 connection point **0** to the partner/node **B** => connection **0B**), and two connections from connection point 1 of the S7 to the junctions A and B of the link partner (connection from the S7 connection point **1** to the partner/node **A** => connection **1A** and connection from the S7 connection point **1** to the partner/node **B** => connection **1B**). The figure illustrates the connection designations:

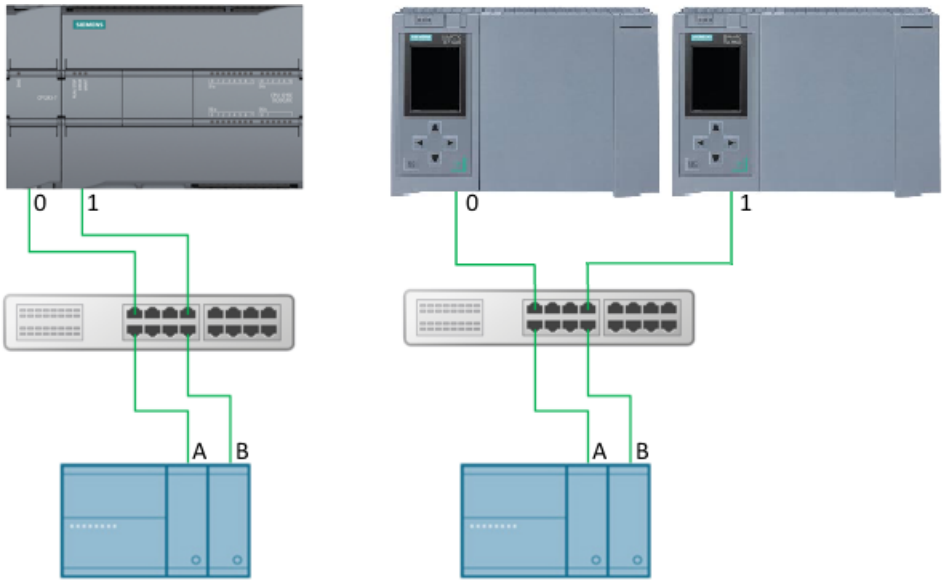


Figure 14-3 Double-sided redundancy

- Frame processing: The frames can be sent via one or via all configured connections:
  - Send frames via one connection: The MODBUS frame is sent via one - the currently active - connection with the setting USE_ALL_CONN = FALSE. In case of a timeout (no response from the server) or a connection fault an attempt is made to send the frame via the other (maximum 4) configured connections. The sequence is then 0A, 1A, 0B and 1B. If a frame was transmitted successfully via a connection, this connection is marked as "active" and the further frame traffic is executed via this connection. In the case of a connection fault of the active connection it is again attempted to send the frame via all configured connections. If all send attempts fail, ERROR and STATUS_x are set accordingly.

    If a response frame was received, a plausibility check is executed. If this check is successful, the required actions are performed and the job is executed without errors; the output DONE is set. If errors are detected during the check, the job is ended without errors, the bit ERROR is set and an error number is displayed at STATUS_x. In this case no new attempt is made to send the frame on the next configured

connection. A switchover to the other configured connections only takes place if a connection fault was detected or no response was received.

– Sending frames via all connections: The MODBUS frame is sent via all configured, established connections with the setting USE_ALL_CONN = TRUE. A validity check is performed after the response frame has been received on one of the connections. If this check is successful, the required actions are performed. If a valid response frame was received on at least one connection, the output DONE is set.

- Redundancy outputs RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR:
  – The redundancy bits RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR are set based on the states of the status outputs:

Number of faulty connections	STATUS_0A	STATUS_0B	STATUS_1A	STATUS_1B	RED_ERR_S7	RED_ERR_DEV	TOT_COM_ERR
0	okay	okay	okay	okay	FALSE	FALSE	FALSE
1	okay	okay	okay	Error	FALSE	FALSE	FALSE
	okay	okay	Error	okay	FALSE	FALSE	FALSE
	okay	Error	okay	okay	FALSE	FALSE	FALSE
	Error	okay	okay	okay	FALSE	FALSE	FALSE
2	okay	okay	Error	Error	TRUE	FALSE	FALSE
	okay	Error	okay	Error	FALSE	TRUE	FALSE
	Error	okay	okay	Error	FALSE	FALSE	FALSE
	okay	Error	Error	okay	FALSE	FALSE	FALSE
	Error	okay	Error	okay	FALSE	TRUE	FALSE
	Error	Error	okay	okay	TRUE	FALSE	FALSE
3	Error	Error	Error	okay	TRUE	TRUE	FALSE
	Error	Error	okay	Error	TRUE	TRUE	FALSE
	Error	okay	Error	Error	TRUE	TRUE	FALSE
	okay	Error	Error	Error	TRUE	TRUE	FALSE
4	Error	Error	Error	Error	TRUE	TRUE	TRUE

Figure 14-4 Display of the interrupt bits for redundancy setup on both sides

Number of faulty connections	STATUS_0A	STATUS_0B	STATUS_1A	STATUS_1B	RED_ERR_S7	RED_ERR_DEV	TOT_COM_ERR
0	okay	0AFF	okay	0AFF	FALSE	FALSE	FALSE
1	okay	0AFF	Error	0AFF	TRUE	TRUE	FALSE
	Error	0AFF	okay	0AFF	TRUE	TRUE	FALSE
2	Error	0AFF	Error	0AFF	TRUE	TRUE	TRUE

Figure 14-5 Display of the interrupt bits for redundancy setup on one side

NOTE

Port numbers for client and server

The Modbus client uses a port number starting at 2000. The Modbus server is usually addressed over the port number 502.

Parameter assignment

You can use the MB_RED_CLIENT instruction **V1.0** and **V1.1** for S7-1200. The CPU implements the connections over the local interface of the CPU or CM/CP. The CPU configures and establishes the connections using the TCON_IP_V4 structure.

Configuration of MB_RED_CLIENT: You make the following settings using the configuration dialog of the MB_RED_CLIENT instruction:

- Connection parameters for the connections 0A, 1A, 0B and 1B (Refer to "Operation and Redundancy", above, for more information on redundancy configuration.)
- Internal parameter (optional)

You can open the configuration dialog with the MB_RED_CLIENT instruction or through the technology objects:

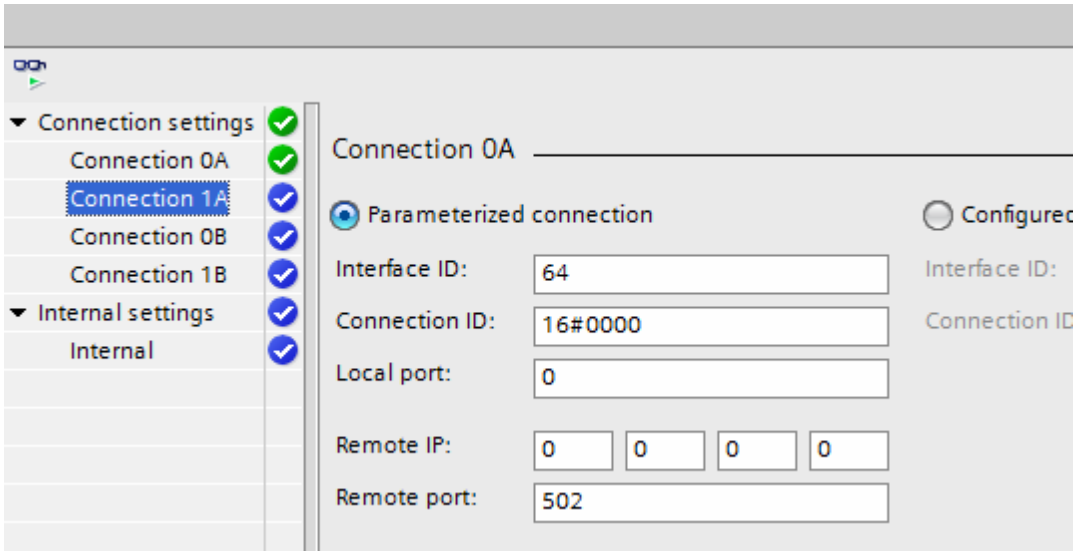


Figure 14-6 Parameterized client connection

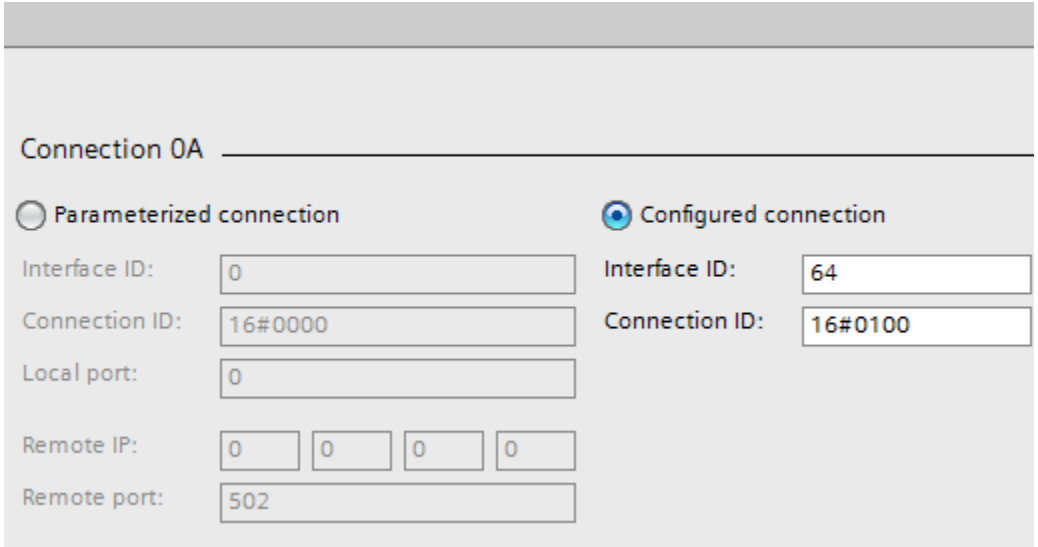


Figure 14-7 Configured client connection

Tag	Start value	Description
Configured connections		
Interface ID	64	HW identifier of the PN interface used
Connection ID	16#0000	Connection IDs for the connections used These connection IDs must be unique throughout the CPU.
Local port	0	Local port number of the client. By default, no port number is entered for the client.
Remote IP	0.0.0.0	Remote IP address of the server
Remote port	502	Remote port number of the server The default port for Modbus/TCP server is 502.
Configured connections		
Interface ID	64	HW identifier of the PN interface used
Connection ID	16#0000	Connection IDs for the connections used These connections are configured in the network view.

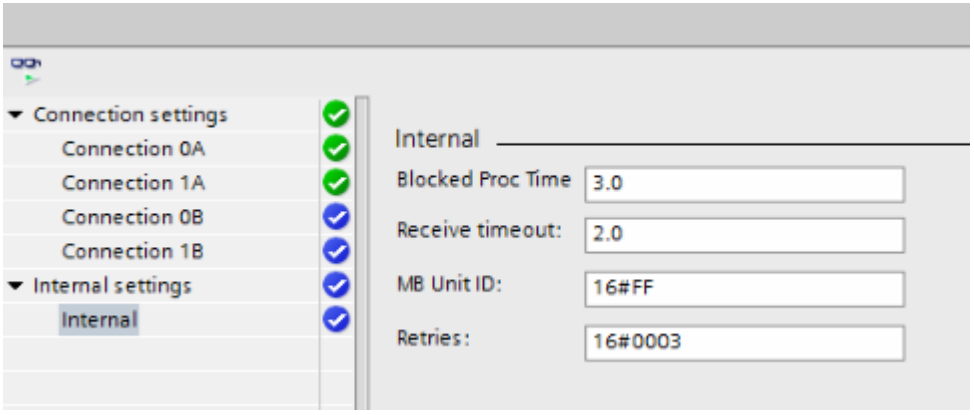


Figure 14-8 Internal parameter (optional)

Tag	Data type	Start value	Description
Blocked Proc Time	REAL	3.0	Wait time in seconds before the static tag ACTIVE is reset if there is a blocked Modbus instance. This can, for example, occur if a client request is output and the execution of the client function aborts before the request was fully executed. The wait time must be between 0.5 s and 55 s.
Receive timeout	REAL	2.0	Time interval in seconds in which the "MB_RED_CLIENT" instruction waits for a response from the server. It must be between 0.5 s and 55 s.
MB_Unit_ID	BYTE	255	Modbus device detection: A Modbus TCP server is addressed using its IP address. For this reason, the MB_UNIT_ID parameter is not used in the case of Modbus TCP addressing. The MB_UNIT_ID parameter corresponds to the field of the slave address in the Modbus RTU protocol. If a Modbus/TCP server is used as a gateway for a Modbus RTU protocol, the slave device in the serial network can be identified using MB_UNIT_ID. The MB_UNIT_ID parameter would in this case forward the request to the correct Modbus RTU slave address. Please note that some Modbus/TCP devices may require the MB_UNIT_ID parameter for the initialization within a limited value range.
Retries	WORD	3	Number of send attempts made by the MB_RED_CLIENT instruction before it returns the error W#16#80C8.

NOTE

Tag MB_Transaction_ID

If the transaction ID in the answer of the Modbus TCP server does not match the transaction ID of the job from MB_RED_CLIENT, the MB_RED_CLIENT instruction waits for the time period RCV_TIMEOUT * RETRIES for the answer of the Modbus TCP server with the correct transaction ID; once this time has expired, it returns the error W#16#80C8.

Licensing

The MB_RED_CLIENT instruction is subject to a fee, and you must license the instruction on each CPU individually. Licensing takes place in two steps:

- Displaying the license IDENT_CODE
- Entering the REG_KEY registration key: You must assign the REG_KEY registration key at each MB_RED_CLIENT instruction. Save the REG_KEY in a global data block from which all MB_RED_CLIENT instructions receive the necessary registration key.

Procedure for displaying the license IDENT_CODE:

1. Assign parameters to the MB_RED_CLIENT instruction in line with your requirements in a cyclic OB. Download the program to the CPU and set the CPU to RUN.
2. Open the instance DB of the Modbus instruction, and click the "Monitor all" button.

3. The instance DB displays an 18-digit character string at the IDENT_CODE output.

	Name	Data type	Start value	Monitor value
1	Input			
2	REG_KEY	String[17]	''	''
3	USE_ALL_CONN	Bool	false	FALSE
4	REQ	Bool	false	FALSE
5	DISCONNECT	Bool	false	FALSE
6	MB_MODE	USInt	0	0
7	MB_DATA_ADDR	UDInt	0	0
8	MB_DATA_LEN	UInt	0	0
9	Output			
10	LICENSED	Bool	false	FALSE
11	IDENT_CODE	String[18]	''	'RTPCFIGDCDIIHJHAH4'
12	DONE	Bool	false	FALSE
13	BUSY	Bool	false	FALSE
14	ERROR	Bool	false	FALSE

Figure 14-9 License

4. Copy this string using copy/paste from the data block and paste it in the form (that was sent to you by email after you ordered the product or is included on the CD).
5. Send the form to Customer support (https://support.industry.siemens.com/my/ww/en/requests/#createRequest) using a service request. You will then receive the registration key for your CPU.

Procedure for entering the registration key REG_KEY:

1. Insert a new global data block with a unique symbolic name, for example "License_DB", using "Add new block...".
2. Create a REG_KEY parameter in this block with the data type STRING[17].

LICENSE_DB

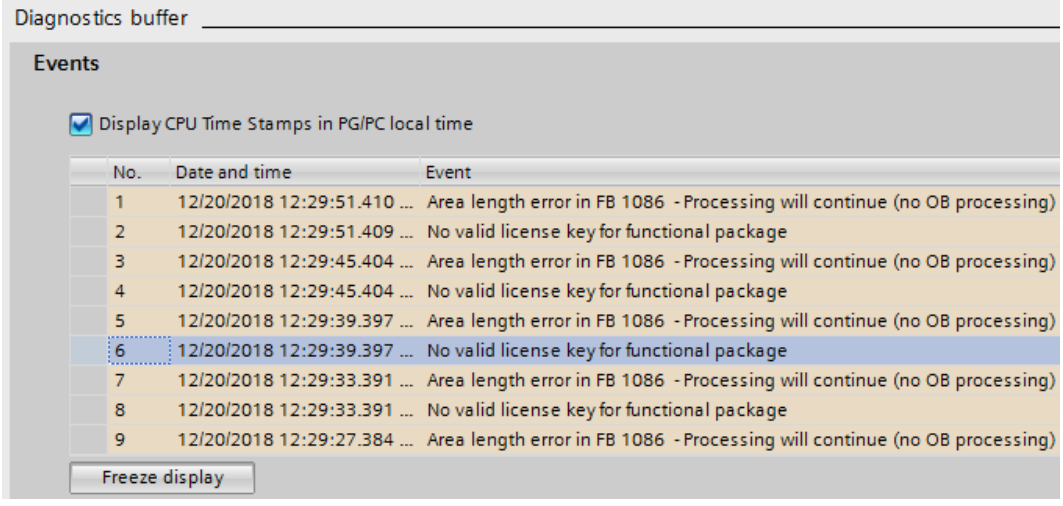
	Name	Data type	Offset	Start value
1	Static			
2	REG_KEY	String[17]	0.0	''

Figure 14-10 REG KEY

3. Copy the transmitted 17-digit registration key using copy/paste to the "Start value" column.
4. In the cyclic OB, enter the name of the license DB and the name of the string (for example, License_DB.REG_KEY) at the REG_KEY parameter of the MB_RED_CLIENT instruction.
5. Download the modified blocks to the CPU. You can enter the registration key during runtime; a change from STOP to RUN is not necessary.
6. The Modbus/TCP communication using the MB_RED_CLIENT instruction is now licensed for this CPU; the LICENSED output bit is TRUE.

Procedure for correcting missing or incorrect licensing:

- If you enter an incorrect registration key or no registration key, the ERROR LED of the CPU flashes. In addition, for the S7-1200, the CPU makes a cyclic entry in the diagnostics buffer regarding the missing license.



No.	Date and time	Event
1	12/20/2018 12:29:51.410 ...	Area length error in FB 1086 - Processing will continue (no OB processing)
2	12/20/2018 12:29:51.409 ...	No valid license key for functional package
3	12/20/2018 12:29:45.404 ...	Area length error in FB 1086 - Processing will continue (no OB processing)
4	12/20/2018 12:29:45.404 ...	No valid license key for functional package
5	12/20/2018 12:29:39.397 ...	Area length error in FB 1086 - Processing will continue (no OB processing)
6	12/20/2018 12:29:39.397 ...	No valid license key for functional package
7	12/20/2018 12:29:33.391 ...	Area length error in FB 1086 - Processing will continue (no OB processing)
8	12/20/2018 12:29:33.391 ...	No valid license key for functional package
9	12/20/2018 12:29:27.384 ...	Area length error in FB 1086 - Processing will continue (no OB processing)

Figure 14-11 Diagnostics buffer

- In the case of a missing or incorrect registration key, the CPU processes the Modbus TCP communication; however, the CPU always displays "W#16#0A90" (No valid license key for functional package) at the STATUS_x output. The LICENSED output bit is FALSE.

Input parameters: MB_MODE, MB_DATA_ADDR, MB_DATA_LEN, and MB_DATA_PTR

The combination of the MB_MODE, MB_DATA_ADDR, and MB_DATA_LEN parameters defines the function code used in the current Modbus message:

- **MB_MODE** contains the information on whether to read or to write:
  Read: MB_MODE = 0, 101, 102, 103 and 104
  Write: MB_MODE = 1, 2, 105, 106, 115 and 116 (Note: With MB_MODE = 2, there is not distinction between Modbus functions 15 and 05 or between Modbus functions 16 and 06.)
- **MB_DATA_ADDR** contains the information on what is to be read or written, as well as address information from which the MB_RED_CLIENT instruction calculates the remote address.
- **MB_DATA_LEN** contains the number of values to be read/written.

The following table shows the relationship between the input parameters MB_MODE, MB_DATA_ADDR, MB_DATA_LEN of the MB_RED_CLIENT instruction and the Modbus function:

MB_MODE	MB_DATA_ADDR	MB_DATA_LEN	Modbus function	Function and data type
0	1 to 9,999	1 to 2,000	01	Read 1 to 2,000 output bits on the remote address 0 to 9,998
0	10,001 to 19,999	1 to 2,000	02	Read 1 to 2,000 input bits on the remote address 0 to 9,998
0	• 40,001 to 49,999 • 400,001 to 465,535	1 to 125	03	• Read 1 to 125 holding registers on the remote address 0 to 9,998 • Read 1 to 125 holding registers on the remote address 0 to 65,534
0	30,001 to 39,999	1 to 125	04	Read 1 to 125 input words on the remote address 0 to 9,998
1	1 to 9,999	1	05	Write 1 output bit on the remote address 0 to 9,998
1	• 40,001 to 49,999 • 400,001 to 465,535	1	06	• Write 1 holding register on the remote address 0 to 9,998 • Write 1 holding register on the remote address 0 to 65,534
1	1 to 9,999	2 to 1,968	15	Write 2 to 1,968 output bits on the remote address 0 to 9,998
1	• 40,001 to 49,999 • 400,001 to 465,535	2 to 123	16	• Write 2 to 123 holding registers on the remote address 0 to 9,998 • Write 2 to 123 holding registers on the remote address 0 to 65,534
2	1 to 9,999	1 to 1,968	15	Write 1 to 1,968 output bits on the remote address 0 to 9,998
2	• 40,001 to 49,999 • 400,001 to 465,535	1 to 123	16	• Write 1 to 123 holding registers on the remote address 0 to 9,998 • Write 1 to 123 holding registers on the remote address 0 to 65,534

MB_MODE	MB_DATA_ADDR	MB_DATA_LEN	Modbus function	Function and data type
11	The instruction does not evaluate the MB_DATA_ADDR and MB_DATA_LEN parameters when this function is executed.		11	Read status word and event counter of the server: • The status word reflects the processing status (0 - not processing, 0xFFFF - processing). • The event counter is incremented when the Modbus request was executed successfully. If an error occurred during execution of a Modbus function, a message is sent by the server but the event counter is not incremented.
80	-	1	08	Check the server status with the diagnostic code 0x0000 (return loop test - the server sends the request back): 1 WORD per call
81	-	1	08	Reset the event counter of the server with the diagnostic code 0x000A: 1 WORD per call
101	0 to 65,535	1 to 2,000	01	Read 1 to 2,000 output bits on the remote address 0 to 65,535
102	0 to 65,535	1 to 2,000	02	Read 1 to 2,000 input bits on the remote address 0 to 65,535
103	0 to 65,535	1 to 125	03	Read 1 to 125 holding registers on the remote address 0 to 65,535
104	0 to 65,535	1 to 125	04	Read 1 to 125 input words on the remote address 0 to 65,535
105	0 to 65,535	1	05	Write 1 output bit on the remote address 0 to 65,535
106	0 to 65,535	1	06	Write 1 holding register on the remote address 0 to 65,535

MB_MODE	MB_DATA_ADDR	MB_DATA_LEN	Modbus function	Function and data type
115	0 to 65,535	1 to 1,968	15	Write 1 to 1,968 output bits on the remote address 0 to 65,535
116	0 to 65,535	1 to 123	16	Write 1 to 123 holding registers on the remote address 0 to 65,535
3 to 10, 12 to 79, 82 to 100, 107 to 114, 117 to 255				Reserved

Example:

Tag	Meaning
MB_MODE = 1 MB_DATA_ADDR = 1 MB_DATA_LEN = 1	Writes 1 output bit with function code 5, starting from the remote address 0.
MB_MODE = 1 MB_DATA_ADDR = 1 MB_DATA_LEN = 2	Writes 2 output bits with function code 15, starting from the remote address 0.
MB_MODE = 104 MB_DATA_ADDR = 17834 MB_DATA_LEN = 125	Reads 125 input words with function code 4, starting from the remote address 17.834.

MB_DATA_PTR:

The MB_DATA_PTR parameter is a pointer to a data buffer for the data to be received from the Modbus server or to be sent to the Modbus server. You can use a global data block or a memory area (M) as the data buffer.

For a buffer in the memory area (M), use a pointer in the ANY format as follows: P#"bit address" "data type" "length" (example: P#M1000.0 WORD 500)

Depending on the memory area in which the data buffer is located, MB_DATA_PTR can reference different data structures:

- When you use a global DB with optimized access, MB_DATA_PTR can reference a tag with elementary data type or an array of elementary data types. The following data types are supported:

Data type	Length in bits
Bool	1
Byte, SInt, USInt, Char	8
Word, Int, WChar, UInt	16
DWord, DInt, UDInt, Real	32

  You can use all supported data types for all Modbus functions. For example, MB_RED_CLIENT can also write a received bit in a tag of the byte type to a specified address without changing other bits in this byte. Therefore, it is not necessary to have an array of bits in order to execute bit-oriented functions.

- If you use a bit memory address area or a global DB with standard access as memory area, there is no longer any restriction to the elementary data types for MB_DATA_PTR; MB_DATA_PTR can then also reference complex data structures such as PLC data types (UDTs) and system data types (SDTs).

NOTE

Using a bit memory address area as data buffer

If you use a bit memory address area as data buffer for MB_DATA_PTR, you need to observe this variable. With the S7-1200 CPUs, it is 8 KB.

Output parameters: STATUS_x, RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR

The CPU displays error messages at the status outputs of the MB_RED_CLIENT instruction:

NOTE

You can display the error status codes as integer or hexadecimal values in the program editor:

1. Open the desired block in the programming editor.
2. Switch on the programming status by clicking "Monitor on/off". (If you have not already established an online connection, the "Go online" dialog opens. In this dialog, you can establish an online connection.)
3. Select the tag that you want to monitor and select the desired display format in the shortcut menu under "Display format".

- STATUS_x parameter (general status information):

STATUS (W#16#)	Description
0000	Instruction executed without errors.
0001	Connection established.
0003	Connection terminated.
0A90	The instruction MB_RED_CLIENT is not licensed. Refer to the "Licensing" section above for further information.
0AFF	The connection is not configured and is not used. The connection "0A" must be configured.
7000	No job active and no connection established (REQ=0, DISCONNECT=1).
7001	Connection establishment triggered.
7002	Intermediate call. Connection is being established.
7003	Connection is being terminated.
7004	Connection established and monitored. No job processing active.
7005	Data is being sent.
7006	Data is being received.

- STATUS_x parameter (protocol error)

STATUS (W#16#)	Description
80C8	No response of the server in the defined period. Check the connection to the Modbus server. This error is only reported on completion of the configured repeated attempts. If the MB_RED_CLIENT instruction does not receive an answer with the originally transferred transaction ID (see static tag MB_TRANSACTION_ID) within the defined period, this error code is output.
8380	Received Modbus frame has incorrect format or too few bytes were received.
8382	– The length of the Modbus frame in the frame header does not match the number of received bytes. – The number of bytes does not match the number of actually transmitted bytes (only functions 1-4). – The start address in the received frame does not match the saved start address (functions 5, 6, 15, and 16). – The number of words does not match the number of actually transmitted words (functions 15 and 16).
8383	Error reading or writing data or access outside the address area of MB_DATA_PTR. Refer to the "MB_DATA_PTR" section above for further information.
8384	– Invalid exception code received. – A different data value was received than was originally sent by the client (functions 5, 6, and 8) – Invalid status value received (function 11)
8385	– Diagnostics code not supported. – A different subfunction code was received than was originally sent by the client (function 8).
8386	Received function code does not match the one sent originally.
8387	The protocol ID of the Modbus TCP frame received by the server is not "0".
8388	The Modbus server sent a different data length than was processed. This error occurs only when using the Modbus functions 5, 6, 15, or 16.

- STATUS_x parameter (parameter error)

STATUS (W#16#)	Description
80B6	Invalid connection type; only TCP connections are supported.
80BB	The ActiveEstablished parameter has an invalid value. Only active connection establishment permitted for client (ActiveEstablished = TRUE).
8188	The MB_MODE parameter has an invalid value.
8189	Invalid addressing of data at the MB_DATA_ADDR parameter
818A	Invalid data length at the MB_DATA_LEN parameter

STATUS (W#16#)	Description
818B	The MB_DATA_PTR parameter has an invalid pointer. You should also check the values of the MB_DATA_ADDR and MB_DATA_LEN parameters. (Refer to the "MB_DATA_ADDR" section above for further information on the "MB_DATA_ADDR".)
818C	Timeout at parameter BLOCKED_PROC_TIMEOUT or RCV_TIMEOUT (see static tags of instruction). BLOCKED_PROC_TIMEOUT and RCV_TIMEOUT must be between 0.5 s and 55.0 s.
8200	– The CPU is currently processing a different Modbus request through the port. – Another instance of MB_RED_CLIENT with the same connection parameters is processing an existing Modbus request.

NOTE

Error codes of internally used communication instructions

With the MB_RED_CLIENT instruction, in addition to the errors listed in the tables, errors caused by the communication instructions (TCON, TDISCON, TSEND, TRCV, T_DIAG, and TRESET), used by the instruction, can occur.

The CPU assigns the error codes through the instance data block of the MB_RED_CLIENT instruction. The CPU displays the error codes for the respective instruction under STATUS in the "Static" section.

The meaning of the error codes is available in the documentation of the corresponding communications instruction.

NOTE

Communication error when sending or receiving data

If a communication error occurs when sending or receiving data, the CPU terminates the existing condition. Errors are as follows:

- 80C4 - Temporary communications error; the specified connection is temporarily terminated.
- 80C5 - The remote partner has actively terminated the connection.
- 80A1 - The specified connection is disconnected or is not yet established.

This means that you can see all returned STATUS values when the connection is terminated and that the STATUS code that caused the connection to be terminated is only output when the connection is terminated.

Example: If a temporary communication error occurs when data is received, the STATUS 7003 (ERROR=false) is output initially and then 80C4 (ERROR=true).

MB_RED_SERVER (Communicating over PROFINET as a Modbus TCP server)

You can use this instruction to establish a connection between an S7-1200 CPU and a device that supports the Modbus TCP protocol.

Table 14-73 MB_RED_SERVER instruction

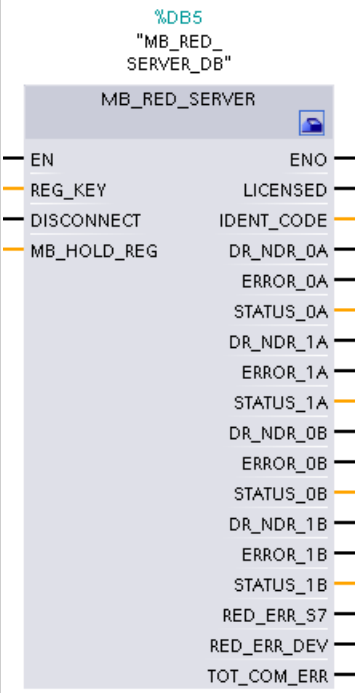
LAD / FBD	SCL	Description
	**"MB_RED_SERVER_DB"(DISCONNECT:=_bool_in_, LICENSED=>_bool_out_ IDENT_CODE=>_string_out_ DR_NDR_0A=>_bool_out, ERROR_0A=>_bool_out, STATUS_0A=>_word_out_, DR_NDR_1A=>_bool_out, ERROR_1A=>_bool_out, STATUS_1A=>_word_out_, DR_NDR_0B=>_bool_out, ERROR_0B=>_bool_out, STATUS_0B=>_word_out_, DR_NDR_1B=>_bool_out, ERROR_1B=>_bool_out, STATUS_1B=>_word_out_, RED_ERR_S7=>_bool_out_, RED_ERR_DEV=>_bool_out_, TOT_COM_ERR=>_bool_out_, MB_HOLD_REG:=_variant_inout_);**	The MB_RED_SERVER instruction communicates as a Modbus TCP server over the PROFINET connection. The instruction MB_RED_SERVER processes connection requests of a Modbus TCP client, receives and processes Modbus requests, and sends responses.

Table 14-74 Data types for the parameters

Parameter and type		Data type	Description
REG_KEY [1]	IN	STRING[17]	Registration code for licensing The MB_RED_SERVER instruction must be licensed on each CPU individually.
DISCONNECT	IN	Bool	You use the MB_RED_SERVER instruction to enter into a passive connection with a partner module. The server responds to a connection request from the IP addresses which are given in the connection descriptions as specified or unspecified. You can use this parameter to control when a connection request is accepted: • 0: The CPU establishes a passive connection when there is no communications connection. • 1: Initialization of the connection termination. If the input is set, the CPU processes no additional client requests, and termination of the connection is initiated. The value "0003" is output at the STATUS_x parameter after successful connection termination.

[1] Refer to the "Licensing" section below for further information.

[2] Refer to the "MB_HOLD_REG input parameter" section below for further information.

[3] Refer to the "Output parameters: ERROR_x, RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR" section below for further information.

Parameter and type		Data type	Description
MB_HOLD_REG [2]	IN_OUT	Variant	Pointer to the Modbus holding register of the MB_RED_SERVER instruction MB_HOLD_REG must always reference a memory area that is larger than two bytes. The holding register contains the values that a Modbus client can access by using the Modbus functions 3 (read), 6 (write), 16 (multiple write), and 23 (reading and writing in one job).
LICENSED [1]	OUT	Bool	• 0: Instruction is not licensed • 1: Instruction is licensed
IDENT_CODE [1]	OUT	STRING[18]	Identification for licensing. Use this string to request the REG_KEY registration code.
DR_NDR_0A	OUT	Bool	"Data Read" or "New Data Ready" to connection 0A: • 0: No new data • 1: New data read or written by the Modbus client
ERROR_0A	OUT	Bool	If an error occurs during a call of the MB_RED_SERVER instruction to connection 0A, the output of the ERROR_0A parameter is set to "1". Detailed information about the cause of the problem is indicated by the STATUS_0A parameter.
STATUS_0A [3]	OUT	Word	Detailed status information of the instruction on connection 0A.
DR_NDR_1A	OUT	Bool	"Data Read" or "New Data Ready" to connection 1A: • 0: No new data • 1: New data read or written by the Modbus client
ERROR_1A	OUT	Bool	If an error occurs during a call of the MB_RED_SERVER instruction to connection 1A, the output of the ERROR_1A parameter is set to "1". Detailed information about the cause of the problem is indicated by the STATUS_1A parameter.
STATUS_1A [3]	OUT	Word	Detailed status information of the instruction on connection 1A.
DR_NDR_0B	OUT	Bool	"Data Read" or "New Data Ready" to connection 0B: • 0: No new data • 1: New data read or written by the Modbus client
ERROR_0B	OUT	Bool	If an error occurs during a call of the MB_RED_SERVER instruction to connection 0B, the output of the ERROR_0B parameter is set to "1". Detailed information about the cause of the problem is indicated by the STATUS_0B parameter.
STATUS_0B [3]	OUT	Word	Detailed status information of the instruction on connection 0B.
DR_NDR_1B	OUT	Bool	"Data Read" or "New Data Ready" to connection 1B: • 0: No new data • 1: New data read or written by the Modbus client
ERROR_1B	OUT	Bool	If an error occurs during a call of the MB_RED_SERVER instruction to connection 1B, the output of the ERROR_1B parameter is set to "1". Detailed information about the cause of the problem is indicated by the STATUS_1B parameter.
STATUS_1B [3]	OUT	Word	Detailed status information of the instruction on connection 1B.

[1] Refer to the "Licensing" section below for further information.

[2] Refer to the "MB_HOLD_REG input parameter" section below for further information.

[3] Refer to the "Output parameters: ERROR_x, RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR" section below for further information.

Parameter and type		Data type	Description
RED_ERR_S7 [3]	OUT	Bool	• 0: No redundancy error in SIMATIC • 1: Redundancy error in SIMATIC
RED_ERR_S7 [3]	OUT	Bool	• 0: No redundancy error on side of link partner • 1: Redundancy error on side of link partner
RED_ERR_S7 [3]	OUT	Bool	• 0: At least 1 configured connection is established • 1: Complete loss of communication, all configured connections are terminated

[1] Refer to the "Licensing" section below for further information.

[2] Refer to the "MB_HOLD_REG input parameter" section below for further information.

[3] Refer to the "Output parameters: ERROR_x, RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR" section below for further information.

WARNING

Risks with access to the process image

Each Modbus TCP client has read and write access to the process image inputs and outputs, and to the data block or bit memory area defined by the Modbus holding register. Unauthorized read and write operations can change PLC variables into invalid values and disrupt process operations.

To reduce the risk of unauthorized access, restrict access to an IP address of a specific Modbus client. For information on additional industrial security measures that can be implemented, please visit the Siemens Industrial Cybersecurity Web site (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

Disruption of process operations can result in death, severe injury and/or property damage.

Multiple server connections

The CPUs can:

- Process multiple server connections
- Accept multiple connections from different clients, simultaneously, at one server port

The maximum number of connections depends on the CPU being used and can be found in the technical specifications of the CPU. The total number of connections of one CPU, including those of the Modbus TCP clients and server must not exceed the maximum number of supported connections.

In the case of server connections, remember the following rules:

- Each MB_RED_SERVER connection must use a unique instance DB.
- One unique connection/connection ID is required for each and every client that wants to connect to the server port.
- The connection IDs must be unique throughout the CPU.

Mapping of Modbus addresses to the process image

The MB_RED_SERVER instruction allows incoming Modbus functions (1, 2, 4, 5, and 15) direct read and write access to the process image inputs and outputs of the CPU (use of the data types BOOL and WORD).

For S7-1200-CPUs, the address space for the process image of the inputs and the process image of the outputs is 1 KB.
The following table shows the address space of the Modbus functions listed above:

Modbus function					
Function code	**Function**	**Data area**	**Address space**		
01	Read: Bits	Output	0	to	65.535
02	Read: Bits	Input	0	to	65.535
04	Read: WORD	Input	0	to	65.535
05	Write: Bit	Output	0	to	65.535
15	Write: Bits	Output	0	to	65.535

Incoming Modbus requests with the function codes 3, 6, 16, and 23 write or read the Modbus holding registers (you specify the holding register with the MB_HOLD_REG parameter or using Data_Area_Array).

Modbus functions

The following table lists all the Modbus functions that are supported by the MB_RED_SERVER instruction:

Function code	Description
01	Read output bits
02	Read input bits
03	Read a holding register
04	Read input words
05	Write an output bit
06	Write a holding register
08	Diagnostics function: • Echo test (subfunction 0x0000): The MB_RED_SERVER instruction receives a data word and returns this unchanged to the Modbus client. • Reset event counter (subfunction 0x000A): The MB_RED_SERVER instruction resets the following event counters: "Success_Count", "Xmt_Rcv_Count", "Exception_Count", "Server_Message_Count", and "Request_Count".
11	Diagnostics function: Fetch event counter of the communication The MB_RED_SERVER instruction uses an internal event counter for communication to record the number of successfully executed read and write requests sent to the Modbus server. The event counter is not incremented with the functions 8 or 11. The same holds true for requests that cause a communications error, for example, if a protocol error has occurred; the function code in the received Modbus request is not supported).
15	Write output bits
16	Write a holding register
23	Write a holding register and read a holding register with a request

Operation and redundancy

The communication nodes can be designed as standalone or redundant. If one of the partners is designed as standalone, we refer to it as single-sided redundancy. If both partners are designed redundantly, we refer to it as double-sided redundancy.

- Single-sided redundancy:
  - One connection each must be configured for each connection between the communication partners. The connection points of the **SIMATIC S7** are referred to as **0** and **1**; the connection points of the **communication partner** are referred to as **A** and **B**.

    The R-CPU or H-CPU 1 refers to the connection point 0, the R-CPU or H-CPU 2 refers to the connection point 1.
  - Configuration: If the S7 is designed redundantly, one connection is created from the S7 connection point 0 to junction A of the link partner (Connection from the S7 connection point **0** to the partner/node **A** => connection **0A**), and one connection from the S7 connection point 1 to junction A of the link partner (Connection from the S7 connection point **1** to the partner/node **A** => connection **1A**). The figure illustrates the connection designations:

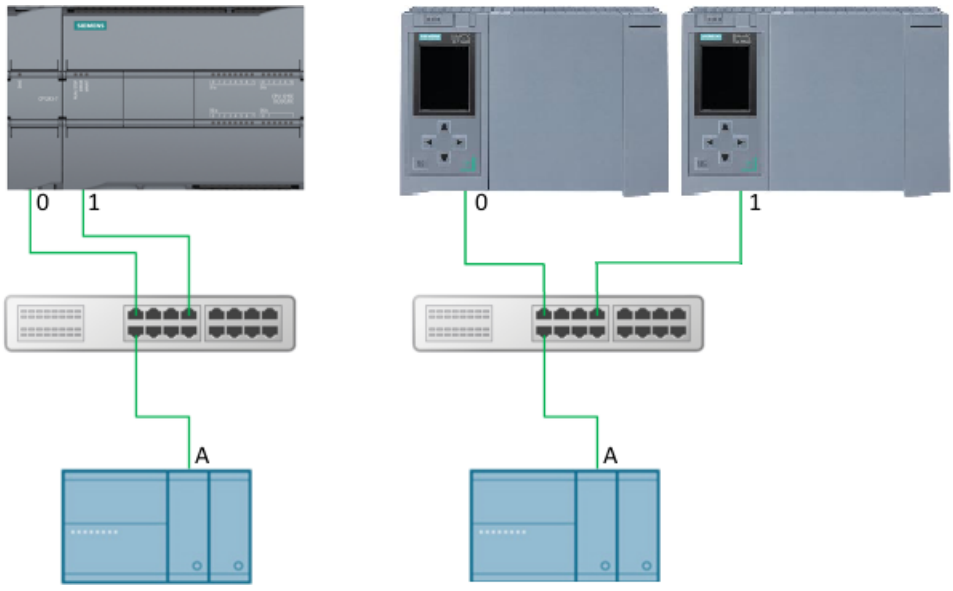


Figure 14-12 Single-sided redundancy S7

– If the S7 is designed as standalone and the link partner is designed redundantly, one connection is created from the S7 connection point 0 to junction A of the link partner (connection from the S7 connection point **0** to the partner/node **A** => connection **0A**), and one connection from the S7 connection point 0 to junction B of the link partner (connection from the S7 connection point **0** to the partner/node **B** => connection **0B**). The figure illustrates the connection designations:

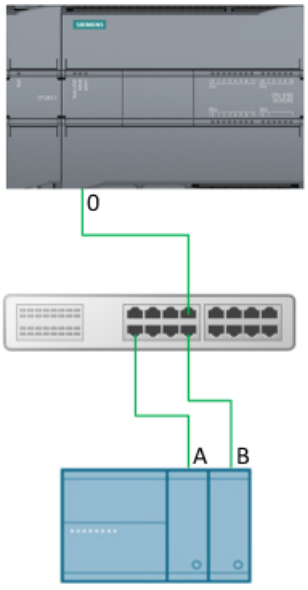


Figure 14-13 Single-sided redundancy partner

- Double-sided redundancy:
  - Description: One connection each must be configured for each connection between the communication partners. The connection points of the SIMATIC S7 are referred to as **0** and **1**; the connection points of the **communication partner** are referred to as **A** and **B**.

    The R-CPU or H-CPU 1 refers to the connection point 0, the R-CPU or H-CPU 2 refers to the connection point 1.
  - Configuration: In the case of double-sided redundancy, two connections are created from connection point 0 (connection from the S7 connection point **0** to the partner/node **A** => connection **0A** and connection from the S7 connection point **0** to the partner/node **B** => connection **0B**), and two connections from connection point 1 of the S7 to the junctions A and B of the link partner (connection from the S7 connection point **1** to the partner/node **A** => connection **1A** and connection from the S7 connection point **1** to the partner/node **B** => connection **1B**). The figure illustrates the connection designations:

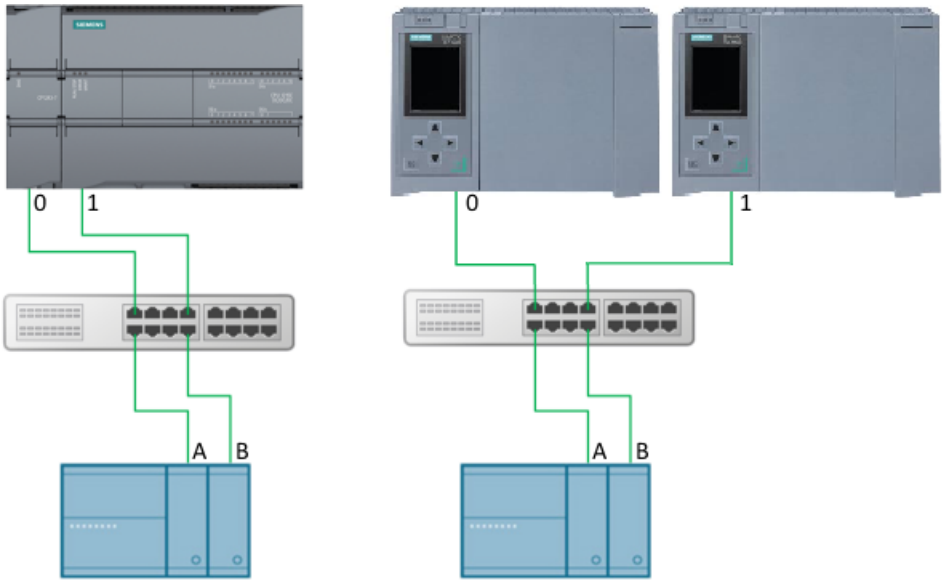


Figure 14-14 Double-sided redundancy

- Frame processing: Frames can be received through all configured connections. The client can send frames either through one connection or through all connections. If a frame was received on a connection, the CPU displays the status at the corresponding output DR_NDR_x or ERROR_x. Each connection runs independently and has no influence on the display of the other connections.

- Redundancy outputs RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR:
  - The redundancy bits RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR are set based on the states of the status outputs:

Number of faulty connections	STATUS_0A	STATUS_0B	STATUS_1A	STATUS_1B	RED_ERR_S7	RED_ERR_DEV	TOT_COM_ERR
0	okay	okay	okay	okay	FALSE	FALSE	FALSE
1	okay	okay	okay	Error	FALSE	FALSE	FALSE
	okay	okay	Error	okay	FALSE	FALSE	FALSE
	okay	Error	okay	okay	FALSE	FALSE	FALSE
	Error	okay	okay	okay	FALSE	FALSE	FALSE
2	okay	okay	Error	Error	TRUE	FALSE	FALSE
	okay	Error	okay	Error	FALSE	TRUE	FALSE
	Error	okay	okay	Error	FALSE	FALSE	FALSE
	okay	Error	Error	okay	FALSE	FALSE	FALSE
	Error	okay	Error	okay	FALSE	TRUE	FALSE
	Error	Error	okay	okay	TRUE	FALSE	FALSE
3	Error	Error	Error	okay	TRUE	TRUE	FALSE
	Error	Error	okay	Error	TRUE	TRUE	FALSE
	Error	okay	Error	Error	TRUE	TRUE	FALSE
	okay	Error	Error	Error	TRUE	TRUE	FALSE
4	Error	Error	Error	Error	TRUE	TRUE	TRUE

Figure 14-15 Display of the interrupt bits for redundancy setup on both sides

Number of faulty connections	STATUS_0A	STATUS_0B	STATUS_1A	STATUS_1B	RED_ERR_S7	RED_ERR_DEV	TOT_COM_ERR
0	okay	0AFF	okay	0AFF	FALSE	FALSE	FALSE
1	okay	0AFF	Error	0AFF	TRUE	TRUE	FALSE
	Error	0AFF	okay	0AFF	TRUE	TRUE	FALSE
2	Error	0AFF	Error	0AFF	TRUE	TRUE	TRUE

Figure 14-16 Display of the interrupt bits for redundancy setup on one side

NOTE

Port numbers for client and server

The Modbus client uses a port number starting at 2000. The Modbus server is usually addressed over the port number 502. Depending on the CPU, it is possible to configure port 502 for multiple connections (Multiport). If the local port 502 was configured for two or more connections, the requesting clients are randomly distributed to the existing server connections in the case of unspecified connections. The first client that wants to connect to the "MB_RED_SERVER" instruction is not automatically assigned the connection 0A. Once the assignment of the client requests to the server connections has taken place, the assignment remains intact during the frame exchange until the connection is terminated.

Parameter assignment

You can use the MB_RED_SERVER instruction **V1.0** and **V1.1** for S7-1200. The CPU implements the connections over the local interface of the CPU or CM/CP. The CPU configures and establishes the connections using the TCON_IP_V4 structure.

Configuration of MB_RED_SERVER: You make the following settings using the configuration dialog of the MB_RED_SERVER instruction:

- Connection parameters for the connections 0A, 1A, 0B and 1B (Refer to "Operation and Redundancy", above, for more information on redundancy configuration.)
- Internal parameter (optional)

You can open the configuration dialog with the MB_RED_SERVER instruction or through the technology objects:

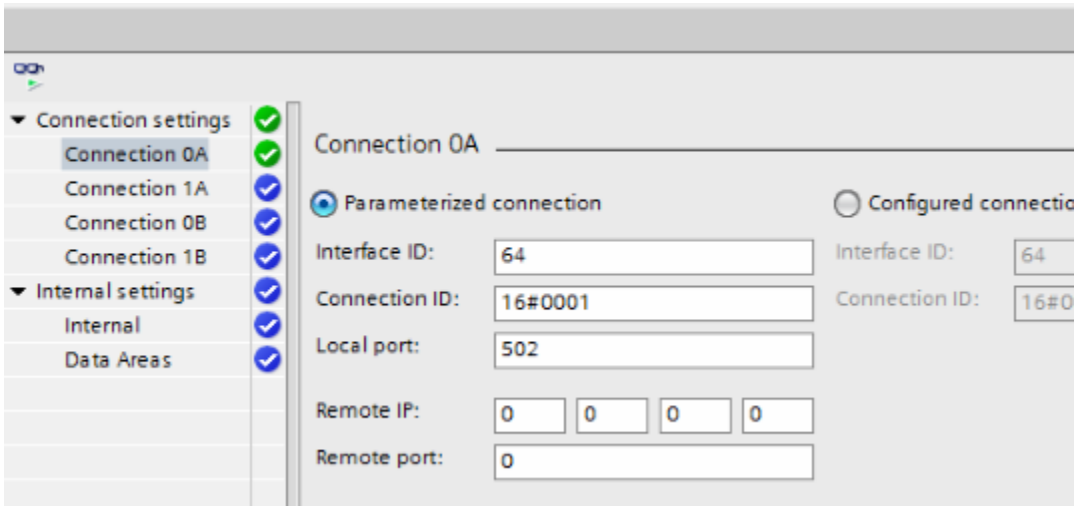


Figure 14-17 Parameterized server connection

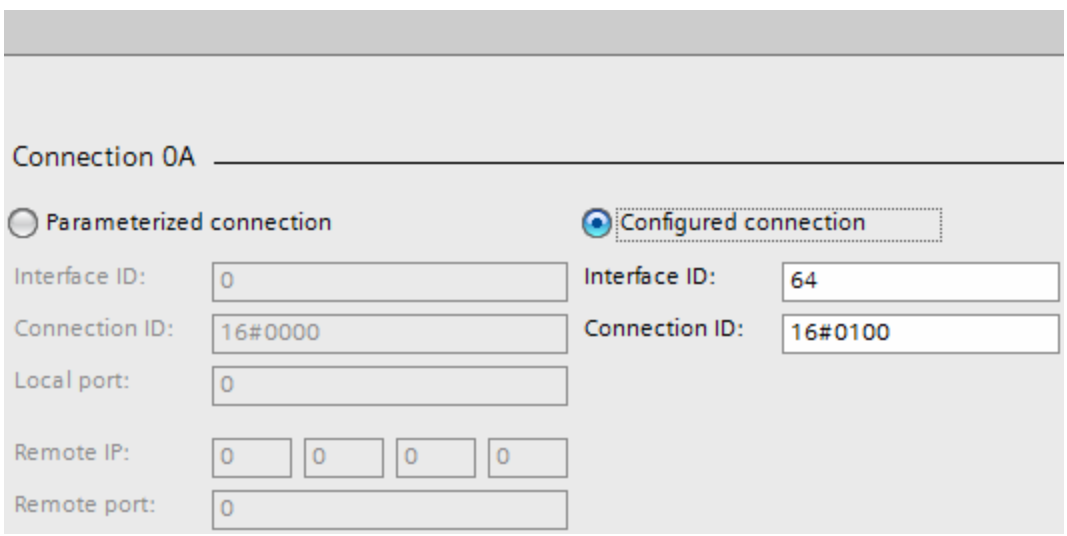


Figure 14-18 Configured server connection

Tag	Start value	Description
Configured connections		
Interface ID	64	HW identifier of the PN interface used
Connection ID	16#0000	Connection IDs for the connections used. These connection IDs must be unique throughout the CPU.
Local port	502	Local port number of the server block. The default port for Modbus/TCP server is 502.
Remote IP	0.0.0.0	Remote IP address of the client. By default, no IP address is entered for the client.
Remote port	0	Remote port number of the client. By default, no port number is entered for the client.
Configured connections		
Interface ID	64	HW identifier of the PN interface used
Connection ID	16#0000	Connection IDs for the connections used. These connections are configured in the network view.

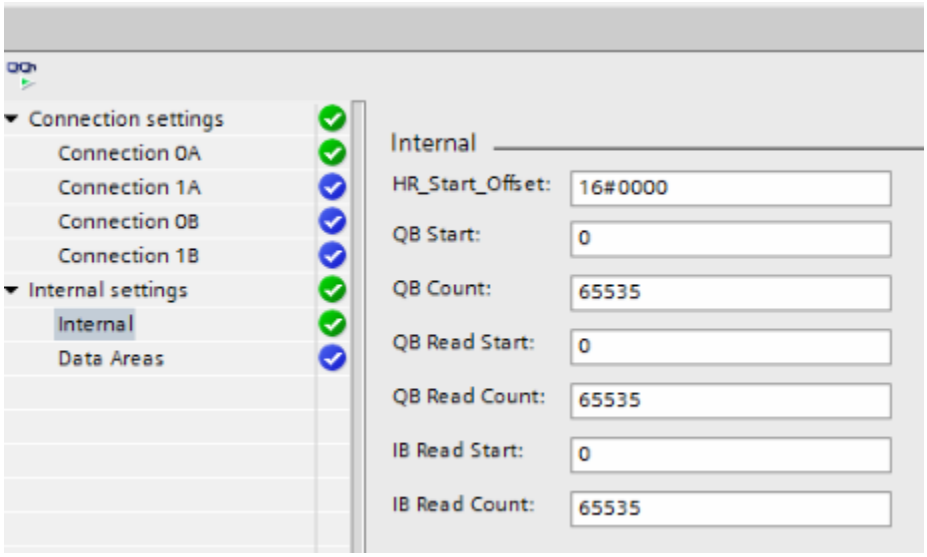


Figure 14-19 Internal parameter (optional)

Tag	Data type	Start value	Description
HR_Start_Offset	WORD	0	Assign the start address of the Modbus holding register.
QB_Start	UINT	0	Start address of the permitted addressing range of the outputs that the Modbus master can write to (bytes 0 to 65535)
QB_Count	UINT	0	Number of output bytes that the Modbus master can write to. *Example:* • QB_Start=0 and QB_Count=10: The Modbus master can write to output bytes 0 to 9. • QB_Count=0: The Modbus master cannot write to any output byte.

Tag	Data type	Start value	Description
QB_Read_Start	UINT	0	Start address of the permitted addressing range of the outputs that the Modbus master can read (bytes 0 to 65535)
QB_Read_Count	UINT	0	Number of output bytes that the Modbus master can read. *Example:* • QB_Read_Start=0 and QB_Read_Count=10: The Modbus master can read output bytes 0 to 9. • QB_Read_Count=0: The Modbus master cannot read any output byte.
IB_Read_Start	UINT	0	Start address of the permitted addressing range of the inputs that the Modbus master can read (bytes 0 to 65535)
IB_Read_Count	UINT	0	Number of input bytes that the Modbus master can read. *Example:* IB_Read_Start=0 and IB_Read_Count=10: The Modbus master can read input bytes 0 to 9. IB_Read_Count=0: The Modbus master cannot read any input byte.
Data_Area_Array	ARRAY [1..8]		
data_type	UINT	0	Data Type: 0 to 4
db	UINT	0	Data block number
start	UINT	0	First Modbus address in the data block
length	UINT	0	Number of Modbus values in the data block

Addressing using the HR_Start_Offset static tag

The addresses of the Modbus holding register start at 0.

Example: The holding register begins at MW100 and has a length of 100 words.

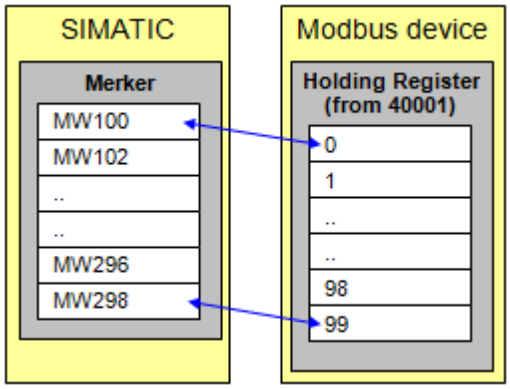


Figure 14-20 HR_Start_Offset_0

You can define the HR_Start_Offset tag so that the Modbus holding register has a start address other than 0.

Example: An offset value of 20 in the HR_Start_Offset parameter means that the start address of the holding register is moved from 0 to 20. This causes an error whenever you address the holding register below the address 20 and above the address 119.

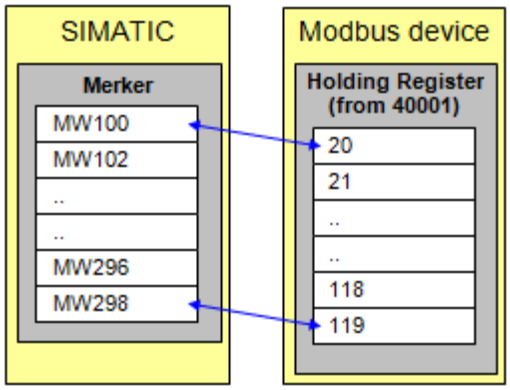


Figure 14-21 HR_Start_Offset_20

Data_Area_Array [1..8]

There are eight data areas available for mapping the MODBUS addresses in the SIMATIC S7 memory. If the data area is defined with the "Holding Register" data type, the MB_HOLD_REG parameter is not evaluated. Instead, the Modbus master writes or reads the Modbus register and bits in the data blocks depending on the job type. The CPU can further process these values in the subsequent execution of the program.

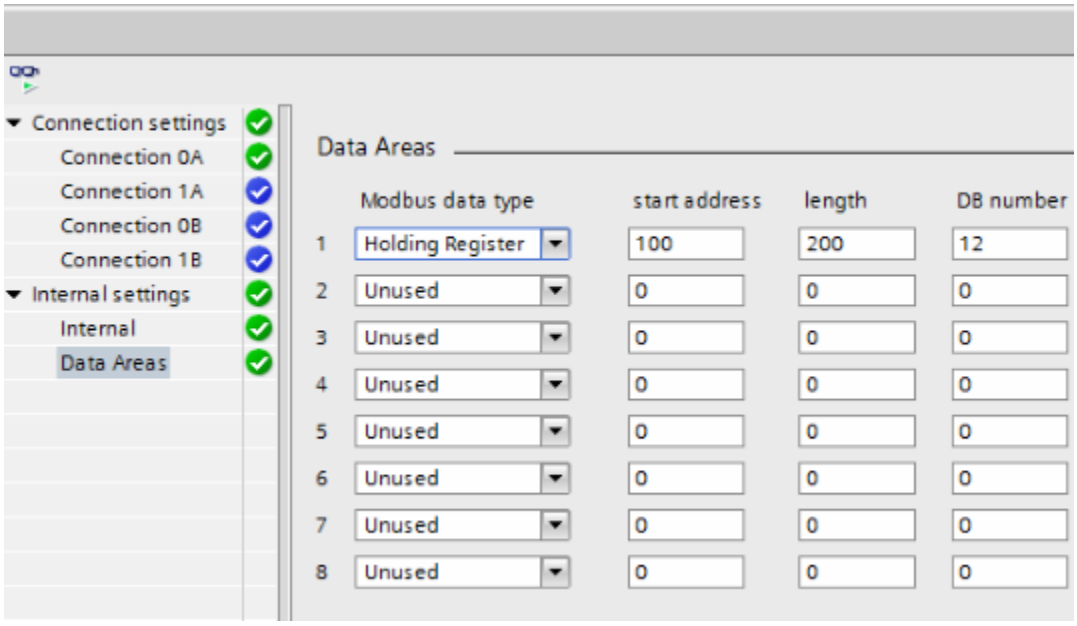


Figure 14-22 Server data areas

You can only read from one DB or write to one DB with any job. Access to registers or bit values that are located in several DBs, even if the numbers are in a sequence without gaps, are to be divided into two jobs. Keep this in mind during configuration. It is possible to map more Modbus areas (registers or bit values) in one data block than the Modbus master can process with one frame.

data_type

The data_type parameter specifies which MODBUS data types the Modbus master maps in this data block. If the value "0" is entered in data_type, the Modbus master does not use the corresponding data area. If the Modbus master is to use multiple Data_Area, you must define these one after the other. The Modbus master does not process any entries after a data_type = 0.

Identifier	Data type	Description
0	Area not used	
1	Output bits (Coils)	Bit
2	Input bits (Inputs)	Bit
3	Holding register	Word
4	Input words (Input Register)	Word

db

The db parameter specifies the data block which maps the MODBUS registers or bit values defined below. The CPU does not permit the DB number 0 because it is reserved for the system.

start, length

start specifies the first Modbus address which the Modbus master maps in data word 0 of the DB. The parameter length defines the length of how many MODBUS addresses the Modbus master maps in the data block. The defined data areas must not overlap. The length parameter must not be 0.

Example: Address mapping with Data_Area_Array

Data area 1	data_type	3: Holding register
	db	11
	start	0
	length	500
Data area 2	data_type	3: Holding register
	db	12
	start	720
	length	181
Data area 3	data_type	4: Input words
	db	13
	start	720
	length	281
Data area 4	data_type	1: Output bits
	db	14
	start	640
	length	611
Data area 5	data_type	2: Input bit
	db	15
	start	1700
	length	601

Data area 6	data_type	1: Output bits
	db	16
	start	1700
	length	601
Data area 7	data_type	Not used
	db	0
	start	0
	length	0
Data area 8	data_type	Not used
	db	0
	start	0
	length	0

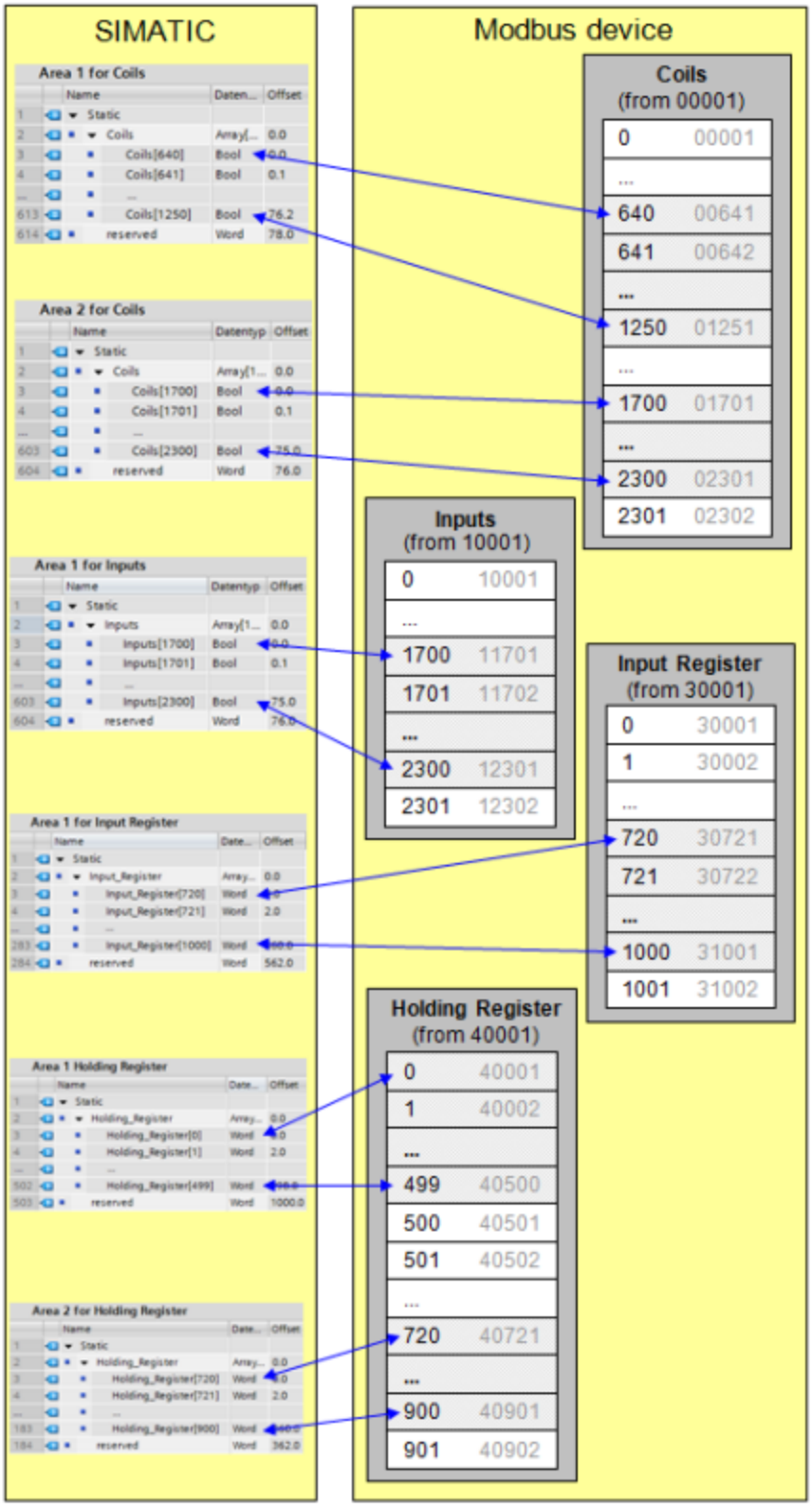


Figure 14-23 Address building

Licensing

The MB_RED_SERVER instruction is subject to a fee, and you must license the instruction on each CPU individually. Licensing takes place in two steps:

- Displaying the license IDENT_CODE
- Entering the REG_KEY registration key: You must assign the REG_KEY registration key at each MB_RED_SERVER instruction. Save the REG_KEY in a global data block from which all MB_RED_SERVER instructions receive the necessary registration key.

Procedure for displaying the license IDENT_CODE:

1. Assign parameters to the MB_RED_SERVER instruction in line with your requirements in a cyclic OB. Download the program to the CPU and set the CPU to RUN.
2. Open the instance DB of the Modbus instruction, and click the "Monitor all" button.
3. The instance DB displays an 18-digit character string at the IDENT_CODE output.

	Name	Data type	Start value	Monitor value
1	Input			
2	REG_KEY	String[17]	''	''
3	USE_ALL_CONN	Bool	false	FALSE
4	REQ	Bool	false	FALSE
5	DISCONNECT	Bool	false	FALSE
6	MB_MODE	USInt	0	0
7	MB_DATA_ADDR	UDInt	0	0
8	MB_DATA_LEN	UInt	0	0
9	Output			
10	LICENSED	Bool	false	FALSE
11	IDENT_CODE	String[18]	''	'RTPCFIGDCDIIHJHAH4'
12	DONE	Bool	false	FALSE
13	BUSY	Bool	false	FALSE
14	ERROR	Bool	false	FALSE

Figure 14-24 License

4. Copy this string using copy/paste from the data block and paste it in the form (that was sent to you by email after you ordered the product or is included on the CD).
5. Send the form to Customer support (https://support.industry.siemens.com/my/ww/en/requests/#createRequest) using a service request. You will then receive the registration key for your CPU.

Procedure for entering the registration key REG_KEY:

1. Insert a new global data block with a unique symbolic name, for example "License_DB", using "Add new block...".
2. Create a REG_KEY parameter in this block with the data type STRING[17].

LICENSE_DB

	Name	Data type	Offset	Start value
1	Static			
2	REG_KEY	String[17]	0.0	''

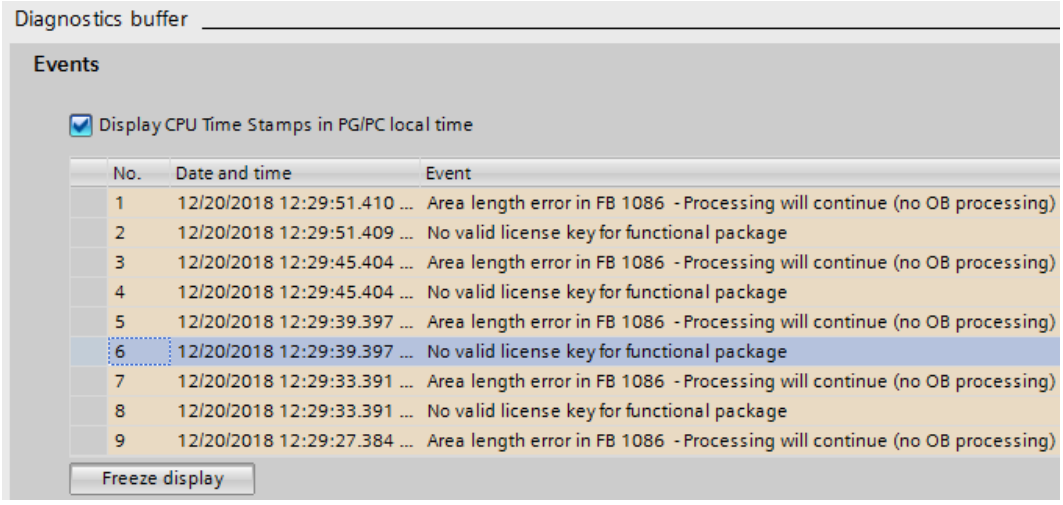
Figure 14-25 REG_KEY

3. Copy the transmitted 17-digit registration key using copy/paste to the "Start value" column.
4. In the cyclic OB, enter the name of the license DB and the name of the string (for example, License_DB.REG_KEY) at the REG_KEY parameter of the MB_RED_SERVER instruction.

5. Download the modified blocks to the CPU. You can enter the registration key during runtime; a change from STOP to RUN is not necessary.
6. The Modbus/TCP communication using the MB_RED_SERVER instruction is now licensed for this CPU; the LICENSED output bit is TRUE.

Procedure for correcting missing or incorrect licensing:

- If you enter an incorrect registration key or no registration key, the ERROR LED of the CPU flashes. In addition, for the S7-1200, the CPU makes a cyclic entry in the diagnostics buffer regarding the missing license.



No.	Date and time	Event
1	12/20/2018 12:29:51.410 ...	Area length error in FB 1086 - Processing will continue (no OB processing)
2	12/20/2018 12:29:51.409 ...	No valid license key for functional package
3	12/20/2018 12:29:45.404 ...	Area length error in FB 1086 - Processing will continue (no OB processing)
4	12/20/2018 12:29:45.404 ...	No valid license key for functional package
5	12/20/2018 12:29:39.397 ...	Area length error in FB 1086 - Processing will continue (no OB processing)
6	12/20/2018 12:29:39.397 ...	No valid license key for functional package
7	12/20/2018 12:29:33.391 ...	Area length error in FB 1086 - Processing will continue (no OB processing)
8	12/20/2018 12:29:33.391 ...	No valid license key for functional package
9	12/20/2018 12:29:27.384 ...	Area length error in FB 1086 - Processing will continue (no OB processing)

Figure 14-26 Diagnostic_buffer

- In the case of a missing or incorrect registration key, the CPU processes the Modbus TCP communication; however, the CPU always displays "W#16#0A90" (No valid license key for functional package) at the STATUS_x output. The LICENSED output bit is FALSE.

MB_HOLD_REG input parameter

The MB_HOLD_REG parameter is a pointer to a data buffer for storing the data to which a Modbus client has read or write access. You can use a global data block (D) or bit memory (M) as memory area:

- The high limit for the number of addresses in the data block (D) is determined by the maximum size of a DB of your CPU.
- The high limit for the number of bit memories (M) is determined by the maximum bit memory area of your CPU.

The following figures show some examples of mapping Modbus addresses to the holding register for the Modbus functions 3 (read multiple WORD), 6 (write one WORD), 16 (write multiple WORD), and 23 (write and read multiple WORD).

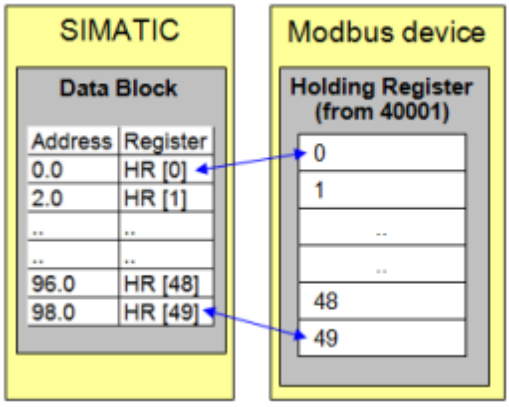


Figure 14-27 MB_HOLD_REG: Data block with offset 0

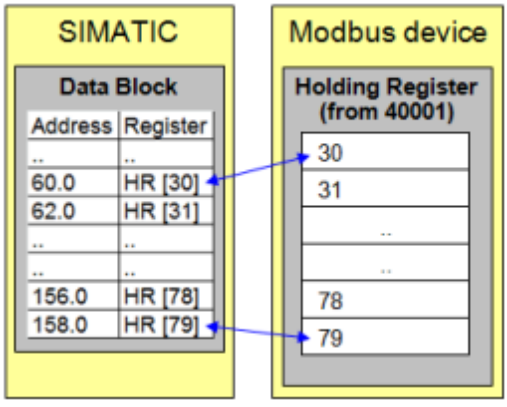


Figure 14-28 MB_HOLD_REG: Data block with offset 60

Data_Area_Array [1..8]: To use the optional parameters Data_Area_Array [1..8], refer to the "Parameter assignment" section above.

Output parameters: ERROR_x, STATUS_x, RED_ERR_S7, RED_ERR_DEV, and TOT_COM_ERR

The CPU displays error messages at the status outputs of the MB_RED_SERVER instruction:

NOTE

You can display the error status codes as integer or hexadecimal values in the program editor:

1. Open the desired block in the programming editor.
2. Switch on the programming status by clicking "Monitor on/off". (If you have not already established an online connection, the "Go online" dialog opens. In this dialog, you can establish an online connection.)
3. Select the tag that you want to monitor and select the desired display format in the shortcut menu under "Display format".

STATUS_x parameter (general status information):

STATUS (W#16#)	Description
0000	Instruction executed without errors.
0001	Connection established.
0003	Connection terminated.
0A90	The instruction MB_RED_SERVER is not licensed. Refer to the "Licensing" section above for further information.
0AFF	The connection is not configured and is not used. The connection 0A must be configured.
7000	No call active and no connection established (REQ=0, DISCONNECT=1).
7001	First call. Connection establishment triggered.
7002	Intermediate call. Connection is being established.
7003	Connection is being terminated.
7005	Data is being sent.
7006	Data is being received.

STATUS_x parameter (protocol error)

STATUS (W#16#)	Error code in the error message from MB_RED_SERVER(B#16#)	Description
8380	-	Received Modbus frame has incorrect format or too few bytes were received.
8381	01	Function code is not supported.
8382	03	Error in data length: • Invalid length specification in received Modbus frame • The frame length entered in the header of the Modbus frame does not match the number of actually received bytes. • The number of bytes entered in the header of the Modbus frame does not match the number of actually received bytes (functions 15 and 16).
8383	02	Error in data address or access outside the address area of the holding register (MB_HOLD_REG parameter). Refer to the "MB_HOLD_REG" section above for further information.
8384	03	Error in the data value (function 05)
8385	03	Diagnostic code is not supported (only with function 08).

STATUS_x parameter (parameter error)

STATUS (W#16#)	Description
80BB	The ActiveEstablished parameter has an invalid value Only passive connection establishment permitted for server (active_established = FALSE).
8187	The MB_HOLD_REG parameter has an invalid pointer. Data area is too small.
8389	Invalid data area definition: • Invalid data_type value • DB number invalid or does not exist: – Invalid db value – DB number does not exist – DB number is already used by another data area – DB with optimized access – DB is not located in the work memory • Invalid length value • Overlapping of MODBUS address ranges that belong to the same MODBUS data type

NOTE

Error codes of internally used communication instructions

With the MB_RED_SERVER instruction, in addition to the errors listed in the tables, errors caused by the communication instructions ("TCON", "TDISCON", "TSEND", "TRCV", "T_DIAG" and "T_RESET") used by the instruction can occur.

The error codes are assigned via the instance data block of the MB_RED_SERVER instruction. The error codes are displayed for the respective instruction under STATUS in the "Static" section of the individual instances.

The meaning of the error codes is available in the documentation of the corresponding communications instruction.

NOTE

Communication error when sending or receiving data

If a communication error occurs when sending or receiving data, the CPU terminates the existing condition. Errors are as follows:

- 80C4 - Temporary communications error; the specified connection is temporarily terminated.
- 80C5 - The remote partner has actively terminated the connection.
- 80A1 - The specified connection is disconnected or is not yet established.

This also means that you can see all STATUS values that are returned when the connection is terminated and that the STATUS code that caused the connection to be terminated is only output when the connection is terminated.

Example: If a temporary communication error occurs when data is received, the STATUS 7003 (ERROR=false) is output initially and then 80C4 (ERROR=true).

14.5.2.3 Modbus TCP examples

Example: MB_SERVER Multiple TCP connections

You can have multiple Modbus TCP server connections. To accomplish this, MB_SERVER must be independently executed for each connection. Each connection must use an independent instance DB, connection ID, and IP port. The S7-1200 allows only one connection per IP port.

For best performance, MB_SERVER should be executed every program cycle, for each connection.

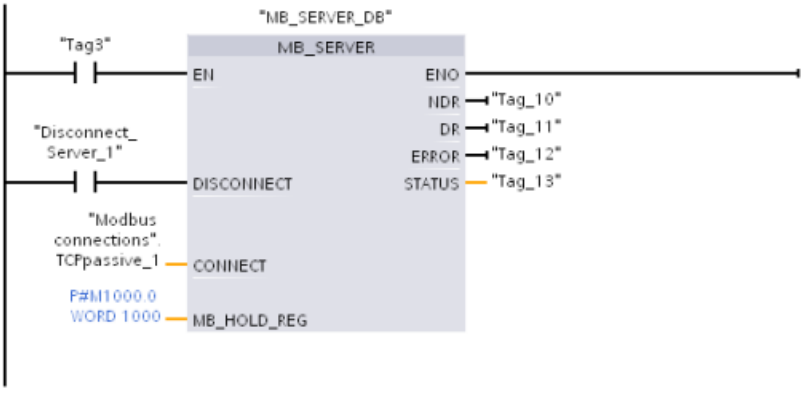
The CONNECT parameter uses system data type TCON_IP_V4. For the example, these data structures are in a DB named "Modbus connections". The "Modbus connections" DB contains two TCON_IP_V4 structures "TCPpassive_1" (for connection 1) and "TCP_passive_2" (for connection 2).The connection properties ID and LocalPort described in the network comments are data elements stored in the CONNECT data structure.

The TCON_IP_V4 CONNECT data also contains an IP address in the RemoteAddress ADDR array. IP address assignments within TCPpassive_1 and TCP_passive_2 do not affect the establishment of TCP server connections, but determine which Modbus TCP clients are allowed to communicate though the connections to each MB_SERVER. MB_SERVER passively listens for a Modbus client message and compares the incoming message IP address with the IP address stored in the corresponding RemoteAddress ADDR array.

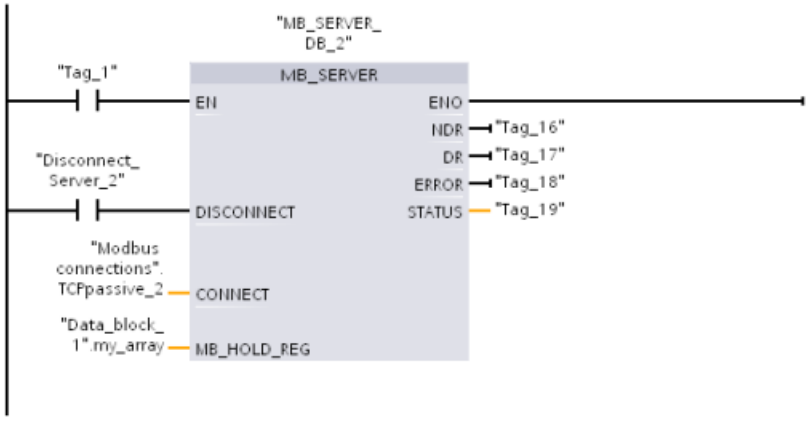
Three MB_SERVER IP address variations are possible for the two MB_SERVER instructions:

- **IP address = 0.0.0.0**
  Each MB_SERVER will respond to all Modbus TCP clients using any IP address.
- **IP address = Same IP address in TCPpassive_1 and TCPpassive_2**
  Both MB_SERVER connections only respond to Modbus clients originating from this IP address.
- **IP address = Different IP number in TCP_passive_1 and TCP_passive_2**
  Each MB_SERVER only responds to Modbus clients that originate from the IP address stored in their TCON_IP_V4 data.

Network 1: Connection #1, Instance DB = "MB_SERVER_DB", within "Modbus connections.TCPpassive_1" (ID = 1 and LocalPort = 502)



Network 2: Connection #2, Instance DB = "MB_SERVER_DB_1, within "Modbus connections.TCPpassive_2" (ID = 2 and LocalPort = 503)



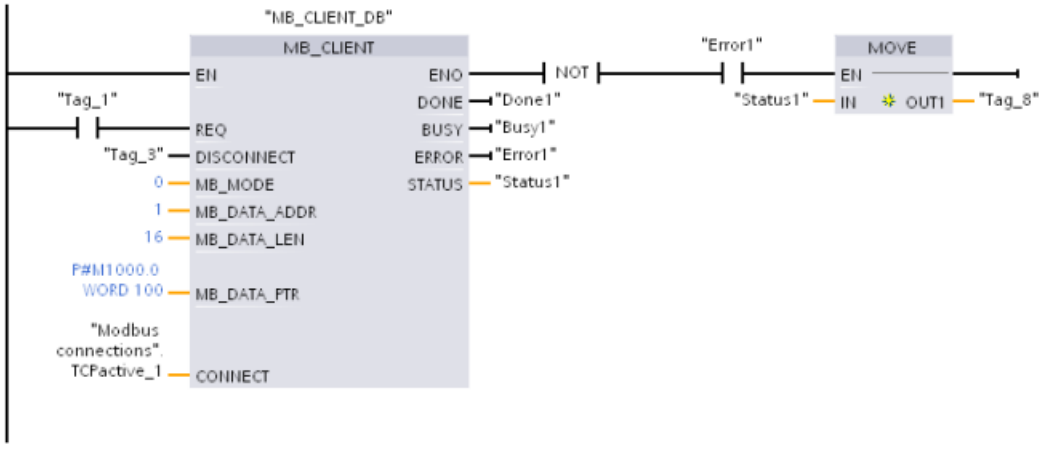
Example: MB_CLIENT 1: Multiple requests with common TCP connection

Multiple Modbus client requests can be sent over the same connection. To accomplish this, use the same instance DB, connection ID, and port number.

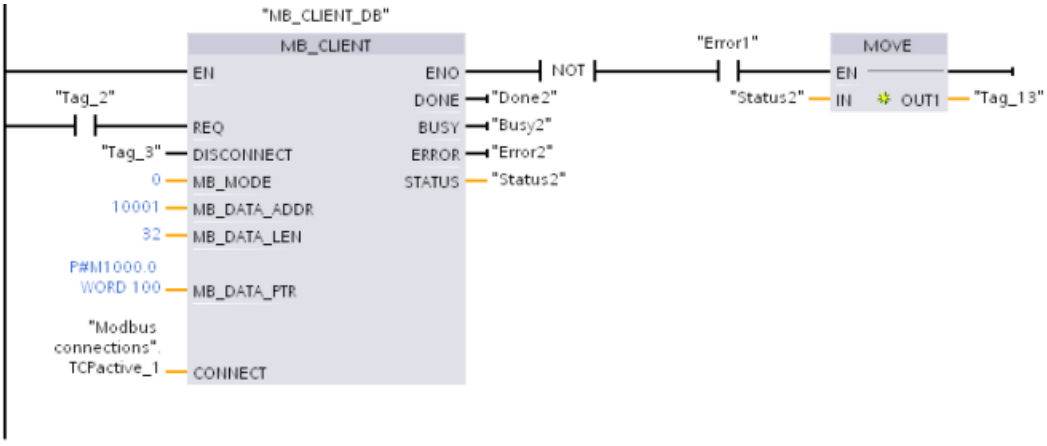
Because both MB_CLIENT boxes use the same CONNECT parameter TCON_IP_v4 data structure ("Modbus_connections".TCPactive_1), the connection ID, port number, and IP address are identical. The CONNECT IP address data assigns the IP address, of the target Modbus TCP server.

Only one MB_CLIENT can be active at any given time. Once a client completes its execution, the next client can begin execution. Your program logic is responsible for the execution sequence logic. The example shows both clients reading remote data from a single Modbus client and transferring the data to the Modbus client's CPU (M memory starting at M1000.0). A returned error is captured, which is optional.

Network 1: Modbus function 1 - Read 16 output bits from a Modbus TCP server with the IP address assigned in "Modbus connections".TCPactive_1.



Network 2: Modbus function 2 - Read 32 input bits from a Modbus TCP server with the IP address assigned in "Modbus connections".TCPactive_1.



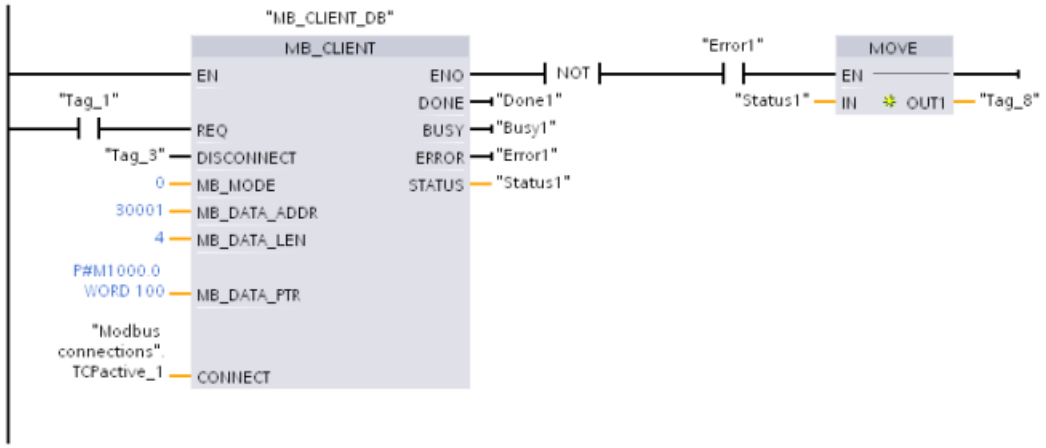
Example: MB_CLIENT 2: Multiple requests with different TCP connections

Modbus TCP client requests can be sent over different connections. To accomplish this, different instance DBs and connection IDs must be used.

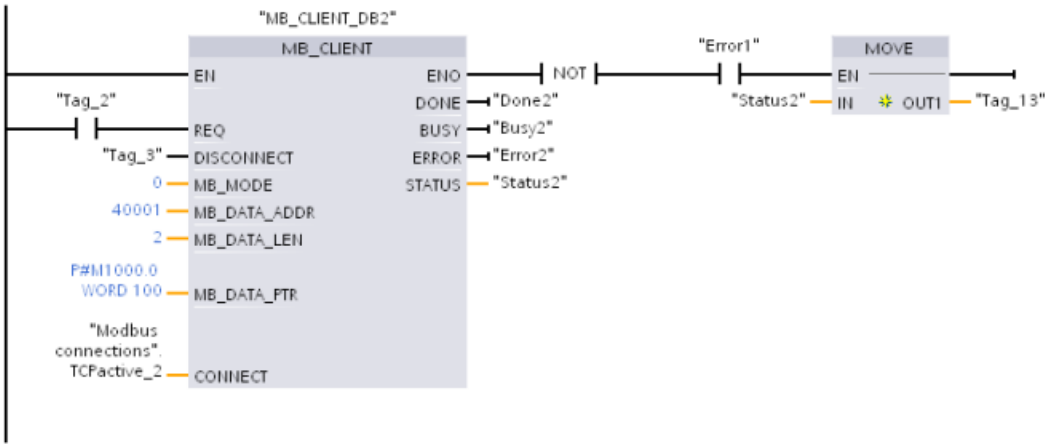
The RemotePort (IP port) number must be different, if the connections are established to the same Modbus server. If the connections are on different servers, there is no IP port number restriction.

The example shows two Modbus TCP clients transferring remote data from two different Modbus TCP servers to the same local CPU memory area, starting at address M1000.0. Also, a returned error is captured which is optional.

Network 1: Modbus function 4 - Read input process image words from a Modbus TCP server CONNECT parameter = "Modbus connections".TCPactive_1: Connection **ID** = 1, **RemoteAddress** = 192.168.2.241, **RemotePort** = 502



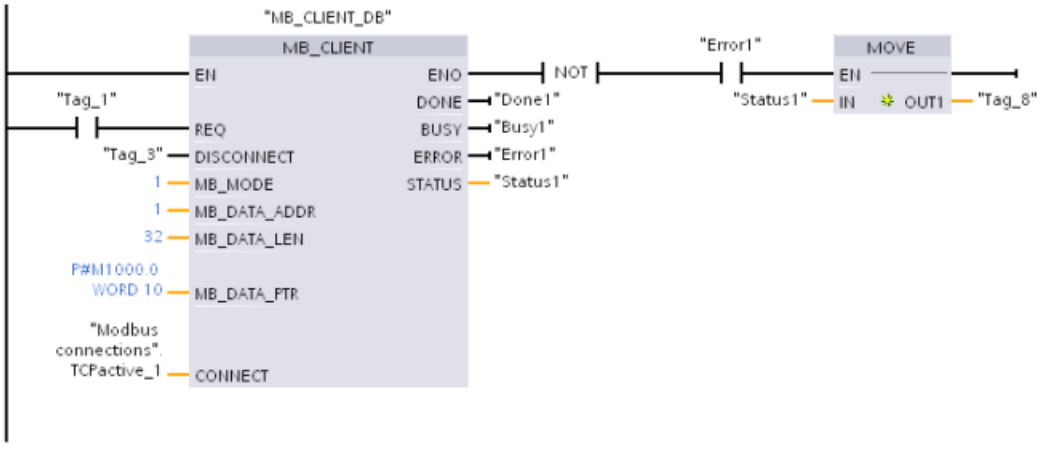
Network 2: Modbus function 3 - Read holding register words from a Modbus TCP server
CONNECT parameter = "Modbus connections".TCPactive_2: Connection **ID** = 2, **RemoteAddress** = 192.168.2.242, **RemotePort** = 502



Example: MB_CLIENT 3: Output image write request

This example shows a Modbus client request that transfers bit data from local CPU memory (starting at M1000.0) to a remote Modbus TCP server.

Network 1: Modbus function 15 - Write output bits in a Modbus server

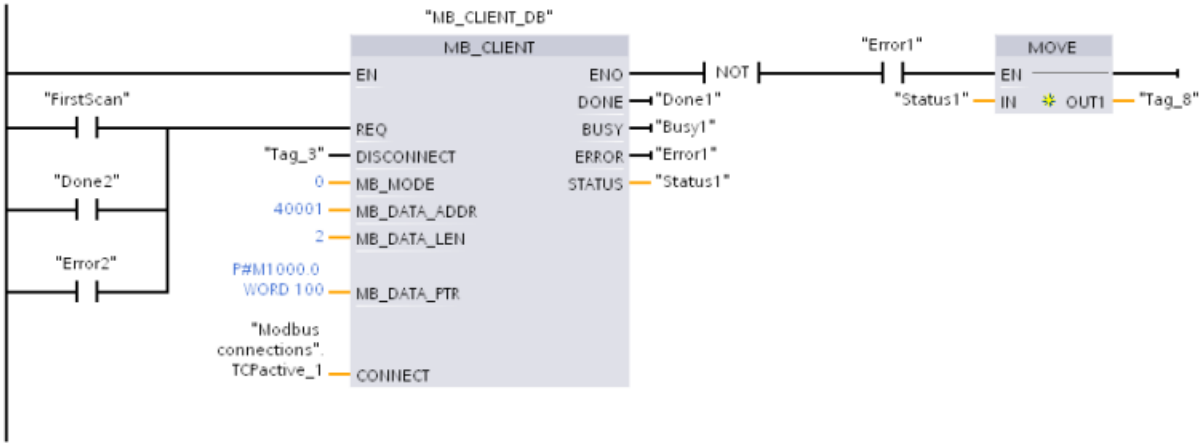


Example: MB_CLIENT 4: Coordinating multiple requests

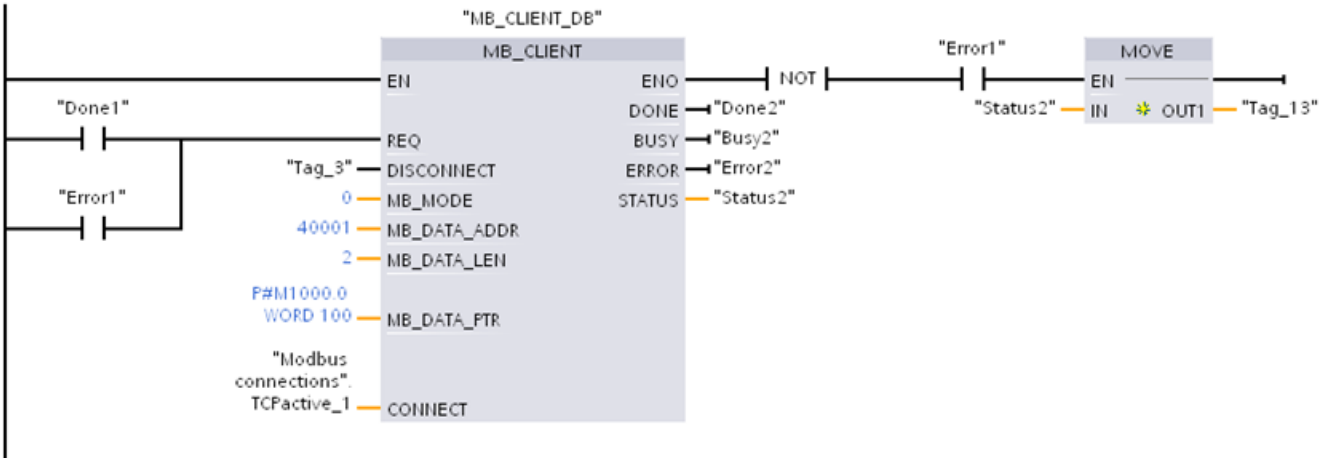
You must ensure that each individual Modbus TCP request finishes execution. The execution sequence must be controlled by your program logic. The example below shows how the outputs of the first and second client requests can control the execution sequence.

The example shows both clients using the same CONNECT connection data (used at different times). The clients transfer holding register data from the same remote Modbus TCP server to the same local CPU memory M address. Also, a returned error is captured which is optional.

Network 1: Modbus function 3 - Read Modbus TCP server holding register words



Network 2: Modbus function 3 - Read Modbus TCP server holding register words



14.5.3 Modbus RTU

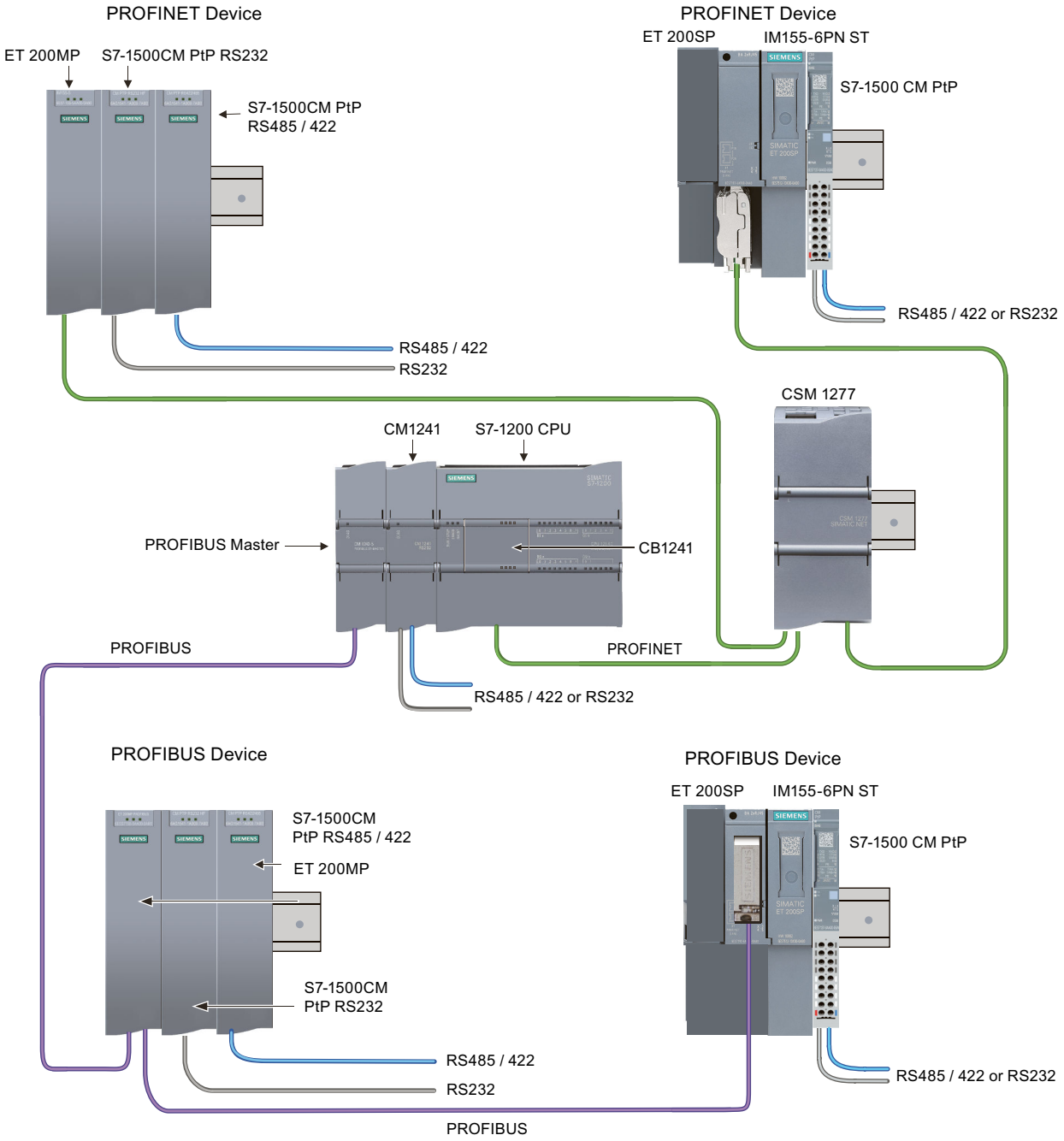
14.5.3.1 Overview

Modbus RTU (Remote Terminal Unit) is a standard network communication protocol that uses the RS232 or RS485 electrical connection for serial data transfer between Modbus network devices. You can add PtP (Point to Point) network ports to a CPU with a RS232 or RS485 CM or a RS485 CB.

Modbus RTU uses a master/slave network where all communications are initiated by a single Master device and slaves can only respond to a master's request. The master sends a request to one slave address and only that slave address responds to the command.

Modbus RTU enables you to use PROFINET or PROFIBUS distributed I/O to communicate to various devices (RFID readers, GPS device, and others):

- PROFINET (Page 530): You connect the Ethernet interface of the S7-1200 CPU to a PROFINET interface module. PtP communication modules in the rack with the interface module can then provide serial communications to external Modbus devices.
- PROFIBUS (Page 691): You insert a PROFIBUS communication module in the left side of the rack with the S7-1200 CPU. You connect the PROFIBUS communication module to a rack containing a PROFIBUS interface module. PtP communication modules in the rack with the interface module can then provide serial communications to external Modbus devices.



Modbus RTU instructions and versions

The Modbus RTU instructions (Page 968) provide the ability to connect to PROFINET and PROFIBUS distributed I/O. They allow you to configure the communications between the PtP communication modules in the distributed I/O rack and the PtP devices. S7-1200 CM 1241 modules must have a minimum firmware version of V2.1 to use these Modbus RTU instructions. Older S7-1200 CPU programs might use Legacy Modbus RTU instructions. (Page 1028)

STEP 7 provides different versions of the Modbus RTU instructions. For information on instruction versions, refer to Use Instruction versions (https://support.industry.siemens.com/cs/ww/en/view/109798671/113722878475) in the STEP 7 Information System.

14.5.3.2 Maximum number of supported Modbus slaves

Modbus addressing supports a maximum of 247 slaves (slave numbers 1 through 247). Each Modbus network segment can have a maximum of 32 devices, based upon the loading and drive capabilities of the RS485 interface. When you reach the 32-device limit, you must use a repeater to expand to the next segment. You need seven repeaters to support the 247 slaves connected to one master for RS485.

Siemens repeaters work only with PROFIBUS; their function is to monitor PROFIBUS token passing. You cannot use Siemens repeaters with other protocols. Therefore, you require third party repeaters for Modbus.

Modbus timeouts are long by default; the use of multiple repeaters does not create a time-delay problem. The Modbus master does not care if a slave is slow to respond or if multiple repeaters delay the response.

14.5.3.3 Modbus RTU instructions

Modbus_Comm_Load (Configure SIPLUS I/O or port on the PtP module for Modbus RTU) instruction

Table 14-75 Modbus_Comm_Load instruction

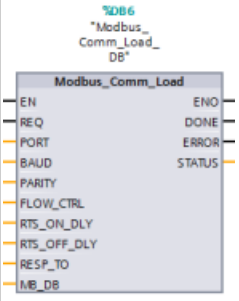
LAD / FBD	SCL	Description
	**"Modbus_Comm_Load_DB"(** **REQ:=_bool_in,** **PORT:=_uint_in_,** **BAUD:=_udint_in_,** **PARITY:=_uint_in_,** **FLOW_CTRL:=_uint_in_,** **RTS_ON_DLY:=_uint_in_,** **RTS_OFF_DLY:=_uint_in_,** **RESP_TO:=_uint_in_,** **DONE=>_bool_out,** **ERROR=>_bool_out_,** **STATUS=>_word_out_,** **MB_DB:=_fbtref_inout_);**	The Modbus_Comm_Load instruction configures SIPLUS I/O or a PtP port for Modbus RTU protocol communications. Modbus RTU port hardware options: Install up to three CMs (RS485 or RS232), plus one CB (R4845). Modbus RTU SIPLUS I/O options: Install ET 200MP S7-1500CM PtP (RS485 / 422 or RS232) or ET 200SP S7-1500 CM PtP (RS485 / 422 or RS232) An instance data block is assigned automatically when you place the Modbus_Comm_Load instruction in your program.

Table 14-76 Data types for the parameters

Parameter and type		Data type	Description
EN	IN	Bool	Note: The Modbus RTU, Modbus_Comm_Load instruction uses the RDREC and WRREC instructions to initialize the PTP module. However, the RDREC/WRREC instruction works asynchronously, which means that it takes several scans for the instruction to complete. Therefore, you must hold the EN parameter of the Modbus_Comm_Load instruction true until completion of the RDREC/WRREC instruction.
REQ	IN	Bool	A low to high (positive edge) signal starts the operation. (Version 2.0 only)
PORT	IN	Port	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table.
BAUD	IN	UDInt	Baud rate selection: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 76800, 115200, all other values are invalid
PARITY	IN	UInt	Parity selection: • 0 – None • 1 – Odd • 2 – Even
FLOW_CTRL [1]	IN	UInt	Flow control selection: • 0 – (default) no flow control • 1 – Hardware flow control with RTS always ON (does not apply to RS485 ports) • 2 – Hardware flow control with RTS switched
RTS_ON_DLY [1]	IN	UInt	RTS ON delay selection: • 0 – (default) No delay from RTS active until the first character of the message is transmitted • 1 to 65535 – Delay in milliseconds from RTS active until the first character of the message is transmitted (does not apply to RS485 ports). RTS delays shall be applied independent of the FLOW_CTRL selection.
RTS_OFF_DLY [1]	IN	UInt	RTS OFF delay selection: • 0 – (default) No delay from the last character transmitted until RTS goes inactive • 1 to 65535 – Delay in milliseconds from the last character transmitted until RTS goes inactive (does not apply to RS485 ports). RTS delays shall be applied independent of the FLOW_CTRL selection.
RESP_TO [1]	IN	UInt	Response timeout: Time in milliseconds allowed by the Modbus_Master for the slave to respond. If the slave does not respond in this time period, the Modbus_Master will retry the request or terminate the request with an error when the specified number of retries has been sent. 5 ms to 65535 ms (default value = 1000 ms).
MB_DB	IN	Variant	A reference to the instance data block used by the Modbus_Master or Modbus_Slave instructions. After Modbus_Master or Modbus_Slave is placed in your program, the DB identifier appears in the parameter helper drop-list available at the MB_DB box connection.

[1] Optional parameters for Modbus_Comm_Load (V 2.x or later). Click the arrow at the bottom of a LAD/FBD box to expand the box and include these parameters.

Parameter and type		Data type	Description
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error. (Version 2.0 only)
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code

[1] Optional parameters for Modbus_Comm_Load (V 2.x or later). Click the arrow at the bottom of a LAD/FBD box to expand the box and include these parameters.

Modbus_Comm_Load is executed to configure a port for the Modbus RTU protocol. Once a port is configured for the Modbus RTU protocol, it can only be used by either the Modbus_Master or Modbus_Slave instructions.

One execution of Modbus_Comm_Load must be used to configure each communication port that is used for Modbus communication. Assign a unique Modbus_Comm_Load instance DB for each port that you use. You can install up to three communication modules (RS232 or RS485) and one communication board (RS485) in the CPU. Call Modbus_Comm_Load from a startup OB and execute it one time or use the first scan system flag (Page 83) to initiate the call to execute it one time. Only execute Modbus_Comm_Load again if communication parameters like baud rate or parity must change.

If you use the Modbus library with a module in a distributed rack, the Modbus_Comm_Load instruction must be executed in a cyclical interrupt routine (for example, once per second or once every 10 seconds). If power is lost to the distributed rack or the module is pulled, upon restoration of module operation, only the HWConfig parameter set is sent to the PtP module. All requests initiated by the Modbus_Master timeout, and the Modbus_Slave goes silent (no response to any message). Cyclic execution of the Modbus_Comm_Load instruction resolves these issues.

An instance data block is assigned for Modbus_Master or Modbus_Slave when you place these instructions in your program. This instance data block is referenced when you specify the MB_DB parameter for the Modbus_Comm_Load instruction.

Modbus_Comm_Load instance data block (DB) tags

The following table shows the public static tags stored in the Modbus_Comm_Load instance DB that can be used in your program:

Table 14-77 Modbus_Comm_Load instance DB static tags

Tag	Data type	Default	Description
ICHAR_GAP	Word	0	Maximum character delay time between characters. This parameter is specified in milliseconds and increases the anticipated period between the received characters. The corresponding number of bit times for this parameter is added to the Modbus default value of 35 bit times (3.5 character times).
RETRIES	Word	2	Number of retries that the master executes before the error code 0x80C8 for "No response" is returned.
EN_SUPPLY_VOLT	Bool	0	Enable diagnostics for missing supply voltage L+.

Tag	Data type	Default	Description
MODE	USInt	0	Operating mode Valid operating modes are as follows: • 0 = Full duplex (RS232) • 1 = Full duplex (RS422) four-wire mode (point-to-point) • 2 = Full duplex (RS422) four-wire mode (multipoint master, CM PtP, ET 200SP) • 3 = Full duplex (RS422) four-wire mode (multipoint slave, CM PtP, ET 200SP) • 4 = Half duplex (RS485) two-wire mode (See Note below.)
LINE_PRE	USInt	0	Receive line initial state Valid initial states are as follows: • 0 = "No" initial state (See Note below.) • 1 = signal R(A) = 5 V DC, signal R(B) = 0 V DC (break detection): Break detection is possible with this initial state. Can only be selected with: "Full duplex (RS422) four-wire mode (point-to-point connection)" and "Full duplex (RS422) four-wire mode (multipoint slave)". • 2 = signal R(A) = 0 V DC, signal R(B) = 5 V DC: This default setting corresponds to the idle state (no active send operation). No break detection is possible with this initial state.
BRK_DET	USInt	0	Break detection The following selections are valid: • 0 = break detection deactivated • 1 = break detection activated
EN_DIAG_ALARM	Bool	0	Activate diagnostics interrupt: • 0 = not activated • 1 = activated
STOP_BITS	USInt	1	Number of stop bits: • 1 = 1 stop bit • 2 = 2 stop bits • 0, 3 to 255 = reserved

NOTE

Required setting for the use of PROFIBUS cables with CM 1241 for RS485

Table 14-78 Modbus_Comm_Load execution condition codes [1]

STATUS (W#16#)	Description
0000	No error
8180	Invalid port ID value (wrong port/hardware identifier for communication module)
8181	Invalid baud rate value
8182	Invalid parity value
8183	Invalid flow control value
8184	Invalid response timeout value (response timeout less than the 5 ms minimum)
8185	MB_DB parameter is not an instance data block of a Modbus_Master or Modbus_Slave instruction.

[1] In addition to the Modbus_Comm_Load errors listed above, errors can be returned from the underlying PtP communication instructions.

Modbus_Master (Communicate using SIPLUS I/O or the PtP port as Modbus RTU master) instruction

Table 14-79 Modbus_Master instruction

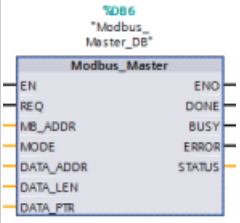
LAD / FBD	SCL	Description
	**"Modbus_Master_DB"(REQ:=_bool_in_, MB_ADDR:=_uint_in_, MODE:=_usint_in_, DATA_ADDR:=_udint_in_, DATA_LEN:=_uint_in_, DONE=>_bool_out_, BUSY=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, DATA_PTR:=_variant_inout_);**	The Modbus_Master instruction communicates as a Modbus master using a port that was configured by a previous execution of the Modbus_Comm_Load instruction. An instance data block is assigned automatically when you place the Modbus_Master instruction in your program. This Modbus_Master instance data block is used when you specify the MB_DB parameter for the Modbus_Comm_Load instruction.

Table 14-80 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	0=No request 1= Request to transmit data to Modbus slave
MB_ADDR	IN	V1.0: USInt V2.0: UInt	Modbus RTU station address: Standard addressing range (1 to 247) Extended addressing range (1 to 65535) The value of 0 is reserved for broadcasting a message to all Modbus slaves. Modbus function codes 05, 06, 15 and 16 are the only function codes supported for broadcast.
MODE	IN	USInt	Mode Selection: Specifies the type of request (read, write, or diagnostic). See the Modbus functions table below for details.
DATA_ADDR	IN	UDInt	Starting Address in the slave: Specifies the starting address of the data to be accessed in the Modbus slave. See the Modbus functions table below for valid addresses.
DATA_LEN	IN	UInt	Data Length: Specifies the number of bits or words to be accessed in this request. See the Modbus functions table below for valid lengths.
DATA_PTR	IN_OUT	Variant	Data Pointer: Points to the M or DB address (non-optimized DB type) for the data being written or read.
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error.
BUSY	OUT	Bool	• 0 – No Modbus_Master operation in progress • 1 – Modbus_Master operation in progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code

Modbus_Master communication rules

- Modbus_Comm_Load must be executed to configure a port before a Modbus_Master instruction can communicate with that port.
- If a port is to be used to initiate Modbus master requests, that port should not be used by a Modbus_Slave. One or more instances of Modbus_Master execution can be used with that port, but all Modbus_Master execution must use the same Modbus_Master instance DB for that port.
- The Modbus instructions do not use communication interrupt events to control the communication process. Your program must poll the Modbus_Master instruction for transmit and receive complete conditions.
- Call all Modbus_Master execution for a given port from a program cycle OB. Modbus_Master instructions may execute in only one of the program cycle or cyclic/time delay execution levels. They must not execute in both execution priority levels. Pre-emption of a Modbus_Master instruction by another Modbus_Master instruction in a higher priority execution priority level will result in improper operation. Modbus_Master instructions must not execute in the startup, diagnostic or time error execution priority levels.
- Once a Modbus_Master instruction initiates a transmission, this instance must be continually executed with the EN input enabled until a DONE=1 state or ERROR=1 state is returned. A particular Modbus_Master instance is considered active until one of these two events occurs. While the original instance is active, any call to any other instance with the REQ input enabled will result in an error. If the continuous execution of the original instance stops, the request state remains active for a period of time specified by the static variable "Blocked_Proc_Timeout". Once this period of time expires, the next Modbus_Master instruction called with an enabled REQ input will become the active instance. This prevents a single Modbus_Master instance from monopolizing or locking access to a port. If the original active instance is not enabled within the period of time specified by the static variable "Blocked_Proc_Timeout", then the next execution by this instance (with REQ not set) will clear the active state. If (REQ is set), then this execution initiates a new Modbus_Master request as if no other instance was active.

REQ parameter

0 = No request; 1 = Request to transmit data to Modbus Slave

You may control this input either through the use of a level or edge triggered contact. Whenever this input is enabled, a state machine is started to ensure that no other Modbus_Master using the same instance DB is allowed to issue a request, until the current request is completed. All other input states are captured and held internally for the current request, until the response is received or an error detected.

If the same instance of Modbus_Master is executed again with REQ input = 1 before the completion of the current request, then no subsequent transmissions are made. However, when the request is completed, a new request is issued whenever a Modbus_Master is executed again with REQ input = 1.

DATA_ADDR and MODE parameters select the Modbus function type

DATA_ADDR (starting Modbus address in the slave): Specifies the starting address of the data to be accessed in the Modbus slave.

The Modbus_Master instruction uses a MODE input rather than a Function Code input. The combination of MODE and Modbus address determine the Function Code that is used in the actual Modbus message. The following table shows the correspondence between parameter MODE, Modbus function code, and Modbus address range.

Table 14-81 Modbus functions

MODE	Modbus function	Data length	Operation and data	Modbus address
0	01	1 to 2000 1 to 1992 [1]	Read output bits: 1 to (1992 or 2000) bits per request	1 to 9999
0	02	1 to 2000 1 to 1992 [1]	Read input bits: 1 to (1992 or 2000) bits per request	10001 to 19999
0	03	1 to 125 1 to 124 [1]	Read Holding registers: 1 to (124 or 125) words per request	40001 to 49999 or 400001 to 465535
0	04	1 to 125 1 to 124 [1]	Read input words: 1 to (124 or 125) words per request	30001 to 39999
104	04	1 to 125 1 to 124 1	Read input words: 1 to (124 or 125) words per request	00000 to 65535
1	05	1	Write one output bit: One bit per request	1 to 9999
1	06	1	Write one holding register: 1 word per request	40001 to 49999 or 400001 to 465535
1	15	2 to 1968 2 to 1960 [1]	Write multiple output bits: 2 to (1960 or 1968) bits per request	1 to 9999
1	16	2 to 123 2 to 122 [1]	Write multiple holding registers: 2 to (122 or 123) words per request	40001 to 49999 or 400001 to 465535
2	15	1 to 1968 2 to 1960 [1]	Write one or more output bits: 1 to (1960 or 1968) bits per request	1 to 9999
2	16	1 to 123 1 to 122 [1]	Write one or more holding registers: 1 to (122 or 123) words per request	40001 to 49999 or 400001 to 465535
11	11	0	Read the slave communication status word and event counter. The status word indicates busy (0 – not busy, 0xFFFF - busy). The event counter is incremented for each successful completion of a message. Both the DATA_ADDR and DATA_LEN operands of the Modbus_Master instruction are ignored for this function.	
80	08	1	Check slave status using data diagnostic code 0x0000 (Loopback test – slave echoes the request) 1 word per request	
81	08	1	Reset slave event counter using data diagnostic code 0x000A 1 word per request	
3 to 10, 12 to 79, 82 to 255			Reserved	

[1] For "Extended Addressing" mode the maximum data lengths are reduced by 1 byte or 1 word depending upon the data type used by the function.

DATA_PTR parameter

The DATA_PTR parameter points to the DB or M address that is written to or read from. If you use a data block, then you must create a global data block that provides data storage for reads and writes to Modbus slaves.

NOTE

The DATA_PTR data block type must allow direct addressing

The data block must allow both direct (absolute) and symbolic addressing. When you create the data block the "Standard" access attribute must be selected.

As of Modbus_Master instruction version V4.0 or later, you can enable the data block attribute "Optimized block access". You can only use a single element, or an array of elements, in optimized memory with the following data types: Bool, Byte, Char, Word, Int, DWord, Dint, Real, USInt, UInt, UDInt, SInt, or WChar.

Data block structures for the DATA_PTR parameter

- These data types are valid for **word reads** of Modbus addresses 30001 to 39999, 40001 to 49999, and 400001 to 465536 and also for **word writes** to Modbus addresses 40001 to 49999 and 400001 to 465536.
  - Standard array of WORD, UINT, or INT data types
  - Named WORD, UINT, or INT structure where each element has a unique name and 16 bit data type.
  - Named complex structure where each element has a unique name and a 16 or 32 bit data type.
- For **bit reads** and writes of Modbus addresses 00001 to 09999 and bit reads of 10001 to 19999.
  - Standard array of Boolean data types.
  - Named Boolean structure of uniquely named Boolean variables.
- Although not required, it is recommended that each Modbus_Master instruction have its own separate memory area. The reason for this recommendation is that there is a greater possibility of data corruption if multiple Modbus_Master instructions are reading and writing to the same memory area.
- There is no requirement that the DATA_PTR data areas be in the same global data block. You can create one data block with multiple areas for Modbus reads, one data block for Modbus writes, or one data block for each slave station.

Modbus_Master instruction data block (DB) variables

The following table shows the public static tags stored in the Modbus_Master instance DB that you can use in your program:

Table 14-82 Modbus_Master instance DB static variables

Tag	Data type	Default	Description
Blocked_Proc_Timeout	Real	3.0	Duration (in seconds) for which to wait for a blocked Modbus_Master instance before this instance is removed as ACTIVE. This can occur, for example, if a Modbus_Master request is issued and the program then stops to call the Modbus_Master function before it has completely finished the request. The time value must be greater than 0 and less than 55 seconds, or an error occurs.
Extended_Addressing	Bool	FALSE	Configures single or double-byte slave station addressing: • FALSE = One-byte address; 0 to 247 • TRUE = Two-byte address (corresponds to extended addressing); 0 to 65535
MB_DB	MB_BASE	-	The MB_DB parameter of the Modbus_Comm_Load instruction must be connected to the MB_DB parameter of the Modbus_Master instruction.

Your program can write values to the Blocked_Proc_Timeout and Extended_Addressing variables to control the Modbus_Master operations. See the Modbus_Slave topic description of HR_Start_Offset (Page 978) and Extended_Addressing (Page 978) for an example of how to use these variables in the program editor and details about Modbus extended addressing.

Condition codes

Table 14-83 Modbus_Master execution condition codes (communication and configuration errors) [1]

STATUS (W#16#)	Description
0000	No error
80C8	Slave timeout. The specified slave did not respond in the specified time. Please check the baud rate, parity, and wiring of the slave device. This error is only reported after any configured retries have been attempted.
80C9	The Modbus_Master instruction has timed out for one of the following reasons: • The instruction is waiting for a response from the module that is being used for communications. • The Blocked_Proc_Timeout value is set too small. This error is reported if a PROFIBUS or PROFINET distributed I/O device returns from one of the following: • An interruption to power or communication • A communication module pull/plug event In these instances, the hardware configuration from the PLC is reloaded, and Modbus_Comm_Load must be executed again to properly configure the communication module.
80D1	The receiver issued a flow control request to suspend an active transmission and never re-enabled the transmission during the specified wait time. This error is also generated during hardware flow control when the receiver does not assert CTS within the specified wait time.
80D2	The transmit request was aborted because no DSR signal is received from the DCE.
80E0	The message was terminated because the receive buffer is full.
80E1	The message was terminated as a result of a parity error.

STATUS (W#16#)	Description
80E2	The message was terminated as a result of a framing error.
80E3	The message was terminated as a result of an overrun error.
80E4	The message was terminated as a result of the specified length exceeding the total buffer size.
8180	Invalid port ID value or error with Modbus_Comm_Load instruction
8186	Invalid Modbus station address
8188	Invalid Mode specified for broadcast request
8189	Invalid Data Address value
818A	Invalid Data Length value
818B	Invalid pointer to the local data source/destination: Size not correct
818C	Invalid pointer for DATA_PTR or invalid Blocked_Proc_Timeout. The data area must be one of the following: • Classic DB • Array of elemental data types in a symbolic or retentive DB • M memory
8200	Port is busy processing a transmit request.
8280	Negative acknowledgement when reading module. Check the input at the PORT parameter. This can be caused by the loss of a PROFIBUS or PROFINET distributed I/O module, either by a station power or communication loss or a module pull.
8281	Negative acknowledgement when writing to module. Check the input at the PORT parameter. This can be caused by the loss of a PROFIBUS or PROFINET distributed I/O module, either by a station power or communication loss or a module pull.

Table 14-84 Modbus_Master execution condition codes (Modbus protocol errors) [1]

STATUS (W#16#)	Response code from slave	Modbus protocol errors
8380	-	CRC error
8381	01	Function code not supported
8382	03	Data length error
8383	02	Data address error or address outside the valid range of the DATA_PTR area
8384	Greater than 03	Data value error
8385	03	Data diagnostic code value not supported (function code 08)
8386	-	Function code in the response does not match the code in the request.
8387	-	Wrong slave responded
8388	-	The slave response to a write request is incorrect. The write request returned by the slave does not match what the master actually sent.

[1] In addition to the Modbus_Master errors listed above, errors can be returned from the underlying PtP communication instructions.

NOTE

Setting the maximum record length for Profibus communication

When using a CM1243-5 Profibus Master module to control an ET 200SP or ET 200MP Profibus device that uses an RS232, RS422, or RS485 point-to-point module, you need to explicitly set the "max_record_len" data block tag to 240 as defined below:

Set "max_record_len" in the Send_P2P section of the instance DB (for example, "Modbus_Master_DB".Send_P2P.max_record_len) to 240 after running Modbus_Comm_Load.

Explicitly assigning max_record_len is only necessary with Profibus communication; Profinet communication already uses a valid max_record_len value.

Modbus_Slave (Communicate using SIPLUS I/O or the PtP port as Modbus RTU slave) instruction

Table 14-85 Modbus_Slave instruction

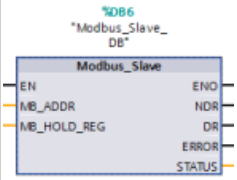
LAD / FBD	SCL	Description
	**"Modbus_Slave_DB"(MB_ADDR:=_uint_in_, NDR=>_bool_out_, DR=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, MB_HOLD_REG:=_variant_inout_);**	The Modbus_Slave instruction allows your program to communicate in one of two ways: • As a Modbus RTU slave through a PtP port on the CM (RS485 or RS232) and CB (RS485) • As a Modbus RTU slave through Modbus RTU SIPLUS I/O options: – Install ET 200MP S7-1500CM PtP (RS485 / 422 or RS232). – Install ET 200SP S7-1500 CM PtP (RS485 / 422 or RS232). When a remote Modbus RTU master issues a request, your user program responds to the request by Modbus_Slave execution. STEP 7 automatically creates an instance DB when you insert the instruction. Use this Modbus_Slave_DB name when you specify the MB_DB parameter for the Modbus_Comm_Load instruction.

Table 14-86 Data types for the parameters

Parameter and type		Data type	Description
MB_ADDR	IN	V1.0: USInt V2.0: UInt	The station address of the Modbus slave: Standard addressing range (1 to 247) Extended addressing range (0 to 65535)
MB_HOLD_REG	IN_OUT	Variant	Pointer to the Modbus Holding Register DB: The Modbus holding register can be M memory or a data block.
NDR	OUT	Bool	New Data Ready: • 0 – No new data • 1 – Indicates that new data has been written by the Modbus master

Parameter and type		Data type	Description
DR	OUT	Bool	Data Read: • 0 – No data read • 1 – Indicates that data has been read by the Modbus master
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. If execution is terminated with an error, then the error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution error code

Modbus communication function codes (1, 2, 4, 5, and 15) can read and write bits and words directly in the input process image and output process image of the CPU. For these function codes, the MB_HOLD_REG parameter must be defined as a data type larger than a byte. The following table shows the example mapping of Modbus addresses to the process image in the CPU.

Table 14-87 Mapping of Modbus addresses to the process image

Modbus functions						S7-1200	
Codes	Function	Data area	Address range			Data area	CPU address
01	Read bits	Output	1	to	8192	Output Process Image	Q0.0 to Q1023.7
02	Read bits	Input	10001	to	18192	Input Process Image	I0.0 to I1023.7
04	Read words	Input	30001	to	30512	Input Process Image	IW0 to IW1022
05	Write bit	Output	1	to	8192	Output Process Image	Q0.0 to Q1023.7
15	Write bits	Output	1	to	8192	Output Process Image	Q0.0 to Q1023.7

Modbus communication function codes (3, 6, 16) use a Modbus holding register which can be an M memory address range or a data block. The type of holding register is specified by the MB_HOLD_REG parameter on the Modbus_Slave instruction.

NOTE

MB_HOLD_REG data block type

A Modbus holding register data block must allow both direct (absolute) and symbolic addressing. When you create the data block the "Standard" access attribute must be selected.

As of Modbus_Slave instruction version V4.0 or later, you can enable the data block attribute "Optimized block access". You can only use a single element, or an array of elements, in optimized memory with the following data types: Bool, Byte, Char, Word, Int, DWord, Dint, Real, USInt, UInt, UDInt, SInt, or WChar.

The following table shows examples of Modbus address to holding register mapping that is used for Modbus function codes 03 (read words), 06 (write word), and 16 (write words). The actual upper limit of DB addresses is determined by the maximum work memory limit and M memory limit, for each CPU model.

Table 14-88 Mapping of Modbus addresses to CPU memory

Modbus master address	**MB_HOLD_REG parameter examples**				
	MW100	**DB10.DBw0**	**MW120**	**DB10.DBW50**	**"Recipe".ingredient**
40001	MW100	DB10.DBW0	MW120	DB10.DBW50	"Recipe".ingredient[1]
40002	MW102	DB10.DBW2	MW122	DB10.DBW52	"Recipe".ingredient[2]
40003	MW104	DB10.DBW4	MW124	DB10.DBW54	"Recipe".ingredient[3]
40004	MW106	DB10.DBW6	MW126	DB10.DBW56	"Recipe".ingredient[4]
40005	MW108	DB10.DBW8	MW128	DB10.DBW58	"Recipe".ingredient[5]

Table 14-89 Diagnostic functions

S7-1200 Modbus_Slave Modbus diagnostic functions		
Codes	Sub-function	Description
08	0000H	Return query data echo test: • Prior to STEP 7 V15.1, the Modbus_Slave echos back to a Modbus master a word of data that is received. • As of STEP 7 V15.1 or later, the Modbus_Slave instruction V4.1 or later echos back one or more words of data that is received.
08	000AH	Clear communication event counter: The Modbus_Slave will clear out the communication event counter that is used for Modbus function 11.
11		Get communication event counter: The Modbus_Slave uses an internal communication event counter for recording the number of successful Modbus read and write requests that are sent to the Modbus_Slave. The counter does not increment on any Function 8, Function 11, or broadcast requests. It is also not incremented on any requests that result in a communication error (for example, parity or CRC errors).

The Modbus_Slave instruction supports broadcast write requests from any Modbus master as long as the request is for accessing valid addresses. Modbus_Slave will produce error code "0x8188" for function codes not supported in broadcast.

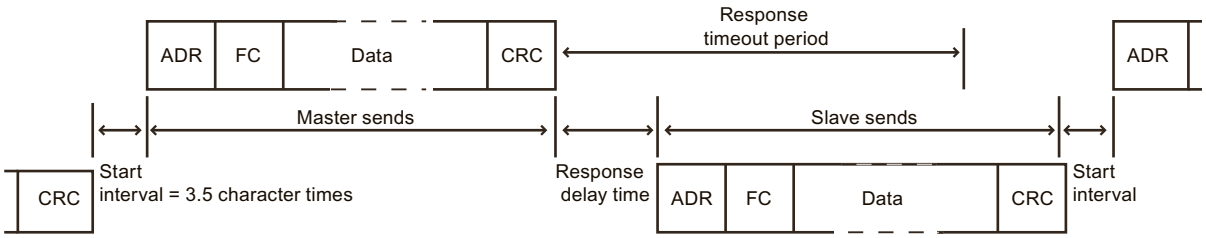
Modbus_Slave communication rules

- Modbus_Comm_Load must be executed to configure a port, before a Modbus_Slave instruction can communicate through that port.
- If a port is to respond as a slave to a Modbus_Master, then do not program that port with the Modbus_Master instruction.
- Only one instance of Modbus_Slave can be used with a given port, otherwise erratic behavior may occur.
- The Modbus instructions do not use communication interrupt events to control the communication process. Your program must control the communication process by polling the Modbus_Slave instruction for transmit and receive complete conditions.

- The Modbus_Slaveinstruction must execute periodically at a rate that allows it to make a timely response to incoming requests from a Modbus_Master. It is recommended that you execute Modbus_Slave every scan from a program cycle OB. Executing Modbus_Slave from a cyclic interrupt OB is possible, but is not recommended because of the potential for excessive time delays in the interrupt routine to temporarily block the execution of other interrupt routines.

Modbus signal timing

Modbus_Slave must be executed periodically to receive each request from the Modbus_Master and then respond as required. The frequency of execution for Modbus_Slave is dependent upon the response timeout period of the Modbus_Master. This is illustrated in the following diagram.



The response timeout period RESP_TO is the amount of time a Modbus_Master waits for the start of a response from a Modbus_Slave. This time period is not defined by the Modbus protocol, but is a parameter of each Modbus_Master. The frequency of execution (the time between one execution and the next execution) of Modbus_Slave must be based upon the particular parameters of your Modbus_Master. At a minimum, you should execute Modbus_Slave twice within the response timeout period of the Modbus_Master.

Modbus_Slave instruction data block (DB) variables

The following table shows the public static tags stored in the Modbus_Slave instance DB that you can use in your program:

Table 14-90 Modbus_Slave instance DB static variables

Variable	Data type	Default	Description
HR_Start_Offset	Word	0	Assigns the starting address of the Modbus holding register (default = 0)
Extended_Addressing	Bool	FALSE	Configures single or double-byte slave addressing: • FALSE = single byte address • TRUE = double-byte address
Request_Count	Word	0	Total of all requests received by this slave
Slave_Message_Count	Word	0	Number of requests received for this specific slave
Bad_CRC_Count	Word	0	Number of requests received that have a CRC error
Broadcast_Count	Word	0	Number of broadcast requests received
Exception_Count	Word	0	Modbus-specific errors that require an acknowledgement with a returned exception to the master
Success_Count	Word	0	Number of requests received for this specific slave that have no protocol errors

Variable	Data type	Default	Description
MB_DB	MB_BASE	-	The MB_DB parameter of the Modbus_Comm_Load instruction must be connected to the MB_DB parameter of the Modbus_Slave instruction.
QB_Start	UInt	0	The starting address of the output bytes to which the CPU can write (QB0 to QB65535)
QB_Count	UInt	65535	The number of bytes to which a remote device can write. If QB_Count = 0, a remote device cannot write to the outputs. Example: To allow only QB10 through QB17 to be writable, QB_Start = 10 and QB_Count = 8.
QB_Read_Start	UInt	0	The starting address of the output bytes to which the CPU can read (QB0 to QB65535)
QB_Read_Count	UInt	65535	The number of output bytes from which a remote device can read. If QB_Count = 0, a remote device cannot read from the outputs. Example: To allow only QB10 through QB17 to be readable, QB_Start = 10 and QB_Count = 8.
IB_Read_Start	UInt	0	The starting address of the input bytes to which the CPU can read (IB0 to IB65535)
IB_Read_Count	UInt	65535	The number of input bytes from which a remote device can read. If IB_Count = 0, a remote device cannot read from the inputs. Example: To allow only IB10 through IB17 to be readable, IB_Start = 10 and IB_Count = 8.

Your program can write data to the control Modbus server operations and the following variables:

- HR_Start_Offset
- Extended_Addressing
- QB_Start
- QB_Count
- QB_Read_Start
- QB_Read_Count
- IB_Read_Start
- IB_Read_Count

Version requirements for Modbus_Slave instruction data block (DB) variables availability are as follows:

Table 14-91 Modbus_Slave instruction data block (DB) variables availability version requirements: Instruction, TIA Portal, and S7-1200 CPU

Modbus_Slave instruction version	TIA Portal version	S7-1200 CPU firmware (FW) version	Data block variables
3.0	V14 SP1	CPU FW V4.0 or later	QB_Start
			QB_Count
4.0 or later	V15 or later	CPU FW V4.2 or later	QB_Start
			QB_Count
			QB_Read_Start
			QB_Read_Count
			IB_Read_Start
			IB_Read_Count

HR_Start_Offset

Modbus holding register addresses begin at 40001 or 400001. These addresses correspond to the beginning PLC memory address of the holding register. However, you can configure the "HR_Start_Offset" variable to start the beginning Modbus holding register address at another value instead of 40001 or 400001.

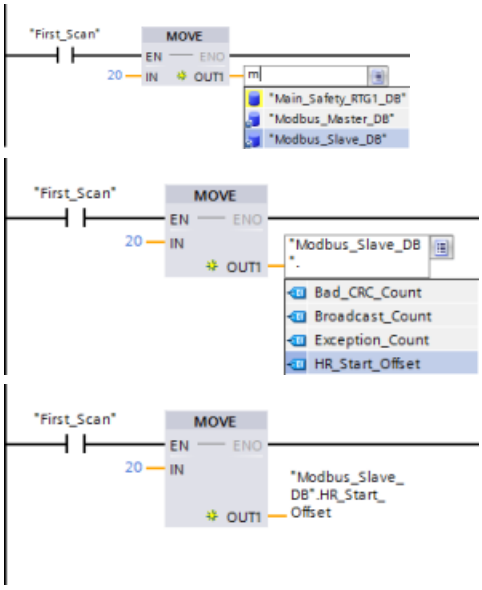
For example, if the holding register is configured to start at MW100 and is 100 words long. An offset of 20 specifies a beginning holding register address of 40021 instead of 40001. Any address below 40021 and above 400119 will result in an addressing error.

Table 14-92 Example of Modbus holding register addressing

HR_Start_Offset	Address	Minimum	Maximum
0	Modbus address (Word)	40001	40099
	S7-1200 address	MW100	MW298
20	Modbus address (Word)	40021	40119
	S7-1200 address	MW100	MW298

HR_Start_Offset is a word value that specifies the starting address of the Modbus holding register and is stored in the Modbus_Slave instance data block. You can set this public static variable value by using the parameter helper drop-list, after Modbus_Slave is placed in your program.

For example, after Modbus_Slave is placed in a LAD network, you can go to a previous network and assign the HR_Start_Offset value. The value must be assigned prior to execution of Modbus_Slave.



Entering a Modbus slave variable using the default DB name:

1. Set the cursor in the parameter field and type an m character.
2. Select "Modbus_Slave_DB" from the drop-list.
3. Set the cursor at the right side of the DB name (after the quote character) and enter a period character.
4. Select "Modbus_Slave_DB.HR_Start_Offset" from the drop list.

Extended_Addressing

The Extended_Addressing variable is accessed in a similar way as the HR_Start_Offset reference discussed above except that the Extended_Addressing variable is a Boolean value. The Boolean value must be written by an output coil and not a move box.

Modbus slave addressing can be configured to be either a single byte (which is the Modbus standard) or double byte. Extended addressing is used to address more than 247 devices within a single network. Selecting extended addressing allows you to address a maximum of 64000 addresses. A Modbus function 1 frame is shown below as an example.

Table 14-93 Single-byte slave address (byte 0)

Function 1	**Byte 0**	**Byte 1**	**Byte 2**	**Byte 3**	**Byte 4**	**Byte 5**	
Request	Slave addr.	F code	Start address		Length of coils		
Valid Response	Slave addr.	F code	Length	Coil data			
Error response	Slave addr.	0x81	E code				

Table 14-94 Double-byte slave address (byte 0 and byte 1)

	Byte 0	**Byte 1**	**Byte 2**	**Byte 3**	**Byte 4**	**Byte 5**	**Byte 6**
Request	Slave address		F code	Start address		Length of coils	
Valid Response	Slave address		F code	Length	Coil data		
Error response	Slave address		0x81	E code			

Access to data areas in data blocks (DB) instead of direct access to Modbus addresses

You can access data areas in DBs in the global DB "Attributes" Property page. You must deselect the "Only store in load memory" and "Optimized block access" check boxes.

If a Modbus request arrives and you did not define a data area for the Modbus data type of the corresponding function code, the Modbus_Slave instruction treats the request as in previous instruction versions: You access process images and holding registers directly.

If you have defined a data area for the Modbus data type of the function code, the Modbus_Slave instruction reads from or writes to that data area. Whether it reads or writes depends on the job type.

NOTE

If a data area is configured, the Modbus_Slave instruction ignores the offsets or ranges configured by the static variables in the instance data block that corresponds to the data_type of the data area. Those offsets and ranges only apply to the process image or the memory referenced by MB_HOLD_REG. The data area start and length parameters provide its own way of defining offsets and ranges

For one individual Modbus request, you can only read from or write to one data area. If, for example, you want to read holding registers that extend over multiple data areas, you require multiple Modbus requests.

These are the rules for defining data areas:

- You can define up to eight data areas in different DBs; each DB must only contain one data area. An individual MODBUS request can only read from precisely one data area or write to precisely one data area. Each data area corresponds to one MODBUS address area. You define the data areas in the "Data_Area_Array" static tag of the instance DB.
- If you want to use less than eight data areas, you must place the required data areas one behind the other, without any gaps. The first blank entry in the data areas ends the data area search during processing. If, for example, you define the field elements 1, 2, 4, and 5, the "Data_Area_Array" only recognizes field elements 1 and 2. as field element 3 is empty.

- The Data_Area_Array field consists of eight elements: Data_Area_Array[1] to Data_Area_Array[8]
- Each field element Data_Area_Array[x], 1 <= x <= 8, is a UDT of the type MB_DataArea and is structured as follows:

Parameter	Data type	Meaning
data_ type	UInt	Identifier for the MODBUS data type that is mapped to this data area: – 0: Identifier for an empty field element or an unused data area. In this case, the values of db, start and length are irrelevant. – 1: Process image output (used with function codes 1, 5, and 15) – 2: Process image input (used with function code 2) – 3: Holding register (used with function codes 3, 6, and 16) – 4: Input register (used with function code 4) Note: If you have defined a data area for a MODBUS data type, the instruction Modbus_Slave can no longer access this MODBUS data type directly. If the address of a MODBUS request for such a data type does not correspond to a defined data area, a value of W#16#8383 is returned in STATUS.
db	UInt	Number of the data block to which the MODBUS register or bits subsequently defined are mapped The DB number must be unique in the data areas. The same DB number must not be defined in multiple data areas. In the global DB "Attributes" Property page, you must deselect the "Only store in load memory" and "Optimized block access" check boxes. Data areas also start with the byte address 0 of the DB. Permitted values: 1 to 60999
start	UInt	First MODBUS address that is mapped to the data block starting from address 0.0 Permitted values: 0 to 65535
length	UInt	Number of bits (for the values 1 and 2 of data_type) or number of registers (for the values 3 and 4 of data_type) The MODBUS address areas of one and the same MODBUS data type must not overlap. Permitted values: 1 to 65535

Examples of the definition of data areas:

- First example: data_type = 3, db = 1, start = 10, length = 6
  The CPU maps the holding registers (data_type = 3) in data block 1 (db = 1), placing the Modbus address 10 (start = 10) at data word 0 and the last valid Modbus address 15 (length = 6) at data word 5.
- Second example: data_type = 2, db = 15, start = 1700, length = 112
  The CPU maps the inputs (data_type = 2) in data block 15 (db = 15), placing the Modbus address 1700 (start = 1700) at data word 0 and the last valid Modbus address 1811 (length = 112) at data word 111.

Condition codes

Table 14-95 Modbus_Slave execution condition codes (communication and configuration errors) [1]

STATUS (W#16#)	Description
80D1	The receiver issued a flow control request to suspend an active transmission and never re-enabled the transmission during the specified wait time. This error is also generated during hardware flow control when the receiver does not assert CTS within the specified wait time.
80D2	The transmit request was aborted because no DSR signal is received from the DCE.
80E0	The message was terminated because the receive buffer is full.
80E1	The message was terminated as a result of a parity error.
80E2	The message was terminated as a result of a framing error.
80E3	The message was terminated as a result of an overrun error.
80E4	The message was terminated as a result of the specified length exceeding the total buffer size.
8180	Invalid port ID value or error with Modbus_Comm_Load instruction
8186	Invalid Modbus station address
8187	Invalid pointer to MB_HOLD_REG DB: Area is too small
818C	Invalid MB_HOLD_REG pointer. The data area must be one of the following: • Classic DB • Array of elemental data types in a symbolic or retentive DB • M memory

Table 14-96 Modbus_Slave execution condition codes (Modbus protocol errors) [1]

STATUS (W#16#)	Response code from slave	Modbus protocol errors
8380	No response	CRC error
8381	01	Function code not supported or not supported within broadcasts
8382	03	Data length error
8383	02	Data address error or address outside the valid range of the DATA_PTR area
8384	03	Data value error
8385	03	Data diagnostic code value not supported (function code 08)
8389		Invalid data area definition: • Invalid data_type value • DB number invalid or does not exist: – Invalid db value – DB number does not exist – DB number is already used by another data area – DB with optimized access – DB is not located in the work memory • Invalid length value • Overlapping of MODBUS address ranges that belong to the same MODBUS data type

[1] In addition to the Modbus_Slave errors listed above, errors can be returned from the underlying PtP communication instructions.

NOTE

Setting the maximum record length for PROFIBUS communication

When using a CM1243-5 PROFIBUS Master module to control an ET 200SP or ET 200MP PROFIBUS device that uses an RS232, RS422, or RS485 point-to-point module, you need to explicitly set the "max_record_len" data block tag to 240 as defined below:

Set "max_record_len" in the Send_P2P section of the instance DB (for example, "Modbus_Slave_DB".Send_P2P.max_record_len) to 240 after running Modbus_Comm_Load.

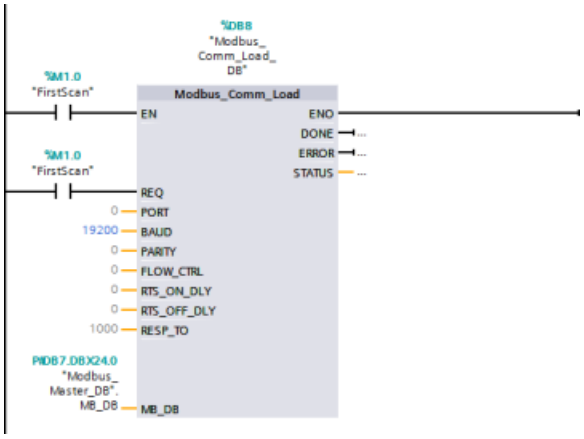
Explicitly assigning max_record_len is only necessary with PROFIBUS communication; PROFINET communication already uses a valid max_record_len value.

14.5.3.4 Modbus RTU examples

Example: Modbus RTU master program

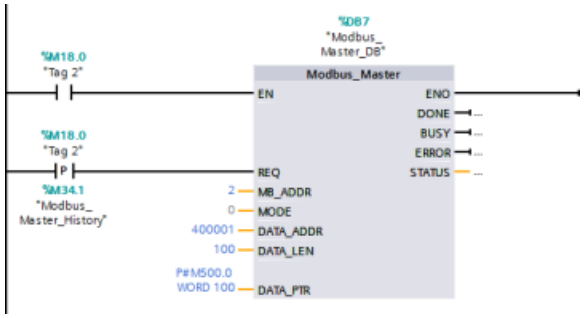
Modbus_Comm_Load is initialized during start-up by using the first scan flag. Execution of Modbus_Comm_Load in this manner should only be done when the serial port configuration will not change at runtime.

Network 1: Configure/initialize the RS485 module communications port only once during the first scan.

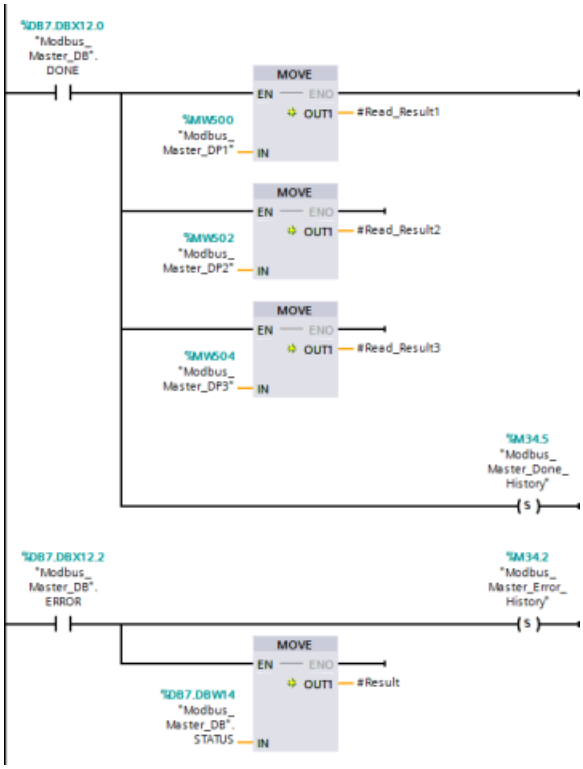


One Modbus_Master instruction is used in the program cycle OB to communicate with a single slave. Additional Modbus_Master instructions can be used in the program cycle OB to communicate with other slaves, or one Modbus_Master FB could be re-used to communicate with additional slaves.

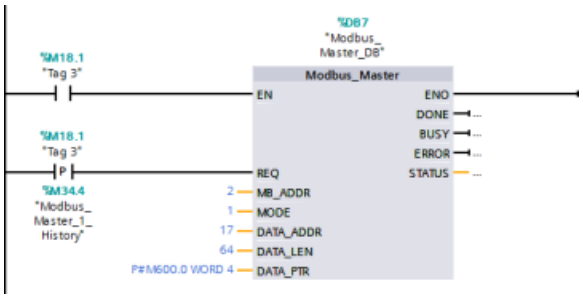
Network 2: Read 100 words of holding register data from location 400001 on slave #2 to memory location MW500-MW698.



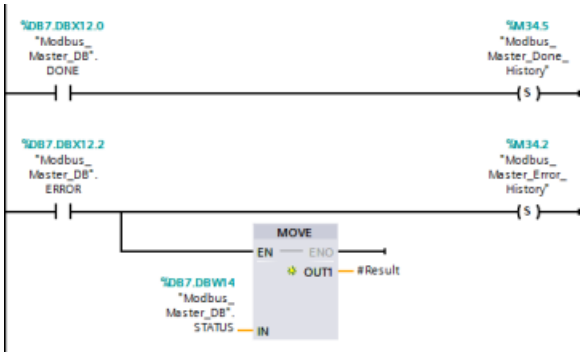
Network 3: Move the first 3 words of the holding register data that has been read to some other location, and set a DONE history bit. This network also sets an ERROR history bit and saves the STATUS word to another location in the event of an error.



Network 4: Write 64 bits of data from MW600-MW607 to output bit locations 00017 to 00081 on slave #2.



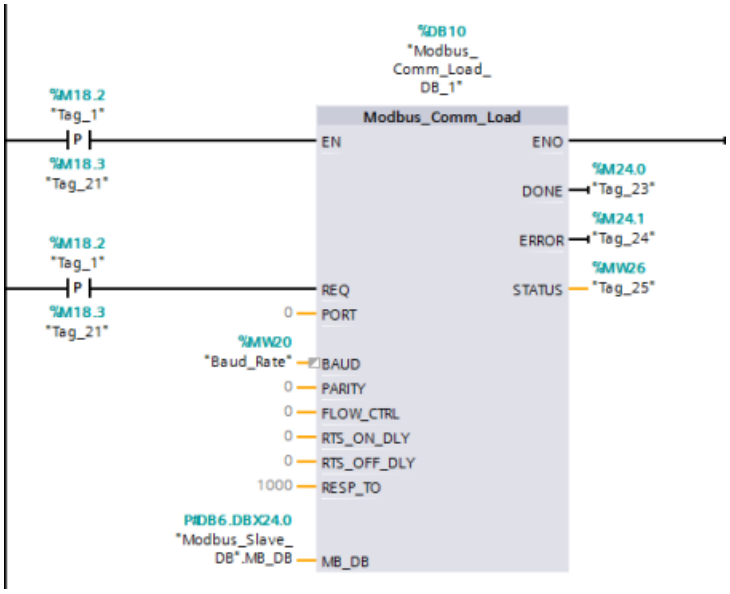
Network 5: Set a DONE history bit when the write is complete. If an error occurs, the program sets an ERROR history bit and saves the STATUS code.



Example: Modbus RTU slave program

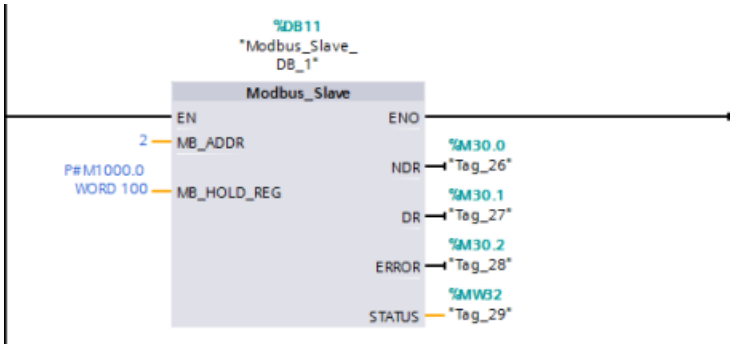
MB_COMM_LOAD shown below is initialized each time "Tag_1" is enabled.
Execution of MB_COMM_LOAD in this manner should only be done when the serial port configuration will change at runtime, as a result of HMI configuration.

Network 1: Initialize the RS485 module parameters each time they are changed by an HMI device.



MB_SLAVE shown below is placed in a cyclic OB that is executed every 10 ms. While this does not give the absolute fastest response by the slave, it does provide good performance at 9600 baud for short messages (20 bytes or less in the request).

Network 2: Check for Modbus master requests during each scan. The Modbus holding register is configured for 100 words starting at MW1000.



14.6 Legacy PtP communication (CM/CB 1241 only)

Prior to the release of STEP 7 V13 SP1 and the S7-1200 V4.1 CPUs, the point-to-point communication instructions existed with different names, and in some cases, slightly different interfaces. The general concepts about point-to-point communication (Page 839), as well as port (Page 842) and parameter configuration (Page 857) apply to both sets of instructions. Refer to the individual legacy point-to-point instructions for programming information.

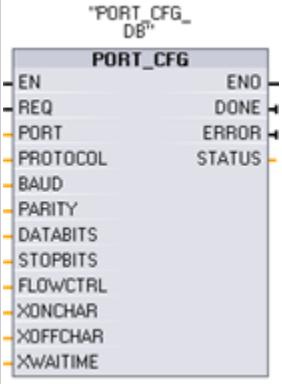
Table 14-97 Common error classes

Class description	Error classes	Description
Port configuration	80Ax	Used to define common port configuration errors
Transmit configuration	80Bx	Used to define common transmit configuration errors
Receive configuration	80Cx	Used to define common receive configuration errors
Transmission runtime	80Dx	Used to define common transmission runtime errors
Reception runtime	80Ex	Used to define common reception runtime errors
Signal handling	80Fx	Used to define common errors associated with all signal handling

14.6.1 Legacy point-to-point instructions

14.6.1.1 PORT_CFG (Configure communication parameters dynamically)

Table 14-98 PORT_CFG (Port Configuration) instruction

LAD / FBD	SCL	Description
	**"PORT_CFG_DB"(** **REQ:=_bool_in_,** **PORT:=_uint_in_,** **PROTOCOL:=_uint_in_,** **BAUD:=_uint_in_,** **PARITY:=_uint_in_,** **DATABITS:=_uint_in_,** **STOPBITS:=_uint_in_,** **FLOWCTRL:=_uint_in_,** **XONCHAR:=_char_in_,** **XOFFCHAR:=_char_in_,** **WAITTIME:=_uint_in_,** **DONE=>_bool_out_,** **ERROR=>_bool_out_,** **STATUS=>_word_out_);**	PORT_CFG allows you to change port parameters such as baud rate from your program. You can set up the initial static configuration of the port in the device configuration properties, or just use the default values. You can execute the PORT_CFG instruction in your program to change the configuration.

[1] STEP 7 automatically creates the DB when you insert the instruction.

The PORT_CFG configuration changes are not permanently stored in the CPU. The parameters configured in the device configuration are restored when the CPU transitions from RUN to STOP mode and after a power cycle. See Configuring the communication ports (Page 842) and Managing flow control (Page 844) for more information.

Table 14-99 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activate the configuration change on rising edge of this input. (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
PROTOCOL	IN	UInt	0 - Point-to-Point communication protocol (Default value) 1..n - future definition for specific protocols
BAUD	IN	UInt	Port baud rate (Default value: 6): 1 = 300 baud, 2 = 600 baud, 3 = 1200 baud, 4 = 2400 baud, 5 = 4800 baud, 6 = 9600 baud, 7 = 19200 baud, 8 = 38400 baud, 9 = 57600 baud, 10 = 76800 baud, 11 = 115200 baud
PARITY	IN	UInt	Port parity (Default value: 1): 1 = No parity, 2 = Even parity, 3 = Odd parity, 4 = Mark parity, 5 = Space parity
DATABITS	IN	UInt	Bits per character (Default value:1): 1 = 8 data bits, 2 = 7 data bits
STOPBITS	IN	UInt	Stop bits (Default value: 1): 1 = 1 stop bit, 2 = 2 stop bits
FLOWCTRL	IN	UInt	Flow control (Default value: 1): 1 = No flow control, 2 = XON/XOFF, 3 = Hardware RTS always ON, 4 = Hardware RTS switched
XONCHAR	IN	Char	Specifies the character that is used as the XON character. This is typically a DC1 character (16#11). This parameter is only evaluated if flow control is enabled. (Default value: 16#11)
XOFFCHAR	IN	Char	Specifies the character that is used as the XOFF character. This is typically a DC3 character (116#3). This parameter is only evaluated if flow control is enabled. (Default value: 16#13)
XWAITIME	IN	UInt	Specifies how long to wait for a XON character after receiving a XOFF character, or how long to wait for the CTS signal after enabling RTS (0 to 65535 ms). This parameter is only evaluated if flow control is enabled. (Default value: 2000)
DONE	OUT	Bool	TRUE for one execution after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one execution after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

Table 14-100 Condition codes

STATUS (W#16#....)	Description
80A0	Specific protocol does not exist.
80A1	Specific baud rate does not exist.
80A2	Specific parity option does not exist.
80A3	Specific number of data bits does not exist.
80A4	Specific number of stop bits does not exist.
80A5	Specific type of flow control does not exist.
80A6	Wait time is 0 and flow control enabled
80A7	XON and XOFF are illegal values (for example, the same value)

14.6.1.2 SEND_CFG (Configure serial transmission parameters dynamically)

Table 14-101 SEND_CFG (Send Configuration) instruction

LAD / FBD	SCL	Description
	"SEND_CFG_DB"(**REQ:=_bool_in_,** **PORT:=_uint_in_,** **RTSONDLY:=_uint_in_,** **RTSOFFDLY:=_uint_in_,** **BREAK:=_uint_in_,** **IDLELINE:=_uint_in_,** **DONE=>_bool_out_,** **ERROR=>_bool_out_,** **STATUS=>_word_out_);**	SEND_CFG allows the dynamic configuration of serial transmission parameters for a PtP communication port. Any queued messages within a CM or CB are discarded when SEND_CFG is executed.

[1] STEP 7 automatically creates the DB when you insert the instruction.

You can set up the initial static configuration of the port in the device configuration properties, or just use the default values. You can execute the SEND_CFG instruction in your program to change the configuration.

The SEND_CFG configuration changes are not permanently stored in the CPU. The parameters configured in the device configuration are restored when the CPU transitions from RUN to STOP mode and after a power cycle. See Configuring transmit (send) parameters (Page 846).

Table 14-102 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activate the configuration change on the rising edge of this input.. (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
RTSONDLY	IN	UInt	Number of milliseconds to wait after enabling RTS before any Tx data transmission occurs. This parameter is only valid when hardware flow control is enabled. The valid range is 0 - 65535 ms. A value of 0 disables the feature. (Default value: 0)

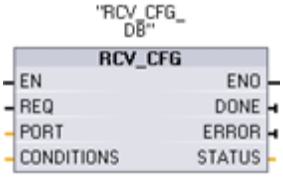
Parameter and type		Data type	Description
RTSOFFDLY	IN	UInt	Number of milliseconds to wait after the Tx data transmission occurs before RTS is disabled: This parameter is only valid when hardware flow control is enabled. The valid range is 0 - 65535 ms. A value of 0 disables the feature. (Default value: 0)
BREAK	IN	UInt	This parameter specifies that a break will be sent upon the start of each message for the specified number of bit times. The maximum is 65535 bit times up to an eight second maximum. A value of 0 disables the feature. (Default value: 12)
IDLELINE	IN	UInt	This parameter specifies that the line will remain idle for the specified number of bit times before the start of each message. The maximum is 65535 bit times up to an eight second maximum. A value of 0 disables the feature. (Default value: 12)
DONE	OUT	Bool	TRUE for one execution after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one execution after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

Table 14-103 Condition codes

STATUS (W#16#....)	Description
80B0	Transmit interrupt configuration is not allowed.
80B1	Break time is greater than the maximum allowed value.
80B2	Idle time is greater than the maximum allowed value.

14.6.1.3 RCV_CFG (Configure serial receive parameters dynamically)

Table 14-104 RCV_CFG (Receive Configuration) instruction

LAD / FBD	SCL	Description
	**"RCV_CFG_DB"(REQ:=_bool_in_, PORT:=_uint_in_, CONDITIONS:=_struct_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	RCV_CFG performs dynamic configuration of serial receiver parameters for a PtP communication port. This instruction configures the conditions that signal the start and end of a received message. Any queued messages within a CM or CB are discarded when RCV_CFG is executed.

[1] STEP 7 automatically creates the DB when you insert the instruction.

You can set up the initial static configuration of the communication port in the device configuration properties, or just use the default values. You can execute the RCV_CFG instruction in your program to change the configuration.

The RCV_CFG configuration changes are not permanently stored in the CPU. The parameters configured in the device configuration are restored when the CPU transitions from RUN to STOP mode and after a power cycle. See Configuring receive parameters (Page 847) for more information.

Table 14-105 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Activate the configuration change on the rising edge of this input. (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
CONDITIONS	IN	CONDITIONS	The Conditions data structure specifies the starting and ending message conditions as described below.
DONE	OUT	Bool	TRUE for one scan, after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one scan, after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

Start conditions for the RCV_PTP instruction

The RCV_PTP instruction uses the configuration specified by the RCV_CFG instruction to determine the beginning and ending of point-to-point communication messages. The start of a message is determined by the start conditions. The start of a message can be determined by one or a combination of start conditions. If more than one start condition is specified, all the conditions must be satisfied before the message is started.

See the topic "Configuring receive parameters (Page 847)" for a description of the message start conditions.

Parameter CONDITIONS data type structure part 1 (start conditions)

Table 14-106 CONDITIONS structure for START conditions

Parameter and type		Data type	Description
STARTCOND	IN	UInt	Specifies the start condition (Default value: 1) • 01H - Start Char • 02H - Any Char • 04H - Line Break • 08H - Idle Line • 10H - Sequence 1 • 20H - Sequence 2 • 40H - Sequence 3 • 80H - Sequence 4
IDLETIME	IN	UInt	The number of bit times required for idle line timeout. (Default value: 40). Only used with an idle line condition. 0 to 65535
STARTCHAR	IN	Byte	The start character used with the start character condition. (Default value: B#16#2)

Parameter and type		Data type	Description
SEQ[1].CTL	IN	Byte	Sequence 1 ignore/compare control for each character: (Default value: B#16#0) These are the enabling bits for each character in start sequence • 01H - Character 1 • 02H - Character 2 • 04H - Character 3 • 08H - Character 4 • 10H - Character 5 Disabling the bit associated with a character means any character will match, in this sequence position.
SEQ[1].STR	IN	Char[5]	Sequence 1 start characters (5 characters). Default value: 0
SEQ[2].CTL	IN	Byte	Sequence 2 ignore/compare control for each character. Default value: B#16#0)
SEQ[2].STR	IN	Char[5]	Sequence 2 start characters (5 characters). Default value: 0
SEQ[3].CTL	IN	Byte	Sequence 3 ignore/compare control for each character. Default value: B#16#0
SEQ[3].STR	IN	Char[5]	Sequence 3 start characters (5 characters). Default value: 0
SEQ[4].CTL	IN	Byte	Sequence 4 ignore/compare control for each character. Default value: B#16#0
SEQ[4].STR	IN	Char[5]	Sequence 4 start characters (5 characters), Default value: 0

Example

Consider the following received hexadecimal coded message: "**68** 10 aa **68** bb 10 aa 16" and the configured start sequences shown in the table below. Start sequences begin to be evaluated when the first 68H character is successfully received. Upon successfully receiving the fourth character (the second 68H), then start condition 1 is satisfied. Once the start conditions are satisfied, the evaluation of the end conditions begins.

The start sequence processing can be terminated due to various parity, framing, or inter-character timing errors. These errors result in no received message, because the start condition was not satisfied.

Table 14-107 Start conditions

Start condition	First Character	First Character +1	First Character +2	First Character +3	First Character +4
1	**68**H	xx	xx	**68**H	xx
2	10H	aaH	xx	xx	xx
3	dcH	aaH	xx	xx	xx
4	e5H	xx	xx	xx	xx

End conditions for the RCV_PTP instruction

The end of a message is determined by the specification of end conditions. The end of a message is determined by the first occurrence of one or more configured end conditions. The section "Message end conditions" in the topic "Configuring receive parameters (Page 847)" describes the end conditions that you can configure in the RCV_CFG instruction.

You can configure the end conditions in either the properties of the communication interface in the device configuration, or from the RCV_CFG instruction. Whenever the CPU transitions from STOP to RUN, the receive parameters (both start and end conditions) return to the device configuration settings. If the STEP 7 user program executes RCV_CFG, then the settings are changed to the RCV_CFG conditions.

Parameter CONDITIONS data type structure part 2 (end conditions)

Table 14-108 CONDITIONS structure for END conditions

Parameter	Parameter type	Data type	Description
ENDCOND	IN	UInt 0	This parameter specifies message end condition: • 01H - Response time • 02H - Message time • 04H - Inter-character gap • 08H - Maximum length • 10H - N + LEN + M • 20H - Sequence
MAXLEN	IN	UInt 1	Maximum message length: Only used when the maximum length end condition is selected. 1 to 1024 bytes
N	IN	UInt 0	Byte position within the message of the length field. Only used with the N + LEN + M end condition. 1 to 1022 bytes
LENGTHSIZE	IN	UInt 0	Size of the length field (1, 2, or 4 bytes). Only used with the N + LEN + M end condition.
LENGTHM	IN	UInt 0	Specify the number of characters following the length field that are not included in the value of the length field. This is only used with the N + LEN + M end condition. 0 to 255 bytes
RCVTIME	IN	UInt 200	Specify how long to wait for the first character to be received. The receive operation will be terminated with an error if a character is not successfully received within the specified time. This is only used with the response time condition. (0 to 65535 bit times with an 8 second maximum) This parameter is not a message end condition since evaluation terminates when the first character of a response is received. It is an end condition only in the sense that it terminates a receiver operation because no response is received when a response is expected. You must select a separate end condition.
MSGTIME	IN	UInt 200	Specify how long to wait for the entire message to be completely received once the first character has been received. This parameter is only used when the message timeout condition is selected. (0 to 65535 milliseconds)
CHARGAP	IN	UInt 12	Specify the number of bit times between characters. If the number of bit times between characters exceeds the specified value, then the end condition will be satisfied. This is only used with the inter-character gap condition. (0 to 65535 bit times up to 8 second maximum)

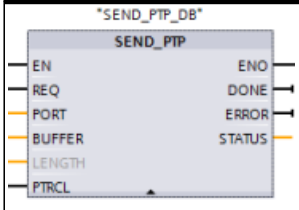
Parameter	Parameter type	Data type	Description
SEQ.CTL	IN	Byte B#16#0	Sequence 1 ignore/compare control for each character: These are the enabling bits for each character for the end sequence. Character 1 is bit 0, character 2 is bit 1, ..., character 5 is bit 4. Disabling the bit associated with a character means any character will match, in this sequence position.
SEQ.STR	IN	Char[5] 0	Sequence 1 start characters (5 characters)

Table 14-109 Condition codes

STATUS (W#16#....)	Description
80C0	Illegal start condition selected
80C1	Illegal end condition selected, no end condition selected
80C2	Receive interrupt enabled and this is not possible.
80C3	Maximum length end condition is enabled and max length is 0 or > 1024.
80C4	Calculated length is enabled and N is >= 1023.
80C5	Calculated length is enabled and length is not 1, 2 or 4.
80C6	Calculated length is enabled and M value is > 255.
80C7	Calculated length is enabled and calculated length is > 1024.
80C8	Response timeout is enabled and response timeout is zero.
80C9	Inter-character gap timeout is enabled and it is zero.
80CA	Idle line timeout is enabled and it is zero.
80CB	End sequence is enabled but all chars are "don't care".
80CC	Start sequence (any one of 4) is enabled but all characters are "don't care".

14.6.1.4 SEND_PTP (Transmit send buffer data)

Table 14-110 SEND_PTP (Send Point-to-Point data) instruction

LAD / FBD	SCL	Description
	**"SEND_PTP_DB"(** **REQ:=_bool_in_,** **PORT:=_uint_in_,** **BUFFER:=_variant_in_,** **LENGTH:=_uint_in_,** **PTRCL:=_bool_in_,** **DONE=>_bool_out_,** **ERROR=>_bool_out_,** **STATUS=>_word_out_);**	SEND_PTP initiates the transmission of the data and transfers the assigned buffer to the communication interface. The CPU program continues while the CM or CB sends the data at the assigned baud rate. Only one send operation can be pending at a given time. The CM or CB returns an error if a second SEND_PTP is executed while the CM or CB is already transmitting a message.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 14-111 Data types for the parameters

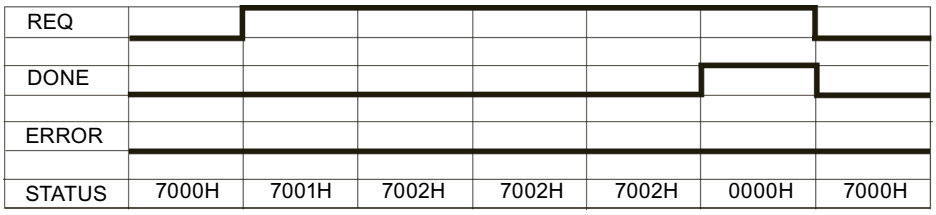
Parameter and type		Data type	Description
REQ	IN	Bool	Activates the requested transmission on the rising edge of this transmission enable input. This initiates transfer of the contents of the buffer to the Point-to-Point communication interface. (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
BUFFER	IN	Variant	This parameter points to the starting location of the transmit buffer. (Default value: 0) **Note:** Boolean data or Boolean arrays are not supported.
LENGTH [1]	IN	UInt	Transmitted frame length in bytes (Default value: 0) When transmitting a complex structure, always use a length of 0.
PTRCL	IN	Bool	Reserved for future use
DONE	OUT	Bool	TRUE for one scan, after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one scan, after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

[1] Optional parameter: Click the arrow at the bottom of a LAD/FBD box to expand the box and include this parameter.

While a transmit operation is in progress, the DONE and ERROR outputs are FALSE. When a transmit operation is complete, either the DONE or the ERROR output will be set TRUE to show the status of the transmit operation. While DONE or ERROR is TRUE, the STATUS output is valid.

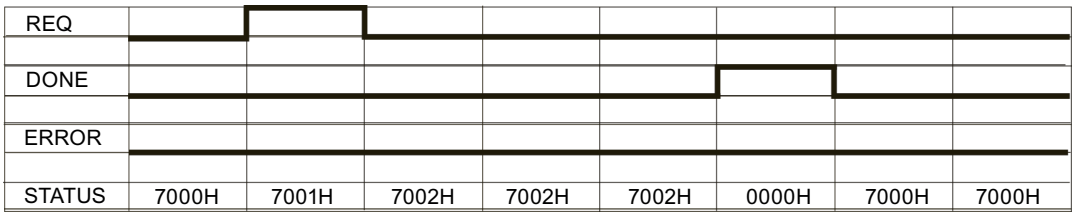
The instruction returns a status of 16#7001 if the communication interface accepts the transmit data. Subsequent SEND_PTP executions return 16#7002, if the CM or CB is still busy transmitting. When the transmit operation is complete, the CM or CB returns the status of the transmit operation as 16#0000 (if no errors occurred). Subsequent executions of SEND_PTP with REQ low return a status of 16#7000 (not busy).

The following diagrams show the relationship of the output values to REQ. This assumes that the instruction is called periodically to check for the status of the transmission process. In the diagram below, it is assumed that the instruction is called every scan (represented by the STATUS values).



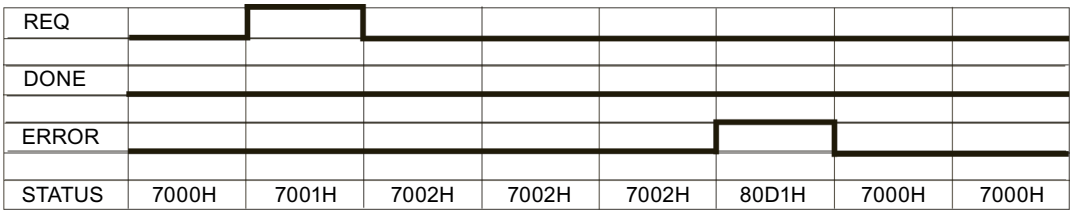
Figure

The following diagram shows how the DONE and STATUS parameters are valid for only one scan if the REQ line is pulsed (for one scan) to initiate the transmit operation.



Figure

The following diagram shows the relationship of DONE, ERROR and STATUS parameters when there is an error.



Figure

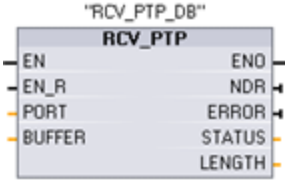
The DONE, ERROR and STATUS values are only valid until SEND_PTP executes again with the same instance DB.

Table 14-112 Condition codes

STATUS (W#16#....)	Description
80D0	New request while transmitter active
80D1	Transmit aborted because of no CTS within wait time
80D2	Transmit aborted because of no DSR from the DCE device
80D3	Transmit aborted because of queue overflow (transmit more than 1024 bytes)
80D5	Reverse bias signal (wire break condition)
833A	The DB for the BUFFER parameter does not exist.

14.6.1.5 RCV_PTP (Enable receive messages)

Table 14-113 RCV_PTP (Receive Point-to-Point) instruction

LAD / FBD	SCL	Description
	**"RCV_PTP_DB"(EN_R:=_bool_in_, PORT:=_uint_in_, BUFFER:=_variant_in_, NDR=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, LENGTH=>_uint_out_);**	RCV_PTP checks for messages that have been received in the CM or CB. If a message is available, it will be transferred from the CM or CB to the CPU. An error returns the appropriate STATUS value.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 14-114 Data types for the parameters

Parameter and type		Data type	Description
EN_R	IN	Bool	When this input is TRUE and a message is available, the message is transferred from the CM or CB to the BUFFER. When EN_R is FALSE, the CM or CB is checked for messages and NDR, ERROR and STATUS output are updated, but the message is not transferred to the BUFFER. (Default value: 0)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
BUFFER	IN	Variant	This parameter points to the starting location of the receive buffer. This buffer should be large enough to receive the maximum length message. Boolean data or Boolean arrays are not supported. (Default value: 0)
NDR	OUT	Bool	TRUE for one execution when new data is ready and operation is complete with no errors.
ERROR	OUT	Bool	TRUE for one execution after the operation was completed with an error.
STATUS	OUT	Word	Execution condition code (Default value: 0)
LENGTH	OUT	UInt	Length of the returned message in bytes (Default value: 0)

Note the following correlation between the EN_R input and the message buffer of the RCV_PTP instruction:

Input EN_R controls the copy of a received message to the BUFFER.

When the EN_R input is TRUE and a message is available, the CPU transfers the message from the CM or CB to the BUFFER and updates the NDR, ERROR, STATUS, and LENGTH outputs.

When EN_R is FALSE, the CPU checks the CM or CB for messages and updates the NDR, ERROR, and STATUS outputs, but does not transfer the message to the BUFFER. (Note that the default value of EN_R is FALSE.)

The recommended practice is to set EN_R to TRUE and control execution of the RCV_PTP instruction with the EN input.

The STATUS value is valid when either NDR or ERROR is TRUE. The STATUS value provides the reason for termination of the receive operation in the CM or CB. This is typically a positive value, indicating that the receive operation was successful and that the receive process terminated normally. If the STATUS value is negative (the Most Significant Bit of the hexadecimal value is set), the receive operation was terminated for an error condition such as parity, framing, or overrun errors.

Each PtP communication interface can buffer up to a maximum of 1024 bytes. This could be one large message or several smaller messages. If more than one message is available in the CM or CB, the RCV_PTP instruction returns the oldest message available. A subsequent RCV_PTP instruction execution returns the next oldest message available.

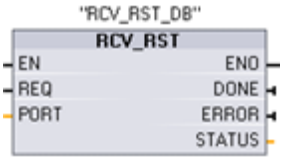
Table 14-115 Condition codes

STATUS (W#16#...)	Description
0000	No buffer present
0094	Message terminated due to received maximum character length
0095	Message terminated because of message timeout
0096	Message terminated because of inter-character timeout
0097	Message terminated because of response timeout
0098	Message terminated because the "N+LEN+M" length condition was satisfied

STATUS (W#16#...)	Description
0099	Message terminated because of end sequence was satisfied
80E0	Message terminated because the receive buffer is full
80E1	Message terminated due to parity error
80E2	Message terminated due to framing error
80E3	Message terminated due to overrun error
80E4	Message terminated because calculated length exceeds buffer size
80E5	Reverse bias signal (wire break condition)
833A	The DB for the BUFFER parameter does not exist.

14.6.1.6 RCV_RST (Delete receive buffer)

Table 14-116 RCV_RST (Receiver Reset) instruction

LAD / FBD	SCL	Description
	**"RCV_RST_DB"(REQ:=_bool_in_, PORT:=_uint_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	RCV_RST clears the receive buffers in the CM or CB.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 14-117 Data types for parameters

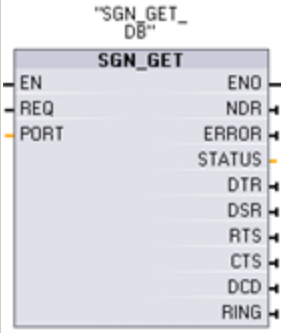
Parameter and type		Data type	Description
REQ	IN	Bool	Activates the receiver reset on the rising edge of this enable input (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
DONE	OUT	Bool	When TRUE for one scan, indicates that the last request was completed without errors.
ERROR	OUT	Bool	When TRUE, shows that the last request was completed with errors. Also, when this output is TRUE, the STATUS output will contain related error codes.
STATUS	OUT	Word	Error code (Default value: 0) See Common parameters for Point-to-Point instructions (Page 857) for communication status codes.

NOTE

You might want to use the RCV_RST instruction to be sure the message buffers are clear following a communications error, or after changing a communication parameter such as the baud rate. Executing RCV_RST causes the module to clear all of the internal message buffers. After clearing the message buffers, you can be assured that when your program executes a subsequent receive instruction, the messages it returns are new messages and not old messages from some time prior to the RCV_RST call.

14.6.1.7 SGN_GET (Query RS-232 signals)

Table 14-118 SGN_GET (Get RS232 signals) instruction

LAD / FBD	SCL	Description
	**"SGN_GET_DB"(** **REQ:=_bool_in_,** **PORT:=_uint_in_,** **NDR=>_bool_out_,** **ERROR=>_bool_out_,** **STATUS=>_word_out_,** **DTR=>_bool_out_,** **DSR=>_bool_out_,** **RTS=>_bool_out_,** **CTS=>_bool_out_,** **DCD=>_bool_out_,** **RING=>_bool_out_);**	SGN_GET reads the current states of RS232 communication signals. This function is valid only for the RS232 CM.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 14-119 Data types for the parameters

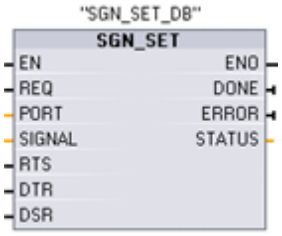
Parameter and type		Data type	Description
REQ	IN	Bool	Get RS232 signal state values on the rising edge of this input (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table.
NDR	OUT	Bool	TRUE for one scan, when new data is ready and the operation is complete with no errors
ERROR	OUT	Bool	TRUE for one scan, after the operation was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)
DTR	OUT	Bool	Data terminal ready, module ready (output). Default value: False
DSR	OUT	Bool	Data set ready, communication partner ready (input). Default value: False
RTS	OUT	Bool	Request to send, module ready to send (output). Default value: False
CTS	OUT	Bool	Clear to send, communication partner can receive data (input). Default value: False
DCD	OUT	Bool	Data carrier detect, receive signal level (always False, not supported)
RING	OUT	Bool	Ring indicator, indication of incoming call (always False, not supported)

Table 14-120 Condition codes

STATUS (W#16#....)	Description
80F0	CM or CB is RS485 and no signals are available

14.6.1.8 SGN_SET (Set RS-232 signals)

Table 14-121 SGN_SET (Set RS232 signals) instruction

LAD / FBD	SCL	Description
	**"SGN_SET_DB"(REQ:=_bool_in_, PORT:=_uint_in_, SIGNAL:=_byte_in_, RTS:=_bool_in_, DTR:=_bool_in_, DSR:=_bool_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_);**	SGN_SET sets the states of RS232 communication signals. This function is valid only for the RS232 CM.

[1] STEP 7 automatically creates the DB when you insert the instruction.

Table 14-122 Data types for parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Start the set RS232 signals operation, on the rising edge of this input (Default value: False)
PORT	IN	PORT	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table. (Default value: 0)
SIGNAL	IN	Byte	Selects which signal to set: (multiple allowed). Default value: 0 • 01H = Set RTS • 02H = Set DTR • 04H = Set DSR
RTS	IN	Bool	Request to send, module ready to send value to set (true or false), Default value: False
DTR	IN	Bool	Data terminal ready, module ready to send value to set (true or false). Default value: False
DSR	IN	Bool	Data set ready (only applies to DCE type interfaces), not used.
DONE	OUT	Bool	TRUE for one execution after the last request was completed with no error
ERROR	OUT	Bool	TRUE for one execution after the last request was completed with an error
STATUS	OUT	Word	Execution condition code (Default value: 0)

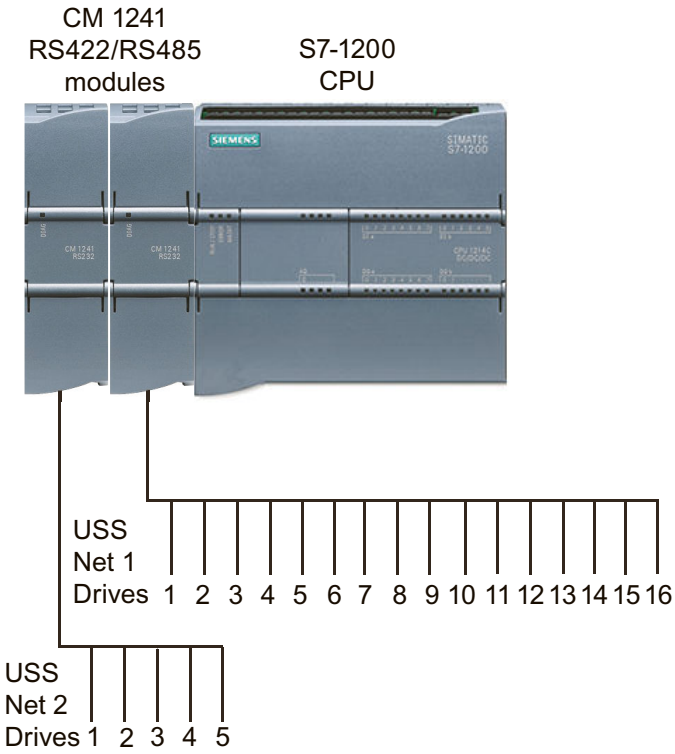
Table 14-123 Condition codes

STATUS (W#16#....)	Description
80F0	CM or CB is RS485 and no signals can be set
80F1	Signals cannot be set because of Hardware flow control
80F2	Cannot set DSR because module is DTE
80F3	Cannot set DTR because module is DCE

14.7 Legacy USS communication (CM/CB 1241 only)

The USS instructions control the operation of motor drives which support the universal serial interface (USS) protocol. You can use the USS instructions to communicate with multiple drives through RS485 connections to CM 1241 RS485 communication modules or a CB 1241 RS485 communication board. Up to three CM 1241 RS422/RS485 modules and one CB 1241 RS485 board can be installed in a S7-1200 CPU. Each RS485 port can operate up to sixteen drives.

The USS protocol uses a master-slave network for communications over a serial bus. The master uses an address parameter to send a message to a selected slave. A slave itself can never transmit without first receiving a request to do so. Direct message transfer between the individual slaves is not possible. USS communication operates in half-duplex mode. The following USS illustration shows a network diagram for an example drive application.



Note that STEP 7 provides different versions of the USS instructions. For information on instruction versions, refer to Use Instruction versions (https://support.industry.siemens.com/cs/ww/en/view/109798671/113722878475) in the STEP 7 Information System.

Requirements for using the USS protocol

The four USS instructions use 2 FBs and 2 FCs to support the USS protocol. For each USS network, one instance data block (DB) is used for USS_Port_Scan and one instance data block for all calls of USS_Drive_Conrol. For further requirements, refer to the topic "Requirements for using the USS protocol (https://support.industry.siemens.com/cs/ww/en/view/109798671/140076559243)" in the STEP 7 Information System or on Siemens Industry Online Support.

14.7.1 Legacy USS instructions

14.7.1.1 USS_PORT (Edit communication using USS network) instruction

Table 14-124 USS_PORT instruction

LAD / FBD	SCL	Description
	USS_PORT(**PORT:=_uint_in_,** **BAUD:=_dint_in_,** **ERROR=>_bool_out_,** **STATUS=>_word_out_,** **USS_DB:=_fbtref_inout_);**	The USS_PORT instruction handles communication over a USS network.

Table 14-125 Data types for the parameters

Parameter and type		Data type	Description
PORT	IN	Port	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table.
BAUD	IN	DInt	The baud rate used for USS communication.
USS_DB	INOUT	USS_BASE	The name of the instance DB that is created and initialized when a USS_DRV instruction is placed in your program.
ERROR	OUT	Bool	When true, this output indicates that an error has occurred and the STATUS output is valid.
STATUS	OUT	Word	The status value of the request indicates the result of the scan or initialization. Additional information is available in the "USS_Extended_Error" variable for some status codes.

Typically, there is only one USS_PORT instruction per PtP communication port in the program, and each call of this function handles a transmission to or from a single drive. All USS functions associated with one USS network and PtP communication port must use the same instance DB.

Your program must execute the USS_PORT instruction often enough to prevent drive timeouts. USS_PORT is usually called from a cyclic interrupt OB to prevent drive timeouts and keep the most recent USS data updates available for USS_DRV calls.

14.7.1.2 USS_DRV (Swap data with drive) instruction

Table 14-126 USS_DRV instruction

LAD / FBD	SCL	Description
Default view Expanded view 	**"USS_DRV_DB"(** **RUN:=_bool_in_,** **OFF2:=_bool_in_,** **OFF3:=_bool_in_,** **F_ACK:=_bool_in_,** **DIR:=_bool_in_,** **DRIVE:=_usint_in_,** **PZD_LEN:=_usint_in_,** **SPEED_SP:=_real_in_,** **CTRL3:=_word_in_,** **CTRL4:=_word_in_,** **CTRL5:=_word_in_,** **CTRL6:=_word_in_,** **CTRL7:=_word_in_,** **CTRL8:=_word_in_,** **NDR=>_bool_out_,** **ERROR=>_bool_out_,** **STATUS=>_word_out_,** **RUN_EN=>_bool_out_,** **D_DIR=>_bool_out_,** **INHIBIT=>_bool_out_,** **FAULT=>_bool_out_,** **SPEED=>_real_out_,** **STATUS1=>_word_out_,** **STATUS3=>_word_out_,** **STATUS4=>_word_out_,** **STATUS5=>_word_out_,** **STATUS6=>_word_out_,** **STATUS7=>_word_out_,** **STATUS8=>_word_out_);**	The USS_DRV instruction exchanges data with a drive by creating request messages and interpreting the drive response messages. A separate function block should be used for each drive, but all USS functions associated with one USS network and PtP communication port must use the same instance data block. You must create the DB name when you place the first USS_DRV instruction and then reference the DB that was created by the initial instruction usage. STEP 7 automatically creates the DB when you insert the instruction.

[1] LAD and FBD: Expand the box to reveal all the parameters by clicking the bottom of the box. The parameter pins that are grayed are optional and parameter assignment is not required.

Table 14-127 Data types for the parameters

Parameter and type		Data type	Description
RUN	IN	Bool	Drive start bit: When true, this input enables the drive to run at the preset speed. When RUN goes to false while a drive is running, the motor will be ramped down to a stop. This behavior differs from the dropping power (OFF2) or braking the motor (OFF3).
OFF2	IN	Bool	Electrical stop bit: When false, this bit causes the drive to coast to a stop with no braking.
OFF3	IN	Bool	Fast stop bit: When false, this bit causes a fast stop by braking the drive rather than just allowing the drive to coast to a stop.
F_ACK	IN	Bool	Fault acknowledge bit: This bit is set to reset the fault bit on a drive. The bit is set after the fault is cleared to indicate to the drive it no longer needs to indicate the previous fault.
DIR	IN	Bool	Drive direction control: This bit is set to indicate that the direction is forward (for positive SPEED_SP).
DRIVE	IN	USInt	Drive address: This input is the address of the USS drive. The valid range is drive 1 to drive 16.

Parameter and type		Data type	Description
PZD_LEN	IN	USInt	Word length: This is the number of words of PZD data. The valid values are 2, 4, 6, or 8 words. The default value is 2.
SPEED_SP	IN	Real	Speed set point: This is the speed of the drive as a percentage of configured frequency. A positive value specifies forward direction (when DIR is true). Valid range is 200.00 to -200.00.
CTRL3	IN	Word	Control word 3: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
CTRL4	IN	Word	Control word 4: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
CTRL5	IN	Word	Control word 5: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
CTRL6	IN	Word	Control word 6: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
CTRL7	IN	Word	Control word 7: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
CTRL8	IN	Word	Control word 8: A value written to a user-configurable parameter on the drive. You must configure this on the drive. (optional parameter)
NDR	OUT	Bool	New data ready: When true, the bit indicates that the outputs contain data from a new communication request.
ERROR	OUT	Bool	Error occurred: When true, this indicates that an error has occurred and the STATUS output is valid. All other outputs are set to zero on an error. Communication errors are only reported on the USS_PORT instruction ERROR and STATUS outputs.
STATUS	OUT	Word	The status value of the request indicates the result of the scan. This is not a status word returned from the drive.
RUN_EN	OUT	Bool	Run enabled: This bit indicates whether the drive is running.
D_DIR	OUT	Bool	Drive direction: This bit indicates whether the drive is running forward.
INHIBIT	OUT	Bool	Drive inhibited: This bit indicates the state of the inhibit bit on the drive.
FAULT	OUT	Bool	Drive fault: This bit indicates that the drive has registered a fault. You must fix the problem and then set the F_ACK bit to clear this bit when set.
SPEED	OUT	Real	Drive Current Speed (scaled value of drive status word 2): The value of the speed of the drive as a percentage of configured speed.
STATUS1	OUT	Word	Drive Status Word 1: This value contains fixed status bits of a drive.
STATUS3	OUT	Word	Drive Status Word 3: This value contains a user-configurable status word on the drive.
STATUS4	OUT	Word	Drive Status Word 4: This value contains a user-configurable status word on the drive.
STATUS5	OUT	Word	Drive Status Word 5: This value contains a user-configurable status word on the drive.
STATUS6	OUT	Word	Drive Status Word 6: This value contains a user-configurable status word on the drive.
STATUS7	OUT	Word	Drive Status Word 7: This value contains a user-configurable status word on the drive.
STATUS8	OUT	Word	Drive Status Word 8: This value contains a user-configurable status word on the drive.

When the initial USS_DRV execution occurs, the drive indicated by the USS address (parameter DRIVE) is initialized in the Instance DB. After this initialization, subsequent executions of USS_PORT can begin communication to the drive at this drive number.

Changing the drive number requires a CPU STOP-to-RUN mode transition that initializes the instance DB. Input parameters are configured into the USS TX message buffer and outputs are read from a "previous" valid response buffer if any exists. There is no data transmission during USS_DRV execution. Drives communicate when USS_PORT is executed. USS_DRV only configures the messages to be sent and interprets data that might have been received from a previous request.

You can control the drive direction of rotation using either the DIR input (Bool) or using the sign (positive or negative) with the SPEED_SP input (Real). The following table indicates how these inputs work together to determine the drive direction, assuming the motor is wired for forward rotation.

Table 14-128 Interaction of the SPEED_SP and DIR parameters

SPEED_SP	DIR	Drive rotation direction
Value > 0	0	Reverse
Value > 0	1	Forward
Value < 0	0	Forward
Value < 0	1	Reverse

14.7.1.3 USS_RPM (Readout parameters from the drive) instruction

Table 14-129 USS_RPM instruction

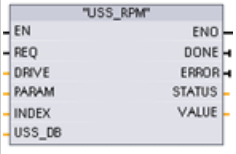
LAD / FBD	SCL	Description
	**USS_RPM(REQ:=_bool_in_, DRIVE:=_usint_in_, PARAM:=_uint_in_, INDEX:=_uint_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, VALUE=>_variant_out_, USS_DB:=_fbtref_inout_);**	The USS_RPM instruction reads a parameter from a drive. All USS functions associated with one USS network and PtP communication port must use the same data block. USS_RPM must be called from a main program cycle OB.

Table 14-130 Data types for the parameters

Parameter type		Data type	Description
REQ	IN	Bool	Send request: When true, REQ indicates that a new read request is desired. This is ignored if the request for this parameter is already pending.
DRIVE	IN	USInt	Drive address: DRIVE is the address of the USS drive. The valid range is drive 1 to drive 16.
PARAM	IN	UInt	Parameter number: PARAM designates which drive parameter is written. The range of this parameter is 0 to 2047. On some drives, the most significant byte can access PARAM values greater than 2047. See your drive manual for details on how to access an extended range.
INDEX	IN	UInt	Parameter index: INDEX designates which Drive Parameter index is to be written. A 16-bit value where the Least Significant Byte is the actual index value with a range of (0 to 255). The Most Significant Byte may also be used by the drive and is drive-specific. See your drive manual for details.
USS_DB	INOUT	USS_BASE	The name of the instance DB that is created and initialized when a USS_DRV instruction is placed in your program.
VALUE	IN	Word, Int, UInt, DWord, DInt, UDInt, Real	This is the value of the parameter that was read and is valid only when the DONE bit is true.
DONE[1]	OUT	Bool	When true, indicates that the VALUE output holds the previously requested read parameter value. This bit is set when USS_DRV sees the read response data from the drive. This bit is reset when either: you request the response data via another USS_RPM poll, or on the second of the next two calls to USS_DRV
ERROR	OUT	Bool	Error occurred: When true, ERROR indicates that an error has occurred and the STATUS output is valid. All other outputs are set to zero on an error. Communication errors are only reported on the USS_PORT instruction ERROR and STATUS outputs.
STATUS	OUT	Word	STATUS indicates the result of the read request. Additional information is available in the "USS_Extended_Error" variable for some status codes.

[1] The DONE bit indicates that valid data has been read from the referenced motor drive and delivered to the CPU. It does not indicate that the USS library is capable of immediately reading another parameter. A blank PKW request must be sent to the motor drive and must also be acknowledged by the instruction before the parameter channel for the specific drive becomes available for use. Immediately calling a USS_RPM or USS_WPM FC for the specified motor drive will result in a 0x818A error.

14.7.1.4 USS_WPM (Change parameters in the drive) instruction

NOTE

EEPROM write operations (for the EEPROM inside a USS drive)

Do not overuse the EEPROM permanent write operation. Minimize the number of EEPROM write operations to extend the EEPROM life.

Table 14-131 USS_WPM instruction

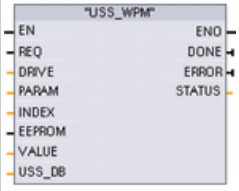
LAD / FBD	SCL	Description
	**USS_WPM(REQ:=_bool_in_, DRIVE:=_usint_in_, PARAM:=_uint_in_, INDEX:=_uint_in_, EEPROM:=_bool_in_, VALUE:=_variant_in_, DONE=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, USS_DB:=_fbtref_inout_);**	The USS_WPM instruction modifies a parameter in the drive. All USS functions associated with one USS network and PtP communication port must use the same data block. USS_WPM must be called from a main program cycle OB.

Table 14-132 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	Send request: When true, REQ indicates that a new write request is desired. This is ignored if the request for this parameter is already pending.
DRIVE	IN	USInt	Drive address: DRIVE is the address of the USS drive. The valid range is drive 1 to drive 16.
PARAM	IN	UInt	Parameter number: PARAM designates which drive parameter is written. The range of this parameter is 0 to 2047. On some drives, the most significant byte can access PARAM values greater than 2047. See your drive manual for details on how to access an extended range.
INDEX	IN	UInt	Parameter index: INDEX designates which Drive Parameter index is to be written. A 16-bit value where the least significant byte is the actual index value with a range of (0 to 255). The most significant byte may also be used by the drive and is drive-specific. See your drive manual for details.
EEPROM	IN	Bool	Store To Drive EEPROM: When true, a write drive parameter transaction will be stored in the drive EEPROM. If false, the write is temporary and will not be retained if the drive is power cycled.
VALUE	IN	Word, Int, UInt, DWord, DInt, UDInt, Real	The value of the parameter that is to be written. It must be valid on the transition of REQ.
USS_DB	INOUT	USS_BASE	The name of the instance DB that is created and initialized when a USS_DRV instruction is placed in your program.
DONE[1]	OUT	Bool	When true, DONE indicates that the input VALUE has been written to the drive. This bit is set when USS_DRV sees the write response data from the drive. This bit is reset when either you request the response data via another USS_WPM poll, or on the second of the next two calls to USS_DRV
ERROR	OUT	Bool	When true, ERROR indicates that an error has occurred and the STATUS output is valid. All other outputs are set to zero on an error. Communication errors are only reported on the USS_PORT instruction ERROR and STATUS outputs.
STATUS	OUT	Word	STATUS indicates the result of the write request. Additional information is available in the "USS_Extended_Error" variable for some status codes.

[1] The DONE bit indicates that valid data has been read from the referenced motor drive and delivered to the CPU. It does not indicate that the USS library is capable of immediately reading another parameter. A blank PKW request must be sent to the motor drive and must also be acknowledged by the instruction before the parameter channel for the specific drive becomes available for use. Immediately calling a USS_RPM or USS_WPM FC for the specified motor drive will result in a 0x818A error.

14.7.2 Legacy USS status codes

USS instruction status codes are returned at the STATUS output of the USS functions.

Table 14-133 STATUS codes [1]

STATUS (W#16#....)	Description
0000	No error
8180	The length of the drive response did not match the characters received from the drive. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
8181	VALUE parameter was not a Word, Real or DWord data type.
8182	The user supplied a Word for a parameter value and received a DWord or Real from the drive in the response.
8183	The user supplied a DWord or Real for a parameter value and received a Word from the drive in the response.
8184	The response telegram from drive had a bad checksum. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
8185	Illegal drive address (valid drive address range: 1 to16)
8186	The speed set point is out of the valid range (valid speed SP range: -200% to 200%).
8187	The wrong drive number responded to the request sent. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
8188	Illegal PZD word length specified (valid range = 2, 4, 6 or 8 words)
8189	Illegal Baud Rate was specified.
818A	The parameter request channel is in use by another request for this drive.
818B	The drive has not responded to requests and retries. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
818C	The drive returned an extended error on a parameter request operation. See the extended error description below this table.
818D	The drive returned an illegal access error on a parameter request operation. See your drive manual for information of why parameter access may be limited.
818E	The drive has not been initialized. This error code is returned to USS_RPM or USS_WPM when USS_DRV, for that drive, has not been called at least once. This keeps the initialization on first scan of USS_DRV from overwriting a pending parameter read or write request, since it initializes the drive as a new entry. To fix this error, call USS_DRV for this drive number.
80Ax-80Fx	Specific errors returned from PtP communication FBs called by the USS Library - These error code values are not modified by the USS library and are defined in the PtP instruction descriptions.

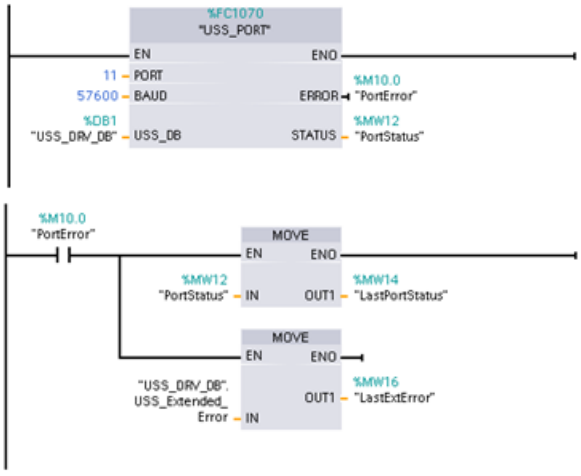
[1] In addition to the USS instruction errors listed above, errors can be returned from the underlying PtP communication instructions (Page 990).

For several STATUS codes, additional information is provided in the "USS_Extended_Error" variable of the USS_DRV Instance DB. For STATUS codes hexadecimal 8180, 8184, 8187, and 818B, USS_Extended_Error contains the drive number where the communication error occurred. For STATUS code hexadecimal 818C, USS_Extended_Error contains a drive error code returned from the drive when using a USS_RPM or USS_WPM instruction.

Example: communication errors reporting

Communication errors (STATUS = 16#818B) are only reported on the USS_PORT instruction and not on the USS_DRV instruction. For example, if the network is not properly terminated

then it is possible for a drive to go to RUN but the USS_DRV instruction will show all 0's for the output parameters. In this case, you can only detect the communication error on the USS_PORT instruction. Since this error is only visible for one scan, you will need to add some capture logic as illustrated in the following example. In this example, when the error bit of the USS_PORT instruction is TRUE, then the STATUS and the USS_Extended_Error values are saved into M memory. The drive number is placed in USS_Extended_Error variable when the STATUS code value is hexadecimal 8180, 8184, 8187, or 818B.



Network 1"PortStatus"port status and"USS_DRV_DB".USS_Extended_Errorextended error code values are only valid for one program scan. The values must be captured for later processing.

Network 2 The "PortError" contact triggers the storage of the "PortStatus" value in "LastPortStatus" and the"USS_DRV_DB".USS_Extended_Errorvalue in "LastExtError".

Read and write access to drive internal parameters

USS drives support read and write access to a drive's internal parameters. This feature allows remote control and configuration of the drive. Drive parameter access operations can fail due to errors such as values out of range or illegal requests for a drive's current mode. The drive generates an error code value that is returned in the "USS_Extended_Error" variable. This error code value is only valid for the last execution of a USS_RPM or USS_WPM instruction. The drive error code is put into USS_Extended_Error variable when the STATUS code value is hexadecimal 818C. The error code value of "USS_Extended_Error" depends on the drive model. See the drive's manual for a description of the extended error codes for read and write parameter operations.

14.7.3 Legacy USS general drive setup requirements

Legacy USS general drive setup requirements consist of the following points:

- The drives must be set to use 4 PKW words.
- The drives can be configured for 2, 4, 6, or 8 PZD words.
- The number of PZD word's in the drive must match PZD_LEN input on the USS_DRV instruction for that drive.
- The baud rate in all the drives must match the BAUD input on the USS_PORT instruction.
- The drive must be set for remote control.
- The drive must be set for frequency set-point to USS on COM Link.
- The drive address must be set to 1 to 16 and match the DRIVE input on the USS_DRV block for that drive.

- The drive direction control must be set to use the polarity of the drive set-point.
- The RS485 network must be terminated properly.

USS general drive connection and setup is the same for USS instructions (V4.1) and legacy USS instructions (V4.0 and earlier). Refer to the Example: USS general drive connection and setup (Page 900) for further information.

14.8 Legacy Modbus TCP communication

14.8.1 Overview

Prior to the release of STEP 7 V13 SP1 and the S7-1200 V4.1 CPUs, the Modbus TCP communication instructions existed with different names, and in some cases, slightly different interfaces. The general concepts apply to both sets of instructions. Refer to the individual legacy Modbus TCP instructions for programming information.

STEP 7 provides different versions of the Modbus TCP instructions. For information on instruction versions, refer to Use Instruction versions (https://support.industry.siemens.com/cs/ww/en/view/109798671/113722878475) in the STEP 7 Information System.

14.8.2 Legacy Modbus TCP instructions

14.8.2.1 MB_CLIENT (Communicate using PROFINET as Modbus TCP client)

Table 14-134 MB_CLIENT instruction

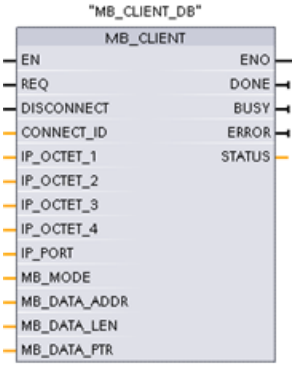
LAD / FBD	SCL	Description
	**"MB_CLIENT_DB"(REQ:=_bool_in_, DISCONNECT:=_bool_in_, CONNECT_ID=_uint_in_, IP_OCTET_1:=_byte_in_, IP_OCTET_2:=_byte_in_, IP_OCTET_3:=_byte_in_, IP_OCTET_4:=_byte_in_, IP_PORT:=_uint_in_, MB_MODE:=_usint_in_, MB_DATA_ADDR:=_udint_in_, MB_DATA_LEN:=_uint_in_, DONE=>_bool_out_, BUSY=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, MB_DATA_PTR:=_variant_inout_);**	MB_CLIENT communicates as a Modbus TCP client through the PROFINET connector on the S7-1200 CPU. No additional communication hardware module is required. MB_CLIENT can make a client-server connection, send a Modbus function request, receive a response, and control the disconnection from a Modbus TCP server.

Table 14-135 Data types for the parameters

Parameter and type		Data type	Description
REQ	In	Bool	FALSE = No Modbus communication request TRUE = Request to communicate with a Modbus TCP server
DISCONNECT	IN	Bool	The DISCONNECT parameter allows your program to control connection and disconnection with a Modbus server device. If DISCONNECT = 0 and a connection does not exist, then MB_CLIENT attempts to make a connection to the assigned IP address and port number. If DISCONNECT = 1 and a connection exists, then a disconnect operation is attempted. Whenever this input is enabled, no other operation will be attempted.
CONNECT_ID	IN	UInt	The CONNECT_ID parameter must uniquely identify each connection within the PLC. Each unique instance of the MB_CLIENT or MB_SERVER instruction must contain a unique CONNECT_ID parameter.
IP_OCTET_1	IN	USInt	Modbus TCP server IP address: Octet 1 8-bit part of the 32-bit IPv4 IP address of the Modbus TCP server to which the client will connect and communicate using the Modbus TCP protocol.
IP_OCTET_2	IN	USInt	Modbus TCP server IP address: Octet 2
IP_OCTET_3	IN	USInt	Modbus TCP server IP address: Octet 3
IP_OCTET_4	IN	USInt	Modbus TCP server IP address: Octet 4
IP_PORT	IN	UInt	Default value = 502: The IP port number of the server to which the client will attempt to connect and ultimately communicate using the TCP/IP protocol.
MB_MODE	IN	USInt	Mode Selection: Assigns the type of request (read, write, or diagnostic). See the Modbus functions table below for details.
MB_DATA_ADDR	IN	UDInt	Modbus starting Address: Assigns the starting address of the data to be accessed by MB_CLIENT. See the Modbus functions table below for valid addresses.
MB_DATA_LEN	IN	UInt	Modbus data Length: Assigns the number of bits or words to be accessed in this request. See the Modbus functions table below for valid lengths
MB_DATA_PTR	IN_OUT	Variant	Pointer to the Modbus data register: The register buffers data going to or coming from a Modbus server. The pointer must assign a non-optimized global DB or a M memory address.
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error.
BUSY	OUT	Bool	• 0 - No MB_CLIENT operation in progress • 1 - MB_CLIENT operation in progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the MB_CLIENT execution was terminated with an error. The error code value at the STATUS parameter is valid only during the single cycle where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code

REQ parameter

FALSE = No Modbus communication request
TRUE = Request to communicate with a Modbus TCP server

If no instance of MB_CLIENT is active and parameter DISCONNECT=0, when REQ=1 a new Modbus request will start. If the connection is not already established then a new connection will be made.

If the same instance of MB_CLIENT is executed again with DISCONNECT=0 and REQ=1, before the completion of the current request, then no subsequent Modbus transmission will be made. However, as soon as the current request is completed, a new request can be processed if MB_CLIENT is executed with REQ=1.

When the current MB_CLIENT communication request is complete, the DONE bit is TRUE for one cycle. The DONE bit can be used as a time gate to sequence multiple MB_CLIENT requests.

NOTE

Input data consistency during MB_CLIENT processing

Once a Modbus client initiates a Modbus operation, all the input states are saved internally and are then compared on each successive call. The comparison is used to determine if this particular call was the originator of the active client request. More than one MB_CLIENT call can be performed using a common instance DB.

As a result, it is important that the inputs are not changed during the period of time that a MB_CLIENT operation is actively being processed. If this rule is not followed, then a MB_CLIENT cannot determine that it is the active instance.

MB_MODE and MB_DATA_ADDR parameters select the Modbus communication function

MB_DATA_ADDR assigns the starting Modbus address of the data to be accessed. The MB_CLIENT instruction uses a MB_MODE input rather than a function code input.

The combination of MB_MODE and MB_DATA_ADDR values determine the function code that is used in the actual Modbus message. The following table shows the correspondence between parameter MB_MODE, Modbus function, and Modbus address range.

Table 14-136 Modbus functions

MB_MODE	Modbus function	Data length	Operation and data	MB_DATA_ADDR
0	01	1 to 2000	Read output bits: 1 to 2000 bits per request	1 to 9999
0	02	1 to 2000	Read input bits: 1 to 2000 bits per request	10001 to 19999
0	03	1 to 125	Read Holding registers: 1 to 125 words per request	40001 to 49999 or 400001 to 465535
0	04	1 to 125	Read input words: 1 to 125 words per request	30001 to 39999
1	05	1	Write one output bit: One bit per request	1 to 9999
1	06	1	Write one holding register: 1 word per request	40001 to 49999 or 400001 to 465535
1	15	2 to 1968	Write multiple output bits: 2 to 1968 bits per request	1 to 9999
1	16	2 to 123	Write multiple holding registers: 2 to 123 words per request	40001 to 49999 or 400001 to 465535

MB_MODE	Modbus function	Data length	Operation and data	MB_DATA_ADDR
2	15	1 to 1968	Write one or more output bits: 1 to 1968 bits per request	1 to 9999
2	16	1 to 123	Write one or more holding registers: 1 to 123 words per request	40001 to 49999 or 400001 to 465535
11	11	0	Read the server communication status word and event counter. The status word indicates busy (0 – not busy, 0xFFFF - busy). The event counter is incremented for each successful completion of a message. Both the MB_DATA_ADDR and MB_DATA_LEN parameters of MB_CLIENT are ignored for this function.	
80	08	1	Check server status using data diagnostic code 0x0000 (Loopback test – server echoes the request) 1 word per request	
81	08	1	Reset server event counter using data diagnostic code 0x000A 1 word per request	
3 to 10, 12 to 79, 82 to 255			Reserved	

NOTE

MB_DATA_PTR assigns a buffer to store data read/written to/from a Modbus TCP server

The data buffer can be in a non-optimized global DB or M memory address.

For a buffer in M memory, use the standard Any Pointer format. This is in the format P#"Bit Address" "Data Type" "Length", an example would be P#M1000.0 WORD 500.

MB_DATA_PTR assigns a communication buffer

- MB_CLIENT communication functions:
  - Read and write 1-bit data from Modbus server addresses (00001 to 09999)
  - Read 1-bit data from Modbus server addresses (10001 to 19999)
  - Read 16-bit word data from Modbus server addresses (30001 to 39999) and (40001 to 49999)
  - Write 16-bit word data to Modbus server addresses (40001 to 49999)
- Word or bit sized data is transferred to/from the DB or M memory buffer assigned by MB_DATA_PTR.

- If a DB is assigned as the buffer by MB_DATA_PTR, then you must assign data types to all DB data elements.
  - The 1-bit Bool data type represents one Modbus bit address
  - 16-bit single word data types like WORD, UInt, and Int represent one Modbus word address
  - 32-bit double word data types like DWORD, DInt, and Real represent two Modbus word addresses
- Complex DB elements can be assigned by MB_DATA_PTR, such as
  - Standard arrays
  - Named structures where each element is unique.
  - Named complex structures where each element has a unique name and a 16 or 32 bit data type.
- There is no requirement that the MB_DATA_PTR data areas be in the same global data block (or M memory area). You can assign one data block for Modbus reads, another data block for Modbus writes, or one data block for each MB_CLIENT station.

Multiple client connections

A Modbus TCP client can support concurrent connections up to the maximum number of Open User Communications connections allowed by the PLC. The total number of connections for a PLC, including Modbus TCP Clients and Servers, must not exceed the maximum number of supported Open User Communications connections (Page 526). The Modbus TCP connections may be shared between Client and/or Server type connections.

Individual client connections must follow these rules:

- Each MB_CLIENT connection must use a distinct instance DB
- Each MB_CLIENT connection must specify a unique server IP address
- Each MB_CLIENT connection must specify a unique connection ID
- Unique IP port numbers may or may not be required depending upon the server configuration

The Connection ID must be unique for each individual connection. This means a single, unique Connection ID must only be used with each individual instance DB. In summary, the instance DB and the Connection ID are paired together and must be unique for every connection.

Table 14-137 MB_CLIENT instance data block user accessible static variables

Variable	Data type	Default	description
Blocked_Proc_Timeout	Real	3.0	Amount of time (in seconds) to wait upon a blocked Modbus client instance before removing this instance as being ACTIVE. This can occur, for example, when a client request has been issued and then application stops executing the client function before it has completely finished the request. The maximum S7-1200 limit is 55 seconds.
MB_Unit_ID	Word	255	Modbus unit identifier: A Modbus TCP server is addressed using its IP address. As a result, the MB_UNIT_ID parameter is not used for Modbus TCP addressing. The MB_UNIT_ID parameter corresponds to the slave address in the Modbus RTU protocol. If a Modbus TCP server is used for a gateway to a Modbus RTU protocol, the MB_UNIT_ID can be used to identify the slave device connected on the serial network. The MB_UNIT_ID would

Variable	Data type	Default	description
			be used to forward the request to the correct Modbus RTU slave address. Some Modbus TCP devices may require the MB_UNIT_ID parameter to be initialized within a restricted range of values.
RCV_TIMEOUT	Real	2.0	Time in seconds that the MB_CLIENT waits for a server to respond to a request.
Connected	Bool	0	Indicates whether the connection to the assigned server is connected or disconnected: 1=connected, 0=disconnected

Table 14-138 MB_CLIENT protocol errors

STATUS (W#16#)	Response code to Modbus client (B#16#)	Modbus protocol errors
8381	01	Function code not supported
8382	03	Data length error
8383	02	Data address error or access outside the bounds of the MB_HOLD_REG address area
8384	03	Data value error
8385	03	Data diagnostic code value not supported (function code 08)

Table 14-139 MB_CLIENT execution condition codes [1]

STATUS (W#16#)	MB_CLIENT parameter errors
7001	MB_CLIENT is waiting for a Modbus server response to a connect or disconnect request, on the assigned TCP port. This is only reported for the first execution of a connect or disconnect operation.
7002	MB_CLIENT is waiting for a Modbus server response to a connect or disconnect request, for the assigned TCP port. This will be reported for any subsequent executions, while waiting for completion of a connect or disconnect operation.
7003	A disconnect operation has successfully completed (Only valid for one PLC scan).
80C8	The server did not respond in the assigned time. MB_CLIENT must receive a response using the transaction ID that was originally transmitted within the assigned time or this error is returned. Check the connection to the Modbus server device. This error is only reported after any configured retries (if applicable) have been attempted.
8188	Invalid mode value
8189	Invalid data address value
818A	Invalid data length value
818B	Invalid pointer to the DATA_PTR area. This can be the combination of MB_DATA_ADDRESS + MB_DATA_LEN.
818C	Pointer to a optimized DATA_PTR area (must be a non-optimized DB area or M memory area)
8200	The port is busy processing an existing Modbus request.
8380	Received Modbus frame is malformed or too few bytes have been received.
8387	The assigned Connection ID parameter is different from the ID used for previous requests. There can only be a single Connection ID used within each MB_CLIENT instance DB. This is also used as an internal error if the Modbus TCP protocol ID received from a server is not 0.
8388	A Modbus server returned a quantity of data that is different than what was requested. This applies to Modbus functions 15 or 16 only.

[1] In addition to the MB_CLIENT errors listed above, errors can be returned from the underlying T block communication instructions (TCON, TDISCON, TSEND, and TRCV (Page 578)).

14.8.2.2 MB_SERVER (Communicate using PROFINET as Modbus TCP server)

The "MB_SERVER" instruction communicates as Modbus TCP server through the PROFINET connector on the S7-1200 CPU. The "MB_SERVER" instruction processes connection requests of a Modbus TCP client, receives and processes Modbus requests, and sends responses.

To use the instruction, you do not require an additional hardware module.

⚠ WARNING

Risks with access to the process image

Each Modbus TCP client has read and write access to the process image inputs and outputs, and to the data block or bit memory area defined by the Modbus holding register. Unauthorized read and write operations can change PLC variables into invalid values and disrupt process operations.

To reduce the risk of unauthorized access, restrict access to an IP address of a specific Modbus client. For information on additional industrial security measures that can be implemented, please visit the Siemens Industrial Cybersecurity site (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

Disruption of process operations can result in death, severe injury and/or property damage.

Table 14-140 MB_SERVER instruction

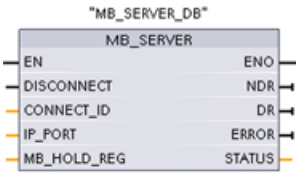
LAD / FBD	SCL	Description
	**"MB_SERVER_DB"(** **DISCONNECT:=_bool_in_,** **CONNECT_ID:=_uint_in_,** **IP_PORT:=_uint_in_,** **NDR=>_bool_out_,** **DR=>_bool_out_,** **ERROR=>_bool_out_,** **STATUS=>_word_out_,** **MB_HOLD_REG:=_variant_inout_);**	MB_SERVER communicates as a Modbus TCP server through the PROFINET connector on the S7-1200 CPU. No additional communication hardware module is required. MB_SERVER can accept a request to connect with Modbus TCP client, receive a Modbus function request, and send a response message.

Table 14-141 Data types for the parameters

Parameter and type		Data type	Description
DISCONNECT	IN	Bool	MB_SERVER attempts to make a "passive" connection with a partner device. This means that the server is passively listening for a TCP connection request from any requesting IP address. If DISCONNECT = 0 and a connection does not exist, then a passive connection can be initiated. If DISCONNECT = 1 and a connection exists, then a disconnect operation is initiated. This allows your program to control when a connection is accepted. Whenever this input is enabled, no other operation will be attempted.
CONNECT_ID	IN	UInt	CONNECT_ID uniquely identifies each connection within the PLC. Each unique instance of the MB_CLIENT or MB_SERVER instruction must contain a unique CONNECT_ID parameter.
IP_PORT	IN	UInt	Default value = 502: The IP port number that identifies the IP port that will be monitored for a connection request from a Modbus client.
MB_HOLD_REG	IN_OUT	Variant	Pointer to the MB_SERVER Modbus holding register: The holding register must either be a non-optimized global DB or a M memory address. This memory area is used to hold the values a Modbus client is allowed to access using Modbus register functions 3 (read), 6 (write), and 16 (write).

Parameter and type		Data type	Description
NDR	OUT	Bool	New Data Ready: 0 = No new data, 1 = Indicates that new data has been written by a Modbus client
DR	OUT	Bool	Data Read: 0 = No data read, 1 = Indicates that data has been read by a Modbus client.
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after MB_SERVER execution was terminated with an error. The error code value at the STATUS parameter is valid only during the single cycle where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code

MB_SERVER allows incoming Modbus function codes (1, 2, 4, 5, and 15) to read or write bits and words directly in the input process image and output process image of the S7-1200 CPU. For data transfer function codes (3, 6, and 16), the MB_HOLD_REG parameter must be defined as a data type larger than a byte. The following table shows the mapping of Modbus addresses to the process image in the CPU.

Table 14-142 Mapping of Modbus addresses to the process image

Modbus functions						S7-1200	
Codes	Function	Data area	Address range			Data area	CPU address
01	Read bits	Output	1	To	8192	Output Process Image	Q0.0 to Q1023.7
02	Read bits	Input	10001	To	18192	Input Process Image	I0.0 to I1023.7
04	Read words	Input	30001	To	30512	Input Process Image	IW0 to IW1022
05	Write bit	Output	1	To	8192	Output Process Image	Q0.0 to Q1023.7
15	Write bits	Output	1	To	8192	Output Process Image	Q0.0 to Q1023.7

Incoming Modbus message function codes function codes (3, 6, and 16) read or write words in a Modbus holding register which can be an M memory address range or a data block. The type of holding register is specified by the MB_HOLD_REG parameter.

NOTE

MB_HOLD_REG parameter assignment

The Modbus Holding Register can be in a non-optimized global DB or an M memory address.

For A Modbus holding register in M memory, use the standard Any Pointer format. This is in the format P#"Bit Address" "Data Type" "Length". An example would be P#M1000.0 WORD 500

The following table shows examples of Modbus address to holding register mapping used for Modbus function codes 03 (read words), 06 (write word), and 16 (write words). The actual upper limit of DB addresses is determined by the maximum work memory limit and M memory limit, for each CPU model.

Table 14-143 Mapping examples of Modbus address to CPU memory address

Modbus Address	MB_HOLD_REG parameter examples		
	P#M100.0 Word 5	P#DB10.DBx0.0 Word 5	"Recipe".ingredient
40001	MW100	DB10.DBW0	"Recipe".ingredient[1]
40002	MW102	DB10.DBW2	"Recipe".ingredient[2]
40003	MW104	DB10.DBW4	"Recipe".ingredient[3]
40004	MW106	DB10.DBW6	"Recipe".ingredient[4]
40005	MW108	DB10.DBW8	"Recipe".ingredient[5]

Multiple server connections

Multiple server connections may be created. This permits a single PLC to establish concurrent connections to multiple Modbus TCP clients.

A Modbus TCP server can support concurrent connections up to the maximum number of Open User Communications connections allowed by the PLC. The total number of connections for a PLC, including Modbus TCP Clients and Servers, must not exceed the maximum number of supported Open User Communications connections (Page 526). The Modbus TCP connections may be shared between Client and/or Server type connections.

Individual server connection must follow these rules:

- Each MB_SERVER connection must use a distinct instance DB.
- Each MB_SERVER connection must be established with a unique IP port number. Only 1 connection per port is supported.
- Each MB_SERVER connection must use a unique connection ID.
- The MB_SERVER must be called individually for each connection (with its respective instance DB).

The Connection ID must be unique for each individual connection. This means a single, unique Connection ID must only be used with each individual instance DB. In summary, the instance DB and the Connection ID are paired together and must be unique for every connection.

Table 14-144 Modbus diagnostic function codes

MB_SERVER Modbus diagnostic functions		
Codes	Sub-function	Description
08	0x0000	Return query data echo test: The MB_SERVER will echo back to a Modbus client a word of data that is received.
08	0x000A	Clear communication event counter: The MB_SEVER will clear out the communication event counter that is used for Modbus function 11.
11		Get communication event counter: The MB_SERVER uses an internal communication event counter for recording the number of successful Modbus read and write requests that are sent to the Modbus server. The counter does not increment on any Function 8 or Function 11 requests. It is also not incremented on any requests that result in a communication error. The broadcast function is not available for Modbus TCP, because only one client-server connection exists at any one time.

MB_SERVER variables

This table shows the public static variables stored in the MB_SERVER instance data block that can be used in your program

Table 14-145 MB_SERVER public static variables

Variable	Data type	Default value	Description
HR_Start_Offset	Word	0	Assigns the starting address of the Modbus Holding register
Request_Count	Word	0	The number of all requests received by this server.
Server_Message_Count	Word	0	The number of requests received for this specific server.
Xmt_Rcv_Count	Word	0	The number of transmissions or receptions that have encountered an error. Also, incremented if a message is received that is an invalid Modbus message.

Variable	Data type	Default value	Description
Exception_Count	Word	0	Modbus specific errors that require a returned exception
Success_Count	Word	0	The number of requests received for this specific server that has no protocol errors.
Connected	Bool	0	Indicates whether the connection to the assigned client is connected or disconnected: 1=connected, 0=disconnected

Your program can write values to the HR_Start_Offset and control Modbus server operations. The other variables can be read to monitor Modbus status.

HR_Start_Offset

Modbus holding register addresses begin at 40001. These addresses correspond to the beginning PLC memory address of the holding register. However, you can configure the "HR_Start_Offset" variable to start the beginning Modbus holding register address at another value instead of 40001.

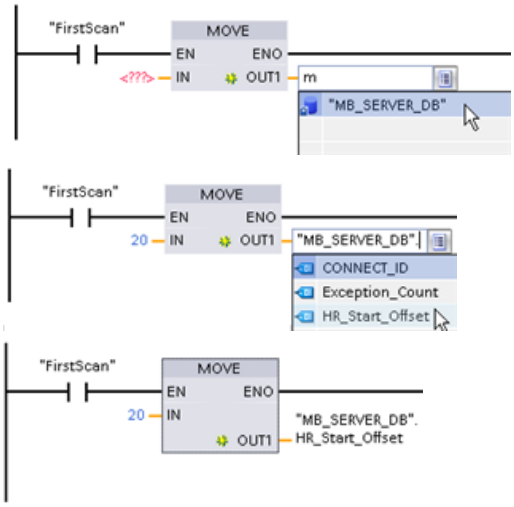
For example, if the holding register is configured to start at MW100 and is 100 words long. An offset of 20 specifies a beginning holding register address of 40021 instead of 40001. Any address below 40021 and above 40119 will result in an addressing error.

Table 14-146 Example of Modbus holding register addressing

HR_Start_Offset	Address	Minimum	Maximum
0	Modbus address (Word)	40001	40099
	S7-1200 address	MW100	MW298
20	Modbus address (Word)	40021	40119
	S7-1200 address	MW100	MW298

HR_Start_Offset is a word value that specifies the starting address of the Modbus holding register and is stored in the MB_SERVER instance data block. You can set this public static variable value by using the parameter helper drop-list, after MB_SERVER is placed in your program.

For example, after MB_SERVER is placed in a LAD network, you can go to a previous network and assign the HR_Start_Offset value. The value must be assigned prior to execution of MB_SERVER.



Entering a Modbus server variable using the default DB name:

1. Set the cursor in the parameter field and type an m character.
2. Select "MB_SERVER_DB" from the drop-list of DB names.
3. Select "MB_SERVER_DB.HR_Start_Offset" from the drop-list of DB variables.

Table 14-147 MB_SERVER execution condition codes [1]

STATUS (W#16#)	Response code to Modbus server (B#16#)	Modbus protocol errors
7001		MB_SERVER is waiting for a Modbus client to connect to the assigned TCP port. This code is reported on the first execution of a connect or disconnect operation.
7002		MB_SERVER is waiting for a Modbus client to connect to the assigned TCP port. This code is reported for any subsequent executions, while waiting for completion of a connect or disconnect operation.
7003		A disconnect operation has successfully completed (Only valid for one PLC scan).
8187		Invalid pointer to MB_HOLD_REG: area is too small
818C		Pointer to an optimized MB_HOLD_REG area (must be a non-optimized DB area or M memory area) or Blocked process timeout exceeds the limit of 55 seconds. (S7-1200 specific)
8381	01	Function code not supported
8382	03	Data length error
8383	02	Data address error or access outside the bounds of the MB_HOLD_REG address area
8384	03	Data value error
8385	03	Data diagnostic code value not supported (function code 08)

[1] In addition to the MB_SERVER errors listed above, errors can be returned from the underlying T block communication instructions (TCON, TDISCON, TSEND, and TRCV (Page 578)).

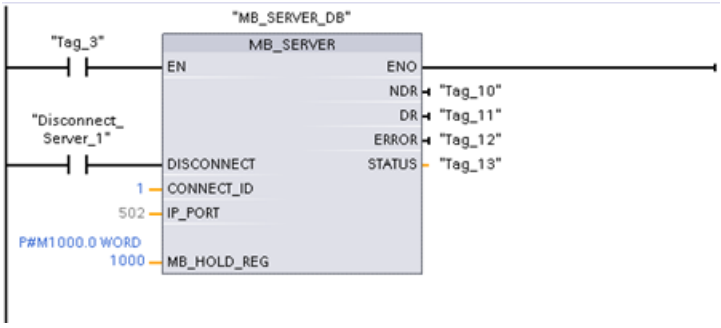
14.8.3 Legacy Modbus TCP examples

14.8.3.1 Example: Legacy MB_SERVER Multiple TCP connections

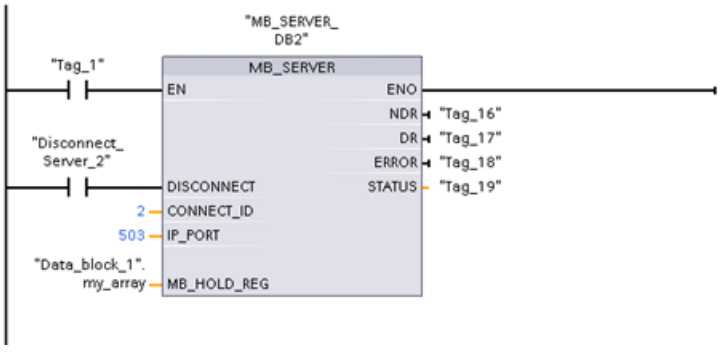
You can have multiple Modbus TCP server connections. To accomplish this, MB_SERVER must be independently executed for each connection. Each connection must use an independent instance DB, connection ID, and IP port. The S7-1200 allows only one connection per IP port.

For best performance, MB_SERVER should be executed every program cycle, for each connection.

Network 1: Connection #1 with independent IP_PORT, connection ID, and instance DB



Network 2: Connection #2 with independent IP_PORT, connection ID, and instance DB



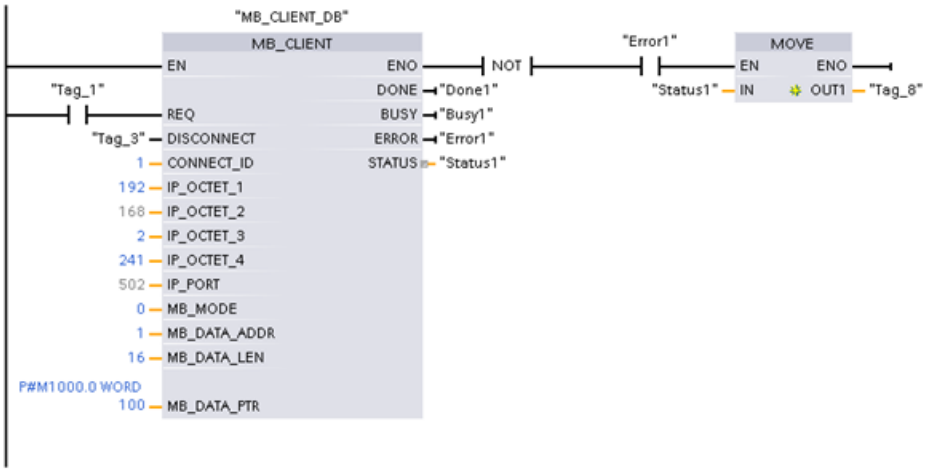
14.8.3.2 Example: Legacy MB_CLIENT 1: Multiple requests with common TCP connection

Multiple Modbus client requests can be sent over the same connection. To accomplish this, use the same instance DB, connection ID, and port number.

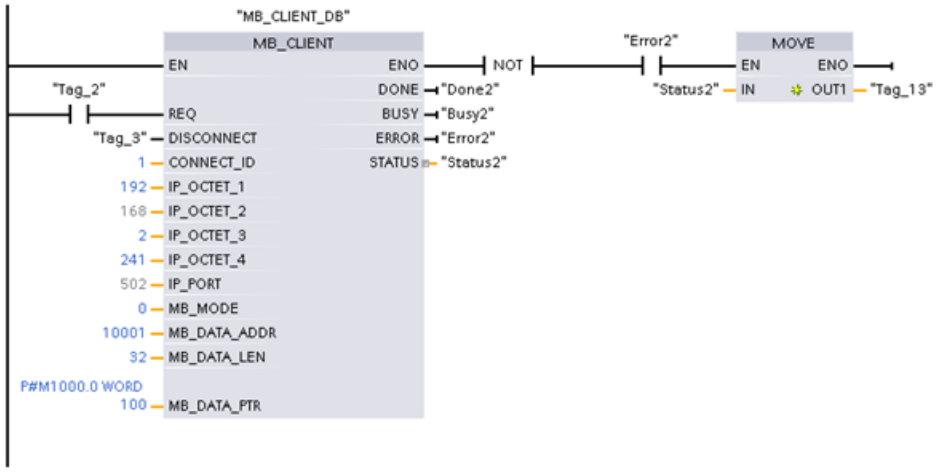
Only 1 client can be active at any given time. Once a client completes its execution, the next client begins execution. Your program is responsible for the order of execution.

The example shows both clients writing to the same memory area. Also, a returned error is captured which is optional.

Network 1: Modbus function 1 - Read 16 output image bits



Network 2: Modbus function 2 - Read 32 input image bits



14.8.3.3 Example: Legacy MB_CLIENT 2: Multiple requests with different TCP connections

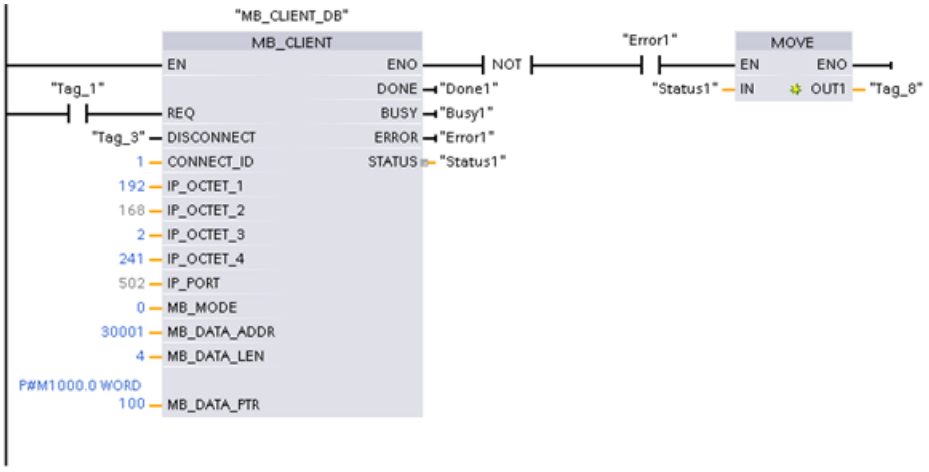
Modbus client requests can be sent over different connections. To accomplish this, different instance DBs, IP addresses, and connection IDs must be used.

The port number must be different if the connections are established to the same Modbus server. If the connections are on different servers, there is no port number restriction.

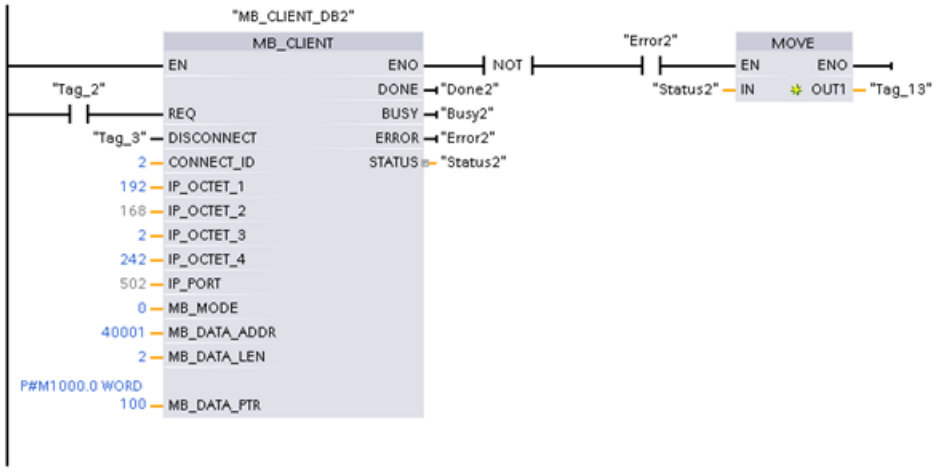
The example shows both clients writing to the same memory area. Also, a returned error is captured which is optional.

Network 1:

Modbus function 4 - Read input words (in S7-1200 memory)



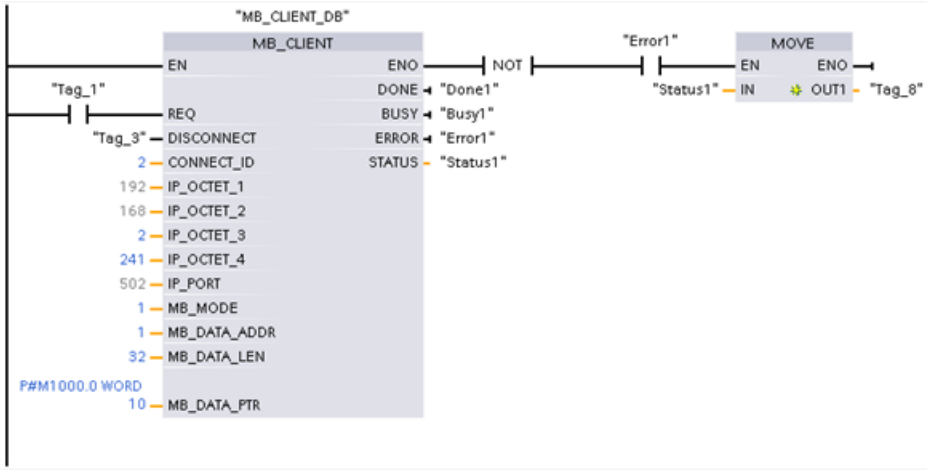
Network 2: Modbus function 3 - Read holding register words from a Modbus TCP server



14.8.3.4 Example: Legacy MB_CLIENT 3: Output image write request

This example shows a Modbus client request to write the S7-1200 output image.

Network 1: Modbus function 15 - Write S7-1200 output image bits

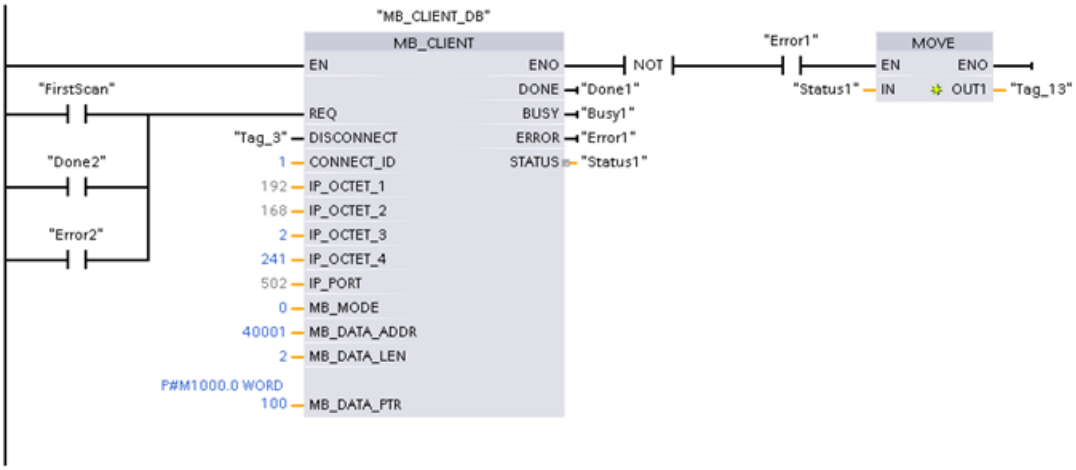


14.8.3.5 Example: Legacy MB_CLIENT 4: Coordinating multiple requests

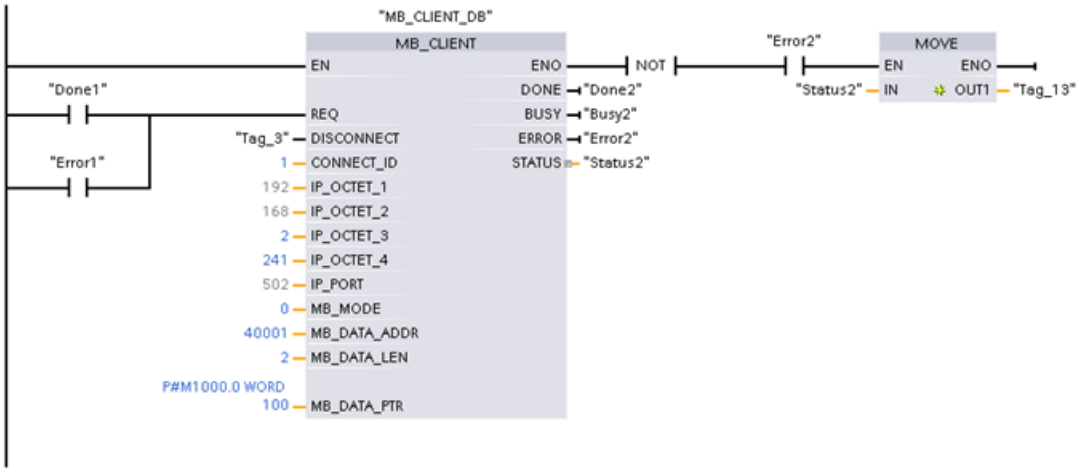
You must ensure that each individual Modbus TCP request finishes execution. This coordination must be provided by your program. The example below shows how the outputs of the first and second client requests can be used to coordinate execution.

The example shows both clients writing to the same memory area. Also, a returned error is captured which is optional.

Network 1: Modbus function 3 - Read holding register words



Network 2: Modbus function 3 - Read holding register words



14.9 Legacy Modbus RTU communication (CM/CB 1241 only)

14.9.1 Overview

Prior to the release of STEP 7 V13 SP1 and the S7-1200 V4.1 CPUs, the Modbus RTU communication instructions existed with different names, and in some cases, slightly different interfaces. The general concepts apply to both sets of instructions. Refer to the individual legacy Modbus RTU instructions for programming information.

STEP 7 provides different versions of the Modbus RTU instructions. For information on instruction versions, refer to Use Instruction versions (https://support.industry.siemens.com/cs/ww/en/view/109798671/113722878475) in the STEP 7 Information System.

14.9.2 Legacy Modbus RTU instructions

14.9.2.1 MB_COMM_LOAD (Configure port on the PtP module for Modbus RTU)

Table 14-148 MB_COMM_LOAD instruction

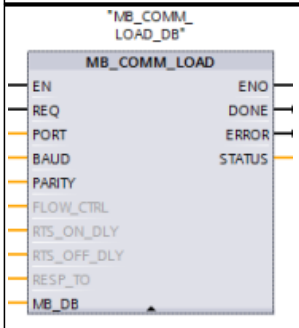
LAD / FBD	SCL	Description
	**"MB_COMM_LOAD_DB"(REQ:=_bool_in, PORT:=_uint_in_, BAUD:=_udint_in_, PARITY:=_uint_in_, FLOW_CTRL:=_uint_in_, RTS_ON_DLY:=_uint_in_, RTS_OFF_DLY:=_uint_in_, RESP_TO:=_uint_in_, DONE=>_bool_out, ERROR=>_bool_out_, STATUS=>_word_out_, MB_DB:=_fbtref_inout_);**	The MB_COMM_LOAD instruction configures a PtP port for Modbus RTU protocol communications. Modbus port hardware options: Install up to three CMs (RS485 or RS232), plus one CB (R4845). An instance data block is assigned automatically when you place the MB_COMM_LOAD instruction in your program.

Table 14-149 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	A low to high (positive edge) signal starts the operation. (Version 2.0 only)
PORT	IN	Port	After you install and configure a CM or CB communication device, the port identifier appears in the parameter helper drop-list available at the PORT box connection. The assigned CM or CB port value is the device configuration property "hardware identifier". The port symbolic name is assigned in the "System constants" tab of the PLC tag table.
BAUD	IN	UDInt	Baud rate selection: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 76800, 115200, all other values are invalid
PARITY	IN	UInt	Parity selection: • 0 – None • 1 – Odd • 2 – Even
FLOW_CTRL [1]	IN	UInt	Flow control selection: • 0 – (default) no flow control • 1 – Hardware flow control with RTS always ON (does not apply to RS485 ports) • 2 – Hardware flow control with RTS switched
RTS_ON_DLY [1]	IN	UInt	RTS ON delay selection: • 0 – (default) No delay from RTS active until the first character of the message is transmitted • 1 to 65535 – Delay in milliseconds from RTS active until the first character of the message is transmitted (does not apply to RS485 ports). RTS delays shall be applied independent of the FLOW_CTRL selection.
RTS_OFF_DLY [1]	IN	UInt	RTS OFF delay selection: • 0 – (default) No delay from the last character transmitted until RTS goes inactive • 1 to 65535 – Delay in milliseconds from the last character transmitted until RTS goes inactive (does not apply to RS485 ports). RTS delays shall be applied independent of the FLOW_CTRL selection.
RESP_TO [1]	IN	UInt	Response timeout: Time in milliseconds allowed by MB_MASTER for the slave to respond. If the slave does not respond in this time period, MB_MASTER will retry the request or terminate the request with an error when the specified number of retries has been sent. 5 ms to 65535 ms (default value = 1000 ms).
MB_DB	IN	Variant	A reference to the instance data block used by the MB_MASTER or MB_SLAVE instructions. After MB_SLAVE or MB_MASTER is placed in your program, the DB identifier appears in the parameter helper drop-list available at the MB_DB box connection.
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error. (Version 2.0 only)
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code

[1] Optional parameters for MB_COMM_LOAD (V 2.x or later). Click the arrow at the bottom of a LAD/FBD box to expand the box and include these parameters.

MB_COMM_LOAD is executed to configure a port for the Modbus RTU protocol. Once a port is configured for the Modbus RTU protocol, it can only be used by either the MB_MASTER or MB_SLAVE instructions.

One execution of MB_COMM_LOAD must be used to configure each communication port that is used for Modbus communication. Assign a unique MB_COMM_LOAD instance DB for each port that you use. You can install up to three communication modules (RS232 or RS485) and one communication board (RS485) in the CPU. Call MB_COMM_LOAD from a startup OB and execute it one time or use the first scan system flag (Page 83) to initiate the call to execute it one time. Only execute MB_COMM_LOAD again if communication parameters like baud rate or parity must change.

An instance data block is assigned for MB_MASTER or MB_SLAVE when you place these instructions in your program. This instance data block is referenced when you specify the MB_DB parameter for the MB_COMM_LOAD instruction.

MB_COMM_LOAD data block variables

The following table shows the public static variables stored in the instance DB for the MB_COMM_LOAD that can be used in your program.

Table 14-150 Static variables in the instance DB

Variable	Data type	Description
ICHAR_GAP	UInt	Delay for Inter-character gap between characters. This parameter is specified in milliseconds and is used to increase the expected amount of time between received characters. The corresponding number of bit times for this parameter is added to the Modbus default of 35 bit times (3.5 character times).
RETRIES	UInt	Number of retries that the master will attempt before returning the no response error code 0x80C8.
STOP_BITS	USInt	Number of stop bits used in framing each character. Valid values are 1 and 2.

Table 14-151 MB_COMM_LOAD execution condition codes [1]

STATUS (W#16#)	Description
0000	No error
8180	Invalid port ID value (wrong port/hardware identifier for communication module)
8181	Invalid baud rate value
8182	Invalid parity value
8183	Invalid flow control value
8184	Invalid response timeout value (response timeout less than the 5 ms minimum)
8185	MB_DB parameter is not an instance data block of a MB_MASTER or MB_SLAVE instruction.

[1] In addition to the MB_COMM_LOAD errors listed above, errors can be returned from the underlying PtP communication instructions.

14.9.2.2 MB_MASTER (Communicate using the PtP port as Modbus RTU master)

Table 14-152 MB_MASTER instruction

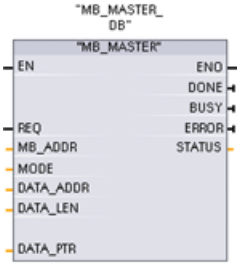
LAD / FBD	SCL	Description
	**"MB_MASTER_DB"(** **REQ:=_bool_in_,** **MB_ADDR:=_uint_in_,** **MODE:=_usint_in_,** **DATA_ADDR:=_udint_in_,** **DATA_LEN:=_uint_in_,** **DONE=>_bool_out_,** **BUSY=>_bool_out_,** **ERROR=>_bool_out_,** **STATUS=>_word_out_,** **DATA_PTR:=_variant_inout_);**	The MB_MASTER instruction communicates as a Modbus master using a port that was configured by a previous execution of the MB_COMM_LOAD instruction. An instance data block is assigned automatically when you place the MB_MASTER instruction in your program. This MB_MASTER instance data block is used when you specify the MB_DB parameter for the MB_COMM_LOAD instruction.

Table 14-153 Data types for the parameters

Parameter and type		Data type	Description
REQ	IN	Bool	0=No request 1= Request to transmit data to Modbus slave
MB_ADDR	IN	V1.0: USInt V2.0: UInt	Modbus RTU station address: Standard addressing range (1 to 247) Extended addressing range (1 to 65535) The value of 0 is reserved for broadcasting a message to all Modbus slaves. Modbus function codes 05, 06, 15 and 16 are the only function codes supported for broadcast.
MODE	IN	USInt	Mode Selection: Specifies the type of request (read, write, or diagnostic). See the Modbus functions table below for details.
DATA_ADDR	IN	UDInt	Starting Address in the slave: Specifies the starting address of the data to be accessed in the Modbus slave. See the Modbus functions table below for valid addresses.
DATA_LEN	IN	UInt	Data Length: Specifies the number of bits or words to be accessed in this request. See the Modbus functions table below for valid lengths.
DATA_PTR	IN	Variant	Data Pointer: Points to the M or DB address (non-optimized DB type) for the data being written or read.
DONE	OUT	Bool	The DONE bit is TRUE for one scan, after the last request was completed with no error.
BUSY	OUT	Bool	• 0 – No MB_MASTER operation in progress • 1 – MB_MASTER operation in progress
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. The error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution condition code

Modbus master communication rules

- MB_COMM_LOAD must be executed to configure a port before a MB_MASTER instruction can communicate with that port.
- If a port is to be used to initiate Modbus master requests, that port should not be used by MB_SLAVE. One or more instances of MB_MASTER execution can be used with that port, but all MB_MASTER execution must use the same MB_MASTER instance DB for that port.

- The Modbus instructions do not use communication interrupt events to control the communication process. Your program must poll the MB_MASTER instruction for transmit and receive complete conditions.
- Call all MB_MASTER execution for a given port from a program cycle OB. Modbus master instructions may execute in only one of the program cycle or cyclic/time delay execution levels. They must not execute in both execution priority levels. Pre-emption of a Modbus Master instruction by another Modbus master instruction in a higher priority execution priority level will result in improper operation. Modbus master instructions must not execute in the startup, diagnostic or time error execution priority levels.
- Once a master instruction initiates a transmission, this instance must be continually executed with the EN input enabled until a DONE=1 state or ERROR=1 state is returned. A particular MB_MASTER instance is considered active until one of these two events occurs. While the original instance is active, any call to any other instance with the REQ input enabled will result in an error. If the continuous execution of the original instance stops, the request state remains active for a period of time specified by the static variable Blocked_Proc_Timeout. Once this period of time expires, the next master instruction called with an enabled REQ input will become the active instance. This prevents a single Modbus master instance from monopolizing or locking access to a port. If the original active instance is not enabled within the period of time specified by the static variable "Blocked_Proc_Timeout", then the next execution by this instance (with REQ not set) will clear the active state. If (REQ is set), then this execution initiates a new master request as if no other instance was active.

REQ parameter

0 = No request; 1 = Request to transmit data to Modbus Slave

You may control this input either through the use of a level or edge triggered contact. Whenever this input is enabled, a state machine is started to ensure that no other MB_MASTER using the same instance DB is allowed to issue a request, until the current request is completed. All other input states are captured and held internally for the current request, until the response is received or an error detected.

If the same instance of MB_MASTER is executed again with REQ input = 1 before the completion of the current request, then no subsequent transmissions are made. However, when the request is completed, a new request is issued whenever MB_MASTER is executed again with REQ input = 1.

DATA_ADDR and MODE parameters select the Modbus function type

DATA_ADDR (starting Modbus address in the slave): Specifies the starting address of the data to be accessed in the Modbus slave.

The MB_MASTER instruction uses a MODE input rather than a Function Code input. The combination of MODE and Modbus address determine the Function Code that is used in the actual Modbus message. The following table shows the correspondence between parameter MODE, Modbus function code, and Modbus address range.

Table 14-154 Modbus functions

MODE	Modbus Function	Data length	Operation and data	Modbus Address
0	01	1 to 2000 1 to 1992 [1]	Read output bits: 1 to (1992 or 2000) bits per request	1 to 9999
0	02	1 to 2000 1 to 1992 [1]	Read input bits: 1 to (1992 or 2000) bits per request	10001 to 19999
0	03	1 to 125 1 to 124 [1]	Read Holding registers: 1 to (124 or 125) words per request	40001 to 49999 or 400001 to 465535
0	04	1 to 125 1 to 124 [1]	Read input words: 1 to (124 or 125) words per request	30001 to 39999
1	05	1	Write one output bit: One bit per request	1 to 9999
1	06	1	Write one holding register: 1 word per request	40001 to 49999 or 400001 to 465535
1	15	2 to 1968 2 to 1960 [1]	Write multiple output bits: 2 to (1960 or 1968) bits per request	1 to 9999
1	16	2 to 123 2 to 122 [1]	Write multiple holding registers: 2 to (122 or 123) words per request	40001 to 49999 or 400001 to 465535
2	15	1 to 1968 2 to 1960 [1]	Write one or more output bits: 1 to (1960 or 1968) bits per request	1 to 9999
2	16	1 to 123 1 to 122 [1]	Write one or more holding registers: 1 to (122 or 123) words per request	40001 to 49999 or 400001 to 465535
11	11	0	Read the slave communication status word and event counter. The status word indicates busy (0 – not busy, 0xFFFF - busy). The event counter is incremented for each successful completion of a message. Both the DATA_ADDR and DATA_LEN operands of MB_MASTER are ignored for this function.	
80	08	1	Check slave status using data diagnostic code 0x0000 (Loopback test – slave echoes the request) 1 word per request	
81	08	1	Reset slave event counter using data diagnostic code 0x000A 1 word per request	
3 to 10, 12 to 79, 82 to 255			Reserved	

[1] For "Extended Addressing" mode the maximum data lengths are reduced by 1 byte or 1 word depending upon the data type used by the function.

DATA_PTR parameter

The DATA_PTR parameter points to the DB or M address that is written to or read from. If you use a data block, then you must create a global data block that provides data storage for reads and writes to Modbus slaves.

NOTE

The DATA_PTR data block type must allow direct addressing

The data block must allow both direct (absolute) and symbolic addressing. When you create the data block the "Standard" access attribute must be selected.

Data block structures for the DATA_PTR parameter

- These data types are valid for **word reads** of Modbus addresses 30001 to 39999, 40001 to 49999, and 400001 to 465536 and also for **word writes** to Modbus addresses 40001 to 49999 and 400001 to 465536.
  - Standard array of WORD, UINT, or INT data types
  - Named WORD, UINT, or INT structure where each element has a unique name and 16 bit data type.
  - Named complex structure where each element has a unique name and a 16 or 32 bit data type.
- For **bit reads** and writes of Modbus addresses 00001 to 09999 and bit reads of 10001 to 19999.
  - Standard array of Boolean data types.
  - Named Boolean structure of uniquely named Boolean variables.
- Although not required, it is recommended that each MB_MASTER instruction have its own separate memory area. The reason for this recommendation is that there is a greater possibility of data corruption if multiple MB_MASTER instructions are reading and writing to the same memory area.
- There is no requirement that the DATA_PTR data areas be in the same global data block. You can create one data block with multiple areas for Modbus reads, one data block for Modbus writes, or one data block for each slave station.

Modbus master data block variables

The following table shows the public static variables stored in the instance DB for MB_MASTER that can be used in your program.

Table 14-155 Static variables in the instance DB

Variable	Data type	Initial value	Description
Blocked_Proc_Timeout	Real	3.0	Amount of time (in seconds) to wait for a blocked Modbus Master instance before removing this instance as being ACTIVE. This can occur, for example, when a Master request has been issued and then the program stops calling the Master function before it has completely finished the request. The time value must be greater than 0 and less than 55 seconds, or an error occurs. The default value is .5 seconds.
Extended_Addressing	Bool	False	Configures single or double-byte slave addressing. The default value = 0. (0=single byte address, 1=double-byte address)

Your program can write values to the Blocked_Proc_Timeout and Extended_Addressing variables to control Modbus master operations. See the MB_SLAVE topic description of HR_Start_Offset and Extended_Addressing for an example of how to use these variables in the program editor and details about Modbus extended addressing (Page 1036).

Condition codes

Table 14-156 MB_MASTER execution condition codes (communication and configuration errors) [1]

STATUS (W#16#)	Description
0000	No error
80C8	Slave timeout. Check baud rate, parity, and wiring of slave.
80D1	The receiver issued a flow control request to suspend an active transmission and never re-enabled the transmission during the specified wait time. This error is also generated during hardware flow control when the receiver does not assert CTS within the specified wait time.
80D2	The transmit request was aborted because no DSR signal is received from the DCE.
80E0	The message was terminated because the receive buffer is full.
80E1	The message was terminated as a result of a parity error.
80E2	The message was terminated as a result of a framing error.
80E3	The message was terminated as a result of an overrun error.
80E4	The message was terminated as a result of the specified length exceeding the total buffer size.
8180	Invalid port ID value or error with MB_COMM_LOAD instruction
8186	Invalid Modbus station address
8188	Invalid Mode specified for broadcast request
8189	Invalid Data Address value
818A	Invalid Data Length value
818B	Invalid pointer to the local data source/destination: Size not correct
818C	Invalid pointer for DATA_PTR or invalid Blocked_Proc_Timeout: The data area must be a DB (that allows both symbolic and direct access) or M memory.
8200	Port is busy processing a transmit request.

Table 14-157 MB_MASTER execution condition codes (Modbus protocol errors) [1]

STATUS (W#16#)	Response code from slave	Modbus protocol errors
8380	-	CRC error
8381	01	Function code not supported
8382	03	Data length error
8383	02	Data address error or address outside the valid range of the DATA_PTR area
8384	Greater than 03	Data value error
8385	03	Data diagnostic code value not supported (function code 08)

[1] In addition to the MB_MASTER errors listed above, errors can be returned from the underlying PtP communication instructions.

STATUS (W#16#)	Response code from slave	Modbus protocol errors
8386	-	Function code in the response does not match the code in the request.
8387	-	Wrong slave responded
8388	-	The slave response to a write request is incorrect. The write request returned by the slave does not match what the master actually sent.

[1] In addition to the MB_MASTER errors listed above, errors can be returned from the underlying PtP communication instructions.

14.9.2.3 MB_SLAVE (Communicate using the PtP port as Modbus RTU slave)

Table 14-158 MB_SLAVE instruction

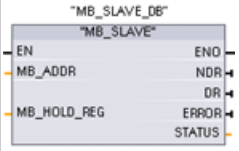
LAD / FBD	SCL	Description
	**"MB_SLAVE_DB"(MB_ADDR:=_uint_in_, NDR=>_bool_out_, DR=>_bool_out_, ERROR=>_bool_out_, STATUS=>_word_out_, MB_HOLD_REG:=_variant_inout_);**	The MB_SLAVE instruction allows your program to communicate as a Modbus slave through a PtP port on the CM (RS485 or RS232) and CB (RS485). When a remote Modbus RTU master issues a request, your user program responds to the request by MB_SLAVE execution. STEP 7 automatically creates an instance DB when you insert the instruction. Use this MB_SLAVE_DB name when you specify the MB_DB parameter for the MB_COMM_LOAD instruction.

Table 14-159 Data types for the parameters

Parameter and type		Data type	Description
MB_ADDR	IN	V1.0: USInt V2.0: UInt	The station address of the Modbus slave: Standard addressing range (1 to 247) Extended addressing range (0 to 65535)
MB_HOLD_REG	IN	Variant	Pointer to the Modbus Holding Register DB: The Modbus holding register can be M memory or a data block.
NDR	OUT	Bool	New Data Ready: • 0 – No new data • 1 – Indicates that new data has been written by the Modbus master
DR	OUT	Bool	Data Read: • 0 – No data read • 1 – Indicates that data has been read by the Modbus master
ERROR	OUT	Bool	The ERROR bit is TRUE for one scan, after the last request was terminated with an error. If execution is terminated with an error, then the error code value at the STATUS parameter is valid only during the single scan where ERROR = TRUE.
STATUS	OUT	Word	Execution error code

Modbus communication function codes (1, 2, 4, 5, and 15) can read and write bits and words directly in the input process image and output process image of the CPU. For these function codes, the MB_HOLD_REG parameter must be defined as a data type larger than a byte. The following table shows the example mapping of Modbus addresses to the process image in the CPU.

Table 14-160 Mapping of Modbus addresses to the process image

Modbus functions						S7-1200	
Codes	Function	Data area	Address range			Data area	CPU address
01	Read bits	Output	1	to	8192	Output Process Image	Q0.0 to Q1023.7
02	Read bits	Input	10001	to	18192	Input Process Image	I0.0 to I1023.7
04	Read words	Input	30001	to	30512	Input Process Image	IW0 to IW1022
05	Write bit	Output	1	to	8192	Output Process Image	Q0.0 to Q1023.7
15	Write bits	Output	1	to	8192	Output Process Image	Q0.0 to Q1023.7

Modbus communication function codes (3, 6, 16) use a Modbus holding register which can be an M memory address range or a data block. The type of holding register is specified by the MB_HOLD_REG parameter on the MB_SLAVE instruction.

NOTE

MB_HOLD_REG data block type

A Modbus holding register data block must allow both direct (absolute) and symbolic addressing. When you create the data block the "Standard" access attribute must be selected.

The following table shows examples of Modbus address to holding register mapping that is used for Modbus function codes 03 (read words), 06 (write word), and 16 (write words). The actual upper limit of DB addresses is determined by the maximum work memory limit and M memory limit, for each CPU model.

Table 14-161 Mapping of Modbus addresses to CPU memory

Modbus Master Address	MB_HOLD_REG parameter examples				
	MW100	**DB10.DBw0**	**MW120**	**DB10.DBW50**	**"Recipe".ingredient**
40001	MW100	DB10.DBW0	MW120	DB10.DBW50	"Recipe".ingredient[1]
40002	MW102	DB10.DBW2	MW122	DB10.DBW52	"Recipe".ingredient[2]
40003	MW104	DB10.DBW4	MW124	DB10.DBW54	"Recipe".ingredient[3]
40004	MW106	DB10.DBW6	MW126	DB10.DBW56	"Recipe".ingredient[4]
40005	MW108	DB10.DBW8	MW128	DB10.DBW58	"Recipe".ingredient[5]

Table 14-162 Diagnostic functions

S7-1200 MB_SLAVE Modbus diagnostic functions		
Codes	Sub-function	Description
08	0000H	Return query data echo test: The MB_SLAVE will echo back to a Modbus master a word of data that is received.
08	000AH	Clear communication event counter: The MB_SLAVE will clear out the communication event counter that is used for Modbus function 11.
11		Get communication event counter: The MB_SLAVE uses an internal communication event counter for recording the number of successful Modbus read and write requests that are sent to the Modbus slave. The counter does not increment on any Function 8, Function 11, or broadcast requests. It is also not incremented on any requests that result in a communication error (for example, parity or CRC errors).

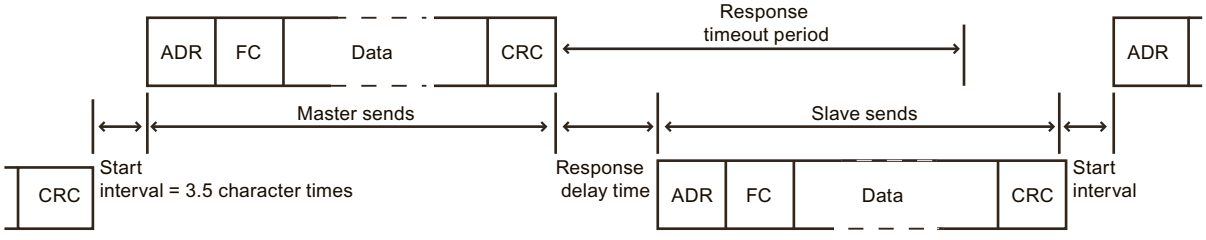
The MB_SLAVE instruction supports broadcast write requests from any Modbus master as long as the request is for accessing valid addresses. MB_SLAVE will produce error code 0x8188 for function codes not supported in broadcast.

Modbus slave communication rules

- MB_COMM_LOAD must be executed to configure a port, before a MB_SLAVE instruction can communicate through that port.
- If a port is to respond as a slave to a Modbus master, then do not program that port with the MB_MASTER instruction.
- Only one instance of MB_SLAVE can be used with a given port, otherwise erratic behavior may occur.
- The Modbus instructions do not use communication interrupt events to control the communication process. Your program must control the communication process by polling the MB_SLAVE instruction for transmit and receive complete conditions.
- The MB_SLAVE instruction must execute periodically at a rate that allows it to make a timely response to incoming requests from a Modbus master. It is recommended that you execute MB_SLAVE every scan from a program cycle OB. Executing MB_SLAVE from a cyclic interrupt OB is possible, but is not recommended because of the potential for excessive time delays in the interrupt routine to temporarily block the execution of other interrupt routines.

Modbus signal timing

MB_SLAVE must be executed periodically to receive each request from the Modbus master and then respond as required. The frequency of execution for MB_SLAVE is dependent upon the response timeout period of the Modbus master. This is illustrated in the following diagram.



The response timeout period RESP_TO is the amount of time a Modbus master waits for the start of a response from a Modbus slave. This time period is not defined by the Modbus protocol, but is a parameter of each Modbus master. The frequency of execution (the time between one execution and the next execution) of MB_SLAVE must be based on the particular parameters of your Modbus master. At a minimum, you should execute MB_SLAVE twice within the response timeout period of the Modbus master.

Modbus slave variables

This table shows the public static variables stored in the MB_SLAVE instance data block that can be used in your program

Table 14-163 Modbus slave variables

Variable	Data type	Description
Request_Count	Word	The number of all requests received by this slave
Slave_Message_Count	Word	The number of requests received for this specific slave
Bad_CRC_Count	Word	The number of requests received that have a CRC error
Broadcast_Count	Word	The number of broadcast requests received
Exception_Count	Word	Modbus specific errors that require a returned exception
Success_Count	Word	The number of requests received for this specific slave that have no protocol errors
HR_Start_Offset	Word	Specifies the starting address of the Modbus Holding register (default = 0)
Extended_Addressing	Bool	Configures single or double-byte slave addressing (0=single byte address, 1=double-byte address, default = 0)

Your program can write values to the HR_Start_Offset and Extended_Addressing variables and control Modbus slave operations. The other variables can be read to monitor Modbus status.

HR_Start_Offset

Modbus holding register addresses begin at 40001 or 400001. These addresses correspond to the beginning PLC memory address of the holding register. However, you can configure the "HR_Start_Offset" variable to start the beginning Modbus holding register address at another value instead of 40001 or 400001.

For example, if the holding register is configured to start at MW100 and is 100 words long. An offset of 20 specifies a beginning holding register address of 40021 instead of 40001. Any address below 40021 and above 400119 will result in an addressing error.

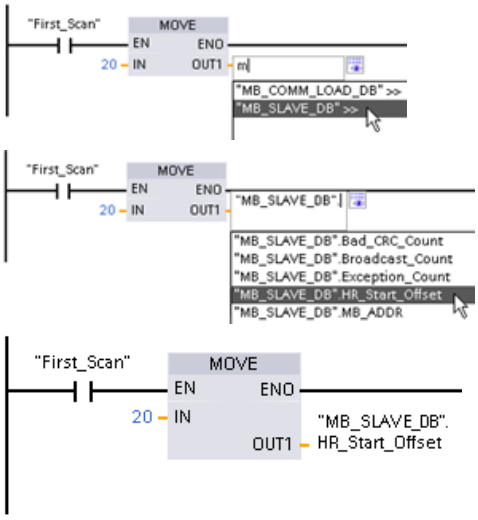
Table 14-164 Example of Modbus holding register addressing

HR_Start_Offset	Address	Minimum	Maximum
0	Modbus address (Word)	40001	40099
	S7-1200 address	MW100	MW298
20	Modbus address (Word)	40021	40119
	S7-1200 address	MW100	MW298

HR_Start_Offset is a word value that specifies the starting address of the Modbus holding register and is stored in the MB_SLAVE instance data block. You can set this public static

variable value by using the parameter helper drop-list, after MB_SLAVE is placed in your program.

For example, after MB_SLAVE is placed in a LAD network, you can go to a previous network and assign the HR_Start_Offset value. The value must be assigned prior to execution of MB_SLAVE.



Entering a Modbus slave variable using the default DB name:

1. Set the cursor in the parameter field and type an m character.
2. Select "MB_SLAVE_DB" from the drop-list.
3. Set the cursor at the right side of the DB name (after the quote character) and enter a period character.
4. Select "MB_SLAVE_DB.HR_Start_Offset" from the drop list.

Extended_Addressing

The Extended_Addressing variable is accessed in a similar way as the HR_Start_Offset reference discussed above except that the Extended_Addressing variable is a Boolean value. The Boolean value must be written by an output coil and not a move box.

Modbus slave addressing can be configured to be either a single byte (which is the Modbus standard) or double byte. Extended addressing is used to address more than 247 devices within a single network. Selecting extended addressing allows you to address a maximum of 64000 addresses. A Modbus function 1 frame is shown below as an example.

Table 14-165 Single-byte slave address (byte 0)

Function 1	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	
Request	Slave addr.	F code	Start address		Length of coils		
Valid Response	Slave addr.	F code	Length	Coil data			
Error response	Slave addr.	0x81	E code				

Table 14-166 Double-byte slave address (byte 0 and byte 1)

	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6
Request	Slave address		F code	Start address		Length of coils	
Valid Response	Slave address		F code	Length	Coil data		
Error response	Slave address		0x81	E code			

Condition codes

Table 14-167 MB_SLAVE execution condition codes (communication and configuration errors) [1]

STATUS (W#16#)	Description
80D1	The receiver issued a flow control request to suspend an active transmission and never re-enabled the transmission during the specified wait time. This error is also generated during hardware flow control when the receiver does not assert CTS within the specified wait time.
80D2	The transmit request was aborted because no DSR signal is received from the DCE.
80E0	The message was terminated because the receive buffer is full.
80E1	The message was terminated as a result of a parity error.
80E2	The message was terminated as a result of a framing error.
80E3	The message was terminated as a result of an overrun error.
80E4	The message was terminated as a result of the specified length exceeding the total buffer size.
8180	Invalid port ID value or error with MB_COMM_LOAD instruction
8186	Invalid Modbus station address
8187	Invalid pointer to MB_HOLD_REG DB: Area is too small
818C	Invalid MB_HOLD_REG pointer to M memory or DB (DB area must allow both symbolic and direct address)

Table 14-168 MB_SLAVE execution condition codes (Modbus protocol errors) [1]

STATUS (W#16#)	Response code from slave	Modbus protocol errors
8380	No response	CRC error
8381	01	Function code not supported or not supported within broadcasts
8382	03	Data length error
8383	02	Data address error or address outside the valid range of the DATA_PTR area
8384	03	Data value error
8385	03	Data diagnostic code value not supported (function code 08)

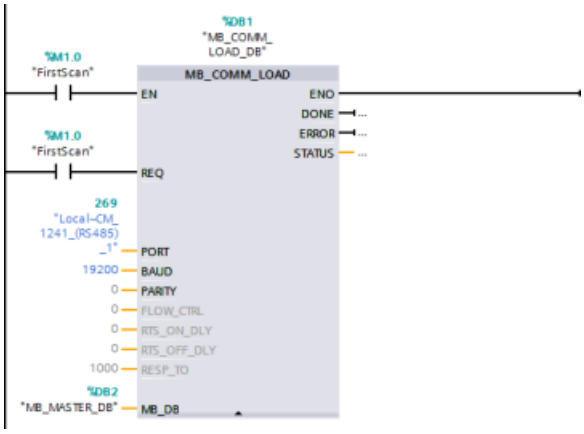
[1] In addition to the MB_SLAVE errors listed above, errors can be returned from the underlying PtP communication instructions.

14.9.3 Legacy Modbus RTU examples

14.9.3.1 Example: Legacy Modbus RTU master program

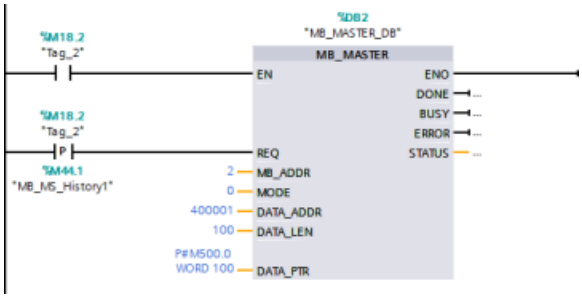
MB_COMM_LOAD is initialized during start-up by using the first scan flag. Execution of MB_COMM_LOAD in this manner should only be done when the serial port configuration will not change at runtime.

Network 1: Configure/initialize the RS485 module communications port only once during the first scan.

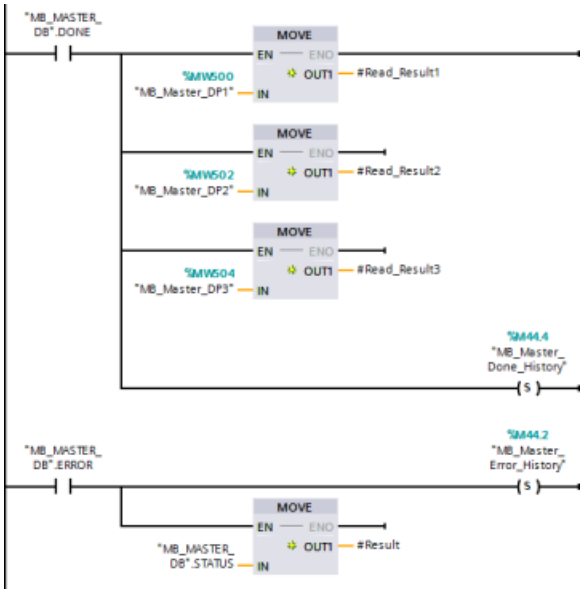


One MB_MASTER instruction is used in the program cycle OB to communicate with a single slave. Additional MB_MASTER instructions can be used in the program cycle OB to communicate with other slaves, or one MB_MASTER FB could be re-used to communicate with additional slaves.

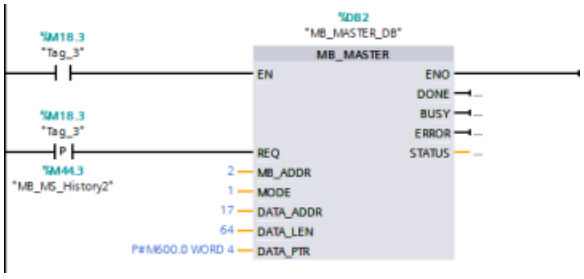
Network 2: Read 100 words of holding register data from location 400001 on slave #2 to memory location MW500-MW698.



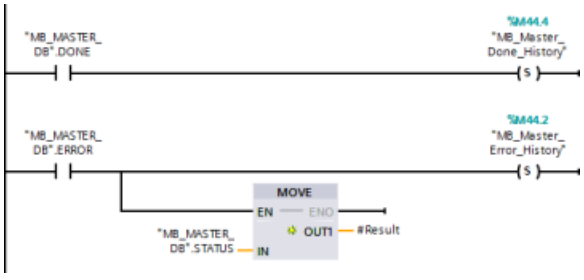
Network 3: Move the first 3 words of the holding register data that has been read to some other location, and set a DONE history bit. This network also sets an ERROR history bit and saves the STATUS word to another location in the event of an error.



Network 4: Write 64 bits of data from MW600-MW607 to output bit locations 00017 to 00081 on slave #2.

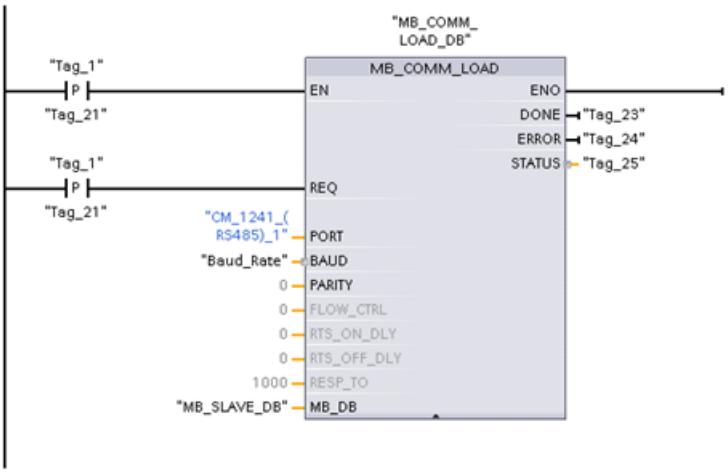


Network 5: Set a DONE history bit when the write is complete. If an error occurs, the program sets an ERROR history bit and saves the STATUS code.

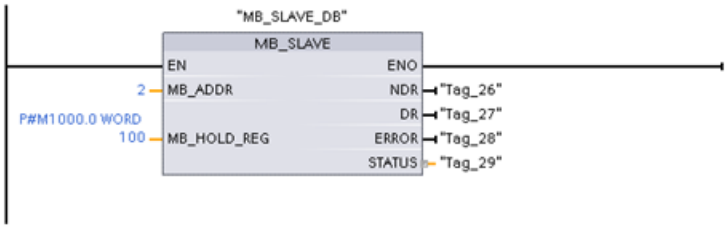


14.9.3.2 Example: Legacy Modbus RTU slave program

MB_COMM_LOAD shown below is initialized each time "Tag_1" is enabled.
Execution of MB_COMM_LOAD in this manner should only be done when the serial port configuration will change at runtime, as a result of HMI configuration.
Network 1: Initialize the RS485 module parameters each time they are changed by an HMI device.



MB_SLAVE shown below is placed in a cyclic OB that is executed every 10ms. While this does not give the absolute fastest response by the slave, it does provide good performance at 9600 baud for short messages (20 bytes or less in the request).
Network 2: Check for Modbus master requests during each scan. The Modbus holding register is configured for 100 words starting at MW1000.



14.10 Industrial Remote Communication (IRC)

14.10.1 Telecontrol CPs overview

Industrial Remote Communication provides access to widely distributed machines, plants, and applications of different sizes securely and economically. Industrial Remote Communications includes the following means of communication through CP modules:

- TeleControl: Telecontrol is the connection of process stations (Remote Terminal Units/RTUs) that are distributed over a wide geographical area to one or more central process control systems for the purpose of monitoring and control. Various different transmission components in the Remote Networks product spectrum support remote communication over a range of public and private networks. Special telecontrol protocols perform event-driven or cyclic exchange of process data, which permits efficient control of the overall process.

- TeleService: Teleservice involves data exchange with distant technical systems (machines, plants, computers, etc.) for the purpose of error detection, diagnostics, maintenance, repair, or optimization.
- Additional applications for remote communication, for example surveillance, smart grid applications, and condition monitoring.

TeleControl CPs for the S7-1200

For TeleControl applications, the following communications processors, many of which also provide access to the S7-1200 Web server (Page 766), are available:

- **CP 1243-1:**
  - Article number: 6GK7 243-1BX30-0XE0
  - Communications processor for connecting the SIMATIC S7-1200 to Industrial Ethernet or via the Internet to the following control center systems:
    - Telecontrol server (OPC server application TCSB V3)
    - DNP3 master station
    - IEC 60870-5 master station
  - With the help of VPN technology and the firewall, the CP allows protected access to the S7-1200.
  - You can use the CP as an interface extension of the CPU. In this role, it serves the purpose of network separation.
  - You communicate between the CP and CPU using configurable data points that access PLC tags.
- **CP 1243-7 LTE-xx:**
  - Communications processor for connecting the SIMATIC S7-1200 via a mobile network to the following control center systems:
    - Telecontrol server (OPC server application TCSB V3)
    - DNP3 master station
    - IEC 60870-5 master station
  - Communications processor for connecting the SIMATIC S7-1200 via mobile network to the following control center systems:
  - Support of the following mobile wireless specifications: GSM, UMTS (3G), LTE (4G)
  - To cover countries with different mobile wireless specifications, the CP is available in two variants:
    - CP 1243-7 LTE-US:
    - North American standard
    - Article number: 6GK7 243-7SX30-0XE0
    - CP 1243-7 LTE-EU:
    - Western European standard
    - Article number: 6GK7 243-7KX30-0XE0
  - With the help of VPN technology and the firewall, the CP allows protected access to the S7-1200.
  - You can use the CP as an additional Ethernet interface of the CPU for S7 communication.
  - You communicate between the CP and CPU using configurable data points that access PLC tags.

- **CP 1243-8 IRC:**
  - Article number: 6GK7 242-8RX30-0XE0
  - Communications processor for connecting the SIMATIC S7-1200 to an ST7 network, data point configuration, and VPN

NOTE

You must have TeleControl Server Basic software for TeleControl applications for CPs other than the CP 1243-1.

Secure communication

The well-proven SINAUT ST7 protocol or the standardized DNP3 or IEC 60870-5 protocol adds security to Industrial Remote Communication (https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-remote-communication.html). The TeleControl solution provides comprehensive measures to prevent data falsification and loss. Each transmission module has a large memory for several thousand data frames, which offers the ability to bridge downtimes in the transmission link. Dedicated VPN solutions protect special IP-based networks.

The CP 1243-1 communications processor securely connects the SIMATIC S7-1200 controller to Ethernet networks. With its integrated firewall (Stateful Inspection) and VPN protocol (IPsec) security functions, the communications processor helps protect S7-1200 stations and lower-level networks against unauthorized access and helps protect data transmission against manipulation and espionage by encryption. Furthermore, the CP can also be used for integrating the S7-1200 station into the TeleControl Server Basic control center software using IP-based remote networks.

14.10.2 Further information

The following CP manuals provide detailed information on connection, requirements, applications, block instructions, accessories, and configuration examples:

- CP 1243-1 Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/103948898)
- CP 1243-7 LTE Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109476704)
- CP 1243-8 IRC Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109777054)

For other information and documentation on these S7-1200 SIMATIC telecontrol CP modules, please visit the following links:

- CP 1243-1 (https://support.industry.siemens.com/cs/ww/en/ps/15922)
- CP 1243-7 LTE (https://support.industry.siemens.com/cs/ww/en/ps/15924)
- CP 1243-8 IRC (https://support.industry.siemens.com/cs/ww/en/ps/21162)
- Firmware updates as available (https://support.industry.siemens.com/cs/ww/en/ps/21770/dl)

Online and diagnostic tools 15

15.1 Status LEDs

The CPU and the I/O modules use LEDs to provide information about the operating state of the CPU and status of the devices.

Status LEDs on a CPU

The CPU provides the following status indicators:

- STOP/RUN
  - Solid yellow indicates STOP mode
  - Solid green indicates RUN mode
  - Flashing (alternating green and yellow) indicates that the CPU is in the STARTUP operating state
- ERROR
  - Flashing red indicates an error, such as an internal error in the CPU, an error with the memory card, or a configuration error (mismatched modules)
  - Flashing red for three seconds indicates an error that is not ongoing. An example is if the real time clock (RTC) resets to the default time due to a power loss.
  - Defective state:
    - Solid red indicates defective hardware
    - All LEDs flash if the firmware detects a defect
- MAINT (Maintenance) flashes whenever you insert a memory card. Power cycle the CPU. The CPU then changes to STOP mode. After the CPU has changed to STOP mode, perform one of the following functions to initiate the evaluation of the memory card:
  - Change the CPU to RUN mode
  - Perform a memory reset (MRES)
  - Power-cycle the CPU

You can also use the LED instruction (Page 382) to determine the status of the LEDs.

Table 15-1 Status LEDs for a CPU

Description	STOP/RUN Yellow / Green	ERROR Red	MAINT Yellow
Power is off	Off	Off	Off
Startup, self-test, or firmware update	Flashing (alternating yellow and green)	-	Off
Stop mode	On (yellow)	-	-
Run mode	On (green)	-	-
Remove the memory card	On (yellow)	-	Flashing
Error	On (either yellow or green)	Flashing	-

Description	STOP/RUN Yellow / Green	ERROR Red	MAINT Yellow
Maintenance requested • Forced I/O • Battery replacement required (if battery board installed)	On (either yellow or green)	-	On
Defective hardware (Page 1050)	On (yellow)	On	Off
LED test or defective CPU firmware (Page 1050)	Flashing (alternating yellow and green)	Flashing	Flashing
Unknown or incompatible version of CPU configuration (Page 1050)	On (yellow)	Flashing	Flashing

The CPU and each digital signal module (SM) provide an I/O Channel LED for each of the digital inputs and outputs. The I/O Channel (green) turns on or off to indicate the state of the individual input or output.

Status LEDs on a Signal Module (SM) and a Signal Board (SB)

In addition, each digital SM provides a DIAG LED that indicates the status of the module:

- Green indicates that the module is operational
- Red indicates that the module is defective or non-operational

Each analog SM provides an I/O Channel LED for each of the analog inputs and outputs.

- Green indicates that the channel has been configured and is active
- Red indicates an error condition of the individual analog input or output

In addition, each analog SM provides a DIAG LED that indicates the status of the module:

- Green indicates that the module is operational
- Red indicates that the module is defective or non-operational

The SM detects the presence or absence of power to the module (field-side power, if required).

Table 15-2 Status LEDs for a signal module (SM)

Description	DIAG (Red / Green)	I/O Channel (Red / Green)
Field-side power is off *	Flashing red	Flashing red
Not configured or update in progress	Flashing green	Off
Module configured with no errors	On (green)	On (green)
Error condition	Flashing red	-
I/O error (with diagnostics enabled)	Flashing red	Flashing red
I/O error (with diagnostics disabled)	On (green)	On (green)

* Status is only supported on analog signal modules.

Each analog SB provides an I/O Channel LED for each of the analog inputs and outputs.

Table 15-3 Status LEDs for a signal board (SB)

Description	I/O Channel (Red / Green)
Not configured or update in progress	Off
Board configured with no errors	On (green)
I/O error (with diagnostics enabled)	Flashing red
I/O error (with diagnostics disabled)	On (green)

Status LEDs for communication on the CPU

The CPU also provides two LEDs that indicate the status of the PROFINET communications. Open the bottom terminal block cover to view the PROFINET LEDs.

- Link (green) turns on to indicate a successful connection
- Rx/Tx (yellow) turns on to indicate transmission activity

See also

Resetting to factory settings (Page 1057)

Transfer card (Page 109)

Setting or deleting the password for protection of confidential PLC configuration data (Page 1056)

Protection of confidential PLC configuration data (Page 145)

Program card (Page 112)

Analog module diagnostics (Page 1049)

15.2 Analog module diagnostics

Analog modules have multiple diagnostics depending on the module and channel type. You can separately enable or disable these diagnostics for each module and channel by using the TIA portal under the projects device configuration/general properties of the module.

Power supply errors are reported as follows:

Power supply error	Error reported
Analog module with a power supply diagnostic error reports:	Overflow: 32767 for all input channels
	Missing power supply diagnostic, if enabled for output modules

You can enable these diagnostics separately by channel and type for each channel. See the table below:

Channel type	Error reported
Voltage input	Overflow: 32767
	Underflow: -32768
Current input (0 to 20 mA)	Overflow: 32767
	Underflow: -32768
Current input (4 to 20 mA) (for < 1.185 mA input)	Broken wire: 32767
	Overflow: 32767
Voltage output (for > 0.5 V output)	Short circuit diagnostic, if enabled
Current output (for > 1.0 mA output)	Open circuit diagnostic, if enabled
RTD input	Broken wire: 32767
	Overflow: 32767
	Underflow: -32768
Resistor input	Broken wire: 32767
	Overflow: 32767
Thermocouple input	Broken wire: 32767
	Overflow: 32767
	Underflow: -32768

An analog input module with a diagnostic error on any channel reports 32767 or -32768 on that channel even if the diagnostics is not enabled. Analog input channels report 32767 when deactivated.

Analog input modules can have diagnostic errors on more than one channel at a time (multiple errors). When this occurs, only the first error is reported to the CPU. After the first error is reported, no additional errors are reported until the cause of the first error is cleared in the module. After the first error is cleared, the second error is then reported if the error condition still exists.

15.3 CPU error behavior

"Unknown or incompatible version of CPU configuration" error

The diagnostics buffer can report an "Unknown or incompatible version of CPU configuration" error, which can occur in one of the following ways:

- Attempting to load an invalid project, for example, an S7-1200 V3.0 program to an S7-1200 V4.x CPU
- Attempting to download a project with different protection of confidential PLC configuration data (Page 145) between the CPU and the project

If you reached this state by using an invalid version transfer card (Page 109), follow these steps to recover:

1. Remove the transfer card.
2. Perform a STOP to RUN transition.
3. Reset the memory (MRES) or cycle power.

If you reach this state by using an invalid project on a program card (Page 112), reset the CPU to factory settings (Page 1057) using the "Format memory card" option .

If your reach this state from a mismatch between the CPU and the project for the protection of confidential PLC configuration data, use the Online & Diagnostics tools (Page 1056) to set the online CPU's password for protection of confidential PLC configuration data to the password in the project, or delete it from the online CPU.

After you recover the CPU from the error condition, you can download a valid program.

S7-1200 behavior following a fatal error

If the CPU firmware detects a fatal error it attempts a defect-mode restart, and if successful, signals the defective mode by continually flashing the STOP/RUN, ERROR and MAINT LEDs. The user program and hardware configuration are not loaded following the defect-mode restart.

If the CPU successfully completes the defect-mode restart, the CPU performs these actions:

- Sets the CPU and signal board outputs to 0
- Sets the outputs of central rack signal modules and distributed I/O to the selection for "Reaction to CPU STOP" in the device configuration of the digital outputs of the module

If the defect-mode restart fails, (for example, due to a hardware fault), the STOP and ERROR LEDs are ON and the MAINT LED is OFF.

WARNING

Operation in defect state cannot be guaranteed

Control devices can fail in an unsafe condition, resulting in unexpected operation of controlled equipment.

Use an emergency stop function, electromechanical overrides or other redundant safeguards that are independent of the PLC.

Such unexpected operations can result in death or serious injury to personnel, and/or damage to equipment.

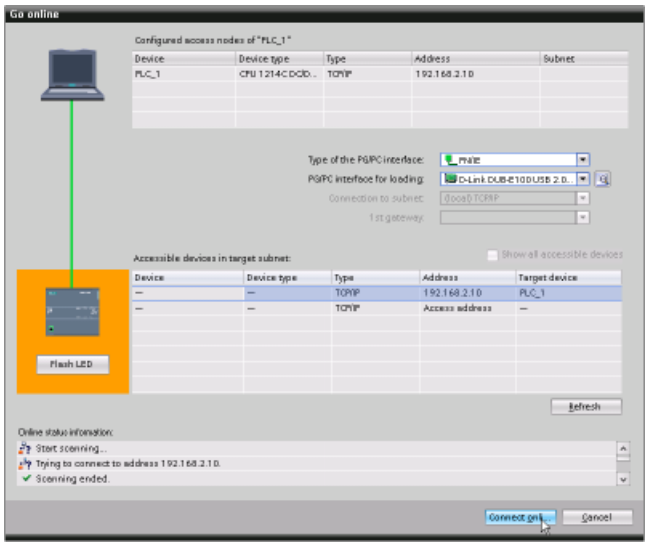
15.4 Going online and connecting to a CPU

You can establish an online connection between the programming device and CPU for loading programs and project engineering data as well as for activities such as the following:

- Testing user programs
- Displaying and changing the operating mode of the CPU (Page 1061)
- Displaying and setting the date and time of day of the CPU (Page 1054)
- Displaying the module information
- Comparing and synchronizing (Page 1063) offline to online program blocks
- Uploading and downloading program blocks
- Displaying diagnostics and the diagnostics buffer (Page 1062)
- Using a watch table (Page 1068) to test the user program by monitoring and modifying values
- Using a force table to force values in the CPU (Page 1070)
- Resetting the CPU to factory settings (Page 1057)

To establish an online connection to a configured CPU, click the CPU from the Project Navigation tree and click the "Go online" button from the Project View: Go online

If this is the first time to go online with this CPU, you must select the type of PG/PC interface and the specific PG/PC interface from the Go Online dialog before establishing an online connection to a CPU found on that interface.



If the CPU has protection of confidential PLC configuration data (Page 145), you might be prompted to trust the CPU. You can display and verify the CPU's certificate and decide whether to trust the CPU online connection or abort the connection.

Logging on to a CPU

When you go online with the CPU, you must first select one of the following user profiles. If your Anonymous user does not have the necessary permissions, STEP 7 will prompt you to enter an access level password or username and password.

- Log on with access level password - if access control via access levels (Page 151) is enabled for your project, STEP 7 prompts you to enter a password you have configured and downloaded. You are then granted access to the functions and memory areas allowed by the selected level of access protection.
- Local user - you assign a local user with a user name and password in "Users and Roles (Page 147)". Enter the configured user name and password to log in.
- Anonymous user - this user is disabled by default; if it is activated under "Users and Roles (Page 147)", you can log in with this user profile.

You then have the rights based on how you logged in. To log off from the online CPU, select the "Online > Delete access rights" menu command.

After connection, the orange color frames indicate an online connection. You can now use the Online & diagnostics tools from the Project tree and the Online tools task card.

See also

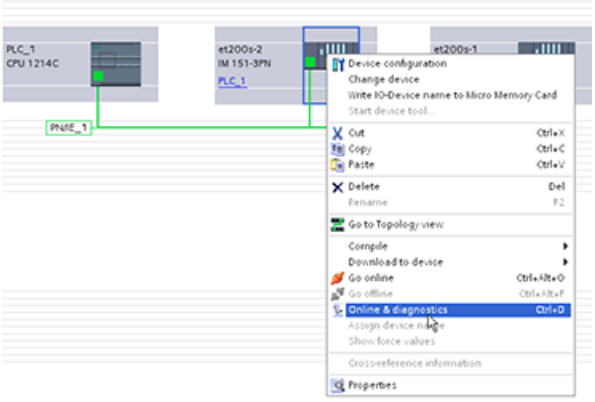
Downloading in RUN mode (Page 1072)

15.5 Assigning a name to a PROFINET IO device online

The devices on your PROFINET network must have an assigned name before you can connect with the CPU. Use the "Devices & networks" editor to assign names to your PROFINET devices if the devices have not already been assigned a name or if the name of the device is to be changed.

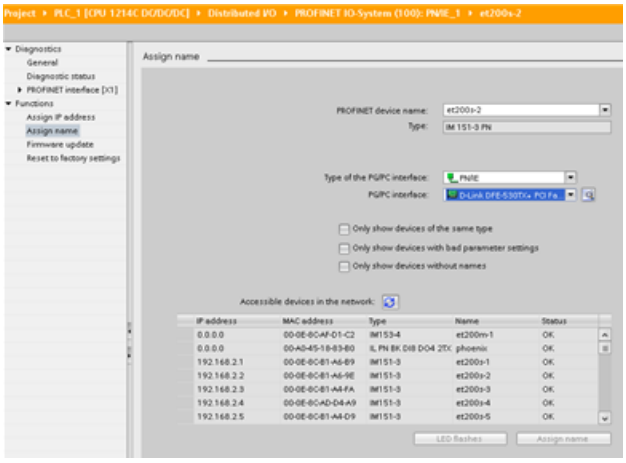
For each PROFINET IO device, you must assign the same name to that device in both the STEP 7 project and, using the "Online & diagnostics" tool, to the PROFINET IO device configuration memory (for example, an ET200 S interface module configuration memory). If a name is missing or does not match in either location, the PROFINET IO data exchange mode will not run.

1. In the "Devices & networks" editor, right-click on the required PROFINET IO device, and select "Online & diagnostics".

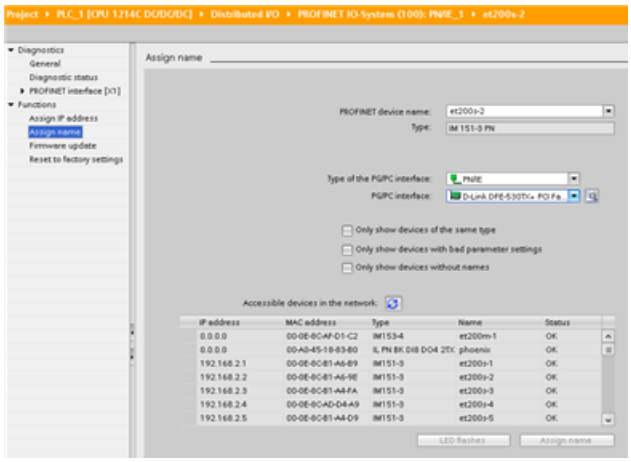


2. In the "Online & diagnostics" dialog, make the following menu selections:
   - "Functions"
   - "Assign PROFINET device name"

   Click the "Update list" button to display all of the PROFINET IO devices on the network.

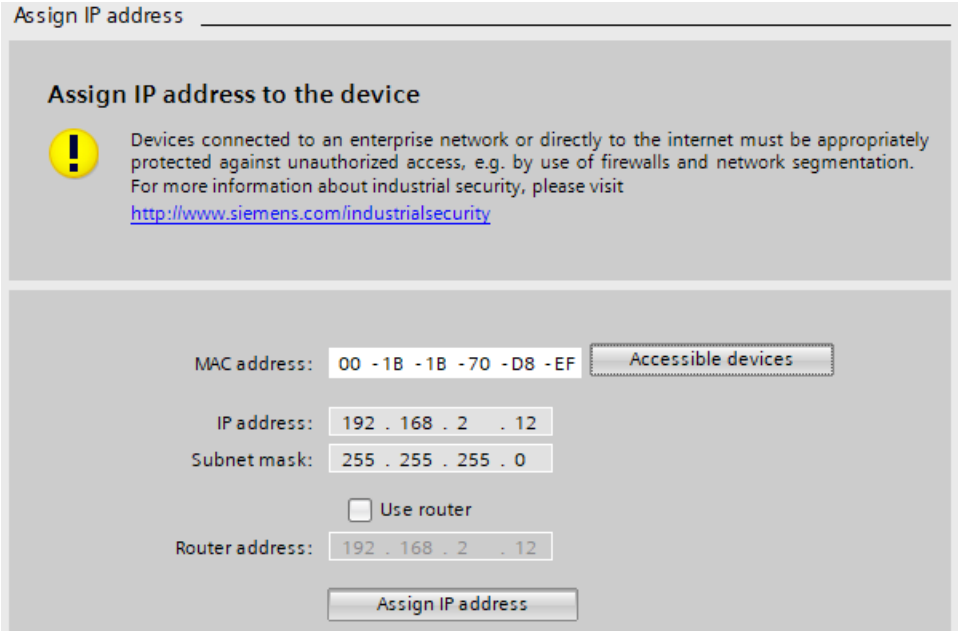


3. In the list that is displayed, click the required PROFINET IO device, and click the "Assign name" button to write the name to the PROFINET IO device configuration memory.



15.6 Setting the IP address and time of day

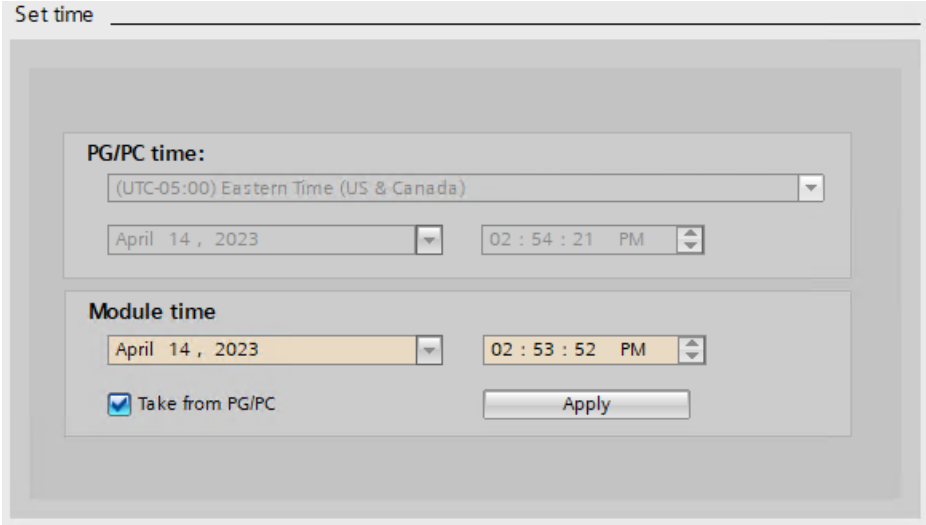
You can set the IP address (Page 537) and time of day in the online CPU. After accessing "Online & diagnostics" from the Project tree for an online CPU, you can display or change the IP address.



NOTE

The IP address must be assigned in the device in order to set the time of day using the Online and diagnostic interface.

You can also display or set the time and date parameters of the online CPU.



15.7 Updating firmware

You can update the firmware of a connected CPU from the STEP 7 online and diagnostics tools, by one of two methods:

- Updating from the CPU in the project
- Updating from the accessible devices in the project tree

NOTE

The firmware update process discards any additional data appended to the firmware update file. Appending data to a firmware update file has no effect on the firmware update or the S7-1200 CPU. You cannot append data, for example, to add components.

Updating the firmware of a CPU in your project

To perform a firmware update, follow these steps:

1. Open the CPU in the Project Tree that corresponds to the connected CPU.
2. Open the Online and Diagnostics view of the connected CPU.
3. Select "Firmware update" from the "Functions" folder.
4. From the "Firmware loader" section, click the Browse button and navigate to the location that contains the firmware update file. This could be a location on your hard drive to which you have downloaded an S7-1200 (http://support.automation.siemens.com/WW/view/en/34612486/133100) firmware update file from the Siemens Industry Online Support Web site (http://support.industry.siemens.com).
5. Select a file that is compatible with your module. For a selected file, the table displays the compatible modules.
6. Click the "Run update" button. Follow the dialogs, if necessary, to change the operating mode of your CPU.

STEP 7 displays progress dialogs as it loads the firmware update. When it finishes, it prompts you to start the module with the new firmware.

NOTE

If you do not choose to start the module with the new firmware, the previous firmware remains active until you reset the module, for example by cycling power. The new firmware becomes active only after you reset the module.

Updating the firmware from the accessible devices

To perform a firmware update for one or more accessible devices, follow these steps:

1. Open "Online access" from the project tree.
2. Open the communications interface to which your CPU is connected.
3. Double-click "Update accessible devices" and wait for STEP 7 to display the online devices.
4. Expand the CPU that you want to update and double-click "Online & diagnostics".
5. Expand "Firmware update" from the "Functions" folder. You will see the PLC as well as local modules for the PLC. From either the "PLC" or "Local modules" selection, you can proceed with updating firmware from the "Firmware loader" section as described above.

NOTE

The IP address must be assigned in the device in order to update the firmware using the Online & diagnostics.

You can also perform a firmware update by one of the following methods:

- Using a SIMATIC memory card (Page 117)
- Using the Web server "Module Information" standard Web page (Page 777)
- Using the SIMATIC Automation Tool (https://support.industry.siemens.com/cs/ww/en/view/98161300)

15.8 Setting or deleting the password for protection of confidential PLC configuration data

The "Protection of confidential PLC configuration data" feature allows you to protect each CPU in your project individually. From the device configuration (Page 145), you can enable this protection and set a password for the "protection of confidential PLC configuration data". Clients such as TIA Portal and the SIMATIC Automation Tool can only access the confidential data in the PLC through use of the password.

You can also use the security wizard (Page 144) to enable this feature and set the password for the "protection of confidential PLC configuration data".

Using the online and diagnostics tools

If the password for protection of PLC configuration data in the CPU does not match the one in the project, the CPU cannot go to RUN mode. You must set the correct password for protection of PLC configuration data or delete it for the CPU to go to RUN mode.

When the CPU is online (Page 1051), follow these steps to set or delete the password for "protection of confidential PLC configuration data" that is in the online CPU:

1. Place the CPU in STOP mode.
2. Open the Online & diagnostics tools for your CPU.
3. If the CPU has an existing password for protection of PLC configuration data, reset the PLC as follows:
   – Select "Reset to factory settings" from the Functions menu.
   – Select "Delete password for protection of PLC configuration data".
   – Click "Reset PLC".
4. Select "Set password for protection of PLC configuration data" from the Functions menu.
5. Click "Setup" to set a password or click "Delete" to delete the existing password for protection of confidential PLC configuration data that is in the online CPU. If "Delete" is not available, the online CPU does not have a password for protection of confidential PLC configuration data.

NOTE

To set or delete the password for protection of confidential PLC configuration data using the Online & diagnostics tools, the Device configuration must specify "IP address is set directly at the device".

15.9 Resetting to factory settings

You can reset an S7-1200 to its original factory settings under the following conditions:

- The CPU has an online connection.
- The CPU is in STOP mode.

NOTE

If the CPU is in RUN mode and you start the reset operation, you can place it in STOP mode after acknowledging a confirmation prompt.

Procedure

To reset a CPU to its factory settings, follow these steps:

1. Open the Online & Diagnostics view of the CPU.
2. Select "Reset to factory settings" from the "Functions" folder.
3. Select the "Delete IP address" check box if you want to delete the IP address.
4. Select the "Delete password for protection of confidential PLC configuration data" check box if you want to delete that password. You might want to delete the password for example, if you plan to load a new project to the CPU or replace the CPU with a new device (Page 1284).
5. Select the "Format memory card" check box if you want to format the memory card that is currently inserted in the online CPU. If you are running your CPU program from the memory card and you want to format the program, select this check box.

6. Click the "Reset PLC" button.
7. Acknowledge the confirmation prompt with "Yes" to confirm that you want to reset the module with your settings.

Result

The module switches to STOP mode if necessary, and it resets the factory settings. The online CPU performs the following actions:

- Deletes the work memory and retentive data areas
- Deletes the load memory if it is internal load memory; deletes load memory on SIMATIC memory card ONLY if you also selected "Format memory card"
- Sets all parameters and operand areas to their configured values
- Clears the diagnostics buffer
- Resets the time of day
- Deletes the I&M (Identification and Maintenance) data except for I&M0
- Resets the runtime meters if you have not saved the values to a memory card
- Retains or deletes the IP address based on the selection you made. (The MAC address is fixed and is never changed.)
  If you did not select "Delete IP address", the CPU retains the IP address, subnet mask, and router address (if used) from the settings in your hardware configuration, unless you have modified these values from the user program or another tool, in which case the CPU restores the modified values.
- Deletes the control data record (Page 128), if present
- Deletes or retains the password for protection of confidential PLC configuration data, depending on your setting
- Formats the memory card if a memory card is installed in the online CPU and you selected the option to format the memory card

15.10 Checking a module for defects (saving service data)

Saving service data

The S7-1200 CPUs allow you to save the service data of a module.
In the event of servicing, the SIEMENS Customer Support requires information about the state of a module of your system for diagnostic purposes. If such a case occurs in your system, Customer Support can ask you to save the service data of the module and send the resulting file to them.

How to save the service data of a module

You can save service data of a module in its online and diagnostics view at the following points:
In the "Functions" folder in the "Save service data" group," the "Save service data" group consists of the following areas:

- Online data
- Saving service data

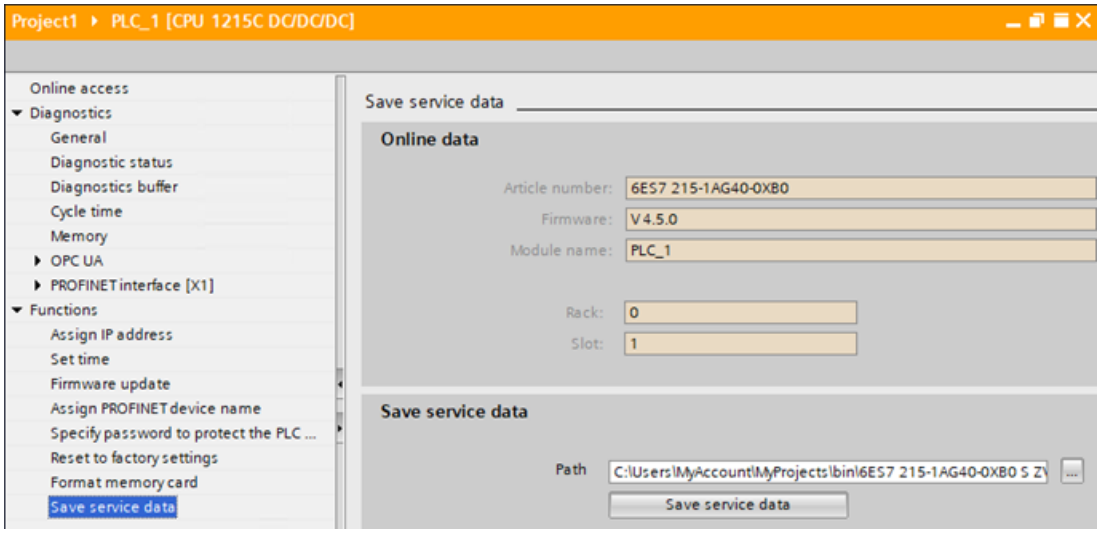
NOTE

The IP address must be assigned in the device in order to save the service data of a module.

"Online data"

The "Online data" area shows the following data of the module:

- Article number (MLFB)
- Firmware version
- Module name (you configured this while configuring the hardware.)
- Rack
- Slot



"Save service data"

Proceed as follows to create and save a file with special service data:

1. Select the point in the file system at which you want to save the file:
   - Use the path preset in the "Path" field.
   - Click the three-dot (browse) button. In the dialog that opens specify the desired path and enter the file name.
2. Click the "Save data" button.
3. A status indication for reading the service data is shown. When the service data extraction completes successfully, the Saving Service Data completed successfully screen is shown.

Some things to note:

- Service data can be extracted from the S7-1200 in either RUN or STOP mode. It cannot be read in the Defect/Fatal state.
- If you have programmed a password protection level into the CPU, you must authenticate the password before extracting service data. The password authentication is required for all levels of password, because the service data extraction process includes a data record write.
- The TIA portal supports saving one service data file
- The S7-1200 service data elements contained in the service data file are encrypted.

15.11 Formatting a SIMATIC memory card from STEP 7

You can format the memory card in a connected CPU from the STEP 7 online and diagnostic tools. Before you do so, read about the associated risks (Page 115).

To format the memory card, follow these steps:

1. Ensure the CPU is in STOP mode. Note that if the CPU is in RUN mode and you start a formatting operation, STEP 7 prompts you to allow STEP 7 to put the CPU in STOP mode.
2. Insert a memory card into the connected CPU.
3. Open Online & diagnostics for the connected CPU from either the CPU in the project or from the accessible devices in Online access in the project tree.
4. If the CPU is not online, select "Go online" for the connected CPU.
5. Select "Format memory card" from the "Functions" menu.
6. Click "Format".
7. Confirm the prompt with "Yes".

STEP 7 then formats the memory card and displays a message in the Info window when complete. The CPU is in STOP at the completion of the format operation with the STOP and MAINT lights blinking. You cannot go to RUN mode at this point; you must take one of the following actions:

- Remove the memory card and restart the CPU: If the internal load memory of the CPU contains a program, the CPU starts with the program.
- Restart the CPU without removing the memory card: If the internal load memory of the CPU contains a program, the CPU copies it to the memory card and starts with that program. If the internal load memory has no program, the CPU changes the memory card to a Program card (Page 112) and waits for a download.

NOTE

The IP address must be assigned in the device in order to Format a SIMATIC memory card from STEP 7.

Risks associated with the decommissioning process

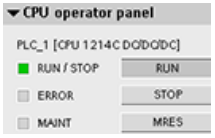
S7-1200 CPUs do not support secure erasure of the memory card and internal flash. Therefore, during the decommissioning process, you must securely dispose of the CPU and memory card to prevent the loss of proprietary or confidential information.

NOTE

Formatting a memory card has no effect on the contents of internal load memory.

If the CPU was using internal load memory when you inserted the memory card and you did not restart the CPU between inserting the card and executing the format operation, the CPU retains the contents of internal load memory.

15.12 CPU operator panel for the online CPU



The "CPU operator panel" displays the operating mode (STOP or RUN) of the online CPU. The panel also shows whether the CPU has an error or if values are being forced.

Use the CPU operating panel of the Online Tools task card to change the operating mode of an online CPU. The Online Tools task card is accessible whenever the CPU is online.

NOTE

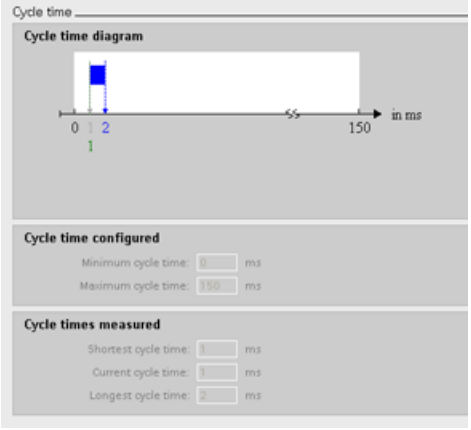
The IP address must be assigned in the device in order to use the CPU operator panel.

15.13 Monitoring the cycle time and memory usage

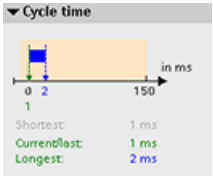
You can monitor the cycle time and memory usage of an online CPU.

After connecting to the online CPU, open the Online tools task card to view the following measurements:

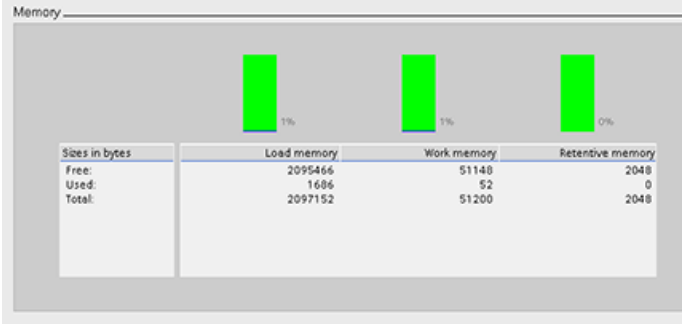
- Cycle time
- Memory usage



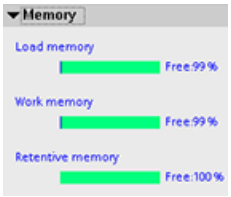
Figure



Figure



Figure



Figure

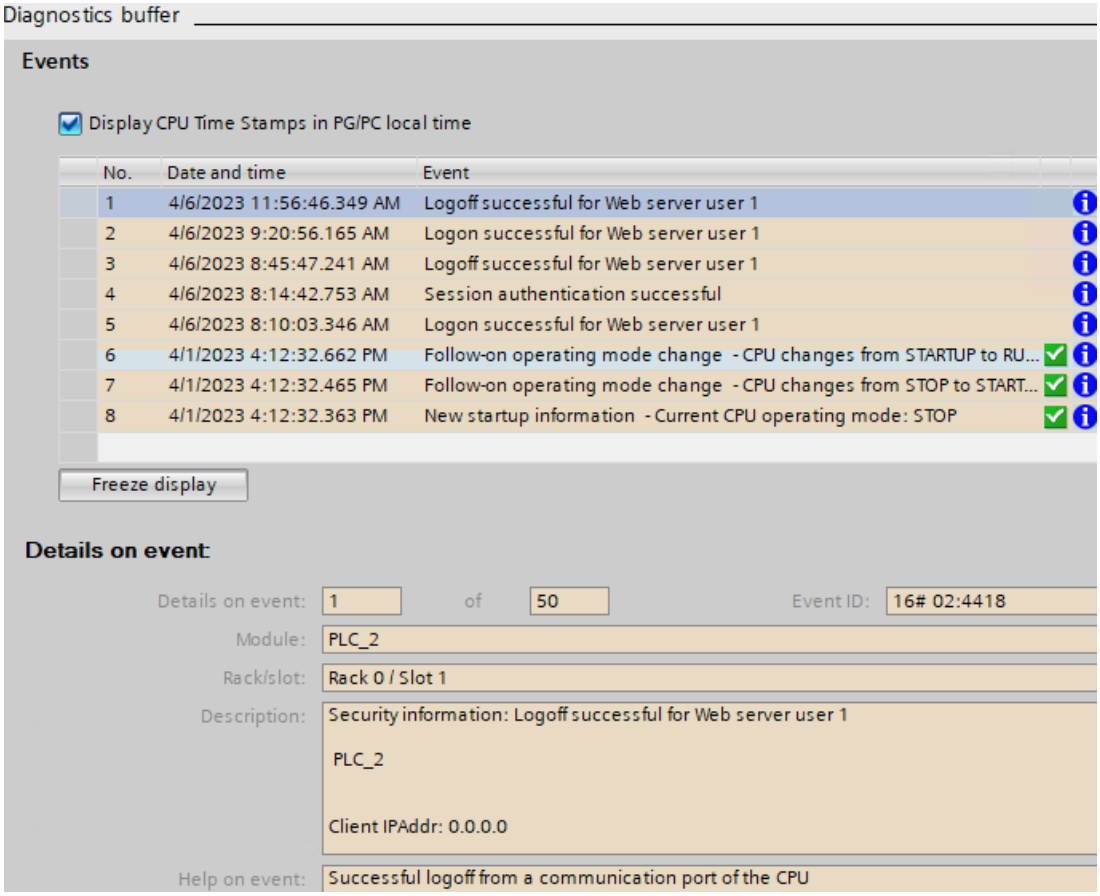
NOTE
The IP address must be assigned in the device in order to monitor the cycle time and memory usage.

15.14 Displaying diagnostic events in the CPU

Use the diagnostics buffer to review the recent activity in the CPU. The diagnostics buffer is accessible from "Online & Diagnostics" for an online CPU in the Project tree. It contains the following entries:

- Diagnostic events
- Changes in the CPU operating mode (transitions to STOP or RUN mode)

The first entry contains the latest event. Each entry in the diagnostics buffer contains the date and time the event was logged, and a description. The maximum number of entries is 500.



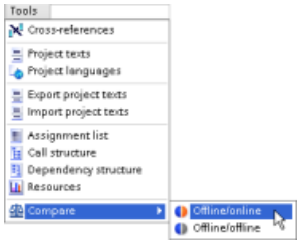
Resetting the CPU to the factory settings resets the diagnostics buffer by deleting the entries. You can also use the GET DIAG instruction (Page 406) to collect the diagnostic information.

NOTE

The IP address must be assigned in the device in order to view the diagnostic events in the CPU.

15.15 Comparing offline and online CPUs

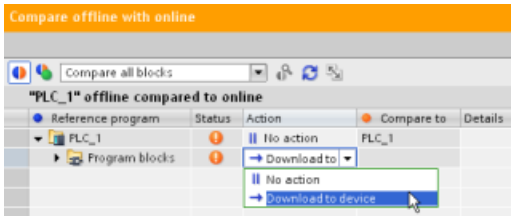
You can compare the code blocks in an online CPU with the code blocks in your project. If the code blocks of your project do not match the code blocks of the online CPU, the "Compare" editor allows you to synchronize your project with the online CPU by downloading the code blocks of your project to the CPU, or by deleting blocks from the project that do not exist in the online CPU.



Figure

Select the CPU in your project.

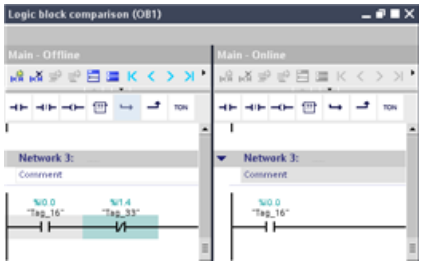
Use the "Compare Offline/online" command to open the "Compare" editor. (Access the command either from the "Tools" menu or by right-clicking the CPU in your project.)



Figure

Click in the "Action" column for an object to select whether to delete the object, take no action, or download the object to the device.

Click the "Synchronize" button to load the code blocks.



Figure

Right-click an object in the "Compare to" column and select "Start detailed comparison" button to show the code blocks side-by-side.

The detailed comparison highlights the differences between the code blocks of online CPU and the code blocks of the CPU in your project.

NOTE

Read access required on protected CPU for the Offline/Online compare operations

For STEP 7, the "HMI access" security level is insufficient to perform the Offline/Online compare operations. You must have "Read access" or "Full access", to do Offline/Online compare operations.

See also Access protection for the CPU (Page 151)

15.16 Performing an online/offline topology comparison

From the topology overview in STEP 7, you can compare the configured offline topology with the actual online topology.

Procedure

To find the differences between the configured and the actual topology, follow these steps:

1. Display the topology overview table of the topology view.
2. Click the "Offline/online comparison" button in the toolbar of the topology overview:

Result

STEP 7 removes the "Partner station, "Partner interface" and "Cable data" columns in the topology overview table and inserts comparison columns for "Status", and "Action". For each device or port in the topology overview, the Status column displays the comparison status as follows:

Icon	Meaning
	Differing topology in at least one lower-level component
	Identical topology
	Topology information is only available offline, or device is disabled
	Topology information is only available online
	Differing topology
	Device does not support topology functions

For each compared port or device, the Action column provides these possible choices:

Icon	Meaning
=	No action possible
←	Adopt the online interconnection

To repeat the comparison, click the toolbar button on the topology overview.

For additional information on the topology view, the topology overview, and online/offline topology comparisons, refer to the STEP 7 Information System. Also you can find additional information in the PROFINET with STEP 7 manual (https://support.industry.siemens.com/cs/ww/en/view/49948856).

15.17 Monitoring and modifying values in the CPU

STEP 7 provides online tools for monitoring the CPU:

- You can display or monitor the current values of the tags. The monitoring function does not change the program sequence. It presents you with information about the program sequence and the data of the program in the CPU.
- You can also use other functions to control the sequence and the data of the user program:
  - You can modify the value for the tags in the online CPU to see how the user program responds.
  - You can force a peripheral output (such as Q0.1:P or "Start":P) to a specific value.
  - You can enable outputs in STOP mode.

NOTE

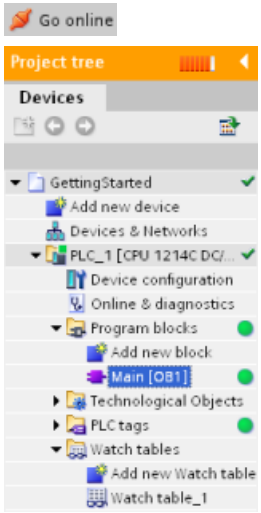
Always exercise caution when using control functions. These functions can seriously influence the execution of the user/system program.

Table 15-4 Online capabilities of the STEP 7 editors

Editor	Monitor	Modify	Force
Watch table	Yes	Yes	No
Force table	Yes	No	Yes
Program editor	Yes	Yes	No
Tag table	Yes	No	No
DB editor	Yes	Yes	No

15.17.1 Going online to monitor the values in the CPU

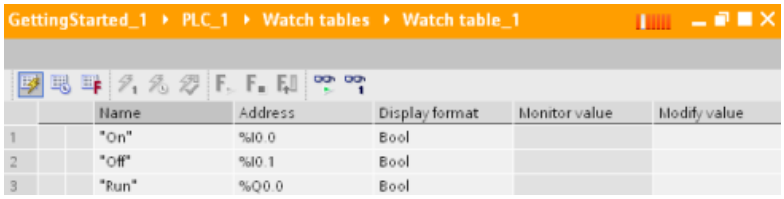
To monitor the tags, you must have an online connection to the CPU. Simply click the "Go online" button in the toolbar.



When you have connected to the CPU, STEP 7 turns the headers of the work areas orange.

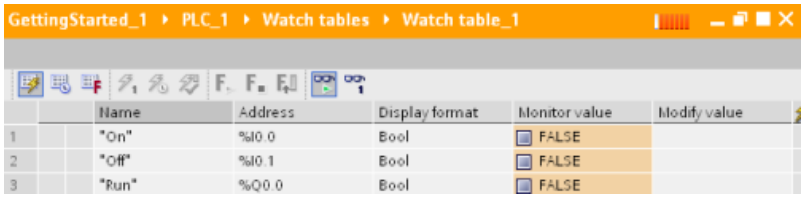
The project tree displays a comparison of the offline project and the online CPU. A green circle means that the CPU and the project are synchronized, meaning that both have the same configuration and user program.

Tag tables show the tags. Watch tables can also show the tags, as well as direct addresses.



Figure

To monitor the execution of the user program and to display the values of the tags, click the "Monitor all" button in the toolbar.



The "Monitor value" field shows the value for each tag.

15.17.2 Displaying status in the program editor

You can monitor the status of up to 50 tags in the LAD and FBD program editors. Use the editor bar to display the LAD editor. The editor bar allows you to change the view between the open editors without having to open or close the editors.

In the toolbar of the program editor, click the "Monitoring on/off" button to display the status of your user program.

The network in the program editor displays power flow in green.

You can also right-click on the instruction or parameter to modify the value for the instruction.

15.17.3 Capturing a snapshot of the online values of a DB for restoring values

You can capture a snapshot of the actual values of data block tags from an online CPU for later use.

Note the following prerequisites:

- You must have an online connection to the CPU.
- You must have the DB open in STEP 7.

Capturing a snapshot

To capture a snapshot, follow these steps:

1. In the DB editor, click the "Monitor all tags" button: The "Monitor value" column displays the actual data values.
2. Click the button to capture a snapshot of the actual values and display them in the "Snapshot" column.

You can use this snapshot at a later time to update the actual CPU values or to replace the start values.

Copying the snapshot values to the CPU

To copy the snapshot values to the actual values of the data block tags in the CPU, click the following button:

The online CPU loads the snapshot values into the actual values. The Monitor value column shows the actual values in the CPU. The scan cycle might subsequently change the values in the CPU from the snapshot values, but at the time you make the copy, the CPU loads the snapshot values in a consistent download.

NOTE

Be aware that if your snapshot contains state information, timer values, or calculated information, the CPU restores those values as of the time you made the snapshot.

Copying the snapshot values to the start values

To copy the snapshot values to the start values of the data block tags, click the following button:

After you compile the DB and download it to the CPU, the DB uses the new start values when the CPU goes to RUN mode.

Copying individual snapshot or monitor values to start values

The data block editor also lets you copy individual values and paste them over start values. Simply right-click a value in any value column and select Copy to place it in the Windows clipboard. Then, you can right-click on any start value and select paste to replace that value with the value in the clipboard.

After you compile the DB and download it to the CPU, the DB uses the new start values when the CPU goes to RUN mode.

15.17.4 Using a watch table to monitor and modify values in the CPU

A watch table allows you to perform monitoring and control functions on data points as the CPU executes your program. These data points can be process image (I or Q), M, DB or physical inputs (I_:P), depending on the monitor or control function. You cannot accurately monitor the physical outputs (Q_:P) because the monitor function can only display the last value written from Q memory and does not read the actual value from the physical outputs.

The monitoring function does not change the program sequence. It presents you with information about the program sequence and the data of the program in the CPU.

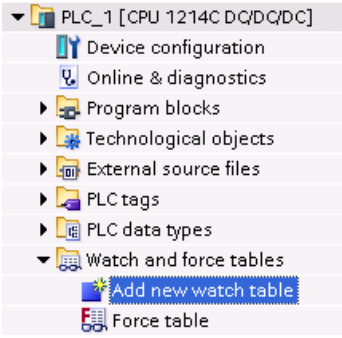
Control functions enable the user to control the sequence and the data of the program. You must exercise caution when using control functions. These functions can seriously influence the execution of the user/system program. The three control functions are Modify, Force and Enable Outputs in STOP.

With the watch table, you can perform the following online functions:

- Monitoring the status of the tags
- Modifying values for the individual tags

You select when to monitor or modify the tag:

- Beginning of scan cycle: Reads or writes the value at the beginning of the scan cycle
- End of scan cycle: Reads or writes the value at the end of the scan cycle
- Switch to stop



To create a watch table:

1. Double-click "Add new watch table" to open a new watch table.
2. Enter the tag name to add a tag to the watch table.

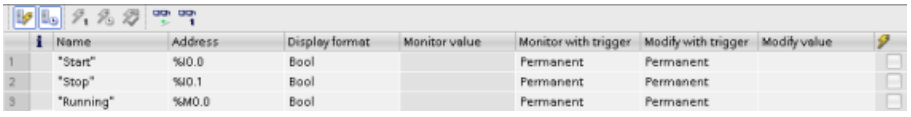
The following options are available for monitoring tags:

- Monitor all: This command starts the monitoring of the visible tags in the active watch table.
- Monitor now: This command starts the monitoring of the visible tags in the active watch table. The watch table monitors the tags immediately and once only.

The following options are available for modifying tags:

- "Modify to 0" sets the value of a selected address to "0".
- "Modify to 1" sets the value of a selected address to "1".
- "Modify now" immediately changes the value for the selected addresses for one scan cycle.
- "Modify with trigger" changes the values for the selected addresses.
  This function does not provide feedback to indicate that the selected addresses were actually modified. If feedback of the change is required, use the "Modify now" function.
- "Enable peripheral outputs" disables the command output disable and is available only when the CPU is in STOP mode.

To monitor the tags, you must have an online connection to the CPU.



	Name	Address	Display format	Monitor value	Monitor with trigger	Modify with trigger	Modify value
1	"Start"	%I0.0	Bool		Permanent	Permanent	
2	"Stop"	%I0.1	Bool		Permanent	Permanent	
3	"Running"	%M0.0	Bool		Permanent	Permanent	

You use the buttons at the top of the watch table to select the various functions.

Enter the tag name to monitor and select a display format from the dropdown selection. With an online connection to the CPU, click the "Monitor" button to display the actual value of the data point in the "Monitor value" field.

15.17.4.1 Using a trigger when monitoring or modifying PLC tags

Triggering determines at what point in the scan cycle the selected address will be monitored or modified.

Table 15-5 Types of triggers

Trigger	Description
Permanent	Continuously collects the data
At scan cycle start	Permanent: Continuously collects the data at the start of the scan cycle, after the CPU reads the inputs
	Once: Collects the data at the start of the scan cycle, after the CPU reads the inputs
At scan cycle end	Permanent: Continuously collects the data at the end of the scan cycle, before the CPU writes the outputs
	Once: Collects the data once at the end of the scan cycle, before the CPU writes the outputs
At transition to STOP	Permanent: Continuously collects data when the CPU transitions to STOP
	Once: Collects the data once after the CPU transitions to STOP

For modifying a PLC tag at a given trigger, select either the start or the end of cycle.

- Modifying an output: The best trigger event for modifying an output is at the end of the scan cycle, immediately before the CPU writes the outputs.

  Monitor the value of the outputs at the beginning of the scan cycle to determine what value is written to the physical outputs. Also, monitor the outputs before the CPU writes the values to the physical outputs in order to check program logic and to compare to the actual I/O behavior.
- Modifying an input: The best trigger event for modifying an input is at the start of the cycle, immediately after the CPU reads the inputs and before the user program uses the input values.

  If you suspect values are changing during the scan, you might want to monitor the value of the inputs at the end of the scan cycle to ensure that the value of the input at the end the scan cycle has not changed from the start of the scan cycle. If there is a difference in the values, your user program might be erroneously writing to inputs.

To diagnose why the CPU might have gone to STOP, use the "Transition to STOP" trigger to capture the last process values.

15.17.4.2 Enabling outputs in STOP mode

The watch table allows you to write to the outputs when the CPU is in STOP mode. This functionality allows you to check the wiring of the outputs and verify that the wire connected to an output pin initiates a high or low signal to the terminal of the process device to which it is connected.

WARNING

Risks in writing to physical outputs in STOP mode

Even though the CPU is in STOP mode, enabling a physical output can activate the process point to which it is connected, possibly resulting in unexpected equipment operation.

Before writing to an output from the watch table, ensure that changing the physical output cannot cause unexpected equipment operation. Always observe safety precautions for your process equipment.

Unexpected equipment operation can cause death or severe personal injury.

You can change the state of the outputs in STOP mode when the outputs are enabled. If the outputs are disabled, you cannot modify the outputs in STOP mode. To enable the modification in STOP mode of the outputs from the watch table, follow these steps:

1. Select the "Expanded mode" menu command from the "Online" menu.
2. Select the "Enable peripheral outputs" option of the "Modify" command of the "Online" menu, or from the context menu after right-clicking the row of the Watch table.

You cannot enable outputs in STOP mode if you have configured distributed I/O. An error is returned when you try to do this.

Setting the CPU to RUN mode disables "Enable peripheral outputs" option.

If any inputs or outputs are forced, the CPU is not allowed to enable outputs while in STOP mode. The force function must first be cancelled.

15.17.5 Forcing values in the CPU

15.17.5.1 Using the force table

A force table provides a "force" function that overwrites the value for an input or output point to a specified value for the peripheral input or peripheral output address. The CPU applies this forced value to the input process image prior to the execution of the user program and to the output process image before the outputs are written to the modules.

NOTE

The force values are stored in the CPU and not in the force table.

You cannot force an input (or "I" address) or an output (or "Q" address). However, you can force a peripheral input or peripheral output. The force table automatically appends a ":P" to the address (for example: "On":P or "Run":P).

	i	Name	Address	Display format	Monitor value	Force value	F
1		"On":P	%I0.0:P	Bool		TRUE	☑
2		"Off":P	%I0.1:P	Bool			☐
3		"Run":P	%Q0.1:P	Bool			☐

In the "Force value" cell, enter the value for the input or output to be forced. You can then use the check box in the "Force" column to enable forcing of the input or output.

Use the "Start or replace forcing" button to force the value of the tags in the force table. Click the "Stop forcing" button to reset the value of the tags.

In the force table, you can monitor the status of the forced value for an input. However, you cannot monitor the forced value of an output.
You can also view the status of the forced value in the program editor.

NOTE

When an input or output is forced in a force table, the force actions become part of the project configuration. If you close STEP 7, the forced elements remain active in the CPU program until they are cleared. To clear these forced elements, you must use STEP 7 to connect with the online CPU and then use the force table to turn off or stop the force function for those elements.

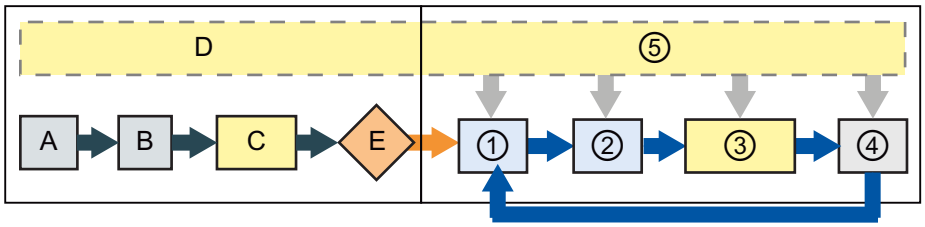
15.17.5.2 Operation of the Force function

The CPU allows you to force input and output point(s) by specifying the physical input or output address (I_:P or Q_:P) in the force table and then starting the force function.
In the program, reads of physical inputs are overwritten by the forced value. The program uses the forced value in processing. When the program writes a physical output, the output value is overwritten by the force value. The forced value appears at the physical output and is used by the process.
When an input or output is forced in the force table, the force actions become part of the user program. Even though the programming software has been closed, the force selections remain active in the operating CPU program until they are cleared by going online with the programming software and stopping the force function. Programs with forced points loaded on another CPU from a memory card will continue to force the points selected in the program.
If the CPU is executing the user program from a write-protected memory card, you cannot initiate or change the forcing of I/O from a watch table because you cannot override the values in the write-protected user program. Any attempt to force the write-protected values generates an error. If you use a memory card to transfer a user program, any forced elements on that memory card will be transferred to the CPU.

NOTE

Digital I/O points assigned to HSC, PWM, and PTO cannot be forced

The digital I/O points used by the high-speed counter (HSC), pulse-width modulation (PWM), and pulse-train output (PTO) devices are assigned during device configuration. When digital I/O point addresses are assigned to these devices, the values of the assigned I/O point addresses cannot be modified by the force function of the force table.



Startup		RUN	
A	The clearing of the I memory area is not affected by the Force function.	①	While writing Q memory to the physical outputs, the CPU applies the force value as the outputs are updated.
B	The initialization of the outputs values is not affected by the Force function.	②	When reading the physical inputs, the CPU applies the force values just prior to copying the inputs into I memory.
C	During the execution of the Startup OBs, the CPU applies the force value when the user program accesses the physical input.	③	During the execution of the user program (program cycle OBs), the CPU applies the force value when the user program accesses the physical input or writes the physical output.
D	The storing of interrupt events into the queue is not affected.	④	Handling of communication requests and self-test diagnostics are not affected by the Force function.
E	The enabling of the writing to the outputs is not affected.	⑤	The processing of interrupts during any part of the scan cycle is not affected.

15.18 Downloading in RUN mode

The CPU supports "Download in RUN mode". This capability allows you to download program changes while the program is running.

⚠ WARNING

Risks when downloading in RUN mode

When you download changes to the CPU in RUN mode, the changes immediately affect process operation. Changing the program in RUN mode can result in unexpected system operation.

Only authorized personnel who understand the effects of RUN mode changes on system operation should perform a download in RUN mode.

Unexpected system operation can cause death or serious injury to personnel, and/or damage to equipment.

The "Download in RUN mode" feature allows you to make changes to a program and download them to your CPU without switching to STOP mode:

- You can make minor changes to your current process without having to shut down (for example, change a parameter value).
- You can debug a program more quickly with this feature (for example, invert the logic for a normally open or normally closed switch).

You can make the following program block and tag changes and download them in RUN mode:

- Create, overwrite, and delete Functions (FC), Function Blocks (FB), and Tag tables.
- Create, delete, and overwrite Data Blocks (DB) and instance data blocks for Function Blocks (FB). You can add to DB structures and download them in RUN mode. The CPU can maintain the values of existing block tags and initialize the new data block tags to their initial values, or the CPU can set all data block tags to initial values, depending on your configuration settings (Page 1077). You cannot download a web server DB (control or fragment) in RUN mode.
- Overwrite Organization Blocks (OB); however, you cannot create or delete OBs.

You can download a maximum number of 20 blocks in RUN mode at one time. If you need to download more than 20 blocks, you must place the CPU in STOP mode.

If you download changes to a running process, you must think through the possible safety consequences to machines and machine operators before you download.

NOTE

If the CPU is in RUN mode and program changes have been made, TIA Portal always tries to download in RUN first. If you do not want this to happen, you must put the CPU into STOP.

If the changes made are not supported in "Download in RUN", TIA Portal prompts you that the CPU must go to STOP.

15.18.1 Prerequisites for "Download in RUN mode"

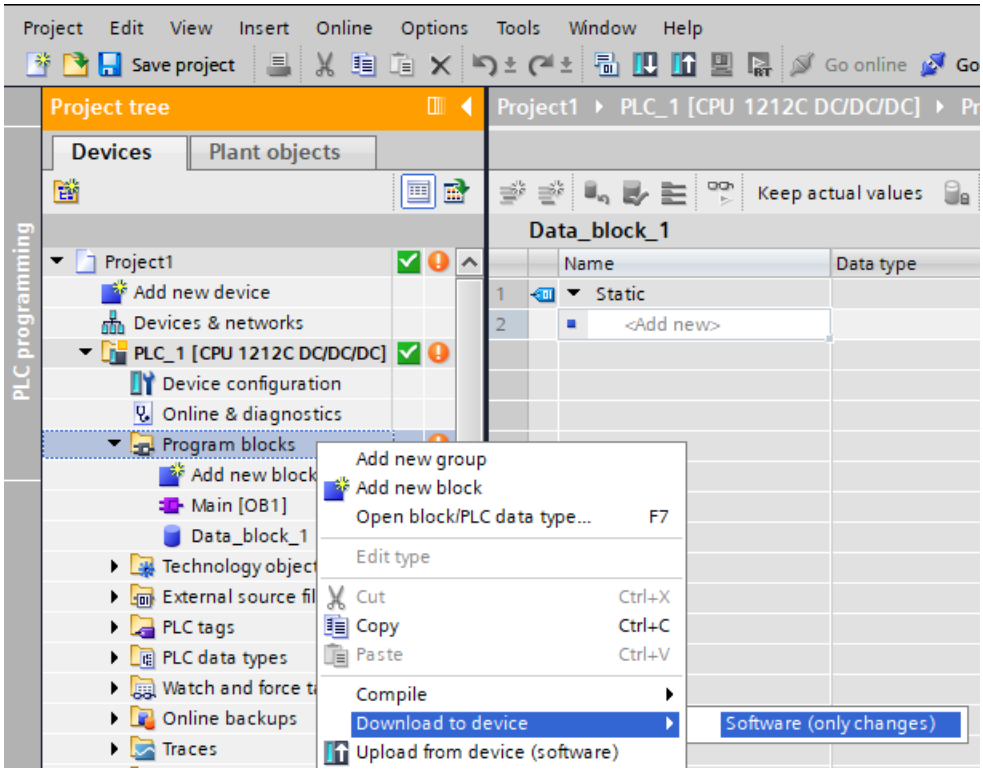
To be able to download your program changes to a CPU that is in RUN mode, you must meet these prerequisites:

- Your program blocks must compile successfully.
- You must have successfully established communication between the CPU and the programming device.

15.18.2 Changing your program in RUN mode

To change the program in RUN mode, you must first ensure that the CPU and program meet the prerequisites (Page 1073), and then follow these steps:

1. To download your program in RUN mode, select one of the following methods:
   - Select the "Download to device" command from the "Online" menu.
   - Click the "Download to device" button in the toolbar.
   - In the "Project tree", right-click "Program blocks" and select the "Download to device > Software (only changes)" command.



   If the program compiles successfully, TIA Portal starts to download the program to the CPU.

2. When TIA Portal prompts you to load your program or cancel the operation, click "Load" to download the program to the CPU.

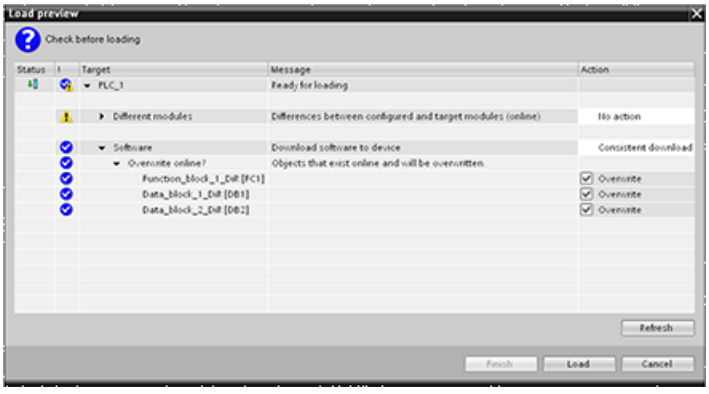
15.18.3 Downloading selected blocks

From the Program blocks folder, you can select a single block or a selection of blocks for downloading.

If you select a single block for downloading, then the only option in the "Action" column is "Consistent download".

You can expand the category line to be sure what blocks are to be loaded. In this example, a small change was made to the offline block, and no other blocks need to be loaded.

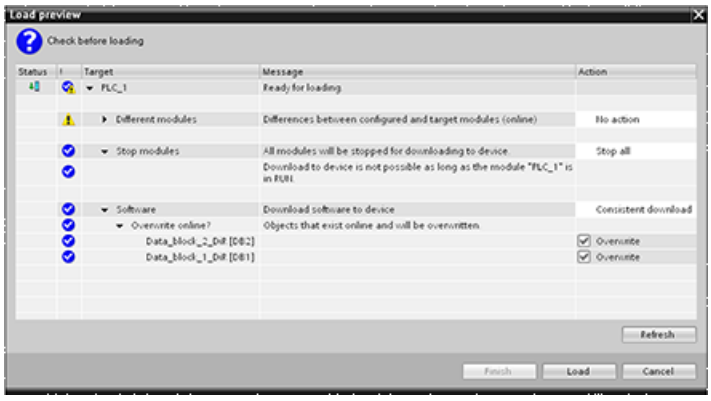
In this example, more than one block is needed for downloading.



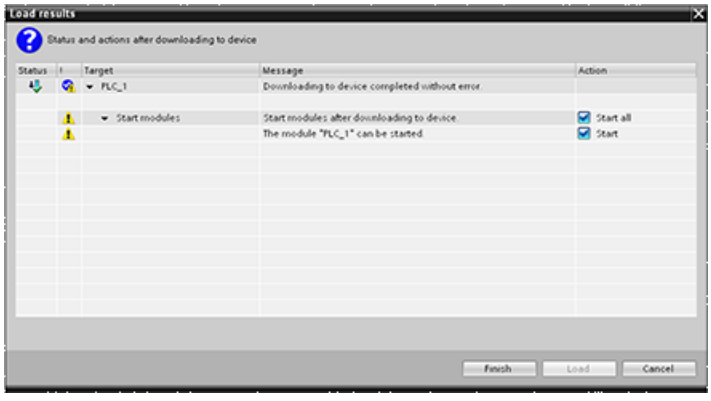
NOTE

You can download a maximum number of 20 blocks in RUN mode at one time. If you need to download more than 20 blocks, you must place the CPU in STOP mode.

If you attempt to download in RUN, but the system detects that this is not possible prior to the actual download, then the Stop modules category line appears in the dialog.

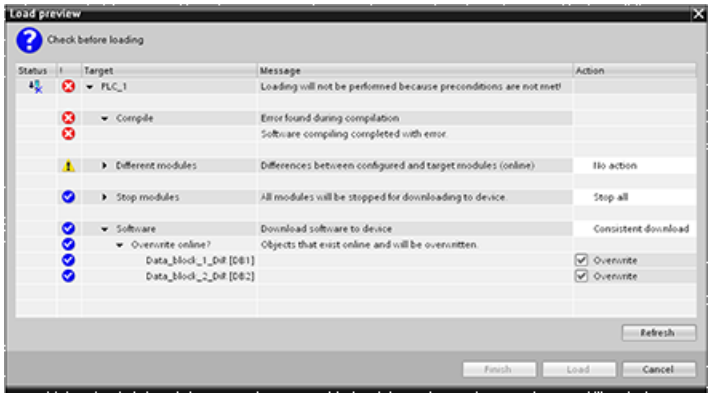


Click the "Load" button, and the "Load results" dialog appears. Click the "Finish" button to complete the download.



15.18.4 Downloading a single selected block with a compile error in another block

If you attempt a consistent download with a compile error in another block, then the dialog indicates an error, and the load button is disabled.



You must correct the compile error in the other block. Then, the "Load" button becomes active.

15.18.5 Modifying and downloading existing tags in RUN mode

The Download in Run feature allows you to add and modify tags in data blocks and function blocks and then download the changed block to the CPU in RUN mode.

Download without reinitialization

Each DB and FB has an amount of reserved memory, which you can use for adding tags to the block that you can subsequently download in RUN mode. By default, the initial size of the memory reserve is 100 bytes. You can add additional tags to your data up to the size of the memory reserve and download the extended block to the CPU in RUN mode. You can also increase the memory reserve if you need more memory for additional tags in your block. If you add more tags than the amount of memory you have allocated, you cannot download the extended block to the CPU in RUN mode.

The "Download without reinitialization" feature allows you to extend a data block by adding more data block tags and download the extended data block in RUN mode. In this way, you can add tags to a data block and download it without reinitializing your program. The CPU retains the values of the existing data block tags and initializes the newly-added tags to their start values.

To enable this function for an online project with a CPU in RUN mode, follow these steps:

1. From the Program blocks folder in the TIA Portal project tree, right-click the block and select "Properties".
2. Click "Download without reinitialization" and select the "Enable download without reinitialization for retentive tags" checkbox in the block editor to enable the function.
3. Click "OK" on the prompt to confirm your choice.
4. Add tags to the block interface and download the block in RUN mode. You can add and download as many new tags as your memory reserve allows.

If you have added more bytes to your block than you have configured for the memory reserve, TIA Portal displays an error when you attempt to download the block in RUN mode. You must edit the block properties to increase the amount. You cannot delete existing entries or modify the “Memory reserve” of the block while the “Download without reinitialization” function is enabled. To disable the "Download without reinitialization" function, follow these steps:

1. From the Program blocks folder in the TIA Portal project tree, right-click the block and select "Properties".
2. Click "Download without reinitialization" and de-select the "Enable download without reinitialization for retentive tags" checkbox in the block editor to disable the function.
3. Click "OK" on the prompt to confirm your choice.
4. Download the block. On the download dialog, you must select "reinitialize" in order to download the extended block.

The download then reinitializes all existing and new block tags to their start values.

Downloading retentive block tags

Downloading retentive block tags in RUN mode requires the allocation of a retentive memory reserve. To configure this retentive memory reserve, follow these steps:

1. From the Program blocks folder in the TIA Portal project tree, right-click the block and select "Properties" from the context menu.
2. Select the "Download without reinitialization" property.
3. Select the check box for "Enable download without reinitialization for retentive tags".
4. Configure the number of bytes available for the retentive memory reserve.
5. Click "OK" to save your changes.
6. Add retentive data block tags to the data block and download the data block in RUN mode. You can add and download as many new retentive data block tags as your retentive memory reserve allows.

If you have added more retentive bytes to your data block than you have configured for the retentive memory reserve, TIA Portal displays an error when you attempt to download the block in RUN mode. You can only add retentive block tags up to the retentive memory reserve in order to be able to download them in RUN mode.

When you download the extended retentive block tags, the tags contain their current values.

Configuring amount of reserved memory for new blocks

The default memory reserve size for new data blocks is 100 bytes. When you create a new block, it has 100 bytes available in reserve. If you want the memory reserve size to be different for new blocks, you can change the setting in the PLC programming settings:

1. From TIA Portal, select the **Options > Settings** menu command.
2. From the Settings dialog, expand "PLC programming" and select "General".
3. In the "Download without reinitialization" section, enter the number of bytes for the memory reserve.

When you create new blocks, TIA Portal uses the memory reserve configuration that you entered for the new blocks.

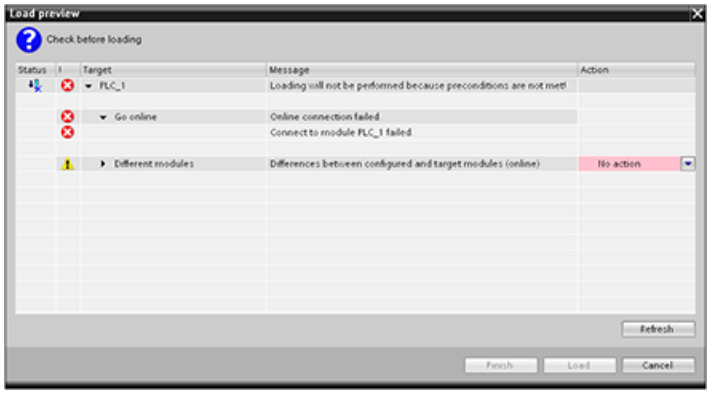
Restrictions

The following restrictions apply to editing and downloading blocks in RUN mode:

- Extending the block interface by adding new tags and downloading in RUN mode is only available for optimized blocks (Page 174).
- You cannot change the structure of a block and download the changed block in RUN mode without reinitializing. Adding new members to a Struct (Page 102) tag, changing tag names, array sizes, data types, or retentive status all require that you reinitialize the block if you download it in RUN mode. The only modifications to existing block tags that you can perform and still download the block in RUN mode without reinitialization are changes to start values (data blocks), default values (function blocks) or comments.
- You cannot download more new block tags in RUN mode than the memory reserve can accommodate.
- You cannot download more new retentive block tags in RUN mode than the retentive memory reserve can accommodate.

15.18.6 System reaction if the download process fails

During the initial Download in RUN operation, if a network connection failure occurs, STEP 7 displays the following "Load preview" dialog:



15.18.7 Considerations when downloading in RUN mode

Before downloading the program in RUN mode, consider the effect of a RUN-mode modification on the operation of the CPU for the following situations:

- If you deleted the control logic for an output, the CPU maintains the last state of the output until the next power cycle or transition to STOP mode.
- If you deleted a high-speed counter or pulse output functions which were running, the high-speed counter or pulse output continues to run until the next power cycle or transition to STOP mode.
- Any logic that is conditional on the state of the first scan bit will not be executed until the next power cycle or transition from STOP to RUN mode. The first scan bit is set only by the transition to RUN mode and is not affected by a download in RUN mode.
- The current values of data blocks (DB) and/or tags can be overwritten.

Requirements

Before you can download your program in RUN mode, the CPU must support changes in RUN mode, the program must compile with no errors, and the communication between TIA Portal, and the CPU must be error-free.

You can make the following changes in program blocks and tags and download them in RUN mode:

- Create, overwrite, and delete Functions (FC), Function Blocks (FB), and Tag tables.
- Create and delete Data Blocks (DB); however, DB structure changes cannot be overwritten. Initial DB values can be overwritten. You cannot download a Web server DB (control or fragment) in RUN mode.
- Overwrite Organization Blocks (OB); however, you cannot create or delete OBs.

You can download a maximum number of 20 blocks in RUN mode at one time. If you need to download more than 20 blocks, you must place the CPU in STOP mode.

Once you initiate a download, you cannot perform other tasks in TIA Portal until the download completes.

Instructions that might fail due to "Download in RUN mode"

The following instructions might experience a temporary error when download in RUN mode changes are being activated in the CPU. The error occurs when the instruction is initiated while the CPU is preparing to activate the downloaded changes. During this time, the CPU suspends initiation of user-program access to the Load Memory, while it completes in-progress user program access to Load Memory. This is done so that downloaded changes can be activated consistently.

Instruction	Response while Activation is Pending
DataLogCreate	STATUS = W#16#80C0, ERROR = TRUE
DataLogOpen	STATUS = W#16#80C0, ERROR = TRUE
DataLogWrite	STATUS = W#16#80C0, ERROR = TRUE
DataLogClose	STATUS = W#16#80C0, ERROR = TRUE
DataLogNewFile	STATUS = W#16#80C0, ERROR = TRUE
DataLogClear	STATUS = W#16#80C0, ERROR = TRUE
DataLogDelete	STATUS = W#16#80C0, ERROR = TRUE

Instruction	Response while Activation is Pending
READ_DBL	RET_VAL = W#16#82C0
WRIT_DBL	RET_VAL = W#16#82C0
Create_DB	RET_VAL = W#16#80C0
Delete_DB	RET_VAL = W#16#80C0
RTM	RET_VAL = 0x80C0

In all cases the RLO output from the instruction will be false when the error occurs. The error is temporary. If it occurs, the instruction should be retried later.

If one of the above instructions fails to execute because a download in RUN mode was in process, retry the failed instruction in a subsequent execution of that OB. If you retry the instruction in the same OB execution, it will fail.

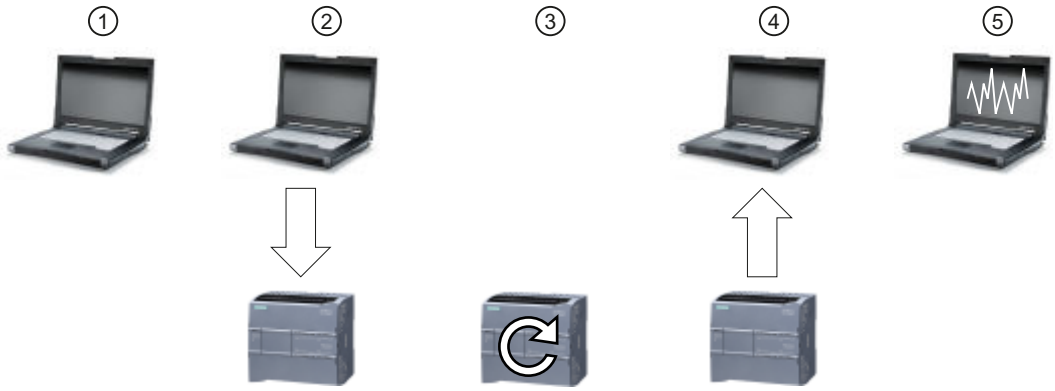
15.19 Tracing and recording CPU data on trigger conditions

STEP 7 provides trace and logic analyzer functions with which you can configure variables for the PLC to trace and record. You can then upload the recorded trace measurement data to your programming device and use STEP 7 tools to analyze, manage, and graph your data. You use the Traces folder in the STEP 7 project tree to create and manage traces.

NOTE

The trace measurement data is available only within the STEP 7 project and is not available for processing by other tools.

The following figure shows the various steps of the trace feature:



① Configure the trace in the trace editor of STEP 7. You can configure the following options:
- Data values to record
- Recording duration
- Recording frequency
- Trigger condition

② Transfer the trace configuration from STEP 7 to the PLC.

③ The PLC executes the program, and when the trigger condition occurs, begins recording the trace data.

④ Transfer the recorded values from the PLC to STEP 7.

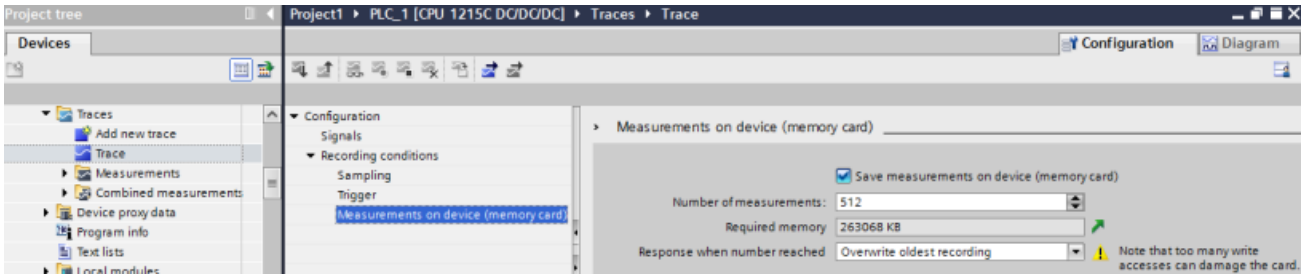
⑤ Use the tools in STEP 7 to analyze, graphically display, and save the data.

The S7-1200 supports two trace jobs with a maximum of 16 variables captured per trigger event. Each trace job provides 524288 bytes of RAM for the recording of trace values and associated overhead, for example variable addresses and time stamps.

Saving trace measurements to the memory card

The S7-1200 CPU can only save trace measurements to the SIMATIC memory card. If you do not have a memory card in your CPU, the CPU will log a diagnostics buffer entry if the program attempts to save trace measurements. The CPU limits the space allocated to trace measurements such that 1 MB of external load memory must always be available. If a trace measurement would require more memory than the maximum allowance, the CPU will not save the measurement and will log a diagnostics buffer entry.

In addition, if you select "Overwrite oldest recording" in STEP 7, the continual writing can reduce the lifetime of load memory. When you select "Overwrite oldest recording", the CPU replaces the oldest measurement with the newest measurement after it has stored the configured number of trace measurements, and continues tracing and saving measurements. Overwriting the oldest measurements is useful in capturing intermittent problems.



The CPU supports a maximum of 999 trace measurement results. During the time that the CPU is saving the trace measurements to external load memory, the CPU does not check the trigger condition for the trace job. Once the CPU finishes saving the trace measurements, the CPU resumes checking for trigger conditions.

Access to examples

See the STEP 7 information system for details about how to program a trace, how to download the configuration, upload the trace data, and display the data in the logic analyzer. You can find detailed examples there in the "Using online and diagnostics functions > Using the trace and logic analyzer function" chapter.

In addition, the online manual "Industry Automation SINAMICS/SIMATIC Using the trace and logic analyzer function" (https://support.industry.siemens.com/cs/ww/en/view/64897128) is an excellent reference.

15.20 Determining the type of wire break condition from an SM 1231 module

As described in the topic Measurement ranges of the analog inputs for voltage and current (SB and SM) (Page 1195), the SM 1231 module returns an analog input value of 32767 (16#7FFF) for both a wire break condition or an overflow condition. These conditions apply to the module only and not the channel. If you want to determine which of these two conditions occurred, you can include logic in your STEP 7 program to make the determination. The method to determine the condition type consists of these tasks:

- Create a Diagnostic error interrupt OB to be called whenever there is an incoming or outgoing diagnostic event.
- Include a call to the RALRM instruction.
- Set up an array of bytes for the AINFO parameter, which includes the information about the condition type.
- Evaluate bytes 32 and 33 of the AINFO structure of the RALRM_DB when the CPU triggers the Diagnostic Interrupt OB..

Creating a Diagnostic error interrupt OB

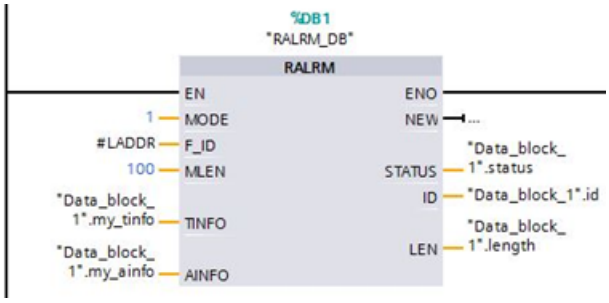
To be able to determine when a wire break condition occurs, create a Diagnostic error interrupt OB. The CPU will call this OB whenever an incoming or outgoing diagnostic event occurs.

When the CPU calls the Diagnostic error interrupt OB, the input parameter LADDR will contain the hardware identifier for the module with the error. You can find the hardware identifier for the SM 1231 module in the STEP 7 device configuration for the SM 1231 module.

Calling the RALRM instruction

To program the RALRM instruction call, follow these steps:

1. Add a call to RALRM in your STEP 7 program.
2. Set the F_ID input parameter to the hardware identifier in the LADDR parameter of the Diagnostic error interrupt OB.
3. Use an array of bytes for the TINFO and AINFO input parameters. Use an array size of 34 bytes or greater.



Interpreting AINFO after a diagnostic interrupt has occurred

The AINFO byte array will contain the information about the module diagnostics after the Diagnostic error interrupt OB executes.

Bytes 0 - 25 are header information. The bytes pertaining to the module diagnostic are as follows:

Byte	Description	
26 and 27	Word value 16#8000 - indicates the diagnostic is a PROFINET style diagnostic	
28 and 29	Word containing channel number responsible for this diagnostic	
30	Bit pattern aaabb000 that indicates the type of channel (aaa) and type of error (bb)	
	aaa	bb
	000: reserved	00: reserved
	001: input channel	01: incoming error
	010: output channel	10: outgoing error
	011: input/output channel	11: outgoing error, other errors present
31	Indication of data format 0: Free data format 1: Bit 2: Two bits 3: Four bits 4: Byte 5: Word (two bytes) 6: Double word (four bytes) 7: Two double words (eight bytes)	
32 and 33	Word that defines the type of error: 16#0000: reserved 16#0001: short circuit 16#0002: undervoltage 16#0003: overvoltage 16#0004: overload 16#0005: over temperature 16#0006: wire break 16#0007: high limit exceeded 16#0008: low limit exceeded 16#0009: error	

For example, consider bytes 26 - 33 of this AINFO structure:

29	my_ainfo[26]	Byte	16#0	16#80
30	my_ainfo[27]	Byte	16#0	16#00
31	my_ainfo[28]	Byte	16#0	16#00
32	my_ainfo[29]	Byte	16#0	16#00
33	my_ainfo[30]	Byte	16#0	16#28
34	my_ainfo[31]	Byte	16#0	16#05
35	my_ainfo[32]	Byte	16#0	16#00
36	my_ainfo[33]	Byte	16#0	16#07

- The Word at bytes 26 and 27 is 16#8000, which indicates that this is a Profinet style diagnostic.
- The Word at bytes 28 and 29 indicates this is a diagnostic for channel 0 or the module.
- Byte 30 is 16#28, which when interpreted as the bit pattern aaa bb 00 is 001 01 000. This value indicates that this diagnostic is for an input channel and is an incoming error.
- Byte 31 is 5, which indicates a Word value
- The word value at bytes 32 and 33 is 16#0007, which indicates high limit exceeded.

By capturing the AINFO information from a Diagnostic error interrupt event, you can thus determine the nature of the diagnostic event.

15.21 Backing up and restoring a CPU

15.21.1 Backup and restore options

You will make a number of changes to your automation system over time, for example, add new devices, replace existing devices or adapt the user program. If these changes were to result in undesirable behavior, you can restore the automation plant to an earlier version if you have a backup. STEP 7 and the S7-1200 CPU offer different options for backing up and restoring the hardware configuration and software.

Backup options

The table below provides an overview of the backup and restoration options of S7 CPUs:

	Snapshot of the monitored values	**Upload from device (software)**	**Upload device as new station (hardware and software)**	**Download backup from online device**
Use case	Restoring a specific status of a data block. The actual values of data blocks including time stamp are accepted in the project.	Upload blocks from a CPU to the project.	Upload of hardware configuration and software from a device to the project.	Create a complete backup of a CPU as a restore point. The backup copy is consistent and cannot be changed or opened.
Requirement	The CPU exists in a project. The data blocks must be identical online and offline.	The CPU exists in the project.	The device is available in the hardware catalog of TIA Portal. Any necessary HSPs or GSD files are installed.	-
Possible in mode	RUN, STOP	RUN, STOP	RUN, STOP	STOP
Possible for F-CPUs	Yes	Yes	No	Yes
Backup can be edited	Yes	Yes	Yes	No

Backup contents

The table below shows which data you can download and back up with which options:

	Snapshot of the monitored values	**Upload from device (software)**	**Upload device as new station (hardware and software)**	**Download backup from online device**
Actual values of the data blocks	Snapshot is possible	Download is possible	Download is possible	Backup is possible
Software blocks	-	Download is possible	Download is possible	Backup is possible
PLC tags (names of tags and constants)	-	Download is possible	Download is possible	Backup is possible
Technology objects	-	Download is possible	Download is possible	Backup is possible
Hardware configuration	-	-	Download is possible	Backup is possible
Monitoring tables (Web server)	-	-	Download is not possible	Backup is possible

	Snapshot of the monitored values	Upload from device (software)	Upload device as new station (hardware and software)	Download backup from online device
Local data, bit memories, timers, counters and process picture	Snapshot is not possible	Download is not possible	Download is not possible	Backup is possible
Archives and recipes (PLC)	-	-	-	Backup is possible
General data on the SIMATIC memory card, for example, help for program blocks or GSD files	-	-	-	Backup is possible

Special considerations during backup of actual values

The "Backup from online device" type of backup backs up the actual values of the tags that are set as retentive. To ensure consistency of the retentive data, disable all write access to retentive data during the backup.

A transition from STOP to RUN mode sets actual values of the non-retentive data to their start values. A CPU backup contains only the start values of non-retentive data.

15.21.2 Backing up an online CPU

Making a backup of your configuration can be useful if you want to return to a specific configuration. You can restore the current configuration at a later time.

Prerequisites

You can create as many backups as you want and store a variety of configurations for a CPU. To make a backup, you must meet the following prerequisites:

- You have already created the CPU in the STEP 7 project.
- You have connected the CPU to the programming device/PC directly using the PROFINET interface of the CPU. Backup and restore operations do not support the PROFIBUS interfaces of the CMs.
- The CPU is online. (If there is no online connection, the backup process establishes an online connection.)
- The CPU is in "STOP" mode. (If the CPU is not in STOP mode, the backup process prompts you to allow the CPU to go to STOP mode.)

Procedure

To create a backup of the current configuration of a CPU, follow these steps:

1. Select the CPU in the project tree.
2. Select the "Backup from online device" command in the "Online" menu.
   If necessary, you must enter the password for read access to the CPU and confirm that the CPU should enter "STOP" mode.

Result

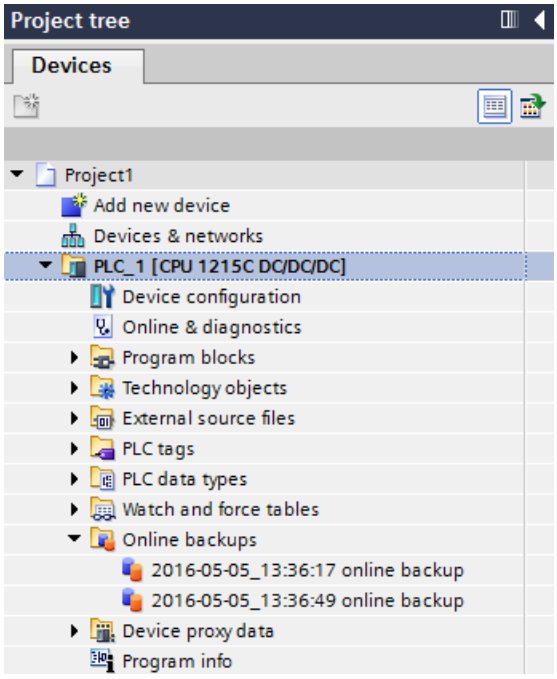
The backups are named with the name of the CPU and the time and date of the backup. The backup includes all data that are needed to restore a particular configuration of a CPU. The CPU backs up the following data:

- Contents of the memory card if one is present and contents of internal load memory otherwise
- Retentive memory areas of data blocks, counters, and bit memory
- Other retentive memory contents, such as IP address parameters

The backup contains the current values of the CPU but does not include the diagnostics buffer.

The backup does not contain the password for protection of confidential PLC configuration data.

You can find the backup in the project tree under the CPU in the "Online backups" folder. The following figure shows an S7-1200 CPU for which two backups have been created:



NOTE

Note that you can also back up the online CPU from the SIMATIC Automation Tool (SAT) or the Web server Online backup standard Web page (Page 787).

When you back files up from STEP 7, STEP 7 stores the files within the STEP 7 project. When you back files up from the Web server, your PC or device saves the backup files in the default folder for downloads. You cannot restore STEP 7 backup files from the Web server and you cannot restore Web server backup files from STEP 7. You can, however, save STEP 7 backup files directly to the download folder of your PC or device. If you do so, then you can restore these files from the Web server.

Saving backup files to your PC or device

To save a backup file to your PC or device, follow these steps:

1. Right-click a file from the Online backups folder in the project tree.
2. Select "Save as" from the context menu.
3. Navigate to the folder where you want to save the file, for example the default folder for downloads on your PC or device.
4. Click Save.

15.21.3 Restoring a CPU

If you have backed up the configuration of a CPU at an earlier point in time, you can transfer the backup to the CPU. The CPU goes to STOP while restoring a backup. If an access level is configured for the CPU, you must supply the password for read access to the CPU.

The backup does not contain the password for protection of confidential PLC configuration data.

WARNING

Potential cybersecurity risks during Restore

If the Restore process is interrupted and you power cycle the CPU before the Restore process is complete, this causes the CPU to lose previously configured protection levels. This can allow attackers with network access to potentially disrupt process operation.

Set up your CPU in a secure environment. When a Restore operation is in progress, do not power cycle the CPU. If a power outage occurs during a Restore operation, retry the operation after power has been restored.

Disruption of process operation can result in death, severe personal injury, and/or property damage.

WARNING

Restoring backups with unknown content

If you restore a backup with unknown content, you can cause malfunctions or program errors.

Make sure that the backup consists of a configuration with known content.

Malfunction and/or program errors can result in death, severe personal injury, and/or property damage.

Restoring a backup to a CPU that has protection of confidential PLC configuration data

If your CPU has protection of confidential PLC configuration data (Page 145), make sure that the configured password in the backup file for protection of confidential PLC configuration data matches the one in the CPU.

If the passwords do not match, the CPU cannot go to RUN mode.

if you attempt to restore a backup file that has a different password for the protection of confidential PLC configuration data than the CPU, the restore succeeds. The CPU, however, will restart in an error state because the protection of confidential PLC configuration data in the CPU did not match the one in the project you restored to the CPU.

In this case, you must set the protection of confidential PLC configuration data in the CPU to match the project that you restored. You can use one of these ways to set or delete the password for protection of confidential PLC configuration data that is in the CPU:

- SIMATIC Automation Tool V4.0 SP3 or greater
- TIA Portal, Online & Diagnostics (Page 1056)
- SIMATIC memory card (Page 115)

Prerequisites

To restore a backup, you must meet the following prerequisites:

- The STEP 7 project includes a configuration for the CPU and a previously-made backup.
- The CPU is connected to the programming device directly through the PROFINET interface of the CPU.
- The CPU is in STOP mode.
- You know the password for full access to the CPU, if an access level (Page 151) was configured.

Procedure

To restore a backup, follow these steps:

1. Open the CPU in the project tree to display the lower-level objects.
2. Select the backup you want to restore from the "Online backups" folder.
3. From the "Online" menu, select the "Download to device" command.
   - If you had previously established an online connection (Page 1051), the "Load preview" dialog opens. This dialog displays alarms and recommends actions needed for the loading operation.
   - If you had not previously established an online connection, the "Extended download to device" dialog opens, and you must first select the interface from which you want to establish the online connection to the CPU.
4. Check the alarms in the "Load preview" dialog, and select the actions in the "Action" column, if necessary.
5. Click the "Load" button (The "Load" button is selectable as soon as downloading is possible.)
6. STEP 7 restores the backup to the CPU. From the "Load results" dialog, you can check whether or not the loading operation was successful and take any further action that might be necessary.
7. After reviewing the "Load results" dialog, click the "Finish" button.

   If prompted, enter the password for full access to the CPU and confirm that the CPU can enter "STOP" mode.

   STEP 7 restores the contents of the backup to the CPU and restarts the CPU.

NOTE

Note that you can also restore a CPU backup from the Web server Online backup standard Web page (Page 787).

Technical specifications

A

A.1 Siemens Online Support Web site

Technical information for these products is available at the Siemens Industry Online Support Web site (https://support.industry.siemens.com/cs/us/en/).

A.2 General technical specifications

Standards compliance

The S7-1200 automation system design conforms with the following standards and test specifications. The test criteria for the S7-1200 automation system are based on these standards and test specifications.

Note that not all S7-1200 models may be certified to these standards, and certification status may change without notification. It is your responsibility to determine applicable certifications by referring to the ratings marked on the product. Consult your local Siemens representative if you need additional information related to the latest listing of exact approvals by part number.

CE approval

The S7-1200 Automation System satisfies requirements and safety related objectives according to the EC directives listed below, and conforms to the harmonized European standards (EN) for the programmable controllers listed in the Official Journals of the European Community.

- 2014/35/EU "Electrical equipment designed for use within certain voltage limits" (Low-Voltage Directive)
- 2014/30/EU "Electromagnetic Compatibility" (EMC Directive)
- 2014/34/EU "Equipment and protective systems intended for use in potentially explosive atmospheres" (Explosion Protection Directive)
- 2011/65/EU "Restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS Directive)

EU declarations of conformity for the respective authorities are available from:

Siemens AG
Digital Industries
Factory Automation
P.O. Box 1963
D-92209 Amberg

The EU declarations of conformity are also available for download from the Siemens Industry Online Support website, under the keyword "Declaration of Conformity".

UK Conformity Assessed marking

The S7-1200 automation system complies with the designated British standards (BS) for programmable controllers published in the official consolidated list of the British Government. The S7-1200 automation system meets the requirements and protection targets of the following regulations and related amendments:

- Electrical Equipment (Safety) Regulations 2016 (Low-Voltage)
- Electromagnetic Compatibility Regulations 2016 (EMC)
- Equipment and Protective Systems Intended for use in Potentially Explosive Atmospheres Regulations 2016 (Explosion Protection)
- Regulations on the restriction of the use of certain hazardous substances in electrical and electronic equipment 2012 (RoHS).

UK Declarations of Conformity for the respective authorities are available from:

Siemens AG
Digital Industries
Factory Automation
P.O. Box 1963
D-92209 Amberg

The UK Declaration of Conformity is also available for download from the Siemens Industry Online Support website under the keyword "Declaration of Conformity".

cULus approval

Underwriters Laboratories Inc. complying with:

- Underwriters Laboratories, Inc.: UL 508 Listed (Industrial Control Equipment)
- Canadian Standards Association: CSA C22.2 Number 142 (Process Control Equipment)

NOTE

The SIMATIC S7-1200 series meets the CSA standard.

The cULus logo indicates that the S7-1200 has been examined and certified by Underwriters Laboratories (UL) to standards UL 508 and CSA 22.2 No. 142.

cULus HAZ. LOC. approval

Underwriters Laboratories Inc. in accordance with:

- ANSI/ISA 12.12.01
- CAN/CSA C22.2 No. 213 (Hazardous Location) APPROVED for use in Class I, Division 2, Group A, B, C, D T3C; Class I, Zone 2, Group IIC T3 Installation Instructions for cULus haz.loc.
- WARNING – Explosion Hazard – Do not disconnect while circuit is live unless area is known to be non-hazardous.
- WARNING – Explosion Hazard – Substitution of components may impair suitability for Class I, Division 2 or Zone 2.
- This equipment is suitable for use in Class I, Division 2, Groups A, B, C, D; Class I, Zone 2, Group IIC; or non-hazardous locations.

IMPORTANT EXCEPTION: See Technical Specifications for the number of inputs or outputs allowed on simultaneously. Some models are de-rated for Ta = 60 °C.

FM approval

FM Approvals
Approval Standard Class Number 3600, 3611 (ANSI/UL 121201), 3810 (ANSI/UL 61010-1), CSA Standard C22.2 No. 0-10, C22.2 No. 213, C22.2 No. 61010-1
Approved for use in:
Class I, Division 2, Group A, B, C, D, Temperature Class T3C Ta = 60 °C [CA, US]
Class I, Zone 2, Group IIC, Temperature Class T3 Ta = 60 °C [US]
Canadian Class I, Zone 2 Installation per CEC 18-150 [CA]

IMPORTANT EXCEPTION: See Technical Specifications for the number of inputs or outputs allowed on simultaneously. Some models are de-rated for Ta = 60 °C.

WARNING

Risk with component substitution

Substitution of components can impair the suitability for Class I, Division 2, and Zone 2.

Repair of units should only be performed by an authorized Siemens Service Center.

Unauthorized improper component substitution can cause death, severe personal injury, and/or property damage.

ATEX approval

According to EN 60079-7 (Electrical apparatus for potentially explosive atmospheres - Part 7: Increased safety "e") and EN IEC 60079-0 (Electrical apparatus for potentially explosive gas atmospheres - Part 0: General requirements).

II 3 G Ex ec IIC T3 Gc

UL 21 ATEX 2622X

Special conditions of use:

1. The equipment shall only be used in an area of not more than pollution degree 2, as defined in EN 60664-1.
2. The equipment shall be installed in an enclosure that provides a degree of protection not less than IP54 in accordance with EN 60079-7.
3. Transient protection shall be provided that is set at a level not exceeding 140% of the peak rated voltage value at the supply terminals to the equipment.

IECEx approval

According to IEC 60079-7 (Explosive atmospheres - Part 7: Equipment protection by increased safety "e") and IEC 60079-0 (Explosive atmospheres - Part 0: Equipment - General requirements).

Ex ec IIC T3 Gc

IECEx UL 21.0107X

Specific conditions of use:

1. The equipment shall only be used in an area of not more than pollution degree 2, as defined in IEC 60664-1.
2. The equipment shall be installed in an enclosure that provides a degree of protection not less than IP54 in accordance with IEC 60079-7.
3. Transient protection shall be provided that is set at a level not exceeding 140% of the peak rated voltage value at the supply terminals to the equipment.

UKEX approval

According to EN 60079-7 (Explosive atmospheres – Part 7: Equipment protection by increased safety "e") and EN IEC 60079-0 (Explosive atmospheres - Part 0: Equipment - General requirements).

II 3 G Ex ec IIC T3 Gc

UL 21UKEX2277X

Specific conditions of use:

1. The equipment shall only be used in an area of not more than pollution degree 2, as defined in EN 60664-1.
2. The equipment shall be installed in an enclosure that provides a degree of protection not less than IP54 in accordance with EN 60079-7.
3. Transient protection shall be provided that is set at a level not exceeding 140% of the peak rated voltage value at the supply terminals to the equipment.

CCCEx approval

According to GB 3836.3 (Explosive atmosphere - Part 3: Equipment protection by increased safety "e")
GB 3836.1 (Explosive atmosphere - Part 1: Equipment - General requirements)
Ex ec IIC T3 Gc
Specific conditions of safety use:

- The equipment shall only be used in an area of not more than pollution degree 2, as defined in GB/T 16935.1.
- The equipment shall be installed in an enclosure that provides a degree of protection not less than IP54 in accordance with GB 3836.3.
- Transient protection shall be provided that is set at a level not exceeding 140% of the peak rated voltage value at the supply terminals to the equipment.

Australia and New Zealand - RCM Mark (Regulatory Compliance Mark)

The S7-1200 automation system satisfies requirements of standards to AS/NZS 61000.6.4 and IEC 610000-6-4 (Class A).

Korea Certification

The S7-1200 automation system satisfies the requirements of the Korean Certification (KC Mark). It has been defined as Class A Equipment and is intended for industrial applications and has not been considered for home use.

Eurasian Customs Union approval (Belarus, Kazakhstan, Russian Federation)

EAC (Eurasion Conformity): Declaration of Conformity according to Technical Regulation of Customs Union (TR CU)

Maritime approval

The S7-1200 products are periodically submitted for special agency approvals related to specific markets and applications. Consult your local Siemens representative if you need additional information related to the latest listing of exact approvals by part number.

Classification societies:

- ABS (American Bureau of Shipping): U.S.A.
- BV (Bureau Veritas): France
- DNV (Det Norske Veritas): Norway
- GL (Germanischer Lloyd): German
- LRS (Lloyds Register of Shipping): England
- Class NK (Nippon Kaiji Kyokai): Japan
- Korean Register of Shipping: Korea
- CSS (China Classification Society): China

Industrial environments

The S7-1200 automation system is designed for use in industrial environments.

Table A-1 Industrial environments

Application field	Emission requirements	Immunity requirements
Industrial	EN 61000-6-4	EN 61000-6-2

Electromagnetic compatibility

Electromagnetic Compatibility (EMC) is the ability of an electrical device to operate as intended in an electromagnetic environment and to operate without emitting levels of electromagnetic interference (EMI) that may disturb other electrical devices in the vicinity.

Table A-2 Immunity

Electromagnetic compatibility - Immunity per EN 61000-6-2	
EN 61000-4-2 Electrostatic discharge	8 kV air discharge to all surfaces 6 kV contact discharge to exposed conductive surfaces
EN 61000-4-3 Radiated, radio-frequency, electro-magnetic field immunity test	80 MHz to1000 MHz, 10V/m, 80% AM (1kHz) 1.4GHz to 6GHz, 3V/m, 80% AM (1kHz)
EN 61000-4-4 Fast transient bursts	2 kV, 5 kHz with coupling network to AC and DC system power 2 kV, 5 kHz with coupling clamp to I/O
EN 61000-4-5 Surge immunity	AC systems - 2 kV common mode, 1 kV differential mode DC systems - 2 kV common mode, 1 kV differential mode For DC systems, refer to Surge immunity below
EN 61000-4-6 Conducted disturbances	150 kHz to 80 MHz, 10 V RMS, 80% AM at 1kHz
EN 61000-4-11 Voltage dips	AC systems 0% for 1 cycle, 40% for 12 cycles, and 70% for 30 cycles at 60 Hz

Table A-3 Emissions

Electromagnetic compatibility - Conducted and radiated emissions per EN 61000-6-4		
Conducted emissions AC power ports	0.15 MHz to 0.5 MHz	< 79 dBµV quasi-peak, < 66 dBµV average
	0.5 MHz to 30 MHz	< 73 dBµV quasi-peak, < 60 dBµV average
Conducted emissions DC power ports	0.15 MHz to 0.5 MHz	< 89 dBµV quasi-peak, < 76 dBµV average
	0.5 MHz to 30 MHz	< 83 dBµV quasi-peak, < 70 dBµV average
Radiated emissions	30 MHz to 230 MHz	< 40 dBµV/m quasi-peak at 10 m
	230 MHz to 1000 MHz	< 47 dBµV/m quasi-peak at 10 m
	1000 MHz to 3000 MHz	< 76 dBµV/m peak, < 56 dBµV/m average at 3 m
	3000 MHz to 6000 MHz	< 80 dBµV/m peak, < 60 dBµV/m average at 3 m

Surge immunity

The wiring of systems subject to surges from coupled lightning strikes must be equipped with external protection. The specification for evaluation of protection from coupled lightning surges is found in EN 61000-4-5, with operational limits established by EN 61000-6-2. You must provide external protection to S7-1200 DC CPUs and signal modules to ensure safe operation when subject to surge voltages that meet or exceed the voltages listed in this specification.

Listed below are some devices that support the needed surge immunity protection. These devices only provide protection if they are installed according to the manufacturer's recommendations. Devices manufactured by other vendors with the same or better specifications can also be used:

Table A-4 Devices that support surge immunity protection

Sub-system	Protection device
+24 V DC power	BLITZDUCTOR VT, BVT AVD 24, Part Number 918 422
Industrial Ethernet	DEHNpatch DPA M CLE RJ45B 48, Part Number 929 121
RS-485	BLITZDUCTOR XT, Basic Unit BXT BAS, Part Number 920 300
	BLITZDUCTOR XT, Module BXT ML2 BD HFS 5, Part Number 920 271
RS-232	BLITZDUCTOR XT, Basic Unit BXT BAS, Part Number 920 300
	BLITZDUCTOR XT, Module BXT ML2 BE S 12, Part Number 920 222
+24 V DC digital inputs	DEHN, Inc., Type DCO SD2 E 24, Part Number 917 988
+24 V DC digital outputs and sensor supply	DEHN, Inc., Type DCO SD2 E 24, Part Number 917 988
Analog IO	DEHN, Inc., Type DCO SD2 E 12, Part Number 917 987
Relay outputs	None required

Environmental conditions

Table A-5 Shipping and storage

Environmental conditions - Shipping and storage	
EN 60068-2-2, Test Bb, Dry heat and EN 60068-2-1, Test Ab, Cold	-40 °C to +70 °C
EN 60068-2-30, Test Db, Damp heat	25 °C to 55 °C, 95% humidity
EN 60068-2-14, Test Na, temperature shock	-40 °C to +70 °C, dwell time 3 hours, 2 cycles
EN 60068-2-32, Free fall	0.3 m, 5 times, product packaging
Atmospheric pressure	1140 to 540 hPa (corresponding to an altitude of -1000 to 5000 m)

Table A-6 Climatic ambient conditions

Environmental conditions - Climatic ambient conditions	
The S7-1200 automation system is suitable for use in weather-proof, fixed locations. The operating conditions are based on requirements according to DIN IEC 60721-3-3: • Class 3M3 (mechanical requirements) • Class 3K3 (climatic requirements)	
Ambient temperature range (Inlet Air 25 mm below unit)	-20 °C to 60 °C horizontal mounting -20 °C to 50 °C vertical mounting 95% non-condensing humidity Unless otherwise specified
Atmospheric pressure	1140 to 795 hPa (corresponding to an altitude of -1000 to 2000 m)[1]
Concentration of contaminants	SO_2: < 0.5 ppm; H_2S: < 0.1 ppm; RH < 60% non-condensing
	ISA-S71.04 severity level G1, G2, G3
EN 60068-2-14, Test Nb, temperature change	0 °C to 60 °C
EN 60068-2-27 Mechanical shock	15 g, 11 ms pulse, 6 shocks in each of 3 axis
EN 60068-2-6 Sinusoidal vibration	DIN rail mount: 3.5 mm from 5-9 Hz, 1G from 8.4 - 150 Hz Panel Mount: 7.0 mm from 5-8.4 Hz, 2G from 8.4 to 150 Hz 10 sweeps each axis, 1 octave per minute

[1] This rating applies to relay output or input AC S7-1200 CPUs.

Contamination level/overvoltage category according to IEC 61131-2

- Pollution degree 2
- Overvoltage category: II

Protection class

- Protection Class II according to EN 61131-2 (Protective conductor not required)

Degree of protection

- IP20 Mechanical Protection, EN 60529
- Protects against finger contact with high voltage as tested by standard probe. External protection required for dust, dirt, water and foreign objects of < 12.5mm in diameter.

Rated voltages

Table A-7 Rated voltages

Rated voltage	Tolerance
24 V DC	20.4 V DC to 28.8 V DC
120/230 V AC	85 V AC to 264 V AC, 47 to 63 Hz

NOTE

When a mechanical contact turns on output power to the S7-1200 CPU, or any digital expansion module, it sends a "1" signal to the digital outputs for approximately 50 microseconds. This could cause unexpected machine or process operation which could result in death or serious injury to personnel and/or damage to equipment. You must plan for this, especially if you are using devices which respond to short duration pulses.

Reverse voltage protection

Reverse voltage protection circuitry is provided on each terminal pair of +24 V DC power or user input power for CPUs, signal modules (SMs), and signal boards (SBs). It is still possible to damage the system by wiring different terminal pairs in opposite polarities.

Some of the 24 V DC power input ports in the S7-1200 system are interconnected, with a common logic circuit connecting multiple M terminals. For example, the following circuits are interconnected when designated as "not isolated" in the data sheets: the 24 V DC power supply of the CPU, the sensor power of the CPU, the power input for the relay coil of an SM, and the power supply for a non-isolated analog input. All non-isolated M terminals must connect to the same external reference potential.

⚠ WARNING

Risks when connecting non-isolated M terminals to different reference potentials

Connecting non-isolated M terminals to different reference potentials will cause unintended current flows that can cause damage or unpredictable operation in the PLC and any connected equipment.

Always ensure that all non-isolated M terminals in an S7-1200 system are connected to the same reference potential.

Failure to comply with these guidelines can cause damage or unpredictable operation which can result in death or severe personal injury and/or property damage.

DC Outputs

Short -circuit protection circuitry is not provided for DC outputs on CPUs, signal modules (SMs) and signal boards (SBs).

Relay electrical service life

The typical performance data estimated from sample tests is shown below. Actual performance may vary depending upon your specific application. An external protection circuit that is adapted to the load will enhance the service life of the contacts. N.C. contacts have a typical service life of about one-third that of the N.O. contact under inductive and lamp load conditions.

An external protective circuit will increase the service life of the contacts.

Table A-8 Typical performance data

Data for selecting an actuator			
Continuous thermal current	2 A max.		
Switching capacity and life of the contacts			
For ohmic load	Voltage	Current	Number of operating cycles (typical)
	24 V DC	2.0 A	0.1 million
	24 V DC	1.0 A	0.2 million
	24 V DC	0.5 A	1.0 million
	48 V AC	1.5 A	1.5 million
	60 V AC	1.5 A	1.5 million
	120 V AC	2.0 A	1.0 million
	120 V AC	1.0 A	1.5 million
	120 V AC	0.5 A	2.0 million
	230 V AC	2.0 A	1.0 million
	230 V AC	1.0 A	1.5 million
	230 V AC	0.5 A	2.0 million
For inductive load (according to IEC 947-5-1 DC13/AC15)	Voltage	Current	Number of operating cycles (typical)
	24 V DC	2.0 A	0.05 million
	24 V DC	1.0 A	0.1 million
	24 V DC	0.5 A	0.5 million
	24 V AC	1.5 A	1.0 million
	48 V AC	1.5 A	1.0 million
	60 V AC	1.5 A	1.0 million
	120 V AC	2.0 A	0.7 million
	120 V AC	1.0 A	1.0 million
	120 V AC	0.5 A	1.5 million
	230 V AC	2.0 A	0.7 million
	230 V AC	1.0 A	1.0 million
	230 V AC	0.5 A	1.5 million
Activating a digital input	Possible		

Data for selecting an actuator	
Switching frequency	
Mechanical	Max. 10 Hz
At ohmic load	Max. 1 Hz
At inductive load (according to IEC 947-5-1 DC13/AC15)	Max. 0.5 Hz
At lamp load	Max. 1Hz

Internal CPU memory retention

- Lifetime of retentive data and data log data: 10 years
- Power down retentive data, Write cycle endurance: 2 million cycles
- Data log data: write cycle endurance: 500 million data log entries

NOTE

Effect of data logs on internal CPU memory

Each data log write consumes at a minimum 2 KB of memory. If your program writes small amounts of data frequently, it is consuming at least 2 KB of memory on each write. A better implementation would be to accumulate the small data items in a data block (DB), and to write the data block to the data log at less frequent intervals.

If your program writes many data log entries at a high frequency, consider using a replaceable SD memory card.

A.3 Altitude specifications

Table A-9 S7-1200 CPUs for maximum installation altitude 5,000 m

Description	Article number	Version	Maximum installation altitude
S7-1200 Standard			
CPU 1211C DC/DC/DC	6ES7211-1AE40-0XB0	FS10 or higher	5,000 m
CPU 1212C DC/DC/DC	6ES7212-1AE40-0XB0	FS10 or higher	5,000 m
CPU 1214C DC/DC/DC	6ES7214-1AG40-0XB0	FS10 or higher	5,000 m
CPU 1215C DC/DC/DC	6ES7215-1AG40-0XB0	FS10 or higher	5,000 m
CPU 1217C DC/DC/DC	6ES7217-1AG40-0XB0	FS10 or higher	5,000 m

Table A-10 S7-1200 I/O modules for maximum installation altitude 5,000 m

Description	Article number	Version	Maximum installation altitude
S7-1200 Standard I/O Modules			
SM 1221, 8 DI, 24 V DC	6ES7221-1BF32-0XB0	FS02 or higher	5,000 m
SM 1221, 16 DI, 24 V DC	6ES7221-1BH32-0XB0	FS03 or higher	5,000 m
SB 1221, 4 DI, 5 V DC 200 kHz	6ES7221-3AD30-0XB0	FS03 or higher	5,000 m
SB 1221, 4 DI, 24 V DC 200 kHz	6ES7221-3BD30-0XB0	FS03 or higher	5,000 m
SB 1222, 4 DQ, 5 V DC 200 kHz	6ES7222-1AD30-0XB0	FS03 or higher	5,000 m
SB 1222, 4 DQ, 24 V DC 200 kHz	6ES7222-1BD30-0XB0	FS03 or higher	5,000 m
SM 1222, 8 DO, 24 V DC	6ES7222-1BF32-0XB0	FS02 or higher	5,000 m
SM 1222, 16 DO, 24 V DC	6ES7222-1BH32-0XB0	FS03 or higher	5,000 m
SM 1222, 16 DO, 24 V DC, sinking	6ES7222-1BH32-1XB0	FS01 or higher	5,000 m
SB 1223, 2 DI/2 DO, 24 V DC	6ES7223-0BD30-0XB0	FS03 or higher	5,000 m
SM 1223, 8 DI/8 DO, 24 V DC	6ES7223-1BH32-0XB0	FS02 or higher	5,000 m
SM 1223, 16 DI/16 DO, 24 V DC	6ES7223-1BL32-0XB0	FS03 or higher	5,000 m
SM 1223, 16 DI/16 DO, 24 V DC, sinking	6ES7223-1BL32-1XB0	FS01 or higher	5,000 m
SB 1223, 2 DI/2 DQ, 24 V DC	6ES7223-3BD30-0XB0	FS03 or higher	5,000 m
SB 1223, 2 DI/2 DQ, 5 V DC	6ES7223-3AD30-0XB0	FS03 or higher	5,000 m
SB 1231, 1 AI, +/-10 V DC	6ES7231-4HA30-0XB0	FS04 or higher	5,000 m
SM 1231, 4 AI, +/-10 V, +/-5 V, +/-2.5 V	6ES7231-4HD32-0XB0	FS05 or higher	5,000 m
SM 1231, 8 AI, +/-10 V, +/-5 V, +/-2.5 V	6ES7231-4HF32-0XB0	FS05 or higher	5,000 m
SM 1231, 4 AI, +/-10 V, +/-5 V, +/- 2.5 V, +/-1.25, 16 bit	6ES7231-5ND32-0XB0	FS02 or higher	5,000 m
SB 1231 RTD, 1 AI RTD, Pt100 and Pt1000	6ES7231-5PA30-0XB0	FS04 or higher	5,000 m
SM 1231 RTD, 4xAI	6ES7231-5PD32-0XB0	FS02 or higher	5,000 m
SM 1231 RTD, 8xAI	6ES7231-5PF32-0XB0	FS02 or higher	5,000 m
SM 1231 TC, 4 AI	6ES7231-5QD32-0XB0	FS02 or higher	5,000 m
SB 1231 TC, 1 AI	6ES7231-5QA30-0XB0	FS04 or higher	5,000 m
SM 1231 TC, 8 AI	6ES7231-5QF32-0XB0	FS02 or higher	5,000 m
SB 1232, 1 AO, +/-10 V DC	6ES7232-4HA30-0XB0	FS03 or higher	5,000 m
SM 1232, 2 AO, +/-10 V	6ES7232-4HB32-0XB0	FS04 or higher	5,000 m
SM 1232, 4 AO, +/-10 V	6ES7232-4HD32-0XB0	FS04 or higher	5,000 m
SM 1234, 4 AI/2 AO, +/-10	6ES7234-4HE32-0XB0	FS06 or higher	5,000 m
CM 1241, RS232	6ES7241-1AH32-0XB0	FS01 or higher	5,000 m

Description	Article number	Version	Maximum installation altitude
CM 1241, RS422/485	6ES7241-1CH32-0XB0	FS03 or higher	5,000 m
CB 1241, RS485	6ES7241-1CH30-1XB0	FS03 or higher	5,000 m
SM1278 IO-Link Master	6ES7278-4BD32-0XB0	FS03 or higher	5,000 m

Table A-11 Restrictions of the maximum ambient temperature specified with regard to the installation altitude

Installation altitude	Derating factor for ambient temperature [1]
-1,000 m to 2,000 m	1.0
2,000 m to 3,000 m	0.9
3,000 m to 4,000 m	0.8
4,000 m to 5,000 m	0.7
[1] Base value for the application of the derating factor is the maximum permissible ambient temperature in C for 2000 m.	

NOTE

- Linear interpolation between altitudes is permissible.
- The derating factors compensate for the decreasing cooling effect of air in higher altitudes due to lower density.
- Note the mounting position of the respective module in the technical specifications. The basis is the standard IEC 61131-2:2017.
- Make sure that the power supplies you use are also rated for altitudes > 2,000 m.

Effects on the availability of modules

The higher cosmic radiation present during operation at altitudes above 2000 m will also start to have an effect on the failure rate of electronic components (the so-called soft error rate). In rare cases this can result in a transition of a safety module into safe state. However, the functional safety of the module is fully retained.

Currently valid markings and approvals

NOTE

Information on the components of the S7-1200 automation system

The markings and approvals printed on the components of the S7-1200 automation system are currently based on an operating altitude of up to 2000 m above sea level.

Shipping and storage conditions for modules

The S7-1200 system meets the specifications regarding shipping and storage conditions pursuant to IEC 61131-2. The following information applies to modules that are shipped and/or stored in their original packaging:

Table A-12 Shipping and storage conditions for S7-1200 modules

Type of condition	Permitted range
Air pressure	From 1140 hPa to 540 hPa (corresponds to an altitude of -1000 m to 5000 m)

A.4 PROFINET interface X1 port pinouts

The S7-1200 CPU connects to the PROFINET network using a standard female RJ45 jack. The connector pinout depends on the CPU type.

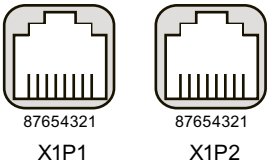
Single-port CPUs

Single-port CPUs (CPU 1211C, CPU 1212C and CPU 1214C) have a standard Ethernet MDI pin configuration as follows:

Pin	Signal name	Description	RJ45 female jack pinout
1	TD+	Transmit data	87654321 X1P1
2	TD-		
3	RD+	Receive data	
4	GND	Ground	
5	GND		
6	RD-	Receive data	
7	GND	Ground	
8	GND		

Dual-port CPUs

The ports of a dual-port CPU (CPU 1215C and CPU1217C) have a standard Ethernet MDI-X pin configuration as follows:

Pin	Signal name	Description	RJ45 female jack pinout
1	TD+	Transmit data	
2	TD-		
3	RD+	Receive data	
4	GND	Ground	
5	GND		
6	RD-	Receive data	
7	GND	Ground	
8	GND		

NOTE

Dual-port CPU

The number shown under the pin indicates that the dual port CPUs do not have any crossover between pins. There is an internal Ethernet switch in the units: the TD+/- and RD+/- pairs are not crossed over internally.

Autonegotiation

If the port's configuration enables autonegotiation, the S7-1200 CPU automatically detects the cable type and swaps the transmit/receive lines, if needed. If the port's configuration disables autonegotiation, the CPU also disables this automatic swap. You configure a port's autonegotiation setting in the TIA Portal's port options dialog. This is a port-specific advanced option for the PROFINET interface (X1) of the CPU's properties. Refer to "Configuring the PROFINET port" in Section 11.2.3.4: "Configuring an IP address for a CPU in your project" (Page 538) for further information.

A.5 CPU 1211C

A.5.1 General specifications and features

Table A-13 General specifications

Technical data	CPU 1211C AC/DC/Relay	CPU 1211C DC/DC/Relay	CPU 1211C DC/DC/DC
Article number	6ES7211-1BE40-0XB0	6ES7211-1HE40-0XB0	6ES7211-1AE40-0XB0
Dimensions W x H x D (mm)	90 x 100 x 75		
Shipping weight	420 grams	380 grams	370 grams
Power dissipation	10 W	8 W	
Electrical current available (CM bus)	750 mA max. (5 V DC)		
Electrical current available (24 V DC)	300 mA max. (sensor power)		
Digital input current consumption (24 V DC)	4 mA/input used		

Table A-14 CPU features

Technical data		Description
User memory (Refer to "General technical specifications" (Page 1090), "Internal CPU memory retention".)	Work	75 Kbytes
	Load	1 Mbyte internal, expandable up to SD card size
	Retentive	14 Kbytes
Onboard digital I/O		6 inputs/4 outputs
Onboard analog I/O		2 inputs
Process image size		1024 bytes of inputs (I) /1024 bytes of outputs (Q)
Bit memory (M)		4096 bytes
Temporary (local) memory		• 16 Kbytes for startup and program cycle (including associated FBs and FCs) • 6 Kbytes for each of the other interrupt priority levels (including FBs and FCs)
Signal modules expansion		none
SB, CB, BB expansion		1 max.
Communication module expansion		3 CMs max.
High-speed counters		Up to 6 configured to use any built-in or SB inputs. Refer to "Hardware input pin assignment" (Page 502) for CPU 1211C: HSC default address assignments. 100/[1]80 kHz (Ia.0 to Ia.5)
Pulse outputs[2]		Up to 4 configured to use any built-in or SB outputs 100 kHz (Qa.0 to Qa.3)
Pulse catch inputs		6
Time delay interrupts		4 total with 1 ms resolution
Cyclic interrupts		4 total with 1 ms resolution

[1] The slower speed is applicable when the HSC is configured for quadrature mode of operation.

[2] For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

Technical data	Description
Edge interrupts	6 rising and 6 falling (10 and 10 with optional signal board)
Memory card	SIMATIC memory card (optional)
Real time clock accuracy	+/- 60 seconds/month
Real time clock retention time	20 days typ./12 days min. at 40 °C (maintenance-free Super Capacitor)

[1] The slower speed is applicable when the HSC is configured for quadrature mode of operation.

[2] For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

Table A-15 Performance

Type of instruction		Execution speed	
		Direct addressing (I, Q and M)	DB accesses
Boolean		0.08 µs/instruction	
Move	Move_Bool	0.3 µs/instruction	1.17 µs/instruction
	Move_Word	0.137 µs/instruction	1.0 µs/instruction
	Move_Real	0.72 µs/instruction	1.0 µs/instruction
Real Math	Add Real	1.48 µs/instruction	1.78 µs/instruction

NOTE

Many variables affect measured times. The above performance times are for the fastest instructions in this category and error-free programs.

A.5.2 Timers, counters, and code blocks supported by CPU 1211C

Table A-16 Blocks, timers and counters supported by CPU 1211C

Element		Description
Blocks	Type	OB, FB, FC, DB
	Size	Up to the size of work memory
	Address range for FBs, FCs, and DBs	FB and FC: 1 to 65535 (such as FB 1 to FB 65535) DB: 1 to 59999
	Nesting depth	16 from the program cycle or startup OB 6 from any interrupt event OB[1]
	Monitoring	Status of 2 code blocks can be monitored simultaneously
OBs	Program cycle	Multiple
	Startup	Multiple
	Time-delay interrupt	4 (1 per event)
	Cyclic interrupts	4 (1 per event)
	Hardware interrupts	50 (1 per event)
	Time error interrupts	1
	Diagnostic error interrupts	1
	Pull or plug of modules	1

[1] Safety programs use two nesting levels. The user program therefore has a nesting depth of four in safety programs.

Element		Description
OBs	Rack or station failure	1
	Time of day	Multiple
	Status	1
	Update	1
	Profile	1
	MC-Interpolator	1
	MC-Servo	1
	MC-PreServo	1
	MC-PostServo	1
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, 16 bytes per timer
Counters	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size dependent upon count type • SInt, USInt: 3 bytes • Int, UInt: 6 bytes • DInt, UDInt: 12 bytes

[1] Safety programs use two nesting levels. The user program therefore has a nesting depth of four in safety programs.

A.5.3 Communications CPU 1211C

Table A-17 Communication

Technical data	Description
Number of ports	1
Type	Ethernet
HMI device	4
Programming device (PG)	1
Connections (Page 526)	34 reserved, 68 max.
Data rates	10/100 Mb/s
Isolation (external signal to logic)	Transformer isolated, 1500 V AC (type test)[1]
Cable type	CAT5e shielded
Interfaces	
Number of PROFINET interfaces	1
Number of interfaces PROFIBUS	0
Interface	
Interface Hardware	
Number of ports	1

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description
Integrated switch	No
RJ-45 (Ethernet)	Yes; X1
Protocols	
PROFINET IO controller	Yes
PROFINET IO device	Yes
SIMATIC communication	Yes
Open IE communication	Yes
Web server	Yes
Media redundancy	No
PROFINET IO controller	
Services	
PG/OP communication	Yes
S7 routing	Yes
Isochronous mode	No
Open IE communication	Yes
IRT	No
MRP	No
PROFIenergy	Yes. The S7-1200 CPU only supports the PROFIenergy entity (with I-device functionality).
Prioritized startup	Yes (max. 16 PROFINET devices)
Number of connectable I/O devices max.	16
Number of IO devices that you can connect for RT, max.	16
Of which are in line, max.	16
Number of IO devices that can be activated/ deactivated simultaneously, max.	8
Update times	The minimum value of the update time also depends on the communication component set for PROFINET IO, on the number of IO devices, and the quantity of configured user data.
With RT	
Send clock of 1 ms	1 ms to 512 ms
PROFINET IO device	
Services	
PG/OP communication	Yes
S7 routing	Yes
Isochronous mode	No
Open IE communication	Yes
IRT, supported	No
MRP, supported	No

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data		Description
PROFIenergy		Yes
Shared device		Yes
Number of IO controllers with shared device, max.		2
SIMATIC communication		
S7 communication, as server		Yes
S7 communication, as client		Yes
User data per job, max.		See online help (S7 communication, user data size)
Open IE communication		
TCP/IP:		Yes
	Data length, max.	8 KB
	Several passive connections per port, supported	Yes
ISO-on-TCP (RFC1006):		Yes
	Data length, max.	8 KB
UDP		Yes
	Data length, max.	2048 bytes
DHCP		No
SNMP		Yes
DCP		Yes
LLDP		Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

A.5.4 Power supply and sensor power

Table A-18 Power supply

Technical data		CPU 1211C AC/DC/Relay	CPU 1211C DC/DC/Relay	CPU 1211C DC/DC/DC
Voltage range		85 to 264 V AC	20.4 V DC to 28.8 V DC	
Line frequency		47 to 63 Hz	--	
Input current	CPU only at max. load	60 mA at 120 V AC 30 mA at 240 V AC	300 mA at 24 V DC	300 mA at 24 V DC
	CPU with all expansion accessories at max. load	180 mA at 120 V AC 90 mA at 240 V AC	900 mA at 24 V DC	
Inrush current (max.)		20 A at 264 V AC	12 A at 28.8 V DC	
I^2 t		0.8 A^2 s	0.5 A^2 s	
Isolation (input power to logic)		1500 V AC	Not isolated	
Ground leakage, AC line to functional earth		0.5 mA max.	--	
Hold up time (loss of power)		20 ms at 120 V AC 80 ms at 240 V AC	10 ms at 24 V DC	
Internal fuse, not user replaceable		3 A, 250 V, slow blow		

Table A-19 Sensor power

Technical data	CPU 1211C AC/DC/Relay	CPU 1211C DC/DC/Relay	CPU 1211C DC/DC/DC
Voltage range	20.4 to 28.8 V DC	L+ minus 4 V DC min.	
Output current rating (max.)	300 mA (short-circuit protected)		
Maximum ripple noise (<10 MHz)	< 1 V peak to peak	Same as input line	
Isolation (CPU logic to sensor power)	Not isolated		

A.5.5 Digital inputs and outputs

Table A-20 Digital inputs

Technical data	CPU 1211C AC/DC/Relay, DC/DC/Relay, and DC/DC/DC
	High speed inputs
Number of inputs	6
Type	Sink/Source (IEC Type 1 sink)
Rated voltage	24 V DC at 6 mA, nominal
Continuous permissible voltage	30 V DC, max. at 8 mA, max.
Surge voltage	35 V DC for 0.5 sec.
Logic 1 signal (min.)	15 V DC at 2.5 mA
Logic 0 signal (max.)	5 V DC at 1 mA
Isolation (field side to logic)	707 V DC (type test)
Isolation groups	1
Filter times	us settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0
HSC clock input rates (max.) (Logic 1 Level = 15 to 26 V DC)	100/80 kHz (Ia.0 to Ia.5)
Number of inputs on simultaneously	6 at 60 °C horizontal, 50 °C vertical
Cable length (meters)	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs

Table A-21 Digital outputs

Technical data	CPU 1211C AC/DC/Relay and CPU 1211C DC/DC/Relay	CPU 1211C DC/DC/DC
Number of outputs	4	
Type	Relay, mechanical	Solid state - MOSFET (sourcing)
Voltage range	5 to 30 V DC or 5 to 250 V AC	20.4 to 28.8 V DC
Logic 1 signal at max. current	--	20 V DC min.
Logic 0 signal with 10 KΩ load	--	0.1 V DC max.
Current (max.)	2.0 A	0.5 A
Lamp load	30 W DC / 200 W AC	5 W
ON state resistance	0.2 Ω max. when new	0.6 Ω max.

[1] For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

[2] Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

Technical data	CPU 1211C AC/DC/Relay and CPU 1211C DC/DC/Relay	CPU 1211C DC/DC/DC
Leakage current per point	--	10 µA max.
Surge current	7 A with contacts closed	8 A for 100 ms max.
Overload protection	No	
Isolation (field side to logic)	1500 V AC (coil to contact) None (coil to logic)	707 V DC (type test)
Isolation groups	1	
Inductive clamp voltage	--	L+ minus 48 V DC, 1 W dissipation
Maximum relay switching frequency	1 Hz	--
Switching delay (Qa.0 to Qa.3)	10 ms max.	1.0 µs max., off to on 3.0 µs max., on to off
Pulse Train Output rate	Not recommended [1]	100 kHz (Qa.0 to Qa.3)[2], 2 Hz min.
Lifetime mechanical (no load)	10,000,000 open/close cycles	--
Lifetime contacts at rated load	100,000 open/close cycles	--
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Control of a digital input	Yes	
Parallel outputs for redundant load control	Yes (with same common)	
Parallel outputs for increased load	No	
Number of outputs on simultaneously	4 at 60 °C horizontal, 50 °C vertical	
Cable length (meters)	500 m shielded, 150 m unshielded	

[1] For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

[2] Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

A.5.6 Analog inputs

Table A-22 Analog inputs

Technical data	Description
Number of inputs	2
Type	Voltage (single-ended)
Full-scale range	0 to 10 V
Full-scale range (data word)	0 to 27648
Overshoot range	10.001 to 11.759 V
Overshoot range (data word)	27649 to 32511
Overflow range	11.760 to 11.852 V
Overflow range (data word)	32512 to 32767

Technical data	Description
Resolution	10 bits
Maximum withstand voltage	35 V DC
Smoothing	None, Weak, Medium, or Strong See the table for Step response (ms) for the analog inputs of the CPU (Page 1112).
Noise rejection	10, 50, or 60 Hz
Impedance	≥100 KΩ
Isolation (field side to logic)	None
Accuracy (25 °C / -20 to 60 °C)	3.0% / 3.5% of full-scale
Cable length (meters)	100 m, shielded twisted pair

A.5.6.1 Step response of the built-in analog inputs of the CPU

Table A-23 Step Response (ms), 0 V to 10 V measured at 95%

Smoothing selection (sample averaging)	Rejection frequency (Integration time)		
	60 Hz	**50 Hz**	**10 Hz**
None (1 cycle): No averaging	50 ms	50 ms	100 ms
Weak (4 cycles): 4 samples	60ms	70 ms	200 ms
Medium (16 cycles): 16 samples	200 ms	240 ms	1150 ms
Strong (32 cycles): 32 samples	400 ms	480 ms	2300 ms
Sample time	**4.17 ms**	**5 ms**	**25 ms**

A.5.6.2 Sample time for the built-in analog ports of the CPU

Table A-24 Sample time for built-in analog inputs of the CPU

Rejection frequency (Integration time selection)	Sample time
60 Hz (16.6 ms)	4.17 ms
50 Hz (20 ms)	5 ms
10 Hz (100 ms)	25 ms

A.5.6.3 Measurement ranges of the analog inputs for voltage (CPUs)

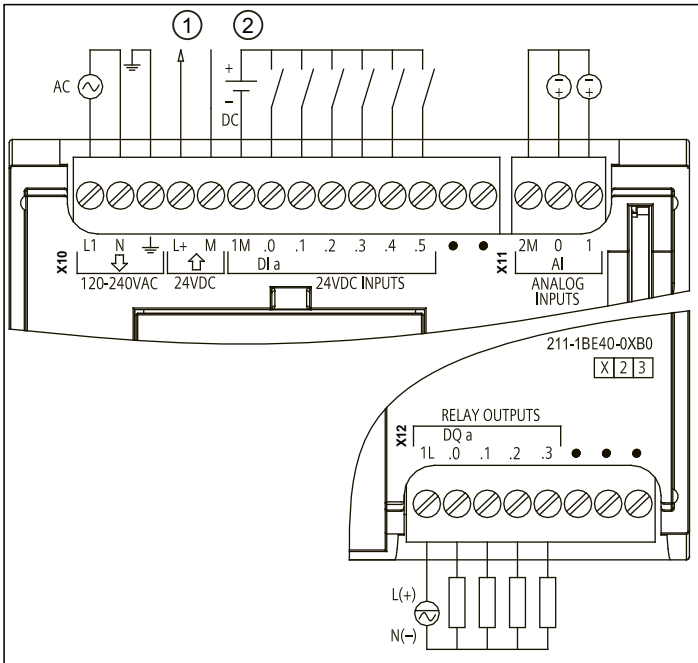
Table A-25 Analog input representation for voltage (CPUs)

System		Voltage Measuring Range	
Decimal	**Hexadecimal**	**0 to 10 V**	
32767	7FFF	11.852 V	Overflow
32512	7F00		
32511	7EFF	11.759 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range

System		Voltage Measuring Range	
Decimal	**Hexadecimal**	**0 to 10 V**	
20736	5100	7.5 V	Rated range
34	22	12 mV	
0	0	0 V	
Negative values		Negative values are not supported	

A.5.7 CPU 1211C wiring diagrams

Table A-26 CPU 1211C AC/DC/Relay (6ES7211-1BE40-0XB0)



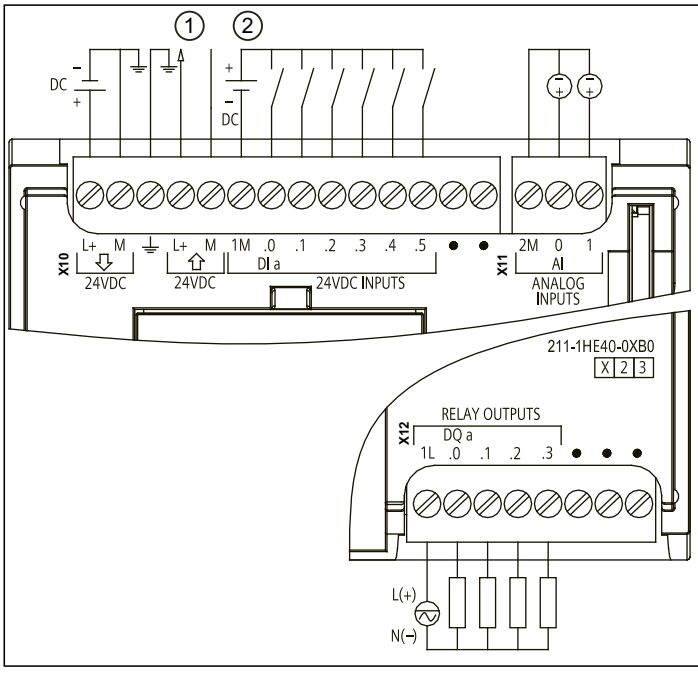
1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.	
Note 2: Either the L1 or N (L2) terminal can be connected to a voltage source up to 240 V AC. The N terminal can be considered L2 and is not required to be grounded. No polarization is required for L1 and N (L2) terminals.	
Note 3: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-27 Connector pin locations for CPU 1211C AC/DC/Relay (6ES7211-1BE40-0XB0)

Pin	X10	X11 (gold)	X12
1	L1 / 120-240 V AC	2 M	1L
2	N / 120-240 V AC	AI 0	DQ a.0
3	Functional Earth	AI 1	DQ a.1
4	L+ / 24 V DC Sensor Out	--	DQ a.2
5	M / 24 V DC Sensor Out	--	DQ a.3
6	1M	--	No connection
7	DI a.0	--	No connection
8	DI a.1	--	No connection

Pin	X10	X11 (gold)	X12
9	DI a.2	--	--
10	DI a.3	--	--
11	DI a.4	--	--
12	DI a.5	--	--
13	No connection	--	--
14	No connection	--	--

Table A-28 CPU 1211C DC/DC/Relay (6ES7211-1HE40-0XB0)



1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.

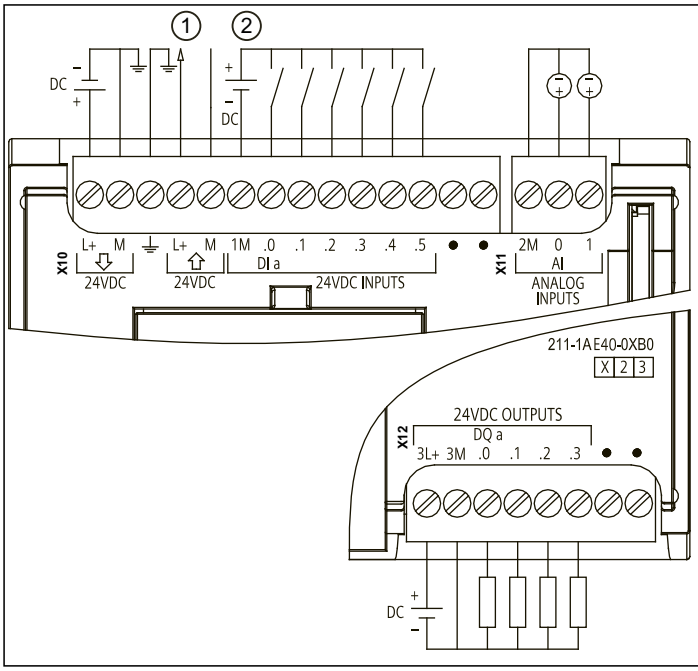
Note 2: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.

Table A-29 Connector pin locations for CPU 1211C DC/DC/Relay (6ES7211-1HE40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24 V DC	2 M	1L
2	M / 24 V DC	AI 0	DQ a.0
3	Functional Earth	AI 1	DQ a.1
4	L+ / 24 V DC Sensor Out	--	DQ a.2
5	M / 24 V DC Sensor Out	--	DQ a.3
6	1M	--	No connection
7	DI a.0	--	No connection
8	DI a.1	--	No connection
9	DI a.2	--	--
10	DI a.3	--	--
11	DI a.4	--	--

Pin	X10	X11 (gold)	X12
12	DI a.5	--	--
13	No connection	--	--
14	No connection	--	--

Table A-30 CPU 1211C DC/DC/DC (6ES7211-1AE40-0XB0)



1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.	
Note 2: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-31 Connector pin locations for CPU 1211C DC/DC/DC (6ES7211-1AE40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24 V DC	2 M	3L+
2	M / 24 V DC	AI 0	3M
3	Functional Earth	AI 1	DQ a.0
4	L+ / 24 V DC Sensor Out	--	DQ a.1
5	M / 24 V DC Sensor Out	--	DQ a.2
6	1M	--	DQ a.3
7	DI a.0	--	No connection
8	DI a.1	--	No connection
9	DI a.2	--	--
10	DI a.3	--	--
11	DI a.4	--	--
12	DI a.5	--	--
13	No connection	--	--
14	No connection	--	--

NOTE

Unused analog inputs should be shorted.

A.6 CPU 1212C

A.6.1 General specifications and features

Table A-32 General

Technical data	CPU 1212C AC/DC/Relay	CPU 1212C DC/DC/Relay	CPU 1212C DC/DC/DC
Article number	6ES7212-1BE40-0XB0	6ES7212-1HE40-0XB0	6ES7212-1AE40-0XB0
Dimensions W x H x D (mm)	90 x 100 x 75		
Shipping weight	425 grams	385 grams	370 grams
Power dissipation	11 W	9 W	
Electrical current available (SM and CM bus)	1000 mA max. (5 V DC)		
Electrical current available (24 V DC)	300 mA max. (sensor power)		
Digital input current consumption (24 V DC)	4 mA/input used		

Table A-33 CPU features

Technical data		Description
User memory (Refer to "General technical specifications (Page 1090)", "Internal CPU memory retention".)	Work	100 Kbytes
	Load	2 Mbytes internal, expandable up to SD card size
	Retentive	14 Kbytes
Onboard digital I/O		8 inputs/6 outputs
Onboard analog I/O		2 inputs
Process image size		1024 bytes of inputs (I)/1024 bytes of outputs (Q)
Bit memory (M)		4096 bytes
Temporary (local) memory		• 16 Kbytes for startup and program cycle (including associated FBs and FCs) • 6 Kbytes for each of the other interrupt priority levels (including FBs and FCs)
Signal modules expansion		2 SMs max.
SB, CB, BB expansion		1 max.
Communication module expansion		3 CMs max.
High-speed counters		Up to 6 configured to use any built-in or SB inputs. Refer to "Hardware input pin assignment" (Page 502) for CPU 1212C: HSC default address assignments. • 100/[1]80 kHz (Ia.0 to Ia.5) • 30 /[1]20 kHz (Ia.6 to Ia.7)

[1] The slower speed is applicable when the HSC is configured for quadrature mode of operation.

[2] For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

Technical data	Description
Pulse outputs[2]	Up to 4 configured to use any built-in or SB outputs • 100 kHz (Qa.0 to Qa.3) • 20 kHz (Qa.4 to Qa.5)
Pulse catch inputs	8
Time delay interrupts	4 total with 1 ms resolution
Cyclic interrupts	4 total with 1 ms resolution
Edge interrupts	8 rising and 8 falling (12 and 12 with optional signal board)
Memory card	SIMATIC memory card (optional)
Real time clock accuracy	+/- 60 seconds/month
Real time clock retention time	20 days typ./12 days min. at 40 °C (maintenance-free Super Capacitor)

1 The slower speed is applicable when the HSC is configured for quadrature mode of operation.

2 For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

Table A-34 Performance

Type of instruction		Execution speed	
		Direct addressing (I, Q and M)	DB accesses
Boolean		0.08 µs/instruction	
Move	Move_Bool	0.3 µs/instruction	1.17 µs/instruction
	Move_Word	0.137 µs/instruction	1.0 µs/instruction
	Move_Real	0.72 µs/instruction	1.0 µs/instruction
Real Math	Add Real	1.48 µs/instruction	1.78 µs/instruction

NOTE

Many variables affect measured times. The above performance times are for the fastest instructions in this category and error-free programs.

A.6.2 Timers, counters, and code blocks supported by CPU 1212C

Table A-35 Blocks, timers and counters supported by CPU 1212C

Element		Description
Blocks	Type	OB, FB, FC, DB
	Size	Up to the size of work memory
	Address range for FBs, FCs, and DBs	FB and FC: 1 to 65535 (such as FB 1 to FB 65535) DB: 1 to 59999
	Nesting depth	16 from the program cycle or startup OB 6 from any interrupt event OB[1]
	Monitoring	Status of 2 code blocks can be monitored simultaneously
OBs	Program cycle	Multiple
	Startup	Multiple

1 Safety programs use two nesting levels. The user program therefore has a nesting depth of four in safety programs.

Element		Description
OBs	Time-delay interrupt	4 (1 per event)
	Cyclic interrupts	4 (1 per event)
	Hardware interrupts	50 (1 per event)
	Time error interrupts	1
	Diagnostic error interrupts	1
	Pull or plug of modules	1
	Rack or station failure	1
	Time of day	Multiple
	Status	1
	Update	1
	Profile	1
	MC-Interpolator	1
	MC-Servo	1
	MC-PreServo	1
	MC-PostServo	1
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, 16 bytes per timer
Counters	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size dependent upon count type • SInt, USInt: 3 bytes • Int, UInt: 6 bytes • DInt, UDInt: 12 bytes

[1] Safety programs use two nesting levels. The user program therefore has a nesting depth of four in safety programs.

A.6.3 Communications CPU 1212C

Table A-36 Communication

Technical data	Description
Number of ports	1
Type	Ethernet
HMI device	4
Programming device (PG)	1
Connections	34 reserved, 68 max.
Data rates	10/100 Mb/s
Isolation (external signal to logic)	Transformer isolated, 1500 V AC (type test)[1]
Cable type	CAT5e shielded

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description
Interfaces	
Number of PROFINET interfaces	1
Number of interfaces PROFIBUS	0
Interface	
Interface Hardware	
Number of ports	1
Integrated switch	No
RJ-45 (Ethernet)	Yes; X1
Protocols	
PROFINET IO controller	Yes
PROFINET IO device	Yes
SIMATIC communication	Yes
Open IE communication	Yes
Web server	Yes
Media redundancy	No
PROFINET IO controller	
Services	
PG/OP communication	Yes
S7 routing	Yes
Isochronous mode	No
Open IE communication	Yes
IRT	No
MRP	No
PROFIenergy	Yes. The S7-1200 CPU only supports the PROFIenergy entity (with I-device functionality).
Prioritized startup	Yes (max. 16 PROFINET devices)
Number of connectable I/O devices max.	16
Number of IO devices that you can connect for RT, max.	16
Of which are in line, max.	16
Number of IO devices that can be activated/ deactivated simultaneously, max.	8
Update times	The minimum value of the update time also depends on the communication component set for PROFINET IO, on the number of IO devices, and the quantity of configured user data.
With RT	
Send clock of 1 ms	1 ms to 512 ms
PROFINET IO device	
Services	

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data		Description
PG/OP communication		Yes
S7 routing		Yes
Isochronous mode		No
Open IE communication		Yes
IRT, supported		No
MRP, supported		No
PROFIenergy		Yes
Shared device		Yes
Number of IO controllers with shared device, max.		2
SIMATIC communication		
S7 communication, as server		Yes
S7 communication, as client		Yes
User data per job, max.		See online help (S7 communication, user data size)
Open IE communication		
TCP/IP:		Yes
	Data length, max.	8 KB
	Several passive connections per port, supported	Yes
ISO-on-TCP (RFC1006):		Yes
	Data length, max.	8 KB
UDP		Yes
	Data length, max.	2048 bytes
DHCP		No
SNMP		Yes
DCP		Yes
LLDP		Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

A.6.4 Power supply and sensor power

Table A-37 Power supply

Technical data		CPU 1212C AC/DC/Relay	CPU 1212C DC/DC/Relay	CPU 1212C DC/DC/DC
Voltage range		85 to 264 V AC	20.4 V DC to 28.8 V DC	
Line frequency		47 to 63 Hz	--	
Input current (max. load)	CPU only	80 mA at 120 V AC 40 mA at 240 V AC	400 mA at 24 V DC	
	CPU with all expansion accessories	240 mA at 120 V AC 120 mA at 240 V AC	1200 mA at 24 V DC	
Inrush current (max.)		20 A at 264 V AC	12 A at 28.8 V DC	

Technical data	CPU 1212C AC/DC/Relay	CPU 1212C DC/DC/Relay	CPU 1212C DC/DC/DC
$I^2 t$	0.8 A^2 s	0.5 A^2 s	
Isolation (input power to logic)	1500 V AC	Not isolated	
Ground leakage, AC line to functional earth	0.5 mA max.	--	
Hold up time (loss of power)	20 ms at 120 V AC 80 ms at 240 V AC	10 ms at 24 V DC	
Internal fuse, not user replaceable	3 A, 250 V, slow blow		

Table A-38 Sensor power

Technical data	CPU 1212C AC/DC/Relay	CPU 1212C DC/DC/Relay	CPU 1212C DC/DC/DC
Voltage range	20.4 to 28.8 V DC	L+ minus 4 V DC min.	
Output current rating (max.)	300 mA (short-circuit protected)		
Maximum ripple noise (<10 MHz)	< 1 V peak to peak	Same as input line	
Isolation (CPU logic to sensor power)	Not isolated		

A.6.5 Digital inputs and outputs

Table A-39 Digital inputs

Technical data	CPU 1212C AC/DC/Relay, DC/DC/Relay, and DC/DC/DC	
	High speed inputs	Standard inputs
Number of inputs	8	
Type	Sink/Source (IEC Type 1 sink)	
Rated voltage	24 V DC at 6 mA, nominal	24 V DC at 4 mA, nominal
Continuous permissible voltage	30 V DC, max. at 8 mA, max.	30 V DC, max. at 6 mA, max.
Surge voltage	35 V DC for 0.5 sec.	
Logic 1 signal (min.)	15 V DC at 2.5 mA	
Logic 0 signal (max.)	5 V DC at 1 mA	
Isolation (field side to logic)	707 V DC (type test)	
Isolation groups	1	
Filter times	us settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
HSC clock input rates (max.) (Logic 1 Level = 15 to 26 V DC)	100/80 kHz (Ia.0 to Ia.5) 30 /20 kHz (Ia.6 to Ia.7)	
Number of inputs on simultaneously	4 (no adjacent points) at 60 °C horizontal or 50 °C vertical 8 at 55 °C horizontal or 45 °C vertical	
Cable length (meters)	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs	

Table A-40 Digital outputs

Technical data	CPU 1212C AC/DC/Relay and DC/DC/Relay	CPU 1212C DC/DC/DC
Number of outputs	6	
Type	Relay, mechanical	Solid state - MOSFET (sourcing)
Voltage range	5 to 30 V DC or 5 to 250 V AC	20.4 to 28.8 V DC
Logic 1 signal at max. current	--	20 V DC min.
Logic 0 signal with 10 KΩ load	--	0.1 V DC max.
Current (max.)	2.0 A	0.5 A
Lamp load	30 W DC / 200 W AC	5 W
ON state resistance	0.2 Ω max. when new	0.6 Ω max.
Leakage current per point	--	10 µA max.
Surge current	7 A with contacts closed	8 A for 100 ms max.
Overload protection	No	
Isolation (field side to logic)	1500 V AC (coil to contact) None (coil to logic)	707 V DC (type test)
Isolation groups	2	1
Isolation (group-to-group)	1500 V AC[1]	--
Inductive clamp voltage	--	L+ minus 48 V DC, 1 W dissipation
Switching delay (Qa.0 to Qa.3)	10 ms max.	1.0 µs max., off to on 3.0 µs max., on to off
Switching delay (Qa.4 to Qa.5)	10 ms max.	5 µs max., off to on 20 µs max., on to off
Maximum relay switching frequency	1 Hz	--
Pulse Train Output rate	Not recommended[2]	100 kHz (Qa.0 to Qa.3)[3], 2 Hz min. 20 kHz (Qa.4 to Qa.5)[3]
Lifetime mechanical (no load)	10,000,000 open/close cycles	--
Lifetime contacts at rated load	100,000 open/close cycles	--
Behavior on RUN to STOP	Last value or substitute value (default value 0)	Last value or substitute value (default value 0)
Control of a digital input	Yes	
Parallel outputs for redundant load control	Yes (with same common)	
Parallel outputs for increased load	No	
Number of outputs on simultaneously	3 (no adjacent points) at 60 °C horizontal or 50 °C vertical 6 at 55 °C horizontal, or 45 °C vertical	
Cable length (meters)	500 m shielded, 150 m unshielded	

1 Relay group-to-group isolation separates line voltage from SELV/PELV and separates different phases up to 250 V AC line to ground.

2 For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

3 Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

A.6.6 Analog inputs

Table A-41 Analog inputs

Technical data	Description
Number of inputs	2
Type	Voltage (single-ended)
Full-scale range	0 to 10 V
Full-scale range (data word)	0 to 27648
Overshoot range	10.001 to 11.759 V
Overshoot range (data word)	27649 to 32511
Overflow range	11.760 to 11.852 V
Overflow range (data word)	32512 to 32767
Resolution	10 bits
Maximum withstand voltage	35 V DC
Smoothing	None, Weak, Medium, or Strong See the table for Step response (ms) for the analog inputs of the CPU (Page 1123).
Noise rejection	10, 50, or 60 Hz
Impedance	≥100 KΩ
Isolation (field side to logic)	None
Accuracy (25 °C / -20 to 60 °C)	3.0% / 3.5% of full-scale
Cable length (meters)	100 m, shielded twisted pair

A.6.6.1 Step response of the built-in analog inputs of the CPU

Table A-42 Step Response (ms), 0 V to 10 V measured at 95%

Smoothing selection (sample averaging)	Rejection frequency (Integration time)		
	60 Hz	**50 Hz**	**10 Hz**
None (1 cycle): No averaging	50 ms	50 ms	100 ms
Weak (4 cycles): 4 samples	60ms	70 ms	200 ms
Medium (16 cycles): 16 samples	200 ms	240 ms	1150 ms
Strong (32 cycles): 32 samples	400 ms	480 ms	2300 ms
Sample time	**4.17 ms**	**5 ms**	**25 ms**

A.6.6.2 Sample time for the built-in analog ports of the CPU

Table A-43 Sample time for built-in analog inputs of the CPU

Rejection frequency (Integration time selection)	Sample time
60 Hz (16.6 ms)	4.17 ms
50 Hz (20 ms)	5 ms
10 Hz (100 ms)	25 ms

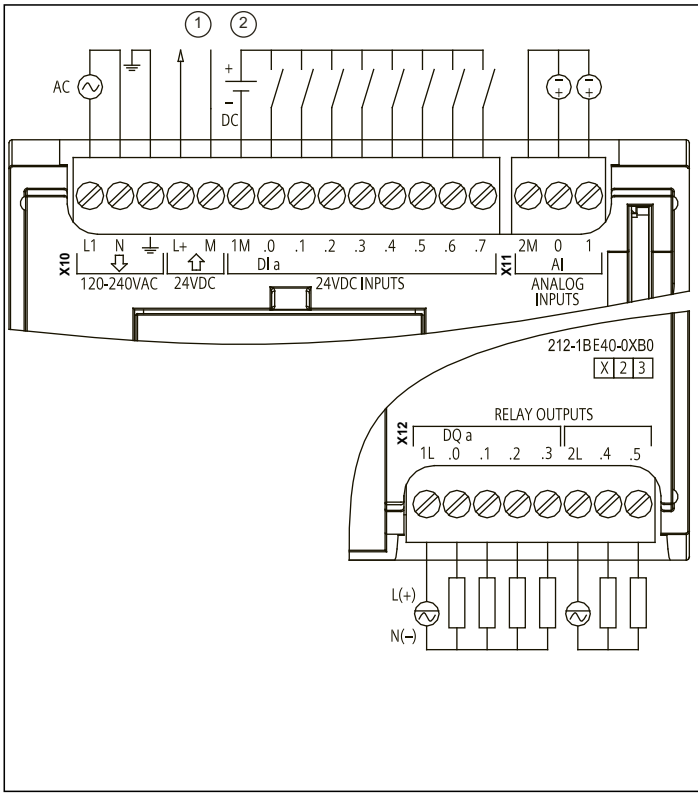
A.6.6.3 Measurement ranges of the analog inputs for voltage (CPUs)

Table A-44 Analog input representation for voltage (CPUs)

System		Voltage Measuring Range	
Decimal	**Hexadecimal**	**0 to 10 V**	
32767	7FFF	11.852 V	Overflow
32512	7F00		
32511	7EFF	11.759 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range
20736	5100	7.5 V	
34	22	12 mV	
0	0	0 V	
Negative values		Negative values are not supported	

A.6.7 CPU 1212C wiring diagrams

Table A-45 CPU 1212C AC/DC/Relay (6ES7212-1BE40-0XB0)

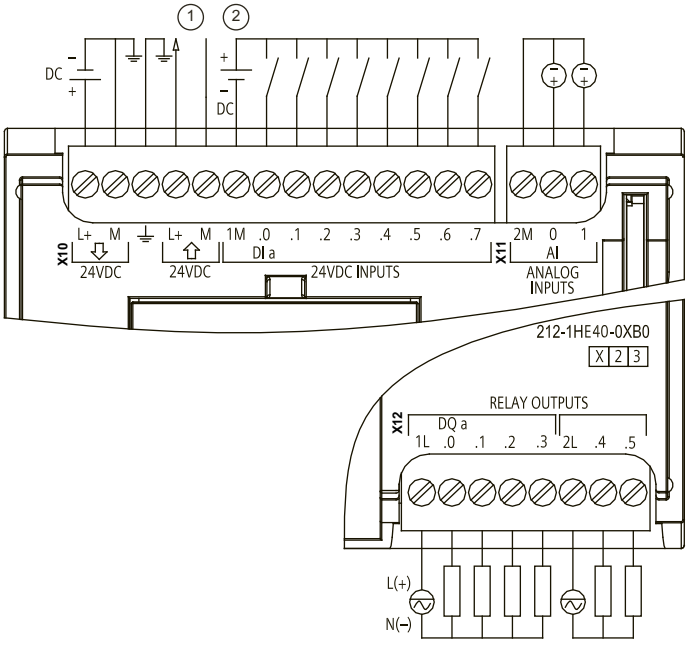


1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.	
Note 2: Either the L1 or N (L2) terminal can be connected to a voltage source up to 240 V AC. The N terminal can be considered L2 and is not required to be grounded. No polarization is required for L1 and N (L2) terminals.	
Note 3: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-46 Connector pin locations for CPU 1212C AC/DC/Relay (6ES7212-1BE40-0XB0)

Pin	X10	X11 (gold)	X12
1	L1 / 120-240 V AC	2 M	1L
2	N / 120-240 V AC	AI 0	DQ a.0
3	Functional Earth	AI 1	DQ a.1
4	L+ / 24 V DC Sensor Out	--	DQ a.2
5	M / 24 V DC Sensor Out	--	DQ a.3
6	1M	--	2L
7	DI a.0	--	DQ a.4
8	DI a.1	--	DQ a.5
9	DI a.2	--	--
10	DI a.3	--	--
11	DI a.4	--	--
12	DI a.5	--	--
13	DI a.6	--	--
14	DI a.7	--	--

Table A-47 CPU 1212C DC/DC/Relay (6ES7212-1HE40-0XB0)

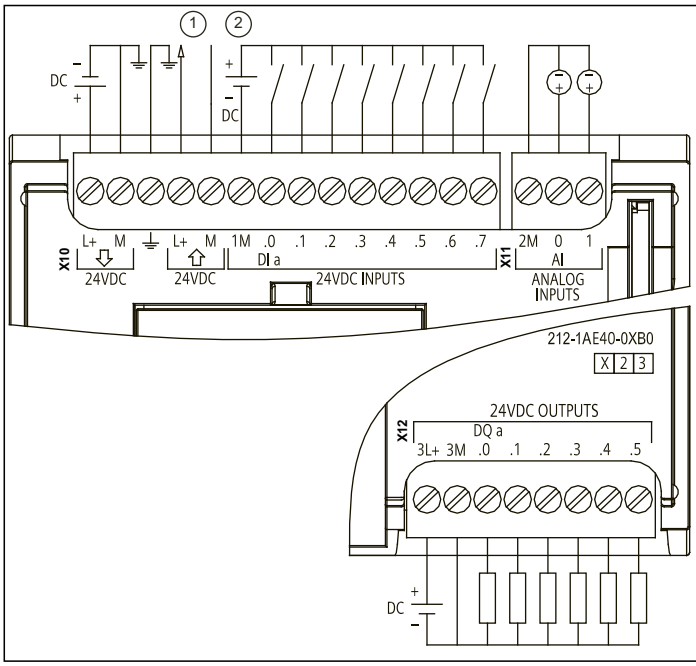


1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.	
Note 2: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-48 Connector pin locations for CPU 1212C DC/DC/Relay (6ES7212-1HE40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24 V DC	2 M	1L
2	M / 24 V DC	AI 0	DQ a.0
3	Functional Earth	AI 1	DQ a.1
4	L+ / 24 V DC Sensor Out	--	DQ a.2
5	M / 24 V DC Sensor Out	--	DQ a.3
6	1M	--	2L
7	DI a.0	--	DQ a.4
8	DI a.1	--	DQ a.5
9	DI a.2	--	--
10	DI a.3	--	--
11	DI a.4	--	--
12	DI a.5	--	--
13	DI a.6	--	--
14	DI a.7	--	--

Table A-49 CPU 1212C DC/DC/DC (6ES7212-1AE40-0XB0)



1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.	
Note 2: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-50 Connector pin locations for CPU 1212C DC/DC/DC (6ES7212-1AE40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24 V DC	2 M	3L+
2	M / 24 V DC	AI 0	3M
3	Functional Earth	AI 1	DQ a.0
4	L+ / 24 V DC Sensor Out	--	DQ a.1
5	M / 24 V DC Sensor Out	--	DQ a.2
6	1M	--	DQ a.3
7	DI a.0	--	DQ a.4
8	DI a.1	--	DQ a.5
9	DI a.2	--	--
10	DI a.3	--	--
11	DI a.4	--	--
12	DI a.5	--	--
13	DI a.6	--	--
14	DI a.7	--	--

NOTE

Unused analog inputs should be shorted.

A.7 CPU 1214C

A.7.1 General specifications and features

Table A-51 General

Technical data	CPU 1214C AC/DC/Relay	CPU 1214C DC/DC/Relay	CPU 1214C DC/DC/DC
Article number	6ES7214-1BG40-0XB0	6ES7214-1HG40-0XB0	6ES7214-1AG40-0XB0
Dimensions W x H x D (mm)	110 x 100 x 75		
Shipping weight	475 grams	435 grams	415 grams
Power dissipation	14 W	12 W	
Electrical current available (SM and CM bus)	1600 mA max. (5 V DC)		
Electrical current available (24 V DC)	400 mA max. (sensor power)		
Digital input current consumption (24 V DC)	4 mA/input used		

Table A-52 CPU features

Technical data		Description
User memory (Refer to "General technical specifications", (Page 1090) "Internal CPU memory retention".)	Work	150 Kbytes
	Load	4 Mbytes internal, expandable up to SD card size
	Retentive	14 Kbytes
Onboard digital I/O		14 inputs/10 outputs
Onboard analog I/O		2 inputs
Process image size		1024 bytes of inputs (I)/1024 bytes of outputs (Q)
Bit memory (M)		8192 bytes
Temporary (local) memory		• 16 Kbytes for startup and program cycle (including associated FBs and FCs) • 6 Kbytes for each of the other interrupt priority levels (including FBs and FCs)
Signal modules expansion		8 SMs max.
SB, CB, BB expansion		1 max.
Communication module expansion		3 CMs max.
High-speed counters		Up to 6 configured to use any built-in or SB inputs. Refer to "Hardware input pin assignment" (Page 502) for CPU 1214C: HSC default address assignments. • 100/[1]80 kHz (Ia.0 to Ia.5) • 30/[1]20 kHz (Ia.6 to Ib.5)
Pulse outputs[2]		Up to 4 configured to use any built-in or SB outputs • 100 kHz (Qa.0 to Qa.3) • 20 kHz (Qa.4 to Qb.1)
Pulse catch inputs		14
Time delay interrupts		4 total with 1 ms resolution
Cyclic interrupts		4 total with 1 ms resolution
Edge interrupts		12 rising and 12 falling (16 and 16 with optional signal board)
Memory card		SIMATIC memory card (optional)
Real time clock accuracy		+/- 60 seconds/month
Real time clock retention time		20 days typ./12 days min. at 40 °C (maintenance-free Super Capacitor)

1 The slower speed is applicable when the HSC is configured for quadrature mode of operation.

2 For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

Table A-53 Performance

Type of instruction		Execution speed	
		Direct addressing (I, Q and M)	DB accesses
Boolean		0.08 µs/instruction	
Move	Move_Bool	0.3 µs/instruction	1.17 µs/instruction
	Move_Word	0.137 µs/instruction	1.0 µs/instruction
	Move_Real	0.72 µs/instruction	1.0 µs/instruction
Real Math	Add Real	1.48 µs/instruction	1.78 µs/instruction

NOTE

Many variables affect measured times. The above performance times are for the fastest instructions in this category and error-free programs.

A.7.2 Timers, counters and code blocks supported by CPU 1214C

Table A-54 Blocks, timers and counters supported by CPU 1214C

Element		Description
Blocks	Type	OB, FB, FC, DB
	Size	OB, FB, FC: 64 Kbytes DB: up to the size of work memory
	Address range for FBs, FCs, and DBs	FB and FC: 1 to 65535 (such as FB 1 to FB 65535) DB: 1 to 59999
	Nesting depth	16 from the program cycle or startup OB 6 from any interrupt event OB[1]
	Monitoring	Status of 2 code blocks can be monitored simultaneously
OBs	Program cycle	Multiple
	Startup	Multiple
	Time-delay interrupts	4 (1 per event)
	Cyclic interrupts	4 (1 per event)
	Hardware interrupts	50 (1 per event)
	Time error interrupts	1
	Diagnostic error interrupts	1
	Pull or plug of modules	1
	Rack or station failure	1
	Time of day	Multiple
	Status	1
	Update	1
	Profile	1
	MC-Interpolator	1
	MC-Servo	1
	MC-PreServo	1
	MC-PostServo	1
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, 16 bytes per timer

[1] Safety programs use two nesting levels. The user program therefore has a nesting depth of four in safety programs.

Element		Description
Counters	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size dependent upon count type • SInt, USInt: 3 bytes • Int, UInt: 6 bytes • DInt, UDInt: 12 bytes

[1] Safety programs use two nesting levels. The user program therefore has a nesting depth of four in safety programs.

A.7.3 Communications CPU 1214C

Table A-55 Communication

Technical data	Description
Number of ports	1
Type	Ethernet
HMI device	4
Programming device (PG)	1
Connections	34 reserved, 68 max.
Data rates	10/100 Mb/s
Isolation (external signal to logic)	Transformer isolated, 1500 V AC (type test)[1]
Cable type	CAT5e shielded
Interfaces	
Number of PROFINET interfaces	1
Number of interfaces PROFIBUS	0
Interface	
Interface Hardware	
Number of ports	1
Integrated switch	No
RJ-45 (Ethernet)	Yes; X1
Protocols	
PROFINET IO controller	Yes
PROFINET IO device	Yes
SIMATIC communication	Yes
Open IE communication	Yes
Web server	Yes
Media redundancy	No
PROFINET IO controller	
Services	
PG/OP communication	Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data		Description
S7 routing		Yes
Isochronous mode		No
Open IE communication		Yes
IRT		No
MRP		No
PROFIenergy		Yes. The S7-1200 CPU only supports the PROFIenergy entity (with I-device functionality).
Prioritized startup		Yes (max. 16 PROFINET devices)
Number of connectable I/O devices max.		16
Number of IO devices that you can connect for RT, max.		16
Of which are in line, max.		16
Number of IO devices that can be activated/ deactivated simultaneously, max.		8
Update times		The minimum value of the update time also depends on the communication component set for PROFINET IO, on the number of IO devices, and the quantity of configured user data.
With RT		
Send clock of 1 ms		1 ms to 512 ms
PROFINET IO device		
Services		
PG/OP communication		Yes
S7 routing		Yes
Isochronous mode		No
Open IE communication		Yes
IRT, supported		No
MRP, supported		No
PROFIenergy		Yes
Shared device		Yes
Number of IO controllers with shared device, max.		2
SIMATIC communication		
S7 communication, as server		Yes
S7 communication, as client		Yes
User data per job, max.		See online help (S7 communication, user data size)
Open IE communication		
TCP/IP:		Yes
	Data length, max.	8 KB
	Several passive connections per port, supported	Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data		Description
ISO-on-TCP (RFC1006):		Yes
	Data length, max.	8 KB
UDP		Yes
	Data length, max.	2048 bytes
DHCP		No
SNMP		Yes
DCP		Yes
LLDP		Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

A.7.4 Power supply and power sensor

Table A-56 Power supply

Technical data		CPU 1214C AC/DC/Relay	CPU 1214C DC/DC/Relay	CPU 1214C DC/DC/DC
Voltage range		85 to 264 V AC	20.4 V DC to 28.8 V DC	
Line frequency		47 to 63 Hz	--	
Input current (max. load)	CPU only	100 mA at 120 V AC 50 mA at 240 V AC	500 mA at 24 V DC	
	CPU with all expansion accessories	300 mA at 120 V AC 150 mA at 240 V AC	1500 mA at 24 V DC	
Inrush current (max.)		20 A at 264 V AC	12 A at 28.8 V DC	
$I^2 t$		0.8 A^2 s	0.5 A^2 s	
Isolation (input power to logic)		1500 V AC	Not isolated	
Ground leakage, AC line to functional earth		0.5 mA max.	-	
Hold up time (loss of power)		20 ms at 120 V AC 80 ms at 240 V AC	10 ms at 24 V DC	
Internal fuse, not user replaceable		3 A, 250 V, slow blow		

Table A-57 Sensor power

Technical data	CPU 1214C AC/DC/Relay	CPU 1214C DC/DC/Relay	CPU 1214C DC/DC/DC
Voltage range	20.4 to 28.8 V DC	L+ minus 4 V DC min.	
Output current rating (max.)	400 mA (short-circuit protected)		
Maximum ripple noise (<10 MHz)	< 1 V peak to peak	Same as input line	
Isolation (CPU logic to sensor power)	Not isolated		

A.7.5 Digital inputs and outputs

Table A-58 Digital inputs

Technical data	CPU 1214C AC/DC/Relay, DC/DC/Relay, and DC/DC/DC	
	High speed inputs	**Standard inputs**
Number of inputs	14	
Type	Sink/Source (IEC Type 1 sink)	
Rated voltage	24 V DC at 6 mA, nominal	24 V DC at 4 mA, nominal
Continuous permissible voltage	30 V DC, max. at 8 mA, max.	30 V DC, max. at 6 mA, max.
Surge voltage	35 V DC for 0.5 sec.	
Logic 1 signal (min.)	15 V DC at 2.5 mA	
Logic 0 signal (max.)	5 V DC at 1 mA	
Isolation (field side to logic)	707 V DC (type test)	
Isolation groups	1	
Filter times	us settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
HSC clock input rates (max.) (Logic 1 Level = 15 to 26 V DC)	100/80 kHz (Ia.0 to Ia.5) 30/20 kHz (Ia.6 to Ib.5	
Number of inputs on simultaneously	• 7 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 14 at 55 °C horizontal or 45 °C vertical	
Cable length (meters)	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs	

Table A-59 Digital outputs

Technical data	CPU 1214C AC/DC/Relay and DC/DC/Relay	CPU 1214C DC/DC/DC
Number of outputs	10	
Type	Relay, mechanical	Solid state - MOSFET (sourcing)
Voltage range	5 to 30 V DC or 5 to 250 V AC	20.4 to 28.8 V DC
Logic 1 signal at max. current	--	20 V DC min.
Logic 0 signal with 10 KΩ load	--	0.1 V DC max.
Current (max.)	2.0 A	0.5 A
Lamp load	30 W DC / 200 W AC	5 W
ON state resistance	0.2 Ω max. when new	0.6 Ω max.
Leakage current per point	--	10 µA max.
Surge current	7 A with contacts closed	8 A for 100 ms max.
Overload protection	No	
Isolation (field side to logic)	1500 V AC (coil to contact) None (coil to logic)	707 V DC (type test)
Isolation groups	2	1

1 Relay group-to-group isolation separates line voltage from SELV/PELV and separates different phases up to 250 V AC line to ground.

2 For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

3 Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

Technical data	CPU 1214C AC/DC/Relay and DC/DC/Relay	CPU 1214C DC/DC/DC
Isolation (group-to-group)	1500 V AC[1]	--
Inductive clamp voltage	--	L+ minus 48 V DC, 1 W dissipation
Switching delay (Qa.0 to Qa.3)	10 ms max.	1.0 µs max., off to on 3.0 µs max., on to off
Switching delay (Qa.4 to Qb.1)	10 ms max.	5 µs max., off to on 20 µs max., on to off
Maximum relay switching frequency	1 Hz	--
Pulse Train Output rate	Not recommended [2]	100 kHz (Qa.0 to Qa.3)[3], 2 Hz min. 20 kHz (Qa.4 to Qb.1)[3]
Lifetime mechanical (no load)	10,000,000 open/close cycles	--
Lifetime contacts at rated load	100,000 open/close cycles	--
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Control of a digital input	Yes	
Parallel outputs for redundant load control	Yes (with same common)	
Parallel outputs for increased load	No	
Number of outputs on simultaneously	• 5 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 10 at 55 °C horizontal or 45 °C vertical	
Cable length (meters)	500 m shielded, 150 m unshielded	

1 Relay group-to-group isolation separates line voltage from SELV/PELV and separates different phases up to 250 V AC line to ground.

2 For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

3 Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

A.7.6 Analog inputs

Table A-60 Analog inputs

Technical data	Description
Number of inputs	2
Type	Voltage (single-ended)
Full-scale range	0 to 10 V
Full-scale range (data word)	0 to 27648
Overshoot range	10.001 to 11.759 V
Overshoot range (data word)	27649 to 32511
Overflow range	11.760 to 11.852 V
Overflow range (data word)	32512 to 32767
Resolution	10 bits
Maximum withstand voltage	35 V DC

Technical data	Description
Smoothing	None, Weak, Medium, or Strong See the table for Step response (ms) for the analog inputs of the CPU (Page 1135).
Noise rejection	10, 50, or 60 Hz
Impedance	≥100 KΩ
Isolation (field side to logic)	None
Accuracy (25 °C / -20 to 60 °C)	3.0% / 3.5% of full-scale
Cable length (meters)	100 m, shielded twisted pair

A.7.6.1 Step response of the built-in analog inputs of the CPU

Table A-61 Step Response (ms), 0 V to 10 V measured at 95%

Smoothing selection (sample averaging)	Rejection frequency (Integration time)		
	60 Hz	**50 Hz**	**10 Hz**
None (1 cycle): No averaging	50 ms	50 ms	100 ms
Weak (4 cycles): 4 samples	60ms	70 ms	200 ms
Medium (16 cycles): 16 samples	200 ms	240 ms	1150 ms
Strong (32 cycles): 32 samples	400 ms	480 ms	2300 ms
Sample time	**4.17 ms**	**5 ms**	**25 ms**

A.7.6.2 Sample time for the built-in analog ports of the CPU

Table A-62 Sample time for built-in analog inputs of the CPU

Rejection frequency (Integration time selection)	Sample time
60 Hz (16.6 ms)	4.17 ms
50 Hz (20 ms)	5 ms
10 Hz (100 ms)	25 ms

A.7.6.3 Measurement ranges of the analog inputs for voltage (CPUs)

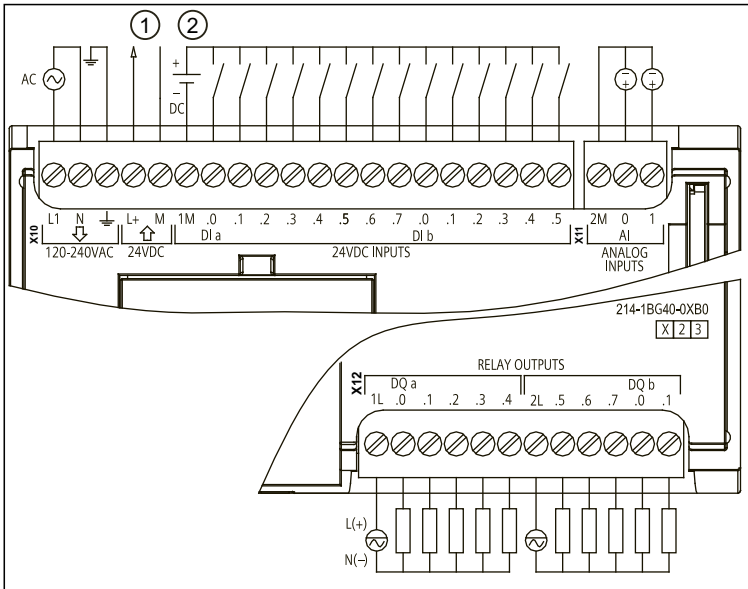
Table A-63 Analog input representation for voltage (CPUs)

System		Voltage Measuring Range	
Decimal	**Hexadecimal**	**0 to 10 V**	
32767	7FFF	11.852 V	Overflow
32512	7F00		
32511	7EFF	11.759 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range
20736	5100	7.5 V	

System		Voltage Measuring Range	
Decimal	**Hexadecimal**	**0 to 10 V**	
34	22	12 mV	Rated range
0	0	0 V	
Negative values		Negative values are not supported	

A.7.7 CPU 1214C wiring diagrams

Table A-64 CPU 1214C AC/DC/Relay (6ES7214-1BG40-0XB0)



1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.

Note 2: Either the L1 or N (L2) terminal can be connected to a voltage source up to 240 V AC. The N terminal can be considered L2 and is not required to be grounded. No polarization is required for L1 and N (L2) terminals.

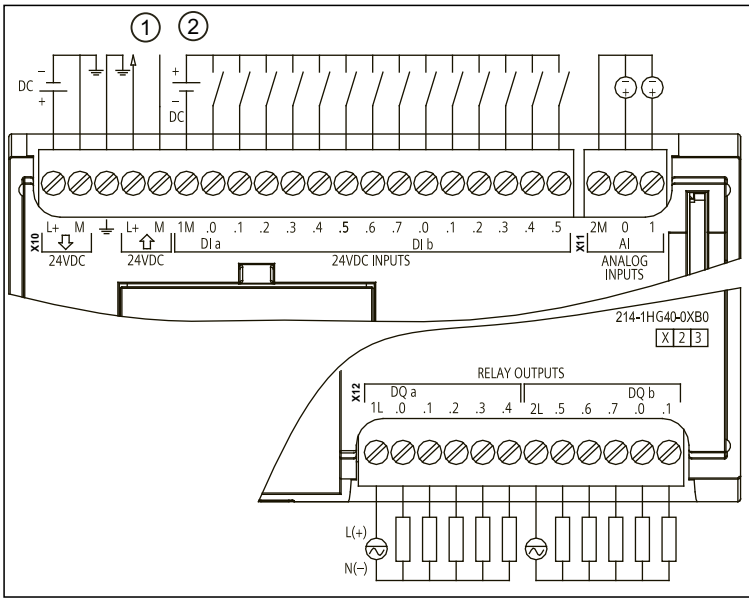
Note 3: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.

Table A-65 Connector pin locations for CPU 1214C AC/DC/Relay (6ES7214-1BG40-0XB0)

Pin	X10	X11 (gold)	X12
1	L1 / 120-240 V AC	2 M	1L
2	N / 120-240 V AC	AI 0	DQ a.0
3	Functional Earth	AI 1	DQ a.1
4	L+ / 24 V DC Sensor Out	--	DQ a.2
5	M / 24 V DC Sensor Out	--	DQ a.3
6	1M	--	DQ a.4
7	DI a.0	--	2L
8	DI a.1	--	DQ a.5
9	DI a.2	--	DQ a.6

Pin	X10	X11 (gold)	X12
10	DI a.3	--	DQ a.7
11	DI a.4	--	DQ b.0
12	DI a.5	--	DQ b.1
13	DI a.6	--	--
14	DI a.7	--	--
15	DI b.0	--	--
16	DI b.1	--	--
17	DI b.2	--	--
18	DI b.3	--	--
19	DI b.4	--	--
20	DI b.5	--	--

Table A-66 CPU 1214C DC/DC/Relay (6ES7214-1HG40-0XB0)



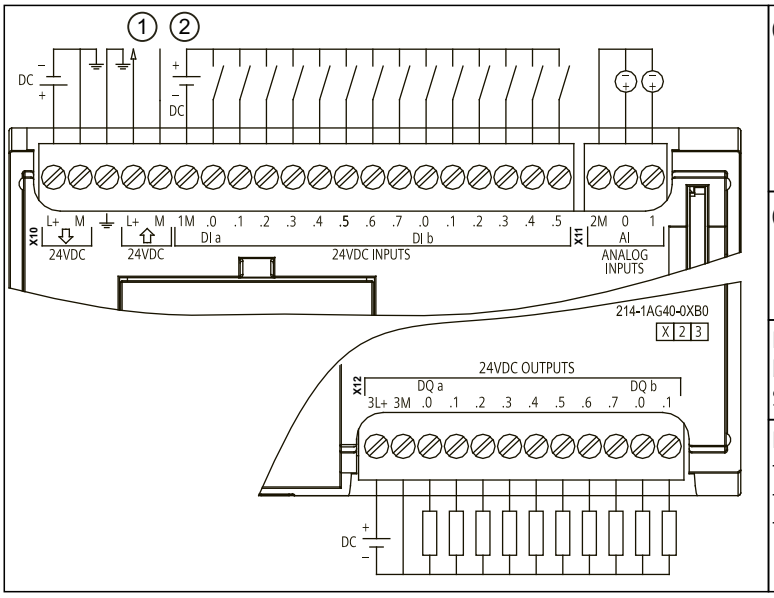
1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.	
Note 2: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-67 Connector pin locations for CPU 1214C DC/DC/Relay (6ES7214-1HG40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24 V DC	2 M	1L
2	M / 24 V DC	AI 0	DQ a.0
3	Functional Earth	AI 1	DQ a.1
4	L+ / 24 V DC Sensor Out	--	DQ a.2
5	M / 24 V DC Sensor Out	--	DQ a.3
6	1M	--	DQ a.4
7	DI a.0	--	2L
8	DI a.1	--	DQ a.5
9	DI a.2	--	DQ a.6

Pin	X10	X11 (gold)	X12
10	DI a.3	--	DQ a.7
11	DI a.4	--	DQ b.0
12	DI a.5	--	DQ b.1
13	DI a.6	--	--
14	DI a.7	--	--
15	DI b.0	--	--
16	DI b.1	--	--
17	DI b.2	--	--
18	DI b.3	--	--
19	DI b.4	--	--
20	DI b.5	--	--

Table A-68 CPU 1214C DC/DC/DC (6ES7214-1AG40-0XB0)



1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.	
Note 2: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-69 Connector pin locations for CPU 1214C DC/DC/DC (6ES7214-1AG40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24 V DC	2 M	3L+
2	M / 24 V DC	AI 0	3M
3	Functional Earth	AI 1	DQ a.0
4	L+ / 24 V DC Sensor Out	--	DQ a.1
5	M / 24 V DC Sensor Out	--	DQ a.2
6	1M	--	DQ a.3
7	DI a.0	--	DQ a.4
8	DI a.1	--	DQ a.5
9	DI a.2	--	DQ a.6
10	DI a.3	--	DQ a.7

Pin	X10	X11 (gold)	X12
11	DI a.4	--	DQ b.0
12	DI a.5	--	DQ b.1
13	DI a.6	--	--
14	DI a.7	--	-
15	DI b.0	--	--
16	DI b.1	--	--
17	DI b.2	--	--
18	DI b.3	--	--
19	DI b.4	--	--
20	DI b.5	--	--

NOTE

Unused analog inputs should be shorted.

A.8 CPU 1215C

A.8.1 General specifications and features

Table A-70 General

Technical data	CPU 1215C AC/DC/Relay	CPU 1215C DC/DC/Relay	CPU 1215C DC/DC/DC
Article number	6ES7215-1BG40-0XB0	6ES7215-1HG40-0XB0	6ES7215-1AG40-0XB0
Dimensions W x H x D (mm)	130 x 100 x 75		
Shipping weight	585 grams	550 grams	520 grams
Power dissipation	14 W	12 W	
Electrical current available (SM and CM bus)	1600 mA max. (5 V DC)		
Electrical current available (24 V DC)	400 mA max. (sensor power)		
Digital input current consumption (24 V DC)	4 mA/input used		

Table A-71 CPU features

Technical data		Description
User memory (Refer to "General technical specifications (Page 1090)", "Internal CPU memory retention".)	Work	200 Kbytes
	Load	4 Mbytes, internal, expandable up to SD card size
	Retentive	14 Kbytes
Onboard digital I/O		14 inputs/10 outputs
Onboard analog I/O		2 inputs/2 outputs
Process image size		1024 bytes of inputs (I)/1024 bytes of outputs (Q)
Bit memory (M)		8192 bytes
Temporary (local) memory		• 16 Kbytes for startup and program cycle (including associated FBs and FCs) • 6 Kbytes for each of the other interrupt priority levels (including FBs and FCs)
Signal modules expansion		8 SMs max.
SB, CB, BB expansion		1 max.
Communication module expansion		3 CMs max.
High-speed counters		Up to 6 configured to use any built-in or SB inputs. Refer to "Hardware input pin assignment" (Page 502) for CPU 1215C: HSC default address assignments. • 100/[1]80 kHz (Ia.0 to Ia.5) • 30/[1]20 kHz (Ia.6 to Ib.5)
Pulse outputs[2]		Up to 4 configured to use any built-in or SB outputs • 100 kHz (Qa.0 to Qa.3) • 20 kHz (Qa.4 to Qb.1)
Pulse catch inputs		14
Time delay interrupts		4 total with 1 ms resolution
Cyclic interrupts		4 total with 1 ms resolution
Edge interrupts		12 rising and 12 falling (16 and 16 with optional signal board)
Memory card		SIMATIC memory card (optional)
Real time clock accuracy		+/- 60 seconds/month
Real time clock retention time		20 days typ./12 days min. at 40 °C (maintenance-free Super Capacitor)

1 The slower speed is applicable when the HSC is configured for quadrature mode of operation.

2 For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

Table A-72 Performance

Type of instruction		Execution speed	
		Direct addressing (I, Q and M)	DB accesses
Boolean		0.08 µs/instruction	
Move	Move_Bool	0.3 µs/instruction	1.17 µs/instruction
	Move_Word	0.137 µs/instruction	1.0 µs/instruction
	Move_Real	0.72 µs/instruction	1.0 µs/instruction
Real Math	Add Real	1.48 µs/instruction	1.78 µs/instruction

NOTE

Many variables affect measured times. The above performance times are for the fastest instructions in this category and error-free programs.

A.8.2 Timers, counters and code blocks supported by CPU 1215C

Table A-73 Blocks, timers and counters supported by CPU 1215C

Element		Description
Blocks	Type	OB, FB, FC, DB
	Size	OB, FB, FC: 64 Kbytes DB: up to the size of work memory
	Address range for FBs, FCs, and DBs	FB and FC: 1 to 65535 (such as FB 1 to FB 65535) DB: 1 to 59999
	Nesting depth	16 from the program cycle or startup OB 6 from any interrupt event OB[1]
	Monitoring	Status of 2 code blocks can be monitored simultaneously
OBs	Program cycle	Multiple
	Startup	Multiple
	Time-delay interrupts	4 (1 per event)
	Cyclic interrupts	4 (1 per event)
	Hardware interrupts	50 (1 per event)
	Time error interrupts	1
	Diagnostic error interrupts	1
	Pull or plug of modules	1
	Rack or station failure	1
	Time of day	Multiple
	Status	1
	Update	1
	Profile	1
	MC-Interpolator	1
	MC-Servo	1
	MC-PreServo	1
	MC-PostServo	1
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, 16 bytes per timer

[1] Safety programs use two nesting levels. The user program therefore has a nesting depth of four in safety programs.

Element		Description
Counters	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size dependent upon count type • SInt, USInt: 3 bytes • Int, UInt: 6 bytes • DInt, UDInt: 12 bytes

[1] Safety programs use two nesting levels. The user program therefore has a nesting depth of four in safety programs.

A.8.3 Communications CPU 1215C

Table A-74 Communication

Technical data	Description
Number of ports	2
Type	Ethernet
HMI device	4
Programming device (PG)	1
Connections (Page 526)	34 reserved, 68 max.
Data rates	10/100 Mb/s
Isolation (external signal to logic)	Transformer isolated, 1500 V AC (type test)[1]
Cable type	CAT5e shielded
Interfaces	
Number of PROFINET interfaces	1
Number of interfaces PROFIBUS	0
Interface	
Interface hardware	
Number of ports	2
Integrated switch	Yes
RJ-45 (Ethernet)	Yes; X1
Protocols	
PROFINET IO controller	Yes
PROFINET IO device	Yes
SIMATIC communication	Yes
Open IE communication	Yes
Web server	Yes
Media redundancy	Yes
PROFINET IO controller	
Services	
PG/OP communication	Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data		Description
S7 routing		Yes
Isochronous mode		No
Open IE communication		Yes
IRT		No
MRP		Yes as MRP client
PROFIenergy		Yes. The S7-1200 CPU only supports the PROFIenergy entity (with I-device functionality).
Prioritized startup		Yes (max. 16 PROFINET devices)
Number of connectable I/O devices max.		16
Number of IO devices that you can connect for RT, max.		16
Of which are in line, max.		16
Number of IO devices that can be activated/ deactivated simultaneously, max.		8
Update times		The minimum value of the update time also depends on the communication component set for PROFINET IO, on the number of IO devices, and the quantity of configured user data.
With RT		
Send clock of 1 ms		1 ms to 512 ms
PROFINET IO device		
Services		
PG/OP communication		Yes
S7 routing		Yes
Isochronous mode		No
Open IE communication		Yes
IRT, supported		No
MRP, supported		Yes
PROFIenergy		Yes
Shared device		Yes
Number of IO controllers with shared device, max.		2
SIMATIC communication		
S7 communication, as server		Yes
S7 communication, as client		Yes
User data per job, max.		See online help (S7 communication, user data size)
Open IE communication		
TCP/IP:		Yes
	Data length, max.	8 KB
	Several passive connections per port, supported	Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data		Description
ISO-on-TCP (RFC1006):		Yes
	Data length, max.	8 KB
UDP:		Yes
	Data length, max.	2048 bytes
DHCP		No
SNMP		Yes
DCP		Yes
LLDP		Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

A.8.4 Power supply and sensor power (CPU 1215C)

Table A-75 Power supply

Technical data		CPU 1215C AC/DC/Relay	CPU 1215C DC/DC/Relay	CPU 1215C DC/DC/DC
Voltage range		85 to 264 V AC	20.4 V DC to 28.8 V DC	
Line frequency		47 to 63 Hz	--	
Input current (max. load)	CPU only	100 mA at 120 V AC 50 mA at 240 V AC	500 mA at 24 V DC	
	CPU with all expansion accessories	300 mA at 120 V AC 150 mA at 240 V AC	1500 mA at 24 V DC	
Inrush current (max.)		20 A at 264 V AC	12 A at 28.8 V DC	
$I^2 t$		0.8 A^2 s	0.5 A^2 s	
Isolation (input power to logic)		1500 V AC	Not isolated	
Ground leakage, AC line to functional earth		0.5 mA max.	-	
Hold up time (loss of power)		20 ms at 120 V AC 80 ms at 240 V AC	10 ms at 24 V DC	
Internal fuse, not user replaceable		3 A, 250 V, slow blow		

Table A-76 Sensor power

Technical data	CPU 1215C AC/DC/Relay	CPU 1215C DC/DC/Relay	CPU 1215C DC/DC/DC
Voltage range	20.4 to 28.8 V DC	L+ minus 4 V DC min.	
Output current rating (max.)	400 mA (short-circuit protected)		
Maximum ripple noise (<10 MHz)	< 1 V peak to peak	Same as input line	
Isolation (CPU logic to sensor power)	Not isolated		

A.8.5 Digital inputs and outputs

Table A-77 Digital inputs

Technical data	CPU 1215C AC/DC/Relay, DC/DC/Relay, and DC/DC/DC	
	High speed inputs	**Standard inputs**
Number of inputs	14	
Type	Sink/Source (IEC Type 1 sink)	
Rated voltage	24 V DC at 6 mA, nominal	24 V DC at 4 mA, nominal
Continuous permissible voltage	30 V DC, max. at 8 mA, max.	30 V DC, max. at 6 mA, max.
Surge voltage	35 V DC for 0.5 sec.	
Logic 1 signal (min.)	15 V DC at 2.5 mA	
Logic 0 signal (max.)	5 V DC at 1 mA	
Isolation (field side to logic)	707 V DC (type test)	
Isolation groups	1	
Filter times	us settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
HSC clock input rates (max.) (Logic 1 Level = 15 to 26 V DC)	100/80 kHz (Ia.0 to Ia.5) 30/20 kHz (Ia.6 to Ib.5)	
Number of inputs on simultaneously	• 7 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 14 at 55 °C horizontal or 45 °C vertical	
Cable length (meters)	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs	

Table A-78 Digital outputs

Technical data	CPU 1215C AC/DC/Relay and CPU 1215C DC/DC/Relay	CPU 1215C DC/DC/DC
Number of outputs	10	
Type	Relay, mechanical	Solid state - MOSFET (sourcing)
Voltage range	5 to 30 V DC or 5 to 250 V AC	20.4 to 28.8 V DC
Logic 1 signal at max. current	--	20 V DC min.
Logic 0 signal with 10 KΩ load	--	0.1 V DC max.
Current (max.)	2.0 A	0.5 A
Lamp load	30 W DC / 200 W AC	5 W
ON state resistance	0.2 Ω max. when new	0.6 Ω max.
Leakage current per point	--	10 µA max.
Surge current	7 A with contacts closed	8 A for 100 ms max.
Overload protection	No	
Isolation (field side to logic)	1500 V AC (coil to contact) None (coil to logic)	707 V DC (type test)
Isolation groups	2	1

1 Relay group-to-group isolation separates line voltage from SELV/PELV and separates different phases up to 250 V AC line to ground.

2 For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

3 Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

Technical data	CPU 1215C AC/DC/Relay and CPU 1215C DC/DC/Relay	CPU 1215C DC/DC/DC
Isolation (group-to-group)	1500 V AC[1]	--
Inductive clamp voltage	--	L+ minus 48 V DC, 1 W dissipation
Switching delay (Qa.0 to Qa.3)	10 ms max.	1.0 µs max., off to on 3.0 µs max., on to off
Switching delay (Qa.4 to Qb.1)	10 ms max.	5 µs max., off to on 20 µs max., on to off
Maximum relay switching frequency	1 Hz	--
Pulse Train Output rate	Not recommended [2]	100 kHz (Qa.0 to Qa.3)[3], 2 Hz min. 20 kHz (Qa.4 to Qb.1)[3]
Lifetime mechanical (no load)	10,000,000 open/close cycles	--
Lifetime contacts at rated load	100,000 open/close cycles	--
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Control of a digital input	Yes	
Parallel outputs for redundant load control	Yes (with same common)	
Parallel outputs for increased load	No	
Number of outputs on simultaneously	• 5 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 10 at 55 °C horizontal or 45 °C vertical	
Cable length (meters)	500 m shielded, 150 m unshielded	

1 Relay group-to-group isolation separates line voltage from SELV/PELV and separates different phases up to 250 V AC line to ground.

2 For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

3 Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

A.8.6 Analog inputs and outputs

Table A-79 Analog inputs

Technical data	Description
Number of inputs	2
Type	Voltage (single-ended)
Full-scale range	0 to 10 V
Full-scale range (data word)	0 to 27648
Overshoot range	10.001 to 11.759 V
Overshoot range (data word)	27649 to 32511
Overflow range	11.760 to 11.852 V
Overflow range (data word)	32512 to 32767
Resolution	10 bits
Maximum withstand voltage	35 V DC

Technical data	Description
Smoothing	None, Weak, Medium, or Strong See the table for Step response (ms) for the analog inputs of the CPU (Page 1147).
Noise rejection	10, 50, or 60 Hz
Impedance	≥100 KΩ
Isolation (field side to logic)	None
Accuracy (25 °C / -20 to 60 °C)	3.0% / 3.5% of full-scale
Cable length (meters)	100 m, shielded twisted pair

A.8.6.1 Step response of built-in analog inputs of the CPU

Table A-80 Step Response (ms), 0 V to 10 V measured at 95%

Smoothing selection (sample averaging)	Rejection frequency (Integration time)		
	60 Hz	**50 Hz**	**10 Hz**
None (1 cycle): No averaging	50 ms	50 ms	100 ms
Weak (4 cycles): 4 samples	60ms	70 ms	200 ms
Medium (16 cycles): 16 samples	200 ms	240 ms	1150 ms
Strong (32 cycles): 32 samples	400 ms	480 ms	2300 ms
Sample time	**4.17 ms**	**5 ms**	**25 ms**

A.8.6.2 Sample time for the built-in analog ports of the CPU

Table A-81 Sample time for built-in analog inputs of the CPU

Rejection frequency (Integration time selection)	Sample time
60 Hz (16.6 ms)	4.17 ms
50 Hz (20 ms)	5 ms
10 Hz (100 ms)	25 ms

A.8.6.3 Measurement ranges of the analog inputs for voltage (CPUs)

Table A-82 Analog input representation for voltage (CPUs)

System		Voltage Measuring Range	
Decimal	**Hexadecimal**	**0 to 10 V**	
32767	7FFF	11.852 V	Overflow
32512	7F00		
32511	7EFF	11.759 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range
20736	5100	7.5 V	

System		Voltage Measuring Range	
Decimal	**Hexadecimal**	**0 to 10 V**	
34	22	12 mV	Rated range
0	0	0 V	
Negative values		Negative values are not supported	

A.8.6.4 Analog output specifications

Table A-83 Analog outputs

Technical data	Description
Number of outputs	2
Type	Current
Full-scale range	0 to 20 mA
Full-scale range (data word)	0 to 27648
Overshoot range	20.01 to 23.52 mA
Overshoot range (data word)	27649 to 32511
Overflow range	see footnote [1]
Overflow range data word	32512 to 32767
Resolution	10 bits
Output drive impedance	≤500 Ω max.
Isolation (field side to logic)	None
Accuracy (25 °C / -20 to 60 °C)	3.0% / 3.5% of full-scale
Settling time	2 ms
Cable length (meters)	100 m, shielded twisted pair

[1] In an overflow condition, analog outputs will behave according to the device configuration properties settings. In the "Reaction to CPU STOP" parameter, select either: "Use substitute value" or "Keep last value".

Table A-84 Analog output representation for current (CPU 1215C and CPU 1217C)

System		Current output range	
Decimal	**Hexadecimal**	**0 mA to 20 mA**	
32767	7FFF	See note 1	Overflow
32512	7F00	See note 1	
32511	7EFF	23.52 mA	Overshoot range
27649	6C01		
27648	6C00	20 mA	Rated range
20736	5100	15 mA	

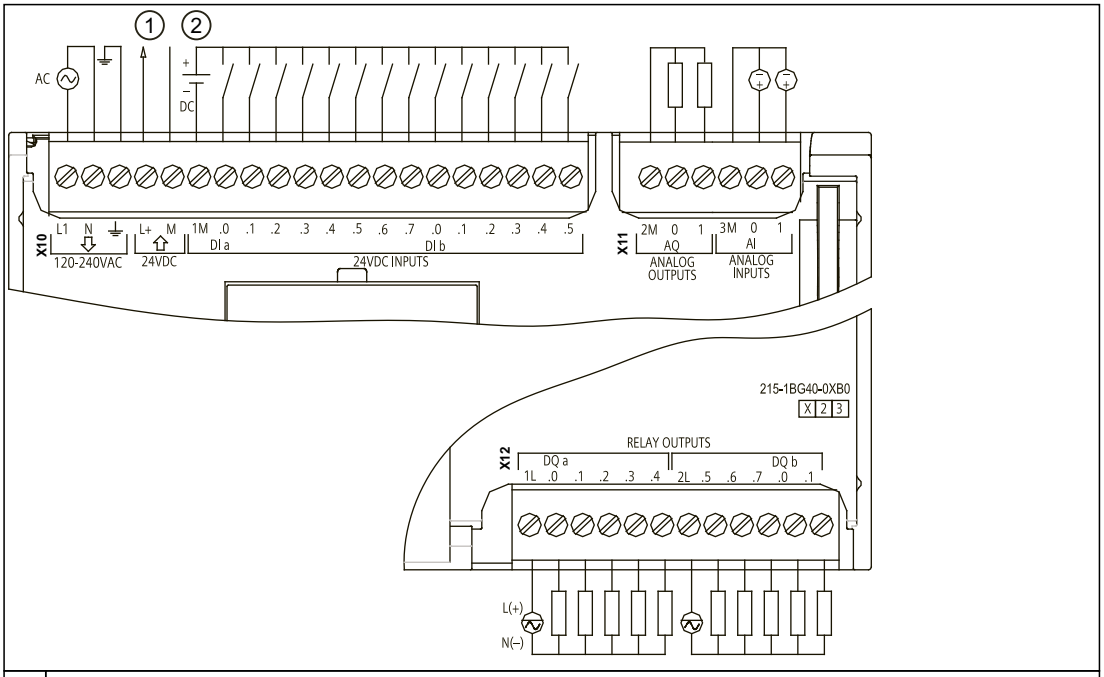
[1] In an overflow condition, analog outputs will behave according to the device configuration properties settings. In the "Reaction to CPU STOP" parameter, select either: "Use substitute value" or "Keep last value".

System		Current output range	
Decimal	**Hexadecimal**	**0 mA to 20 mA**	
34	22	0.0247 mA	Rated range
0	0	0 mA	
Negative values		Negative values are not supported	

[1] In an overflow condition, analog outputs will behave according to the device configuration properties settings. In the "Reaction to CPU STOP" parameter, select either: "Use substitute value" or "Keep last value".

A.8.7 CPU 1215C wiring diagrams

Table A-85 CPU 1215C AC/DC/Relay (6ES7215-1BG40-0XB0)

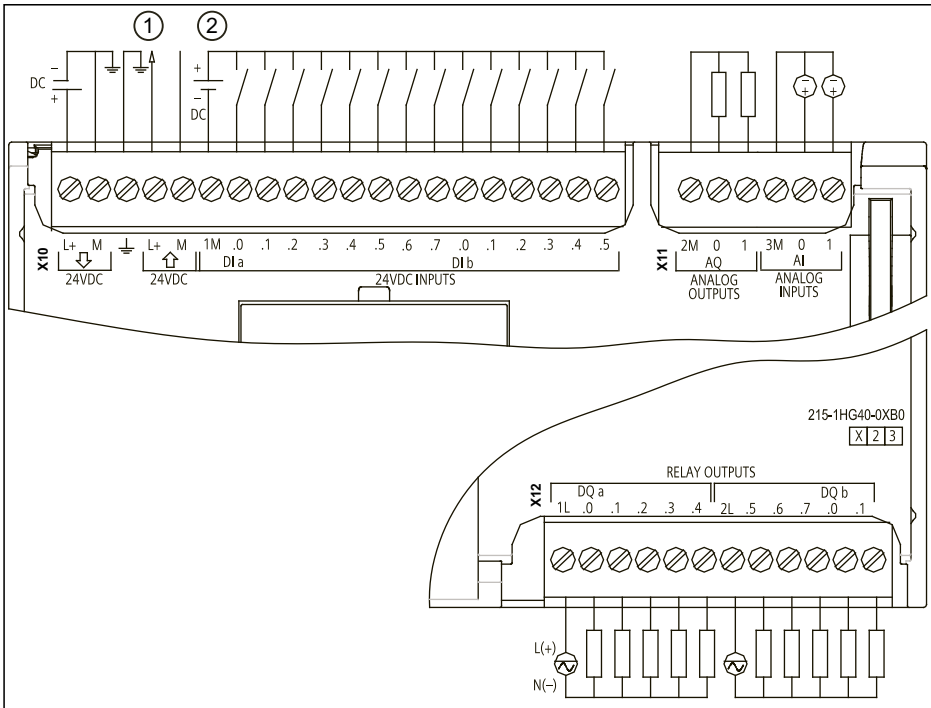


1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.	
Note 2: Either the L1 or N (L2) terminal can be connected to a voltage source up to 240 V AC. The N terminal can be considered L2 and is not required to be grounded. No polarization is required for L1 and N (L2) terminals.	
Note 3: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-86 Connector pin locations for CPU 1215C AC/DC/Relay (6ES7215-1BG40-0XB0)

Pin	X10	X11 (gold)	X12
1	L1 /120-240 V AC	2 M	1L
2	N / 120 - 240 V AC	AQ 0	DQ a.0
3	Functional Earth	AQ 1	DQ a.1
4	L+ / 24 V DC Sensor Out	3M	DQ a.2
5	M / 24 V DC Sensor Out	AI 0	DQ a.3
6	1M	AI 1	DQ a.4
7	DI a.0	--	2L
8	DI a.1	--	DQ a.5
9	DI a.2	--	DQ a.6
10	DI a.3	--	DQ a.7
11	DI a.4	--	DQ b.0
12	DI a.5	--	DQ b.1
13	DI a.6	--	--
14	DI a.7	--	--
15	DI b.0	--	--
16	DI b.1	--	--
17	DI b.2	--	--
18	DI b.3	--	--
19	DI b.4	--	--
20	DI b.5	--	--

Table A-87 CPU 1215C DC/DC/Relay (6ES7215-1HG40-0XB0)



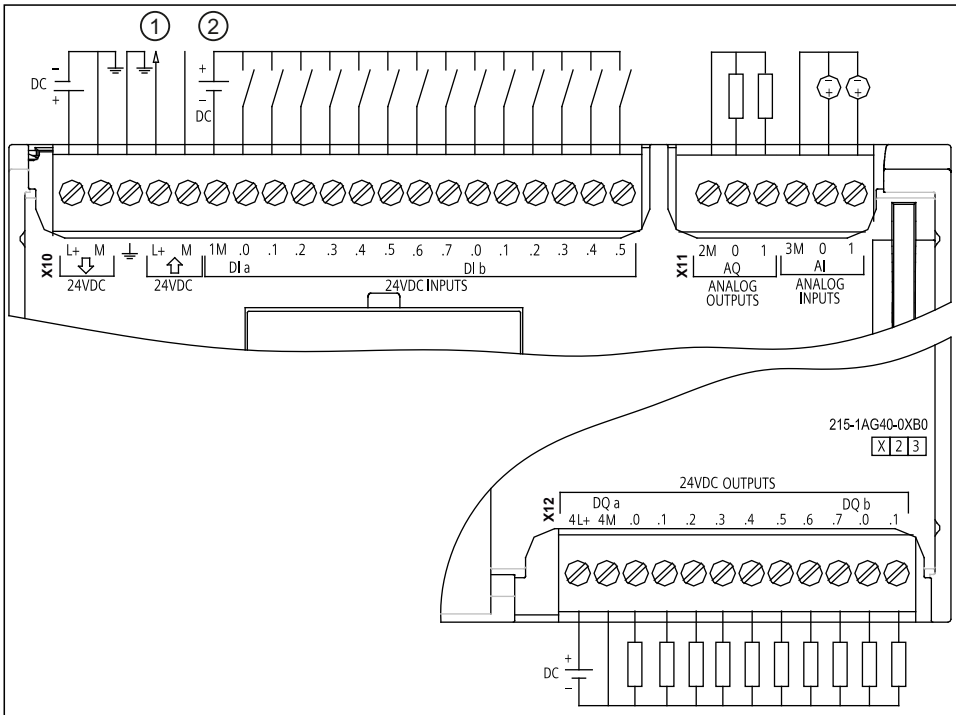
1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.	
Note 2: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-88 Connector pin locations for CPU 1215C DC/DC/Relay (6ES7215-1HG40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24 V DC	2 M	1L
2	M / 24 V DC	AQ 0	DQ a.0
3	Functional Earth	AQ 1	DQ a.1
4	L+ / 24 V DC Sensor Out	3M	DQ a.2
5	M / 24 V DC Sensor Out	AI 0	DQ a.3
6	1M	AI 1	DQ a.4
7	DI a.0	--	2L
8	DI a.1	--	DQ a.5
9	DI a.2	--	DQ a.6
10	DI a.3	--	DQ a.7
11	DI a.4	--	DQ b.0
12	DI a.5	--	DQ b.1
13	DI a.6	--	--
14	DI a.7	--	--
15	DI b.0	--	--

Pin	X10	X11 (gold)	X12
16	DI b.1	--	--
17	DI b.2	--	--
18	DI b.3	--	--
19	DI b.4	--	--
20	DI b.5	--	--

Table A-89 CPU 1215C DC/DC/DC (6ES7215-1AG40-0XB0)



1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note 1: X11 connectors must be gold. See Appendix C, Spare Parts for article number.	
Note 2: See Device Configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-90 Connector pin locations for CPU 1215C DC/DC/DC (6ES7215-1AG40-0XB0)

Pin	X10	X11 (gold)	X12
1	L1 / 24 V DC	2 M	4L+
2	M / 24 V DC	AQ 0	4M
3	Functional Earth	AQ 1	DQ a.0
4	L+ / 24 V DC Sensor Out	3M	DQ a.1
5	M / 24 V DC Sensor Out	AI 0	DQ a.2
6	1M	AI 1	DQ a.3
7	DI a.0	--	DQ a.4
8	DI a.1	--	DQ a.5

Pin	X10	X11 (gold)	X12
9	DI a.2	--	DQ a.6
10	DI a.3	--	DQ a.7
11	DI a.4	--	DQ b.0
12	DI a.5	--	DQ b.1
13	DI a.6	--	--
14	DI a.7	--	--
15	DI b.0	--	--
16	DI b.1	--	--
17	DI b.2	--	--
18	DI b.3	--	--
19	DI b.4	--	--
20	DI b.5	--	--

NOTE

Unused analog inputs should be shorted.

A.9 CPU 1217C

A.9.1 General specifications and features

Table A-91 General

Technical data	CPU 1217C DC/DC/DC
Article number	6ES7217-1AG40-0XB0
Dimensions W x H x D (mm)	150 x 100 x 75
Shipping weight	530 grams
Power dissipation	12 W
Electrical current available (SM and CM bus)	1600 mA max. (5 V DC)
Electrical current available (24 V DC)	400 mA max. (sensor power)
Digital input current consumption (24 V DC)	4 mA/input used

Table A-92 CPU features

Technical data		Description
User memory (Refer to "General technical specifications (Page 1090)", Internal CPU memory retention".)	Work	250 Kbytes
	Load	4 Mbytes, internal, expandable up to SD card size
	Retentive	14 Kbytes
Onboard digital I/O		14 inputs/ 10 outputs
Onboard analog I/O		2 inputs/ 2 outputs
Process image size		1024 bytes of inputs (I) / 1024 bytes of outputs (Q)
Bit memory (M)		8192 bytes
Temporary (local) memory		• 16 Kbytes for startup and program cycle (including associated FBs and FCs) • 6 Kbytes for each of the other interrupt priority levels (including FBs and FCs)
Signal modules expansion		8 SMs max.
SB, CB, BB expansion		1 max.
Communication module expansion		3 CMs max.
High-speed counters		Up to 6 configured to use any built-in or SB inputs (refer to CPU 1217C Digital input (DI) H/W configuration table) (Page 1159) • 1 MHz (Ib.2 to Ib.5) • 100/[1]80 kHz (Ia.0 to Ia.5) • 30/[1]20 kHz (Ia.6 to Ib.1)
Pulse outputs		Up to 4 configured to use any built-in or SB outputs (refer to CPU 1217C Digital output (DQ) H/W configuration table) (Page 1159) • 1 MHz (Qa.0 to Qa.3) • 100 kHz (Qa.4 to Qb.1)
Pulse catch inputs		14
Time delay interrupts		4 total with 1 ms resolution
Cyclic interrupts		4 total with 1 ms resolution
Edge interrupts		12 rising and 12 falling (16 and 16 with optional signal board)
Memory card		SIMATIC memory card (optional)
Real time clock accuracy		+/- 60 seconds/month
Real time clock retention time		20 days typ./12 days min. at 40 °C (maintenance-free Super Capacitor)

[1] The slower speed is applicable when the HSC is configured for quadrature mode of operation.

Table A-93 Performance

Type of instruction		Execution speed	
		Direct addressing (I, Q and M)	DB accesses
Boolean		0.08 µs/instruction	
Move	Move_Bool	0.3 µs/instruction	1.17 µs/instruction
	Move_Word	0.137 µs/instruction	1.0 µs/instruction
	Move_Real	0.72 µs/instruction	1.0 µs/instruction
Real Math	Add Real	1.48 µs/instruction	1.78 µs/instruction

NOTE

Many variables affect measured times. The above performance times are for the fastest instructions in this category and error-free programs.

A.9.2 Timers, counters and code blocks supported by CPU 1217C

Table A-94 Blocks, timers and counters supported by CPU 1217C

Element		Description
Blocks	Type	OB, FB, FC, DB
	Size	OB, FB, FC: 64 Kbytes DB: up to the size of work memory
	Address range for FBs, FCs, and DBs	FB and FC: 1 to 65535 (such as FB 1 to FB 65535) DB: 1 to 59999
	Nesting depth	16 from the program cycle or startup OB 6 from any interrupt event OB[1]
	Monitoring	Status of 2 code blocks can be monitored simultaneously
OBs	Program cycle	Multiple
	Startup	Multiple
	Time-delay interrupts	4 (1 per event)
	Cyclic interrupts	4 (1 per event)
	Hardware interrupts	50 (1 per event)
	Time error interrupts	1
	Diagnostic error interrupts	1
	Pull or plug of modules	1
	Rack or station failure	1
	Time of day	Multiple
	Status	1
	Update	1
	Profile	1
	MC-Interpolator	1
	MC-Servo	1
	MC-PreServo	1
	MC-PostServo	1
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, 16 bytes per timer

[1] Safety programs use two nesting levels. The user program therefore has a nesting depth of four in safety programs.

Element		Description
Counters	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size dependent upon count type • SInt, USInt: 3 bytes • Int, UInt: 6 bytes • DInt, UDInt: 12 bytes

[1] Safety programs use two nesting levels. The user program therefore has a nesting depth of four in safety programs.

A.9.3 Communications CPU 1217C

Table A-95 Communication

Technical data	Description
Number of ports	2
Type	Ethernet
HMI device	4
Programming device (PG)	1
Connections (Page 526)	34 reserved, 68 max.
Data rates	10/100 Mb/s
Isolation (external signal logic)	Transformer isolated, 1500 V AC (type test)[1]
Cable type	CAT5e shielded
Interfaces	
Number of PROFINET interfaces	1
Number of interfaces PROFIBUS	0
Interface	
Interface hardware	
Number of ports	2
Integrated switch	Yes
RJ-45 (Ethernet)	Yes; X1
Protocols	
PROFINET IO controller	Yes
PROFINET IO device	Yes
SIMATIC communication	Yes
Open IE communication	Yes
Web server	Yes
Media redundancy	Yes
PROFINET IO controller	
Services	
PG/OP communication	Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data		Description
S7 routing		Yes
Isochronous mode		No
Open IE communication		Yes
IRT		No
MRP		Yes as MRP client
PROFIenergy		Yes. The S7-1200 CPU only supports the PROFIenergy entity (with I-device functionality).
Prioritized startup		Yes (max. 16 PROFINET devices)
Number of connectable I/O devices max.		16
Number of IO devices that you can connect for RT, max.		16
Of which are in line, max.		16
Number of IO devices that can be activated/ deactivated simultaneously, max.		8
Update times		The minimum value of the update time also depends on the communication component set for PROFINET IO, on the number of IO devices, and the quantity of configured user data.
With RT		
Send clock of 1 ms		1 ms to 512 ms
PROFINET IO device		
Services		
PG/OP communication		Yes
S7 routing		Yes
Isochronous mode		No
Open IE communication		Yes
IRT, supported		No
MRP, supported		Yes
PROFIenergy		Yes
Shared device		Yes
Number of IO controllers with shared device, max.		2
SIMATIC communication		
S7 communication, as server		Yes
S7 communication, as client		Yes
User data per job, max.		See online help (S7 communication, user data size)
Open IE communication		
TCP/IP:		Yes
	Data length, max.	8 KB
	Several passive connections per port, supported	Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data		Description
ISO-on-TCP (RFC1006):		Yes
	Data length, max.	8 KB
UDP:		Yes
	Data length, max.	2048 bytes
DHCP		No
SNMP		Yes
DCP		Yes
LLDP		Yes

[1] Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

A.9.4 Power supply and sensor power (CPU 1217C)

Table A-96 Power supply

Technical data		CPU 1217C DC/DC/DC
Voltage range		20.4 V DC to 28.8 V DC
Line frequency		--
Input current (max. load)	CPU only	600 mA at 24 V DC
	CPU with all expansion accessories	1600 mA at 24 V DC
Inrush current (max.)		12 A at 28.8 V DC
I^2 t		0.5 A^2 s
Isolation (input power to logic)		Not isolated
Hold up time (from loss of power)		10 ms at 24 V DC
Internal fuse, not user replaceable		3 A, 250 V, slow blow

Table A-97 Sensor power

Technical data	CPU 1217C DC/DC/DC
Voltage range	L+ minus 4 V DC min.
Output current rating (max.)	400 mA (short-circuit protected)
Maximum ripple noise (<10 MHz)	Same as input line
Isolation (CPU logic to sensor power)	Not isolated

A.9.5 Digital inputs and outputs

Table A-98 Digital inputs

Technical data	CPU 1217C DC/DC/DC	
	High speed inputs	**Standard inputs**
Number of inputs	14: total: 10: Sink/source (IEC Type 1 sink) 4: Differential (RS422/RS485)	
Type: Sink/source (IEC Type 1 sink)	Ia.0 to Ia.7, Ib.0 to Ib.1	
Rated voltage	24 V DC at 6 mA, nominal	24 V DC at 4 mA, nominal
Continuous permissible voltage	30 V DC, max. at 8 mA, max.	30 V DC, max. at 6 mA, max.
Surge voltage	35 V DC for 0.5 sec.	
Logic 1 signal (min.)	15 V DC at 2.5 mA	
Logic 0 signal (max.)	5 V DC at 1 mA	
Isolation (field side to logic)	707 V DC (type test)	
Isolation groups	1	
Filter times	us settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
HSC clock input rates (max.) (Logic 1 Level = 15 to 26 V DC)	100/80 kHz (Ia.0 to Ia.5) 30/20 kHz (Ia.6 to Ib.1)	
Type: Differential input (RS422/RS485)	Ib.2 to Ib.5 (.2+ .2- to .5+ .5-)	
Common mode voltage range	-7 V to +12 V, 1 second, 3 VRMS continuous (RS422/RS485 characteristics)	
Built-in termination and bias	390 Ω to 2M on Ib'-', 390 Ω to +5 V on Ib'-', (biased OFF when T/B open-circuit) 220 Ω between Ib'+' and Ib'-'	
Receiver input impedance	100 Ω including bias and termination	
Differential receiver threshold/sensitivity	+/- 0.2 V min., 60 mV typical hysteresis (RS422/RS485 characteristics)	
Isolation (field side to logic)	707 V DC (type test)	
Isolation groups	1	
Filter times	us settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
HSC clock input rates (max.)	Single phase: 1 MHz (Ib.2 to Ib.5) Quadrature phase: 1 MHz (Ib.2 to Ib.5)	
Differential input channel-to-channel skew	40 ns max.	
General specifications (all digital inputs)		
Number of inputs on simultaneously	5 Sink/source inputs (no adjacent points) and 4 differential inputs at 60 °C horizontal or 50 °C vertical 14 at 55 °C horizontal or 45 °C vertical	
Cable length (meters)	500 m shielded, 300 m unshielded 50 m shielded for HSC inputs (sink/source) 50 m shielded, twisted pair for all differential inputs	

Table A-99 CPU 1217C Digital input (DI) H/W configuration table

Input	Type and rate
DIa.0	Type: 24 V, source-sink Type 1 input High-speed counter input rate: 100 kHz max.
DIa.1	Type: 24 V, source-sink Type 1 input High-speed counter input rate: 100 kHz max.
DIa.2	Type: 24 V, source-sink Type 1 input High-speed counter input rate: 100 kHz max.
DIa.3	Type: 24 V, source-sink Type 1 input High-speed counter input rate: 100 kHz max.
DIa.4	Type: 24 V, source-sink Type 1 input High-speed counter input rate: 100 kHz max.
DIa.5	Type: 24 V, source-sink Type 1 input High-speed counter input rate: 100 kHz max.
DIa.6	Type: 24 V, source-sink Type 1 input High-speed counter input rate: 30 kHz max.
DIa.7	Type: 24 V, source-sink Type 1 input High-speed counter input rate: 30 kHz max.
DIb.0	Type: 24 V, source-sink Type 1 input High-speed counter input rate: 30 kHz max.
DIb.1	Type: 24 V, source-sink Type 1 input High-speed counter input rate: 30 kHz max.
DIb.2+ .2-	Type: RS422/RS485 differential input High-speed counter input rate: 1 MHz max.
DIb.3+ .3-	Type: RS422/RS485 differential input High-speed counter input rate: 1 MHz max.
DIb.4+ .4-	Type: RS422/RS485 differential input High-speed counter input rate: 1 MHz max.
DIb.5+ .5-	Type: RS422/RS485 differential input High-speed counter input rate: 1 MHz max.

Table A-100 Digital outputs

Technical data	CPU 1217C DC/DC/DC
Number of outputs	10 total 6: Solid state - MOSFET (sourcing) 4: Differential (RS422/RS485)
Type: Solid state - MOSFET (sourcing output)	Qa.4 to Qb.1
Voltage range	20.4 to 28.8 V DC
Logic 1 signal at max. current	20 V DC min.
Logic 0 signal with 10 KΩ load	0.1 V DC max.
Current (max.)	0.5 A
Lamp load	5 W
ON state resistance	0.6 Ω max.

[1] Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

Technical data	CPU 1217C DC/DC/DC
Leakage current per point	10 µA max.
Surge current	8 A for 100 ms max.
Overload protection	No
Isolation (field side to logic)	707 V DC (type test)
Isolation groups	1
Inductive clamp voltage	L+ minus 48 V DC, 1 W dissipation
Switching delay (Qa.4 to Qb.1)	1.0 µs max., off to on 3.0 µs max., on to off
Maximum relay switching frequency	--
Pulse Train Output rate	100 kHz max. (Qa.4 to Qb.1)[1], 2 Hz min.
Type: Differential output (RS422/RS485)	Qa.0 to Qa.3 (.0+ 0- to .3+ .3-)
Common mode voltage range	-7 V to +12 V, 1 second, 3 VRMS continuous (RS422/RS485 characteristics)
Transmitter differential output voltage	2 V min. at RL = 100 Ω, 1.5 V min. at RL = 54 Ω (RS422/RS485 characteristics)
Built-in termination	100 Ω between Qa'+' and Qa'-'
Driver output impedance	100 Ω including termination
Isolation (field side to logic)	707 V DC (type test)
Isolation groups	1
Switching delay (DQa.0 to DQa.3)	100 ns max.
Differential output channel-to-channel skew	40 ns max.
Pulse train output rate	1 MHz (Qa.0 to Qa.3), 2 Hz min.
General specifications (all digital outputs)	
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes
Parallel outputs for redundant load control	Yes (Qa.4 to Qb.1 only; with same common)
Parallel outputs for increased load	No
Number of outputs on simultaneously	3 Solid state - MOSFET (sourcing) outputs (no adjacent points) and 4 differential outputs at 60 °C horizontal or 50 °C vertical 10 at 55 °C horizontal or 45 °C vertical
Cable length (meters)	500 m shielded, 150 m unshielded

[1] Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

Table A-101 CPU 1217C Digital output (DQ) H/W configuration table

Output	Type and rate
DQa.0+ .0-	Type: RS422/RS485 differential output Pulse train output rate: 1 MHz max., 2 Hz min.
DQa.1+ .1-	Type: RS422/RS485 differential output Pulse train output rate: 1 MHz max., 2 Hz min.
DQa.2+ .2-	Type: RS422/RS485 differential output Pulse train output rate: 1 MHz max., 2 Hz min.
DQa.3+ .3-	Type: RS422/RS485 differential output Pulse train output rate: 1 MHz max., 2 Hz min.
DQa.4	Type: 24 V Sourcing output Pulse train output rate: 100 kHz max., 2 Hz min.
DQa.5	Type: 24 V Sourcing output Pulse train output rate: 100 kHz max., 2 Hz min.
DQa.6	Type: 24 V Sourcing output Pulse train output rate: 100 kHz max., 2 Hz min.
DQa.7	Type: 24 V Sourcing output Pulse train output rate: 100 kHz max., 2 Hz min.
DQb.0	Type: 24 V Sourcing output Pulse train output rate: 100 kHz max., 2 Hz min.
DQb.1	Type: 24 V Sourcing output Pulse train output rate: 100 kHz max., 2 Hz min.

A.9.6 Analog inputs and outputs

A.9.6.1 Analog input specifications

Table A-102 Analog inputs

Technical data	Description
Number of inputs	2
Type	Voltage (single-ended)
Full-scale range	0 to 10 V
Full-scale range (data word)	0 to 27648
Overshoot range	10.001 to 11.759 V
Overshoot range (data word)	27649 to 32511
Overflow range	11.760 to 11.852 V
Overflow range (data word)	32512 to 32767
Resolution	10 bits
Maximum withstand voltage	35 V DC
Smoothing	None, Weak, Medium, or Strong See the table for Step response (ms) for the analog inputs of the CPU (Page 1163).
Noise rejection	10, 50, or 60 Hz
Impedance	≥100 KΩ

Technical data	Description
Isolation (field side to logic)	None
Accuracy (25 °C / -20 to 60 °C)	3.0% / 3.5% of full-scale
Cable length (meters)	100 m, shielded twisted pair

A.9.6.2 Step response of built-in analog inputs of the CPU

Table A-103 Step Response (ms), 0 V to 10 V measured at 95%

Smoothing selection (sample averaging)	Rejection frequency (Integration time)		
	60 Hz	**50 Hz**	**10 Hz**
None (1 cycle): No averaging	50 ms	50 ms	100 ms
Weak (4 cycles): 4 samples	60ms	70 ms	200 ms
Medium (16 cycles): 16 samples	200 ms	240 ms	1150 ms
Strong (32 cycles): 32 samples	400 ms	480 ms	2300 ms
Sample time	**4.17 ms**	**5 ms**	**25 ms**

A.9.6.3 Sample time for the built-in analog ports of the CPU

Table A-104 Sample time for built-in analog inputs of the CPU

Rejection frequency (Integration time selection)	Sample time
60 Hz (16.6 ms)	4.17 ms
50 Hz (20 ms)	5 ms
10 Hz (100 ms)	25 ms

A.9.6.4 Measurement ranges of the analog inputs for voltage (CPUs)

Table A-105 Analog input representation for voltage (CPUs)

System		Voltage Measuring Range	
Decimal	**Hexadecimal**	**0 to 10 V**	
32767	7FFF	11.852 V	Overflow
32512	7F00		
32511	7EFF	11.759 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range
20736	5100	7.5 V	
34	22	12 mV	
0	0	0 V	
Negative values		Negative values are not supported	

A.9.6.5 Analog output specifications

Table A-106 Analog outputs

Technical data	Description
Number of outputs	2
Type	Current
Full-scale range	0 to 20 mA
Full-scale range (data word)	0 to 27648
Overshoot range	20.01 to 23.52 mA
Overshoot range (data word)	27649 to 32511
Overflow range	see footnote [1]
Overflow range data word	32512 to 32767
Resolution	10 bits
Output drive impedance	≤500 Ω max.
Isolation (field side to logic)	None
Accuracy (25 °C / -20 to 60 °C)	3.0% / 3.5% of full-scale
Settling time	2 ms
Cable length (meters)	100 m, shielded twisted pair

[1] In an overflow condition, analog outputs will behave according to the device configuration properties settings. In the "Reaction to CPU STOP" parameter, select either: "Use substitute value" or "Keep last value".

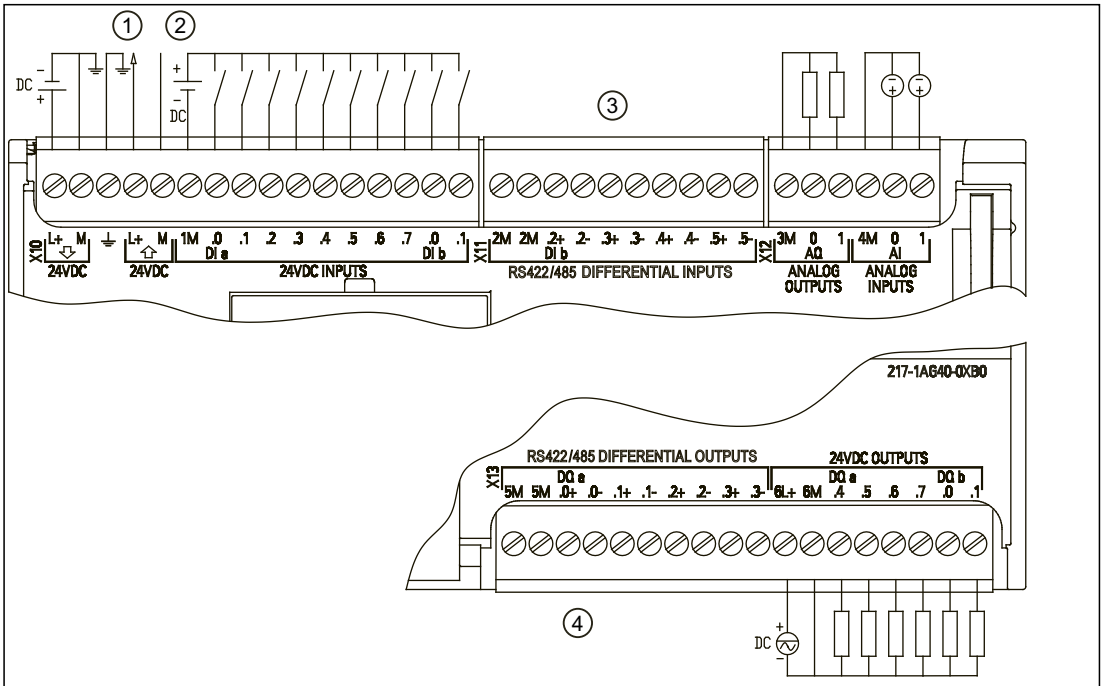
Table A-107 Analog output representation for current (CPU 1215C and CPU 1217C)

System		Current output range	
Decimal	**Hexadecimal**	**0 mA to 20 mA**	
32767	7FFF	See note 1	Overflow
32512	7F00	See note 1	
32511	7EFF	23.52 mA	Overshoot range
27649	6C01		
27648	6C00	20 mA	Rated range
20736	5100	15 mA	
34	22	0.0247 mA	
0	0	0 mA	
Negative values		Negative values are not supported	

[1] In an overflow condition, analog outputs will behave according to the device configuration properties settings. In the "Reaction to CPU STOP" parameter, select either: "Use substitute value" or "Keep last value".

A.9.7 CPU 1217C wiring diagrams

Table A-108 CPU 1217C DC/DC/DC (6ES7217-1AG40-0XB0)



1	24 V DC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
2	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
3	See CPU 1217C Differential input (DI) detail and application example (Page 1167).
4	See CPU 1217C Differential output (DQ) detail and application example (Page 1168).
Note 1: X12 connectors must be gold. See Appendix C, Spare Parts (Page 1277) for article number.	
Note 2: See Device configuration (Page 121) for information about the Ethernet port of the CPU.	

Table A-109 Connector pin locations for CPU 1217C DC/DC/DC (6ES7217-1AG40-0XB0)

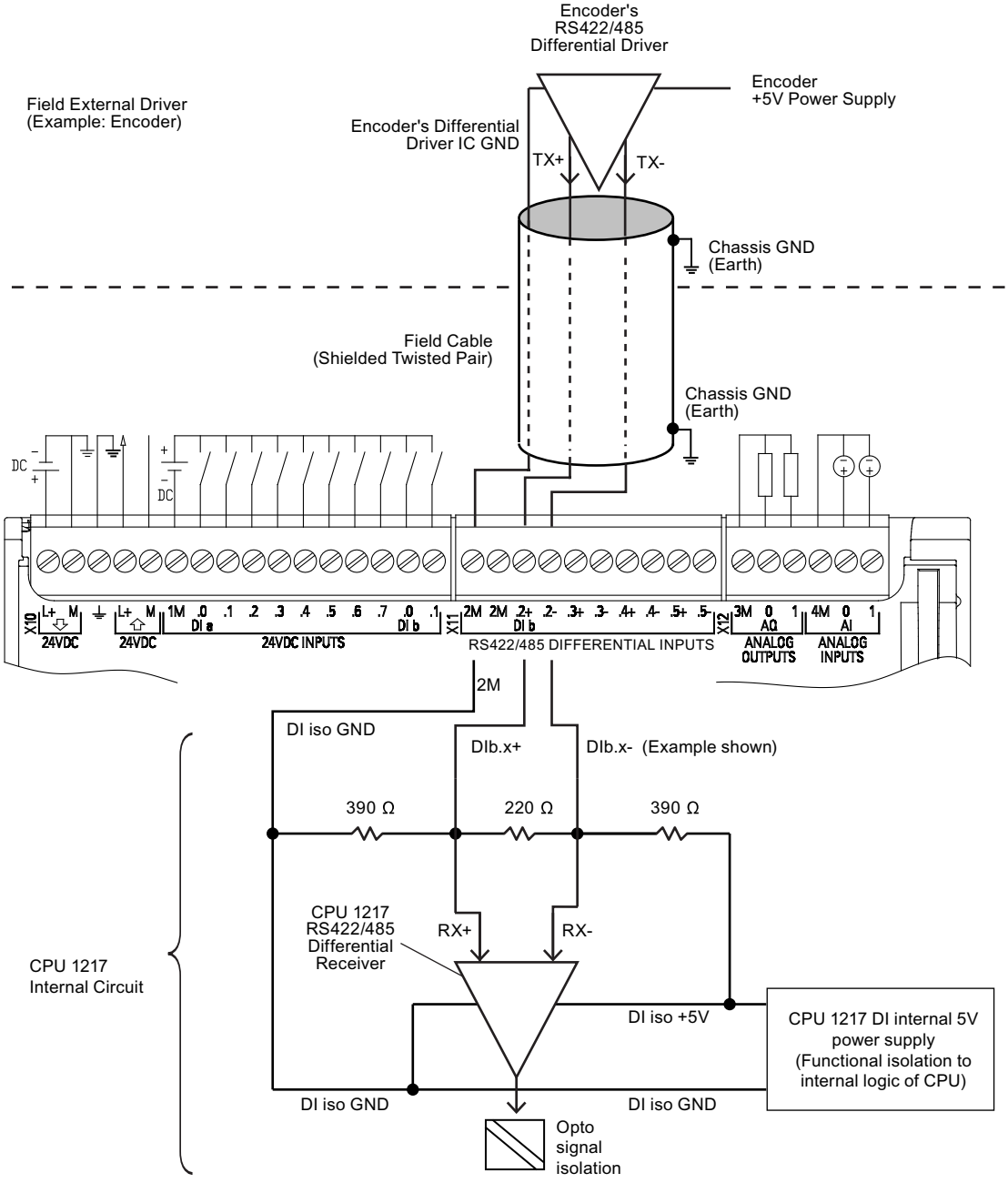
Pin	X10	X11	X12 (gold)	X13
1	L+ / 24 V DC	2M	3M	5M
2	M / 24 V DC	2M	AQ 0	5M
3	Functional Earth	DI b.2+	AQ 1	DQ a.0+
4	L+ / 24 V DC Sensor Out	DI b.2-	4M	DQ a.0-
5	M / 24 V DC Sensor Out	DI b.3+	AI 0	DQ a.1+
6	1M	DI b.3-	AI 1	DQ a.1-
7	DI a.0	DI b.4+	--	DQ a.2+
8	DI a.1	DI b.4-	--	DQ a.2-
9	DI a.2	DI b.5+	--	DQ a.3+
10	DI a.3	DI b.5-	--	DQ a.3-
11	DI a.4	--	--	6L+

Pin	X10	X11	X12 (gold)	X13
12	DI a.5	--	--	6M
13	DI a.6	--	--	DQ a.4
14	DI a.7	--	--	DQ a.5
15	DI b.0	--	--	DQ a.6
16	DI b.1	--	--	DQ a.7
17	--	--	--	DQ b.0
18	--	--	--	DQ b.1

NOTE

Unused analog inputs should be shorted.

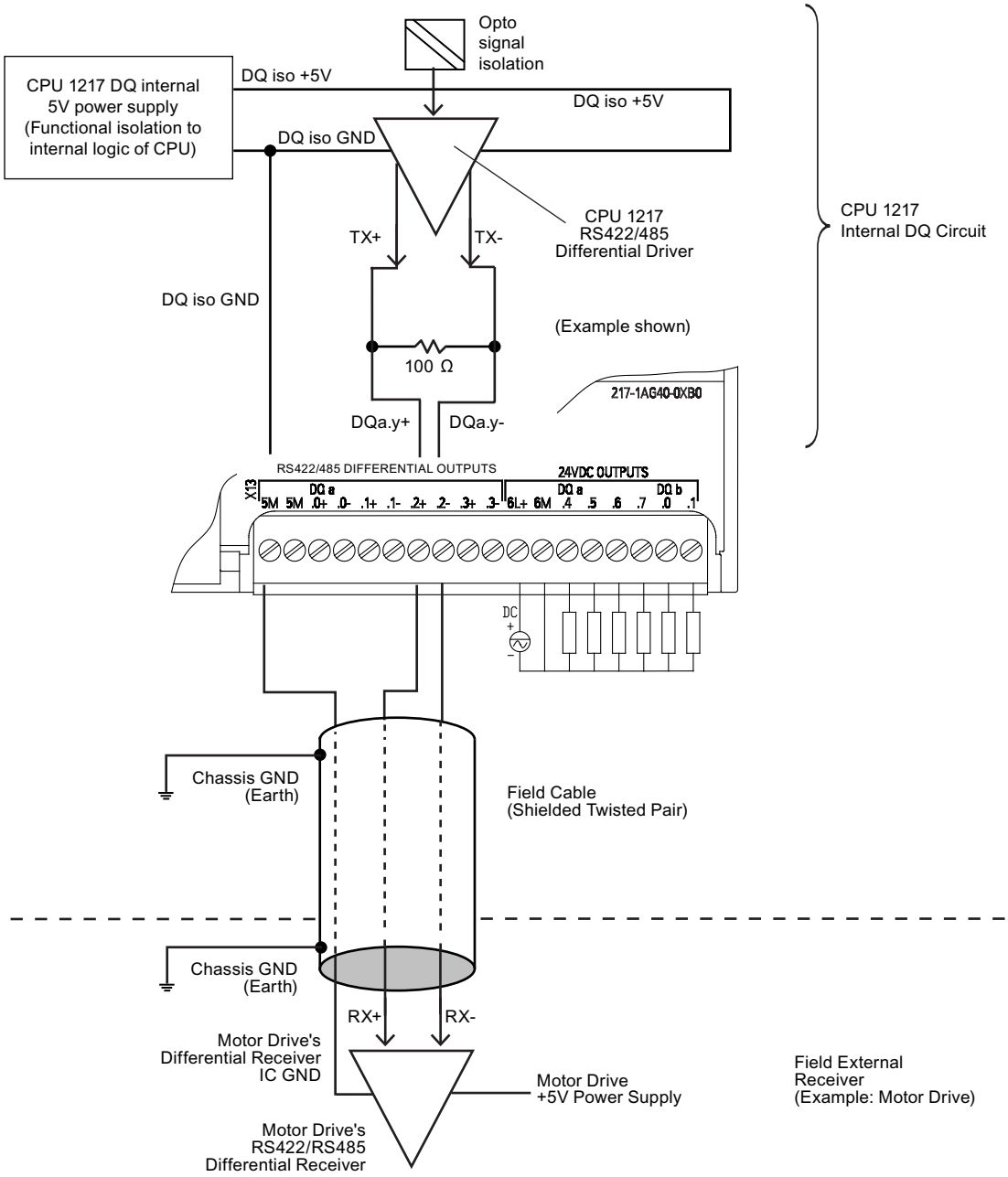
A.9.8 CPU 1217C Differential Input (DI) detail and application example



Notes

- Each differential DI is biased "OFF" when terminal block screws are open-circuit.
- Built-in DI Termination and Bias = 100 Ω equivalent impedance.
- Built-in DI Termination and Bias resistors limit the continuous common mode voltage range. See electrical specifications for detail.

A.9.9 CPU 1217C Differential Output (DQ) detail and application example



Note

- Built-in DQ Termination resistor limits the continuous common mode voltage range. See electrical specifications for detail.

A.10 Digital signal modules (SMs)

A.10.1 SM 1221 digital input specifications

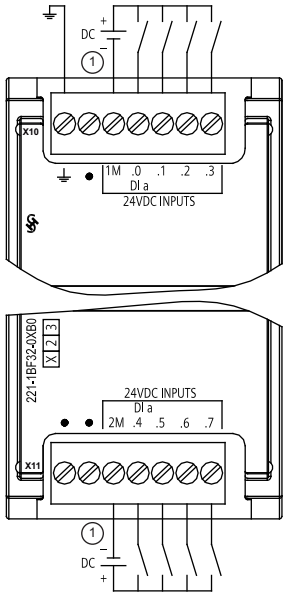
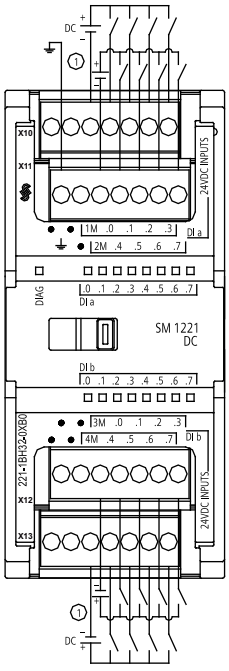
Table A-110 General specifications

Model	SM 1221 DI 8 x 24 V DC	SM 1221 DI 16 x 24 V DC
Article number	6ES7221-1BF32-0XB0	6ES7221-1BH32-0XB0
Dimensions W x H x D (mm)	45 x 100 x 75	
Weight	170 grams	210 grams
Power dissipation	1.5 W	2.5 W
Current consumption (SM Bus)	105 mA	130 mA
Current consumption (24 V DC)	4 mA / input used	

Table A-111 Digital inputs

Model	SM 1221 DI 8 x 24 V DC	SM 1221 DI 16 x 24 V DC
Number of inputs	8	16
Type	Sink/Source (IEC Type 1 sink)	
Rated voltage	24 V DC at 4 mA, nominal	
Continuous permissible voltage	30 V DC, max. at 6 mA, max.	
Surge voltage	35 V DC for 0.5 sec.	
Logic 1 signal (min.)	15 V DC at 2.5 mA	
Logic 0 signal (max.)	5 V DC at 1 mA	
Isolation (field side to logic)	707 V DC (type test)	
Isolation groups	2	4
Filter times	0.2, 0.4, 0.8, 1.6, 3.2, 6.4, and 12.8 ms (selectable in groups of 4)	0.2, 0.4, 0.8, 1.6, 3.2, 6.4, and 12.8 ms (selectable in groups of 4)
Number of inputs on simultaneously	8	16
Cable length (meters)	500 m shielded, 300 unshielded	

Table A-112 Wiring diagrams for the digital input SMs

SM 1221 DI 8 x 24 V DC (6ES7221-1BF32-0XB0)	SM 1221 DI 16 x 24 V DC (6ES7221-1BH32-0XB0)
	

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

Table A-113 Connector pin locations for SM 1221 DI 8 x 24 V DC (6ES7221-1BF32-0XB0)

Pin	X10	X11
1	Functional Earth	No connection
2	No connection	No connection
3	1M	2M
4	DI a.0	DI a.4
5	DI a.1	DI a.5
6	DI a.2	DI a.6
7	DI a.3	DI a.7

Table A-114 Connector pin locations for SM 1221 DI 16 x 24 V DC (6ES7221-1BH32-0XB0)

Pin	X10	X11	X12	X13
1	No connection	Functional Earth	No connection	No connection
2	No connection	No connection	No connection	No connection
3	1M	2M	3 M	4 M
4	DI a.0	DI a.4	DI b.0	DI b.4
5	DI a.1	DI a.5	DI b.1	DI b.5
6	DI a.2	DI a.6	DI b.2	DI b.6
7	DI a.3	DI a.7	DI b.3	DI b.7

A.10.2 SM 1222 8-point digital output specifications

Table A-115 General specifications

Model	SM 1222 DQ 8 x Relay	SM 1222 DQ 8 Relay Changeover	SM 1222 DQ 8 x 24 V DC
Article number	6ES7222-1HF32-0XB0	6ES7222-1XF32-0XB0	6ES7222-1BF32-0XB0
Dimensions W x H x D (mm)	45 x 100 x 75	70 x 100 x 75	45 x 100 x 75
Weight	190 grams	310 grams	180 grams
Power dissipation	4.5 W	5 W	1.5 W
Current consumption (SM Bus)	120 mA	140 mA	120 mA
Current consumption (24 V DC)	11 mA / Relay coil used	16.7 mA/Relay coil used	50 mA

Table A-116 Digital outputs

Model	SM 1222 DQ 8 x Relay	SM 1222 DQ 8 Relay Changeover	SM 1222 DQ 8 x 24 V DC
Number of outputs	8	8	8
Type	Relay, mechanical	Relay change over contact	Solid state - MOSFET (sourcing)
Voltage range	5 to 30 V DC or 5 to 250 V AC	5 to 30 V DC or 5 to 250 V AC	20.4 to 28.8 V DC
Logic 1 signal at max. current	--	--	20 V DC min.
Logic 0 signal with 10K Ω load	--	--	0.1 V DC max
Current (max.)	2.0 A	2.0 A	0.5 A
Lamp load	30 W DC/200 W AC	30 W DC/200 W AC	5 W
ON state contact resistance	0.2 Ω max. when new	0.2 Ω max. when new	0.6 Ω max.
Leakage current per point	--	--	10 µA max.
Surge current	7 A with contacts closed	7 A with contacts closed	8 A for 100 ms max.
Overload protection	No	No	No
Isolation (field side to logic)	1500 V AC (coil to contact) None (coil to logic)	1500 V AC (coil to contact)	707 V DC (type test)
Isolation groups	2	8	1
Current per common (max.)	10 A	2 A	4 A
Inductive clamp voltage	--	--	L+ minus 48 V, 1 W dissipation

Model	SM 1222 DQ 8 x Relay	SM 1222 DQ 8 Relay Changeover	SM 1222 DQ 8 x 24 V DC
Switching delay	10 ms max.	10 ms max.	50 µs max. off to on 200 µs max. on to off
Maximum relay switching frequency	1 Hz	1 Hz	--
Lifetime mechanical (no load)	10,000,000 open/close cycles	10,000,000 open/close cycles	--
Lifetime contacts at rated load (N.O. contact)	100,000 open/close cycles	100,000 open/close cycles	--
Behavior on RUN to STOP	Last value or substitute value (default value 0)	Last value or substitute value (default value 0)	Last value or substitute value (default value 0)
Control of a digital input	Yes		
Parallel outputs for redundant load control	Yes (with same common)		
Parallel outputs for increased load	No		
Number of outputs on simultaneously	8	• 4 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 8 at 55 °C horizontal or 45 °C vertical	8
Cable length (meters)	500 m shielded, 150 m unshielded	500 m shielded, 150 m unshielded	500 m shielded, 150 m unshielded

A.10.3 SM 1222 16-point digital output specifications

Table A-117 General specifications

Model	SM 1222 DQ 16 x Relay	SM 1222 DQ 16 x 24 V DC	SM 1222 DQ 16 x 24 V DC sinking
Article number	6ES7222-1HH32-0XB0	6ES7222-1BH32-0XB0	6ES7222-1BH32-1XB0
Dimensions W x H x D (mm)	45 x 100 x 75	45 x 100 x 75	45 x 100 x 75
Weight	260 grams	220 grams	220 grams
Power dissipation	8.5 W	2.5 W	2.5 W
Current consumption (SM Bus)	135 mA	140 mA	140 mA
Current consumption (24 V DC)	11 mA / Relay coil used	100 mA	40 mA

Table A-118 Digital outputs

Model	SM 1222 DQ 16 x Relay	SM 1222 DQ 16 x 24 V DC	SM 1222 DQ 16 x 24 V DC sinking
Number of outputs	16	16	16
Type	Relay, mechanical	Solid state - MOSFET (sourcing)	Solid state - MOSFET (sinking)
Voltage range	5 to 30 V DC or 5 to 250 V AC	20.4 to 28.8 V DC	20.4 to 28.8 V DC
Logic 1 signal at max. current	-	20 V DC min.	0.5 V DC
Logic 0 signal with 10K Ω load	-	0.1 V DC max.	24 V (typical) minus 0.75 V DC

Model	SM 1222 DQ 16 x Relay	SM 1222 DQ 16 x 24 V DC	SM 1222 DQ 16 x 24 V DC sinking
Current (max.)	2.0 A	0.5 A	0.5 A
Lamp load	30 W DC/200 W AC	5 W	5 W
ON state contact resistance	0.2 Ω max. when new	0.6 Ω max.	0.5 Ω max.
Leakage current per point	--	10 µA max.	75 µA max.
Surge current	7 A with contacts closed	8 A for 100 ms max.	8 A for 100 ms max.
Overload protection	No		Yes, current limit protected range 1 A to 3.5 A
Isolation (field side to logic)	1500 V AC (coil to contact) None (coil to logic)	707 V DC (type test)	707 V DC (type test)
Isolation groups	4	1	1
Current per common (max.)	10 A	8 A	Current limit protected
Inductive clamp voltage	-	L+ minus 48 V, 1 W dissipation	45 V
Switching delay	10 ms max.	50 µs max. off to on 200 µs max. on to off	20 µs max. off to on 350 µs max. on to off
Maximum relay switching frequency	1 Hz	-	-
Lifetime mechanical (no load)	10,000,000 open/close cycles	-	-
Lifetime contacts at rated load (N.O. contact)	100,000 open/close cycles	-	-
Behavior on RUN to STOP	Last value or substitute value (default value 0)	Last value or substitute value (default value 0)	Last value or substitute value (default value 0)
Control of a digital input	Yes	Yes	Yes (sourcing input)
Parallel outputs for redundant load control	Yes (with same common)		
Parallel outputs for increased load	No		
Number of outputs on simultaneously	• 8 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 16 at 55 °C horizontal or 45 °C vertical	16	16
Cable length (meters)	500 m shielded, 150 m unshielded		

Table A-119 Wiring diagrams for the 8-point digital output SMs

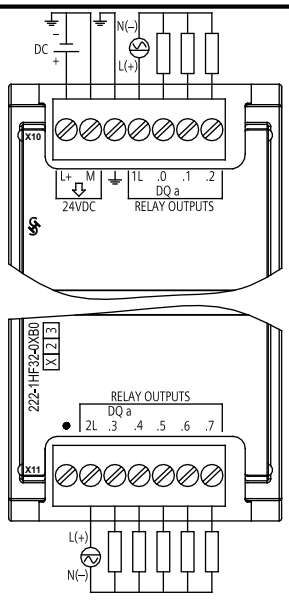
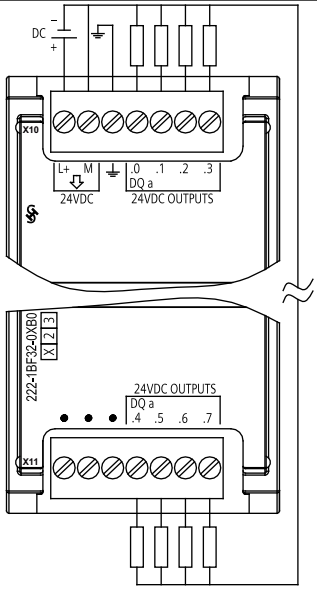
SM 1222 DQ 8 x Relay (6ES7222-1HF32-0XB0)	SM 1222 DQ 8 x 24 V DC (6ES7222-1BF32-0XB0)
	

Table A-120 Connector pin locations for SM 1222 DQ 8 x Relay (6ES7222-1HF32-0XB0)

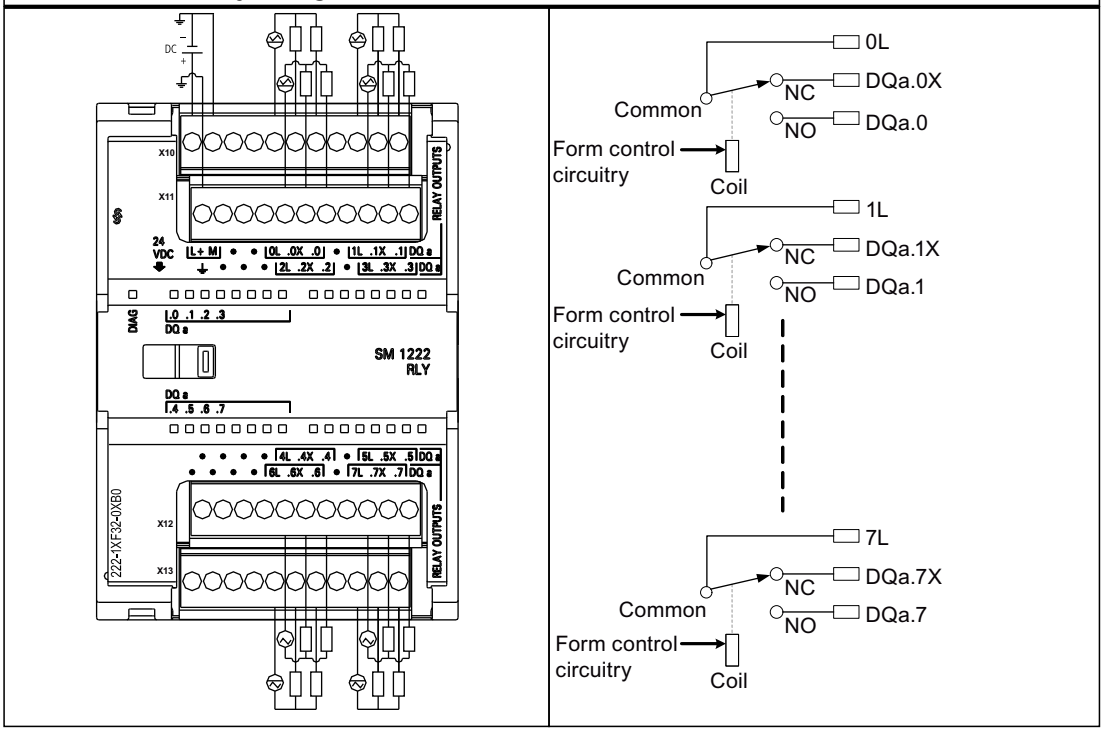
Pin	X10	X11
1	L+ / 24 V DC	No connection
2	M / 24 V DC	2L
3	Functional Earth	DQ a.3
4	1L	DQ a.4
5	DQ a.0	DQ a.5
6	DQ a.1	DQ a.6
7	DQ a.2	DQ a.7

Table A-121 Connector pin locations for SM 1222 DQ 8 x 24 V DC (6ES7222-1BF32-0XB0)

Pin	X10	X11
1	L+ / 24 V DC	No connection
2	M / 24 V DC	No connection
3	Functional Earth	No connection
4	DQ a.0	DQ a.4
5	DQ a.1	DQ a.5
6	DQ a.2	DQ a.6
7	DQ a.2	DQ a.7

Table A-122 Wiring diagram for the 8-point digital output relay changeover SM

SM 1222 DQ 8 x Relay Changeover (6ES7222-1XF32-0XB0)



A changeover relay output controls two circuits using a common terminal: one normally closed contact, and one normally open contact. Using output "0" as an example, when the output point is OFF, the common (0L) is connected to the normally closed contact (.0X) and disconnected from the normally open contact (.0). When the output point is ON, the common (0L) is disconnected from the normally closed contact (.0X) and connected to the normally open contact (.0).

Table A-123 Connector pin locations for SM 1222 DQ 8 x Relay Changeover (6ES7222-1XF32-0XB0)

Pin	X10	X11	X12	X13
1	L+ / 24 V DC	Functional Earth	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	No connection	No connection	No connection	No connection
4	No connection	No connection	No connection	No connection
5	0L	2L	4L	6L
6	DQ a.0X	DQ a.2X	DQ a.4X	DQ a.6X
7	DQ a.0	DQ a.2	DQ a.4	DQ a.6
8	No connection	No connection	No connection	No connection
9	1L	3L	5L	7L
10	DQ a.1X	DQ a.3X	DQ a.5X	DQ a.7X
11	DQ a.1	DQ a.3	DQ a.5	DQ a.7

Table A-124 Wiring diagrams for the 16-point digital output SMs

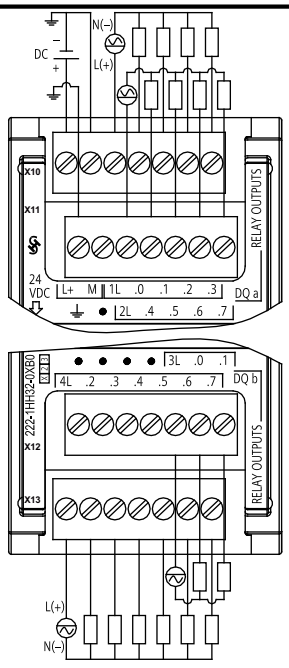
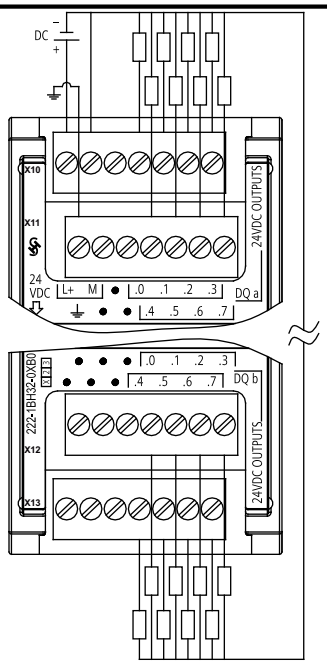
SM 1222 DQ 16 x Relay (6ES7222-1HH32-0XB0)	SM 1222 DQ 16 x 24 V DC (6ES7222-1BH32-0XB0)
	

Table A-125 Connector pin locations for SM 1222 DQ 16 x Relay (6ES7222-1HH32-0XB0)

Pin	X10	X11	X12	X13
1	L+ / 24 V DC	Functional Earth	No connection	4L
2	M / 24 V DC	No connection	No connection	DQ b.2
3	1L	2L	No connection	DQ b.3
4	DQ a.0	DQ a.4	No connection	DQ b.4
5	DQ a.1	DQ a.5	3L	DQ b.5
6	DQ a.2	DQ a.6	DQ b.0	DQ b.6
7	DQ a.3	DQ a.7	DQ b.1	DQ b.7

Table A-126 Connector pin locations for SM 1222 DQ 16 x 24 V DC (6ES7222-1BH32-0XB0)

Pin	X10	X11	X12	X13
1	L+ / 24 V DC	Functional Earth	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	No connection	No connection	No connection	No connection
4	DQ a.0	DQ a.4	DQ b.0	DQ b.4
5	DQ a.1	DQ a.5	DQ b.1	DQ b.5
6	DQ a.2	DQ a.6	DQ b.2	DQ b.6
7	DQ a.3	DQ a.7	DQ b.3	DQ b.7

Table A-127 Wiring diagram for the 16-point digital output 24 V DC sinking SM

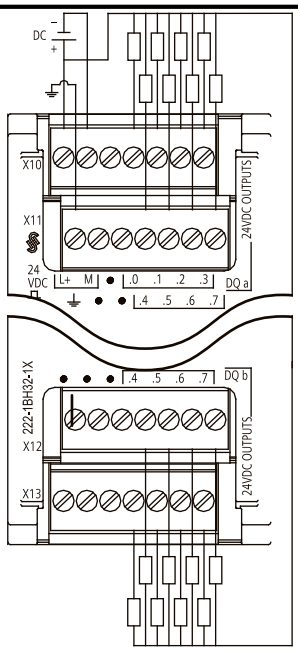
SM 1222 DQ 16 x 24 V DC sinking (6ES7222-1BH32-1XB0)	
	

Table A-128 Connector pin locations for SM 1222 DQ 16 x 24 V DC sinking (6ES7222-1BH32-1XB0)

Pin	X10	X11	X12	X13
1	L+ / 24 V DC	Functional Earth	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	No connection	No connection	No connection	No connection
4	DQ a.0	DQ a.4	DQ b.0	DQ b.4
5	DQ a.1	DQ a.5	DQ b.1	DQ b.5
6	DQ a.2	DQ a.6	DQ b.2	DQ b.6
7	DQ a.3	DQ a.7	DQ b.3	DQ b.7

A.10.4 SM 1223 digital input/output V DC specifications

Table A-129 General specifications

Model	**SM 1223 DI 8 x 24 V DC, DQ 8 x Relay**	**SM 1223 DI 16 x 24 V DC, DQ 16 x Relay**	**SM 1223 DI 8 x 24 V DC, DQ 8 x 24 V DC**	**SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC**	**SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC sinking**
Article number	6ES7223-1PH32-0-XB0	6ES7223-1PL32-0-XB0	6ES7223-1BH32-0-XB0	6ES7223-1BL32-0-XB0	6ES7223-1BL32-1-XB0
Dimensions W x H x D (mm)	45 x 100 x 75	70 x 100 x 75	45 x 100 x 75	70 x 100 x 75	
Weight	230 grams	350 grams	210 grams	310 grams	

Model	SM 1223 DI 8 x 24 V DC, DQ 8 x Relay	SM 1223 DI 16 x 24 V DC, DQ 16 x Relay	SM 1223 DI 8 x 24 V DC, DQ 8 x 24 V DC	SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC	SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC sinking
Power dissipation	5.5 W	10 W	2.5 W	4.5 W	
Current consumption (SM Bus)	145 mA	180 mA	145 mA	185 mA	
Current consumption (24 V DC)	4 mA / Input used 11 mA / Relay coil used		150 mA	200 mA	40 mA

Table A-130 Digital inputs

Model	SM 1223 DI 8 x 24 V DC, DQ 8 x Relay	SM 1223 DI 16 x 24 V DC, DQ 16 x Relay	SM 1223 DI 8 x 24 V DC, DQ 8 x 24 V DC	SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC	SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC sinking
Number of inputs	8	16	8	16	
Type	Sink/Source (IEC Type 1 sink)				
Rated voltage	24 V DC at 4 mA, nominal				
Continuous permissible voltage	30 V DC, max. at 6 mA, max.				
Surge voltage	35 V DC for 0.5 sec.				
Logic 1 signal (min.)	15 V DC at 2.5 mA				
Logic 0 signal (max.)	5 V DC at 1 mA				
Isolation (field side to logic)	707 V DC (type test)				
Isolation groups	2				
Filter times	0.2, 0.4, 0.8, 1.6, 3.2, 6.4, and 12.8 ms, selectable in groups of 4				
Number of inputs on simultaneously	8	• 8 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 16 at 55 °C horizontal or 45 °C vertical	8	16	
Cable length (meters)	500 m shielded, 300 m unshielded				

Table A-131 Digital outputs

Model	SM 1223 DI 8 x 24 V DC, DQ 8 x Relay	SM 1223 DI 16 x 24 V DC, DQ 16 x Relay	SM 1223 DI 8 x 24 V DC, DQ 8 x 24 V DC	SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC	SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC sinking
Number of outputs	8	16	8	16	16
Type	Relay, mechanical		Solid state - MOSFET (sourcing)		Solid state - MOSFET (sinking)
Voltage range	5 to 30 V DC or 5 to 250 V AC		20.4 to 28.8 V DC		
Logic 1 signal at max. current	--		20 V DC, min.		0.5 V DC

Model	**SM 1223 DI 8 x 24 V DC, DQ 8 x Relay**	**SM 1223 DI 16 x 24 V DC, DQ 16 x Relay**	**SM 1223 DI 8 x 24 V DC, DQ 8 x 24 V DC**	**SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC**	**SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC sinking**
Logic 0 signal with 10 KΩ load	--		0.1 V DC, max.		24 V (typical) minus 0.75 V DC
Current (max.)	2.0 A		0.5 A		
Lamp load	30 W DC / 200 W AC		5 W		
ON state contact resistance	0.2 Ω max. when new		0.6 Ω max.		0.5 Ω max
Leakage current per point	--		10 µA max.		75 µA max.
Surge current	7 A with contacts closed		8 A for 100 ms max.		Current limit protected
Overload protection	No				Yes, Current limit protected range 1 A to 3.5 A
Isolation (field side to logic)	1500 V AC (coil to contact) None (coil to logic)		707 V DC (type test)		
Isolation groups	2	4	1		
Current per common	10A	8 A	4 A	8 A	
Inductive clamp voltage	--		L+ minus 48 V, 1 W dissipation		45 V
Switching delay	10 ms max.		50 µs max. off to on 200 µs max. on to off		20 µs max. off to on 350 µs max. on to off
Maximum relay switching frequency	1 Hz		--		
Lifetime mechanical (no load)	10,000,000 open/close cycles		--		
Lifetime contacts at rated load (N.O. contact)	100,000 open/close cycles		--		
Behavior on RUN to STOP	Last value or substitute value (default value 0)				
Control of a digital input	Yes				Yes (sourcing input)
Parallel outputs for redundant load control	Yes (with same common)				

Model	SM 1223 DI 8 x 24 V DC, DQ 8 x Relay	SM 1223 DI 16 x 24 V DC, DQ 16 x Relay	SM 1223 DI 8 x 24 V DC, DQ 8 x 24 V DC	SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC	SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC sinking
Parallel outputs for increased load	No				
Number of outputs on simultaneously	8	• 8 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 16 at 55 °C horizontal or 45 °C vertical	8	16	
Cable length (meters)	500 m shielded, 150 m unshielded				

Table A-132 Wiring diagrams for the digital input V DC/output relay SMs

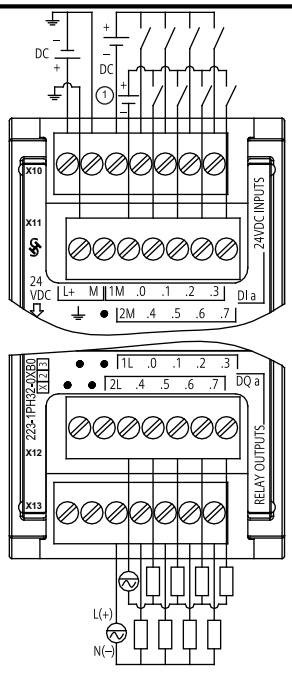
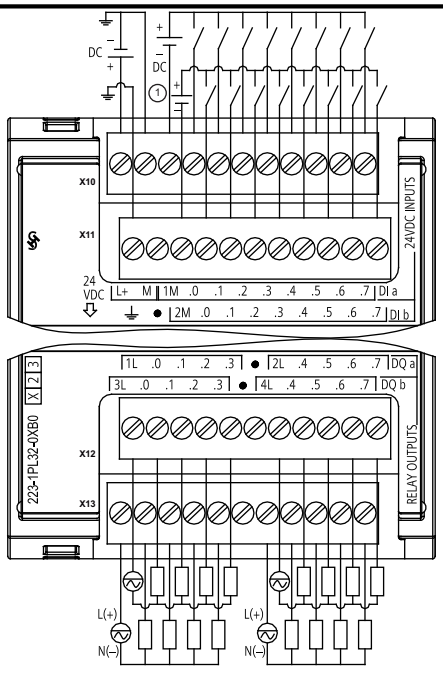
SM 1223 DI 8 x 24 V DC, DQ 8 x Relay (6ES7223-1PH32-0XB0)	SM 1223 DI 16 x 24 V DC, DQ 16 x Relay (6ES7223-1PL32-0XB0)	Notes
		1 For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

Table A-133 Connector Pin Locations for SM 1223 DI 8 x 24 V DC, DQ 8 x Relay (6ES7223-1PH32-0XB0)

Pin	X10	X11	X12	X13
1	L+ / 24 V DC	Functional Earth	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	1M	2M	1L	2L
4	DI a.0	DI a.4	DQ a.0	DQ a.4
5	DI a.1	DI a.5	DQ a.1	DQ a.5
6	DI a.2	DI a.6	DQ a.2	DQ a.6
7	DI a.3	DI a.7	DQ a.3	DQ a.7

Table A-134 Connector Pin Locations for SM 1223 DI 16 x 24 V DC, DQ 16 x Relay (6ES7223-1PL32-0XB0)

Pin	X10	X11	X12	X13
1	L+ / 24 V DC	Functional Earth	1L	3L
2	M / 24 V DC	No connection	DQ a.0	DQ b.0
3	1M	2M	DQ a.1	DQ b.1
4	DI a.0	DI b.0	DQ a.2	DQ b.2
5	DI a.1	DI b.1	DQ a.3	DQ b.3
6	DI a.2	DI b.2	No connection	No connection
7	DI a.3	DI b.3	2L	4L
8	DI a.4	DI b.4	DQ a.4	DQ b.4
9	DI a.5	DI b.5	DQ a.5	DQ b.5
10	DI a.6	DI b.6	DQ a.6	DQ b.6
11	DI a.7	DI b.7	DQ a.7	DQ b.7

Table A-135 Wiring diagrams for the digital input V DC/output SMs

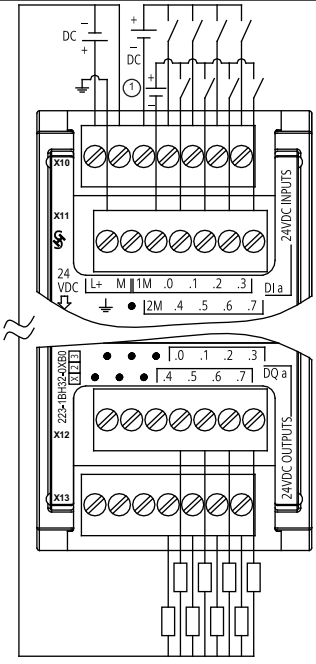
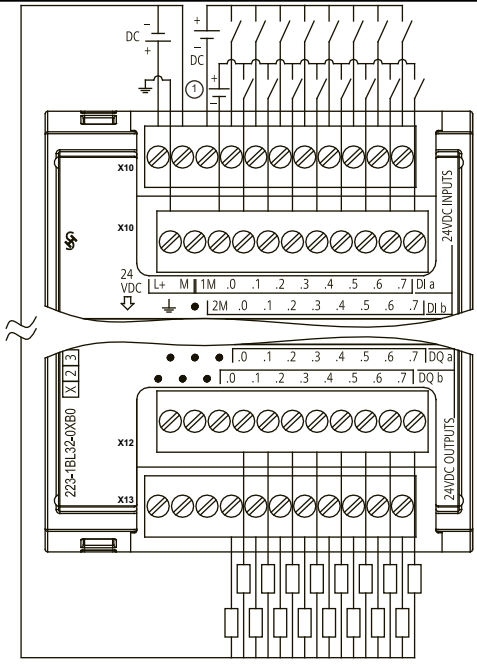
SM 1223 DI 8 x 24 V DC, DQ 8 x 24 V DC (6ES7223-1BH32-0XB0)	SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC (6ES7223-1BL32-0XB0)	Notes
		① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

Table A-136 Connector Pin Locations for SM 1223 DI 8 x 24 V DC, DQ 8 x 24 V DC (6ES7223-1BH32-0XB0)

Pin	X10	X11	X12	X13
1	L+ / 24 V DC	Functional Earth	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	1M	2M	No connection	No connection
4	DI a.0	DI a.4	DQ a.0	DQ a.4
5	DI a.1	DI a.5	DQ a.1	DQ a.5
6	DI a.2	DI a.6	DQ a.2	DQ a.6
7	DI a.3	DI a.7	DQ a.3	DQ a.7

Table A-137 Connector Pin Locations for SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC (6ES7223-1BL32-0XB0)

Pin	X10	X11	X12	X13
1	L+ / 24 V DC	Functional Earth	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	1M	2M	No connection	No connection
4	DI a.0	DI b.0	DQ a.0	DQ b.0
5	DI a.1	DI b.1	DQ a.1	DQ b.1
6	DI a.2	DI b.2	DQ a.2	DQ b.2
7	DI a.3	DI b.3	DQ a.3	DQ b.3
8	DI a.4	DI b.4	DQ a.4	DQ b.4

Pin	X10	X11	X12	X13
9	DI a.5	DI b.5	DQ a.5	DQ b.5
10	DI a.6	DI b.6	DQ a.6	DQ b.6
11	DI a.7	DI b.7	DQ a.7	DQ b.7

Table A-138 Wiring diagram for the digital input V DC/output SMs

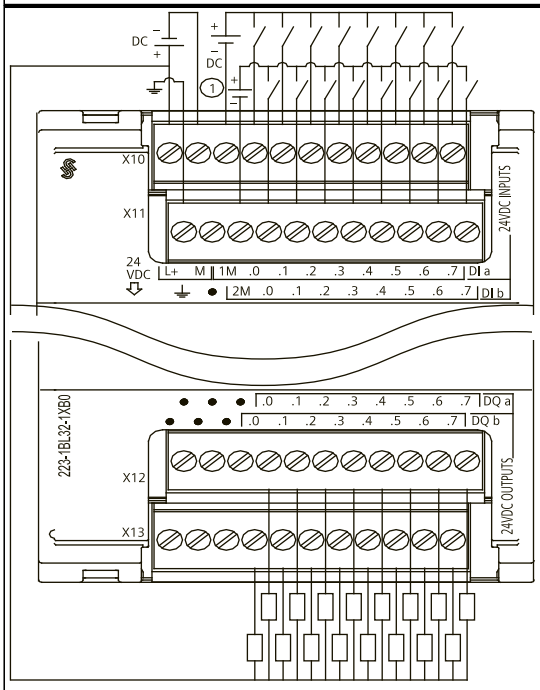
SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC sinking (6ES7223-1BL32-1XB0)	Notes
	1 For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

Table A-139 Connector Pin Locations for SM 1223 DI 16 x 24 V DC, DQ 16 x 24 V DC sinking (6ES7223-1BL32-1XB0)

Pin	X10	X11	X12	X13
1	L+ / 24 V DC	Functional Earth	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	1M	2M	No connection	No connection
4	DI a.0	DI b.0	DQ a.0	DQ b.0
5	DI a.1	DI b.1	DQ a.1	DQ b.1
6	DI a.2	DI b.2	DQ a.2	DQ b.2
7	DI a.3	DI b.3	DQ a.3	DQ b.3
8	DI a.4	DI b.4	DQ a.4	DQ b.4
9	DI a.5	DI b.5	DQ a.5	DQ b.5
10	DI a.6	DI b.6	DQ a.6	DQ b.6
11	DI a.7	DI b.7	DQ a.7	DQ b.7

A.10.5 SM 1223 digital input/output V AC specifications

Table A-140 General specifications

Model	SM 1223 DI 8 x120/230 V AC / DQ 8 x Relay
Article number	6ES7223-1QH32-0XB0
Dimensions W x H x D (mm)	45 x 100 x 75 mm
Weight	190 grams
Power dissipation	7.5 W
Current consumption (SM Bus)	120 mA
Current consumption (24 V DC)	11 mA per output when on

Table A-141 Digital inputs

Model	SM 1223 DI 8 x 120/230 V AC / DQ 8 x Relay
Number of inputs	8
Type	IEC Type 1
Rated voltage	120 V AC at 6 mA, 230 V AC at 9 mA
Continuous permissible voltage	264 V AC
Surge voltage	--
Logic 1 signal (min.)	79 V AC at 2.5 mA
Logic 0 signal (max.)	20 V AC at 1 mA
Leakage current (max.)	1 mA
Isolation (field side to logic)	1500 V AC
Isolation groups[1]	4
Input delay times	Typical: 0.2 to 12.8 ms, user selectable Maximum: -
Connection of 2 wire proximity sensor (Bero) (max.)	1 mA
Cable length	Unshielded: 300 meters Shielded: 500 meters
Number of inputs on simultaneously	8

[1] Channels within a group must be of the same phase.

Table A-142 Digital outputs

Model	SM 1223 DI 8 x 120/230 V AC / DQ 8 x Relay
Number of outputs	8
Type	Relay, mechanical
Voltage range	5 to 30 V DC or 5 to 250 V AC
Logic 1 signal at max. current	--
Logic 0 signal with 10K Ω load	--
Current (max.)	2.0 A
Lamp load	30 W DC / 200 W AC
ON state contact resistance	0.2 Ω max. when new
Leakage current per point	--

Model	SM 1223 DI 8 x 120/230 V AC / DQ 8 x Relay
Surge current	7 A with contacts closed
Overload protection	No
Isolation (field side to logic)	1500 V AC (coil to contact) None (coil to logic)
Isolation groups	2
Current per common (max.)	10 A
Inductive clamp voltage	--
Switching delay (max.)	10 ms
Maximum relay switching frequency	1 Hz
Lifetime mechanical (no load)	10,000,000 open/close cycles
Lifetime contacts at rated load	100,000 open/close cycles
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes
Parallel outputs for redundant load control	Yes (with same common)
Parallel outputs for increased load	No
Number of outputs on simultaneously	• 4 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 8 at 55 °C horizontal or 45 °C vertical
Cable length (meters)	500 m shielded, 150 m unshielded

Table A-143 SM 1223 DI 8 x 120/230 V AC, DQ 8 x Relay (6ES7223-1QH32-0XB0)

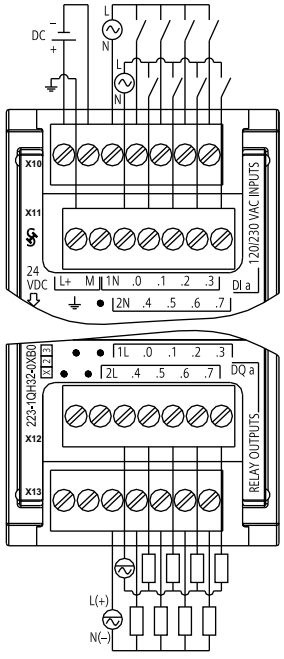


Table A-144 Connector Pin Locations for SM 1223 DI 8 x 120/240 V AC, DQ 8 x Relay (6ES7223-1QH32-0XB0)

Pin	X10	X11	X12	X13
1	L+ / 24 V DC	Functional Earth	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	1N	2N	1L	2L
4	DI a.0	DI a.4	DQ a.0	DQ a.4
5	DI a.1	DI a.5	DQ a.1	DQ a.5
6	DI a.2	DI a.6	DQ a.2	DQ a.6
7	DI a.3	DI a.7	DQ a.3	DQ a.7

A.11 Analog signal modules (SMs)

A.11.1 SM 1231 analog input module specifications

Table A-145 General specifications

Model	SM 1231 AI 4 x 13 bit	SM 1231 AI 8 x 13 bit	SM 1231 AI 4 x 16 bit
Article number	6ES7231-4HD32-0XB0	6ES7231-4HF32-0XB0	6ES7231-5ND32-0XB0
Dimensions W x H x D (mm)	45 x 100 x 75		
Weight	180 grams		
Power dissipation	2.2 W	2.3 W	2.0 W
Current consumption (SM Bus)	80 mA	90 mA	80 mA
Current consumption (24 V DC)	45 mA	60 mA	65 mA

Table A-146 Analog inputs

Model	SM 1231 AI 4 x 13 bit	SM 1231 AI 8 x 13 bit	SM 1231 AI 4 x 16 bit
Number of inputs	4	8	4
Type	Voltage or current (differential): Selectable in groups of 2		Voltage or current (differential)
Range	±10 V, ±5 V, ±2.5 V, 0 to 20 mA, or 4 mA to 20 mA		±10 V, ±5 V, ±2.5 V, ±1.25 V, 0 to 20 mA or 4 mA to 20 mA
Full scale range (data word)	-27648 to 27648 voltage / 0 to 27648 current		
Overshoot/undershoot range (data word) Refer to the section on analog input ranges for voltage and current (Page 1195).	Voltage: 32511 to 27649 / -27649 to -32,512 Current: 32511 to 27649 / 0 to -4864		
Overflow/underflow (data word) Refer to the section on input ranges for voltage and current (Page 1195).	Voltage: 32767 to 32512 / -32513 to -32768 Current 0 to 20 mA: 32767 to 32512 / -4865 to -32768 Current 4 to 20 mA: 32767 to 32512 (values below -4864 indicate open wire)		
Resolution1	12 bits + sign bit		15 bits + sign bit

[1] Voltages outside the operational range applied to one channel may cause interference on other channels.

Model	SM 1231 AI 4 x 13 bit	SM 1231 AI 8 x 13 bit	SM 1231 AI 4 x 16 bit
Maximum withstand voltage/current	±35 V / ±40 mA		
Smoothing	None, weak, medium, or strong Refer to the section on step response times (Page 1195).		
Noise rejection	400, 60, 50, or 10 Hz Refer to the section on sample rates (Page 1195).		
Input impedance Before parameterization Voltage Current	≥ 1 MΩ ≥ 9 MΩ, FS 06 and above ≥ 1 MΩ ≥ 270 Ω, < 290 Ω		≥ 1 MΩ ≥ 1 MΩ < 315 Ω, > 280 Ω
Isolation Field side to logic Logic to 24 V DC Field side to 24 V DC Channel to channel	None		707 V DC (type test) 707 V DC (type test) 500 V DC (type test) None
Accuracy (25 °C / -20 to 60 °C)	±0.1% / ±0.2% of full scale		±0.1% / ±0.3% of full scale
Measuring principle	Actual value conversion		
Common mode rejection	40 dB, DC to 60 Hz		
Operational signal range[1]	Signal plus common mode voltage must be less than +12 V and greater than -12 V		
Cable length (meters)	100 m, twisted and shielded		

[1] Voltages outside the operational range applied to one channel may cause interference on other channels.

Table A-147 Diagnostics

Model	SM 1231 AI 4 x 13 bit	SM 1231 AI 8 x 13 bit	SM 1231 AI 4 x 16 bit
Overflow/underflow	Yes		
24 V DC low voltage	Yes		
Open wire	4 to 20 mA range only (if input is below -4864; 1.185 mA)		

SM 1231 current measurement

You can implement current measurement with either a 2-wire transducer or 4-wire transducer as shown in the following figure:

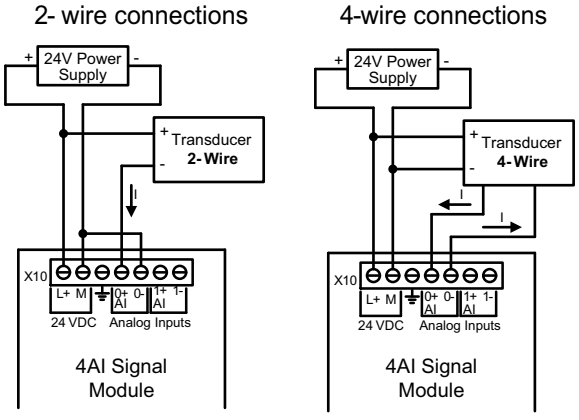


Table A-148 Wiring diagrams for the analog input SMs

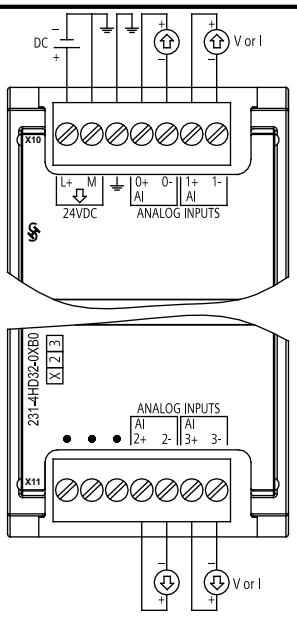
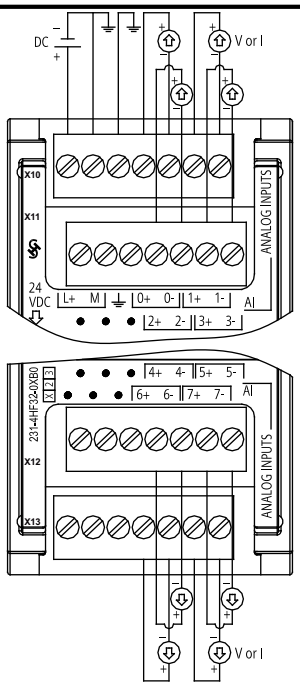
SM 1231 AI 4 x 13 bit (6ES7231-4HD32-0XB0)	SM 1231 AI 8 x 13 bit (6ES7231-4HF32-0XB0)
	
Note: Connectors must be gold. See Appendix C, Spare Parts for article number.	

Table A-149 Connector pin locations for SM 1231 AI 4 x 13 bit (6ES7231-4HD32-0XB0)

Pin	X10 (gold)	X11 (gold)
1	L+ / 24 V DC	No connection
2	M / 24 V DC	No connection
3	Functional Earth	No connection
4	AI 0+	AI 2+
5	AI 0-	AI 2-
6	AI 1+	AI 3+
7	AI 1-	AI 3-

Table A-150 Connector pin locations for SM 1231 AI 8 x 13 bit (6ES7231-4HF32-0XB0)

Pin	X10 (gold)	X11 (gold)	X12 (gold)	X13 (gold)
1	L+ / 24 V DC	No connection	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	Functional Earth	No connection	No connection	No connection
4	AI 0+	AI 2+	AI 4+	AI 6+
5	AI 0-	AI 2-	AI 4-	AI 6-
6	AI 1+	AI 3+	AI 5+	AI 7+
7	AI 1-	AI 3-	AI 5-	AI 7-

Table A-151 Wiring diagram for the analog input SM

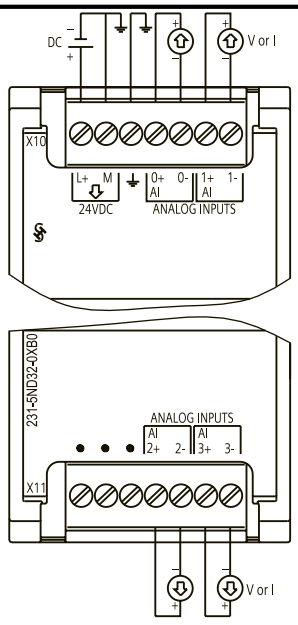
SM 1231 AI 4 x 16 bit (6ES7231-5ND32-0XB0)	
	
Note: Connectors must be gold. See Appendix C, Spare Parts for article number.	

Table A-152 Connector pin locations for SM 1231 AI 4 x 16 bit (6ES7231-5ND32-0XB0)

Pin	X10 (gold)	X11 (gold)
1	L+ / 24 V DC	No connection
2	M / 24 V DC	No connection
3	Functional Earth	No connection
4	AI 0+	AI 2+
5	AI 0-	AI 2-
6	AI 1+	AI 3+
7	AI 1-	AI 3-

NOTE

Unused voltage input channels should be shorted.

Unused current input channels should be set to the 0 to 20 mA range and/or disable broken wire error reporting.

Inputs configured for current mode will not conduct loop current unless the module is powered and configured.

Current input channels will not operate unless external power is supplied to the transmitter.

A.11.2 SM 1232 analog output module specifications

Table A-153 General specifications

Technical data	SM 1232 AQ 2 x 14 bit	SM 1232 AQ 4 x 14 bit
Article number	6ES7232-4HB32-0XB0	6ES7232-4HD32-0XB0
Dimensions W x H x D (mm)	45 x 100 x 75	
Weight	180 grams	
Power dissipation	1.8 W	2.0 W
Current consumption (SM Bus)	80 mA	
Current consumption (24 V DC)	45 mA (no load)	

Table A-154 Analog outputs

Technical data	SM 1232 AQ 2 x 14 bit	SM 1232 AQ 4 x 14 bit
Number of outputs	2	4
Type	Voltage or current	
Range	±10 V, 0 to 20 mA, or 4 mA to 20 mA	
Resolution	Voltage: 14 bits Current: 13 bits	
Full scale range (data word)	Voltage: -27,648 to 27,648 ; Current: 0 to 27,648 Refer to the output ranges for voltage and current (Page 1196).	
Accuracy (25 °C / -20 to 60 °C)	±0.3% / ±0.6% of full scale	
Settling time (95% of new value)	Voltage: 300 µs (R), 750 µs (1 uF) Current: 600 µs (1 mH), 2 ms (10 mH)	
Load impedance	Voltage: ≥ 1000 Ω Current: ≤ 600 Ω	
Maximum output short circuit current	Voltage mode: ≤ 24 mA Current mode: ≥ 38.5 mA	
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Isolation (field side to logic)	none	
Isolation (24 V to output)	none	
Cable length (meters)	100 m twisted and shielded	

Table A-155 Diagnostics

Technical data	SM 1232 AQ 2 x 14 bit	SM 1232 AQ 4 x 14 bit
Overflow/underflow	Yes	
Short to ground (voltage mode only)	Yes	
Wire break (current mode only)[1]	Yes	
24 V DC low voltage[2]	Yes	

[1] Short circuit detection is only possible when the output voltage is less than -0.5 V or greater than +0.5 V.

[2] Wire break detection is only possible when the output current is greater than 1 mA.

Table A-156 Wiring diagrams for the analog output SMs

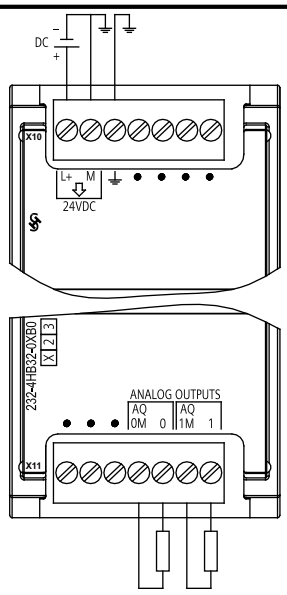
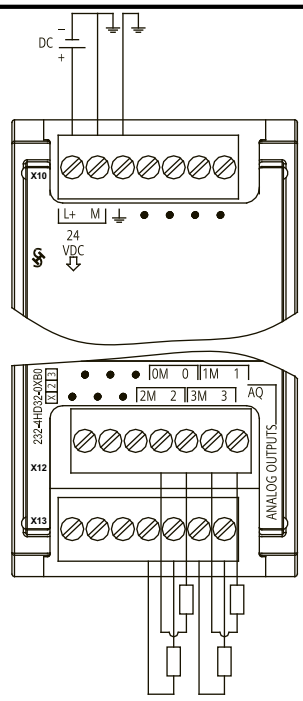
SM 1232 AQ 2 x 14 bit (6ES7232-4HB32-0XB0)	SM 1232 AQ 4 x 14 bit (6ES7232-4HD32-0XB0)
	
Note: Connectors must be gold. See Appendix C, Spare Parts for article number.	

Table A-157 Connector pin locations for SM 1232 AQ 2 x 14 bit (6ES7232-4HB32-0XB0)

Pin	X10 (gold)	X11 (gold)
1	L+ / 24 V DC	No connection
2	M / 24 V DC	No connection
3	Functional Earth	No connection
4	No connection	AQ 0M
5	No connection	AQ 0
6	No connection	AQ 1M
7	No connection	AQ 1

Table A-158 Connector pin locations for SM 1232 AQ 4 x 14 bit (6ES7232-4HD32-0XB0)

Pin	X10 (gold)	X12 (gold)	X13 (gold)
1	L+ / 24 V DC	No connection	No connection
2	M / 24 V DC	No connection	No connection
3	Functional Earth	No connection	No connection
4	No connection	AQ 0M	AQ 2M
5	No connection	AQ 0	AQ 2
6	No connection	AQ 1M	AQ 3M
7	No connection	AQ 1	AIQ 3

A.11.3 SM 1234 analog input/output module specifications

Table A-159 General specifications

Technical data	SM 1234 AI 4 x 13 bit / AQ 2 x 14 bit
Article number	6ES7234-4HE32-0XB0
Dimensions W x H x D (mm)	45 x 100 x 75
Weight	220 grams
Power dissipation	2.4 W
Current consumption (SM Bus)	80 mA
Current consumption (24 V DC)	60 mA (no load)

Table A-160 Analog inputs

Model	SM 1234 AI 4 x 13 bit / AQ 2 x 14 bit
Number of inputs	4
Type	Voltage or Current (differential): Selectable in groups of 2
Range	±10 V, ±5 V, ±2.5 V, 0 to 20 mA, or 4 mA to 20 mA
Full scale range (data word)	-27648 to 27648
Overshoot/undershoot range (data word)	Voltage: 32511 to 27649 / -27649 to -32512 Current: 32511 to 27649 / 0 to -4864 Refer to the section on input ranges for voltage and current (Page 1195).
Overflow/underflow (data word)	Voltage: 32767 to 32512 / -32513 to -32768 Current: 32767 to 32512 / -4865 to -32768 Refer to the section on input ranges for voltage and current (Page 1195).
Resolution	12 bits + sign bit
Maximum withstand voltage/current	±35 V / ±40 mA
Smoothing	None, weak, medium, or strong Refer to the section on step response times (Page 1195).
Noise rejection	400, 60, 50, or 10 Hz Refer to the section on sample rates (Page 1195).
Input impedance	≥ 9 MΩ, FS 07 and above ≥ 1 MΩ (voltage) / ≥ 270 Ω, < 290 Ω (current)
Isolation (field side to logic)	None
Accuracy (25 °C / -20 to 60 °C)	±0.1% / ±0.2% of full scale
Analog to digital conversion time	625 µs (400 Hz rejection)
Common mode rejection	40 dB, DC to 60 Hz
Operational signal range[1]	Signal plus common mode voltage must be less than +12 V and greater than -12 V
Cable length (meters)	100 m, twisted and shielded

[1] Voltages outside the operational range applied to one channel may cause interference on other channels.

Table A-161 Analog outputs

Technical data	SM 1234 AI 4 x 13 bit / AQ 2 x 14 bit
Number of outputs	2
Type	Voltage or current
Range	±10 V or 0 to 20 mA or 4 mA to 20 mA
Resolution	Voltage: 14 bits ; Current: 13 bits
Full scale range (data word)	Voltage: -27648 to 27648; Current: 0 to 27648 Refer to the section on output ranges for voltage and current (Page 1196).
Accuracy (25 °C / -20 to 60 °C)	±0.3% / ±0.6% of full scale
Settling time (95% of new value)	Voltage: 300 µs (R), 750 µs (1 uF) Current: 600 µs (1 mH), 2 ms (10 mH)
Load impedance	Voltage: ≥ 1000 Ω Current: ≤ 600 Ω
Maximum output short circuit current	Voltage mode: ≤ 24 mA Current mode: ≥ 38.5 mA
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Isolation (field side to logic)	none
Isolation (24 V to output)	none
Cable length (meters)	100 m twisted and shielded

Table A-162 Diagnostics

Model	SM 1234 AI 4 x 13 bit / AQ 2 x 14 bit
Overflow/underflow	Yes
Short to ground (voltage mode only)[1]	Yes on outputs
Wire break (current mode only)[2]	Yes on outputs
24 V DC low voltage	Yes

1 Short circuit detection is only possible when the output voltage is less than -0.5 V or greater than +0.5 V.

2 Wire break detection is only possible when the output current is greater than 1 mA.

SM 1234 current measurement

You can implement current measurement with either a 2-wire transducer or 4-wire transducer as shown in the following figure:

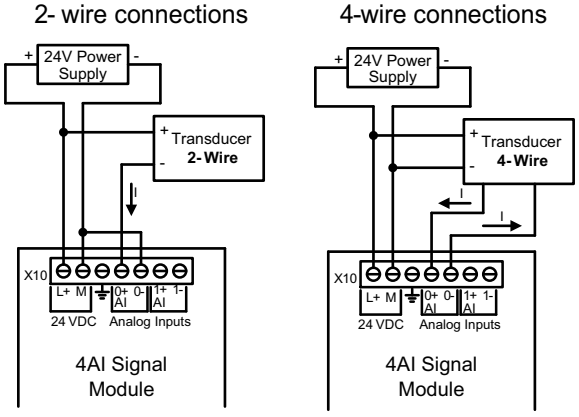


Table A-163 Wiring diagrams for the analog input/output SM

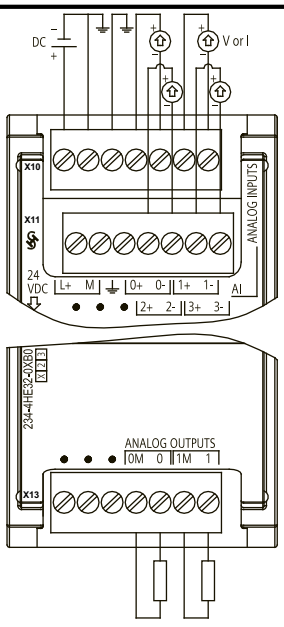
SM 1234 AI 4 x 13 Bit / AQ 2 x 14 bit (6ES7234-4HE32-0XB0)	
	
Note: Connectors must be gold. See Appendix C, Spare Parts for article number.	

Table A-164 Connector pin locations for SM 1234 AI 4 x 13 Bit / AQ 2 x 14 bit (6ES7234-4HE32-0XB0)

Pin	X10 (gold)	X11 (gold)	X13 (gold)
1	L+ / 24 V DC	No connection	No connection
2	M / 24 V DC	No connection	No connection
3	Functional Earth	No connection	No connection
4	AI 0+	AI 2+	AQ 0M
5	AI 0-	AI 2-	AQ 0
6	AI 1+	AI 3+	AQ 1M
7	AI 1-	AI 3-	AQ 1

NOTE

Unused voltage input channels should be shorted.

Unused current input channels should be set to the 0 to 20 mA range and/or disable broken wire error reporting.

Inputs configured for current mode will not conduct loop current unless the module is powered and configured.

Current input channels will not operate unless external power is supplied to the transmitter.

A.11.4 Step response of the analog inputs

Table A-165 Step response (ms), 0 to full-scale measured at 95%

Smoothing selection (sample averaging)	Noise reduction/rejection frequency (Integration time selection)			
	400 Hz (2.5 ms)	60 Hz (16.6 ms)	50 Hz (20 ms)	10 Hz (100 ms)
None (1 cycle): No averaging	4 ms	18 ms	22 ms	100 ms
Weak (4 cycles): 4 samples	9 ms	52 ms	63 ms	320 ms
Medium (16 cycles): 16 samples	32 ms	203 ms	241 ms	1200 ms
Strong (32 cycles): 32 samples	61 ms	400 ms	483 ms	2410 ms

A.11.5 Sample time and update times for the analog inputs

Table A-166 Sample and module update times for all channels

Rejection frequency (Integration time)	Sample and module update times for all channels			
	400 Hz (2.5 ms)	60 Hz (16.6 ms)	50 Hz (20 ms)	10 Hz (100 ms)
4-channel x 13 bit SM	0.625 ms	4.17 ms	5 ms	25 ms
8-channel x 13 bit SM	1.25 ms	4.17 ms	5 ms	25 ms
4-channel x 16 bit SM	0.417 ms	0.397 ms	0.400 ms	0.400 ms

A.11.6 Measurement ranges of the analog inputs for voltage and current (SB and SM)

Table A-167 Analog input representation for voltage (SB and SM)

System		Voltage Measuring Range				
Decimal	Hexadecimal	±10 V	±5 V	±2.5 V	±1.25 V	
32767	7FFF[1]	11.851 V	5.926 V	2.963 V	1.481 V	Overflow
32512	7F00					
32511	7EFF	11.759 V	5.879 V	2.940 V	1.470 V	Overshoot range
27649	6C01					
27648	6C00	10 V	5 V	2.5 V	1.250 V	Rated range
20736	5100	7.5 V	3.75 V	1.875 V	0.938 V	
1	1	361.7 µV	180.8 µV	90.4 µV	45.2 µV	
0	0	0 V	0 V	0 V	0 V	
-1	FFFF					
-20736	AF00	-7.5 V	-3.75 V	-1.875 V	-0.938 V	
-27648	9400	-10 V	-5 V	-2.5 V	-1.250 V	
-27649	93FF					Undershoot range
-32512	8100	-11.759 V	-5.879 V	-2.940 V	-1.470 V	
-32513	80FF					Underflow
-32768	8000	-11.851 V	-5.926 V	-2.963 V	-1.481 V	

[1] 7FFF can be returned for one of the following reasons: overflow (as noted in this table), before valid values are available (for example immediately upon a power up), or if a wire break is detected.

Table A-168 Analog input representation for current (SB and SM)

System		Current measuring range		
Decimal	**Hexadecimal**	**0 mA to 20 mA**	**4 mA to 20 mA**	
32767	7FFF	> 23.52 mA	> 22.81 mA	Overflow
32511	7EFF	23.52 mA	22.81 mA	Overshoot range
27649	6C01			
27648	6C00	20 mA	20 mA	Nominal range
20736	5100	15 mA	16 mA	
1	1	723.4 nA	4 mA + 578.7 nA	
0	0	0 mA	4 mA	
-1	FFFF			Undershoot range
-4864	ED00	-3.52 mA	1.185 mA	
32767[1]	7FFF		< 1.185 mA	Wire break (4 to 20 mA) (Page 1083)
-32768	8000	< -3.52 mA		Underflow (0 to 20 mA)

[1] The wire break value of 32767 (16#7FFF) is always returned regardless of the state of the wire break alarm.

A.11.7 Measurement ranges of the analog outputs for voltage and current (SB and SM)

Table A-169 Analog output representation for voltage (SB and SM)

System		Voltage Output Range	
Decimal	**Hexadecimal**	**± 10 V**	
32767	7FFF	See note 1	Overflow
32512	7F00	See note 1	
32511	7EFF	11.76 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range
20736	5100	7.5 V	
1	1	361.7 µ V	
0	0	0 V	
-1	FFFF	-361.7 µ V	
-20736	AF00	-7.5 V	
-27648	9400	-10 V	
-27649	93FF		Undershoot range
-32512	8100	-11.76 V	
-32513	80FF	See note 1	Underflow
-32768	8000	See note 1	

[1] In an overflow or underflow condition, analog outputs will take on the substitute value of the STOP mode.

Table A-170 Analog output representation for current (SB and SM)

System		Current output range		
Decimal	**Hexadecimal**	**0 mA to 20 mA**	**4 mA to 20 mA**	
32767	7FFF	See note 1	See note 1	Overflow
32512	7F00	See note 1	See note 1	
32511	7EFF	23.52 mA	22.81 mA	Overshoot range
27649	6C01			
27648	6C00	20 mA	20 mA	Rated range
20736	5100	15 mA	16 mA	
1	1	723.4 nA	4 mA + 578.7 nA	
0	0	0 mA	4mA	
-1	FFFF		4 mA to 578.7 nA	Undershoot range
-6912	E500		0 mA	
-6913	E4FF			Not possible. Output value limited to 0 mA.
-32512	8100			
-32513	80FF	See note 1	See note 1	Underflow
-32768	8000	See note 1	See note 1	

[1] In an overflow or underflow condition, analog outputs will take on the substitute value of the STOP mode.

A.12 Thermocouple and RTD signal modules (SMs)

A.12.1 SM 1231 Thermocouple

Table A-171 General specifications

Model	**SM 1231 AI 4 x 16 bit TC**	**SM 1231 AI 8 x 16 bit TC**
Article number	6ES7231-5QD32-0XB0	6ES7231-5QF32-0XB0
Dimensions W x H x D (mm)	45 x 100 x 75	
Weight	180 grams	190 grams
Power dissipation	1.5 W	
Current consumption (SM Bus)	80 mA	
Current consumption (24 V DC) [1]	40 mA	

[1] 20.4 to 28.8 V DC (Class 2, Limited Power, or sensor power from PLC)

Table A-172 Analog inputs

Model		**SM 1231 AI 4 x 16 bit TC**	**SM 1231 AI 8 x 16 bit TC**
Number of inputs		4	8
Range Nominal range (data word) Overrange/underrange (data word) Overflow/underflow (data word)		See Thermocouple selection table (Page 1201).	
Resolution	Temperature	0.1 °C/0.1 °F	
	Voltage	15 bits plus sign	

Model		SM 1231 AI 4 x 16 bit TC	SM 1231 AI 8 x 16 bit TC
Maximum withstand voltage		± 35 V	
Noise rejection		85 dB for selected filter setting (10 Hz, 50 Hz, 60 Hz or 400 Hz)	
Common mode rejection		> 120 dB at 120 V AC	
Impedance		≥ 10 MΩ	
Isolation	Field to logic	707 VDC (type test)	
	Field to 24 V DC	707 V DC (type test)	
	24 V DC to logic	707 V DC (type test)	
Channel to channel		120 V AC	
Accuracy		See Thermocouple selection table (Page 1201).	
Repeatability		±0.05% FS	
Measuring principle		Integrating	
Module update time		See Noise reduction selection table (Page 1201).	
Cold junction error		±1.5 °C	
Cable length (meters)		100 meters to sensor max.	
Wire resistance		100 Ω max.	

Table A-173 Diagnostics

Model	SM 1231 AI 4 x 16 bit TC	SM 1231 AI 8 x 16 bit TC
Overflow/underflow [1]	Yes	
Wire break [2, 3]	Yes	
24 V DC low voltage [1]	Yes	

[1] The overflow, underflow and low voltage diagnostic alarm information will be reported in the analog data values even if the alarms are disabled in the module configuration.

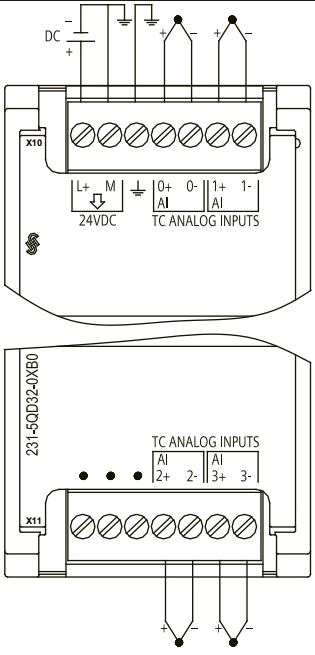
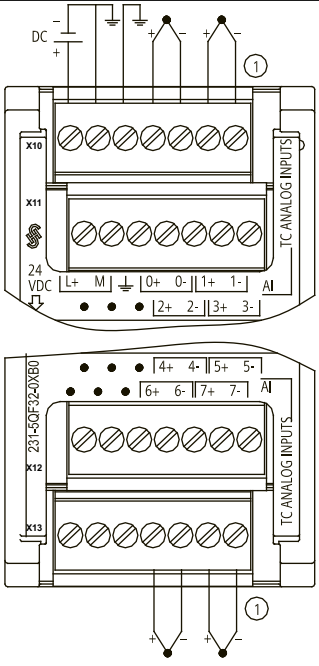
[2] When wire break alarm is disabled and an open wire condition exists in the sensor wiring, the module may report random values.

[3] The module performs wire break testing every 6 seconds, which extends the update time by 9 ms for each enable channel once every 6 seconds.

The SM 1231 Thermocouple (TC) analog signal module measures the value of voltage connected to the module inputs. The temperature measurement type can be either "Thermocouple" or "Voltage".

- "Thermocouple": The value will be reported in degrees multiplied by ten (for example, 25.3 degrees will be reported as decimal 253).
- "Voltage": The nominal range full scale value will be decimal 27648.

Table A-174 Wiring diagrams for the thermocouple SMs

SM 1231 AI 4 x TC 16 bit (6ES7231-5QD32-0XB0)	SM 1231 AI 8 x TC bit (6ES7231-5QF32-0XB0)
	
Note: Connectors must be gold. See Appendix C, Spare Parts for article number.	

① TC 2, 3, 4, and 5 not shown connected for clarity.

Table A-175 Connector pin locations for SM 1231 AI 4 x TC 16 bit (6ES7231-5QD32-0XB0)

Pin	X10 (gold)	X11 (gold)
1	L+ / 24 V DC	No connection
2	M / 24 V DC	No connection
3	Functional Earth	No connection
4	AI 0+ /TC	AI 2+ /TC
5	AI 0- /TC	AI 2- /TC
6	AI 1+ /TC	AI 3+ /TC
7	AI 1- /TC	AI 3- /TC

Table A-176 Connector Pin Locations for SM 1231 AI 8 x TC bit (6ES7231-5QF32-0XB0)

Pin	X10 (gold)	X11 (gold)	X12 (gold)	X13 (gold)
1	L+ / 24 V DC	No connection	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	Functional Earth	No connection	No connection	No connection
4	AI 0+ /TC	AI 2+ /TC	AI 4+ /TC	AI 6+ /TC
5	AI 0- /TC	AI 2- /TC	AI 4- /TC	AI 6- /TC
6	AI 1+ /TC	AI 3+ /TC	AI 5+ /TC	AI 7+ /TC
7	AI 1- /TC	AI 3- /TC	AI 5- /TC	AI 7- /TC

NOTE

Unused analog inputs should be shorted.

The thermocouple unused channels can be deactivated. No error will occur if an unused channel is deactivated.

A.12.1.1 Basic operation for a thermocouple

Thermocouples are formed whenever two dissimilar metals are electrically bonded to each other. A voltage is generated that is proportional to the junction temperature. This voltage is small; one microvolt could represent many degrees. Measuring the voltage from a thermocouple, compensating for extra junctions, and then linearizing the result forms the basis of temperature measurement using thermocouples.

When you connect a thermocouple to the SM 1231 Thermocouple module, the two dissimilar metal wires are attached to the module at the module signal connector. The place where the two dissimilar wires are attached to each other forms the sensor thermocouple.

Two more thermocouples are formed where the two dissimilar wires are attached to the signal connector. The connector temperature causes a voltage that adds to the voltage from the sensor thermocouple. If this voltage is not corrected, then the temperature reported will deviate from the sensor temperature.

Cold junction compensation is used to compensate for the connector thermocouple. Thermocouple tables are based on a reference junction temperature, usually zero degrees Celsius. The cold junction compensation compensates the connector to zero degrees Celsius. The cold junction compensation restores the voltage added by the connector thermocouples. The temperature of the module is measured internally, and then converted to a value to be added to the sensor conversion. The corrected sensor conversion is then linearized using the thermocouple tables.

For optimum operation of the cold junction compensation, the thermocouple module must be located in a thermally stable environment. Slow variation (less than 0.1 °C/minute) in ambient module temperature is correctly compensated within the module specifications. Air movement across the module will also cause cold junction compensation errors.

If better cold junction error compensation is needed, an external iso-thermal terminal block may be used. The thermocouple module provides for use of a 0 °C referenced or 50 °C referenced terminal block.

A.12.1.2 Selection tables for the SM 1231 thermocouple

The ranges and accuracy for the different thermocouple types supported by the SM 1231 Thermocouple signal module are shown in the table below.

Table A-177 Thermocouple selection table

Type	Under-range minimum[1]	Nominal range low limit	Nominal range high limit	Over-range maximum[2]	Normal range [3, 4] accuracy @ 25 °C	Normal range [1, 2, 6] accuracy -20 °C to 60 °C
J	-210.0 °C	-150.0 °C	1200.0 °C	1450.0 °C	±0.3 °C	±0.6 °C
	-346.0 °F	-238.0 °F	2192.0 °F	2642.0 °F	±0.5 °F	±1.1 °F
K	-270.0 °C	-200.0 °C	1372.0 °C	1622.0 °C	±0.4 °C	±1.0 °C
	-454.0 °F	-328.0 °F	2501.6 °F	2951.6 °F	±0.7 °F	±1.8 °F
T	-270.0 °C	-200.0 °C	400.0 °C	540.0 °C	±0.5 °C	±1.0 °C
	-454.0 °F	-328.0 °F	752.0 °F	1004.0 °F	±0.9 °F	±1.8 °F
E	-270.0 °C	-200.0 °C	1000.0 °C	1200.0 °C	±0.3 °C	±0.6 °C
	-454.0 °F	-328.0 °F	1832.0 °F	2192.0 °F	±0.5 °F	±1.1 °F
R & S	-50.0 °C	100.0 °C	1768.0 °C	2019.0 °C	±1.0 °C	±2.5 °C
	-58.0 °C	212.0 °F	3214.4 °F	3276.6 °F [5]	±1.8 °F	±4.5 °F
B	0.0 °C	200.0 °C	800.0 °C	--	±2.0 °C	±2.5 °C
	32.0 °F	392.0 °F	1472.0 °F	--	±3.6 °F	±4.5 °F
	--	800.0 °C	1820.0 °C	1820.0 °C	±1.0 °C	±2.3 °C
	--	1472.0 °F	3276.6 °F [5]	3276.6 °F [5]	±1.8 °F	±4.1 °F
N	-270.0 °C	-200.0 °C	1300.0 °C	1550.0 °C	±1.0 °C	±1.6 °C
	-454.0 °F	-328.0 °F	2372.0 °F	2822.0 °F	±1.8 °F	±2.9 °F
C	0.0 °C	100.0 °C	2315.0 °C	2500.0 °C	±0.7 °C	±2.7 °C
	32.0 °F	212.0 °F	3276.6 °F [5]	3276.6 °F [5]	±1.3 °F	±4.9 °F
TXK/XK(L)	-200.0 °C	-150.0 °C	800.0 °C	1050.0 °C	±0.6 °C	±1.2 °C
	-328.0 °F	302.0 °F	1472.0 °F	1922.0 °F	±1.1 °F	±2.2 °F
Voltage	-32512	-27648 -80mV	27648 80mV	32511	±0.05%	±0.1%

[1] Thermocouple values below the under-range minimum value are reported as -32768.

[2] Thermocouple values above the over-range maximum value are reported as 32767.

[3] Internal cold junction error is ±1.5 °C for all ranges. This adds to the error values in this table. The module requires at least 30 minutes of warm-up time to meet this specification. For module ambient temperatures below -10 °C internal cold junction error can be greater than 1.5 °C.

[4] In the presence of radiated radio frequency of 970 MHz to 990 MHz, the accuracy of the SM 1231 AI 4 x 16 bit TC may be degraded.

[5] Lower limit of 3276.6 with °F reporting

[6] Cold junction compensation error has not been characterized for module ambient temperatures below 0 °C and may exceed the specified value.

NOTE

Thermocouple channel

Each channel on the Thermocouple signal module can be configured with a different thermocouple type (selectable in the software during configuration of the module).

Table A-178 Noise reduction and update times for the SM 1231 Thermocouple

Rejection frequency selection	Integration time	4 Channel module update time (seconds)	8 Channel module update time (seconds)
400 Hz (2.5 ms)	10 ms [1]	0.143	0.285
60 Hz (16.6 ms)	16.67 ms	0.223	0.445
50 Hz (20 ms)	20 ms	0.263	0.525
10 Hz (100 ms)	100 ms	1.225	2.450

[1] To maintain module resolution and accuracy when 400 Hz rejection is selected, the integration time is 10 ms. This selection also rejects 100 Hz and 200 Hz noise.

It is recommended for measuring thermocouples that a 100 ms integration time be used. The use of smaller integration times will increase the repeatability error of the temperature readings.

NOTE

After power is applied, the module performs internal calibration for the analog-to-digital converter. During this time the module reports a value of 32767 on each channel until valid data is available on that channel. Your user program may need to allow for this initialization time. Because the configuration of the module can vary the length of the initialization time, you should verify the behavior or the module in your configuration. If required, you can include logic in your user program to accommodate the initialization time of the module. You can implement this logic using a polling read in the "Startup OB" which blocks operation until the initialization is complete. You must implement the polling read using immediate access. If the value of the thermocouple polling read is 32767, then the read must be repeated until the value changes. For each module this polling only needs to be executed for the highest numbered used input point in the module (the module inputs are initialized in order from 0 to 7).

Representation of analog values for Thermocouple Type J

A representation of the analog values of thermocouples type J is shown in the table below.

Table A-179 Representation of analog values of thermocouples Type J

Type J in °C	Units		Type J in °F	Units		Range
	Decimal	Hexadecimal		Decimal	Hexadecimal	
> 1450.0	32767	7FFF	> 2642.0	32767	7FFF	Overflow
1450.0 : 1200.1	14500 : 12001	38A4 : 2EE1	2642.0 : 2192.2	26420 : 21922	6734 : 55A2	Over-range
1200.0 : -150	12000 : 1500	2EE0 : FA24	2192.0 : -238.0	21920 : -2380	55A0 : F6B4	Rated range
-150.1 : -210	-1501 : -2100	FA23 : F7CC	-238.1 : -346.0	-2381 : -3460	F6B3 : F27C	Under-range
< -210.0	-32768	8000	< -346.0	-32768	8000	Underflow[1]

[1] Faulty wiring (for example, polarity reversal, or open inputs) or sensor error in the negative range (for example, wrong type of thermocouple) may cause the thermocouple module to signal underflow.

A.12.2 SM 1231 RTD

SM 1231 RTD specifications

Table A-180 General specifications

Technical data	SM 1231 AI 4 x RTD x 16 bit	SM 1231 AI 8 x RTD x 16 bit
Article number	6ES7231-5PD32-0XB0	6ES7231-5PF32-0XB0
Dimensions W x H x D (mm)	45 x 100 x 75	70 x 100 x 75
Weight	220 grams	270 grams
Power dissipation	1.5 W	
Current consumption (SM Bus)	80 mA	90 mA
Current consumption (24 V DC) [1]	40 mA	

[1] 20.4 to 28.8 V DC (Class 2, Limited Power, or sensor power from CPU)

Table A-181 Analog inputs

Technical data		SM 1231 AI 4 x RTD x 16 bit	SM 1231 AI 8 x RTD x16 bit
Number of inputs		4	8
Type		Module referenced RTD and Ω	
Range Nominal range (data word) Overshoot/undershoot range (data word) Overflow/underflow (data word)		See RTD Sensor selection table (Page 1206).	
Resolution	Temperature	0.1 °C/0.1 °F	

Technical data		SM 1231 AI 4 x RTD x 16 bit	SM 1231 AI 8 x RTD x16 bit
Resolution	Resistance	15 bits plus sign	
Maximum withstand voltage		± 35 V	
Noise rejection		85 dB for the selected noise reduction (10 Hz, 50 Hz, 60 Hz or 400 Hz)	
Common mode rejection		> 120dB	
Impedance		≥ 10 MΩ	
Isolation	Field side to logic	707 V DC (type test)	
	Field to 24 V DC	707 V DC (type test)	
	24 V DC to logic	707 V DC (type test)	
Channel to channel isolation		none	
Accuracy		See RTD Sensor selection table (Page 1206).	
Repeatability		±0.05% FS	
Maximum sensor dissipation		0.5 m W	
Measuring principle		Integrating	
Module update time		See Noise reduction selection table (Page 1206).	
Cable length (meters)		100 meters to sensor max.	
Wire resistance		20 Ω, 2.7 Ω for 10 Ω RTD max.	

Table A-182 Diagnostics

Technical data	SM 1231 AI 4 x RTD x 16 bit	SM 1231 AI 8 x RTD x16 bit
Overflow/underflow [1,2]	Yes	
Wire break [3]	Yes	
24 V DC low voltage [1]	Yes	

[1] The overflow, underflow and low voltage diagnostic alarm information will be reported in the analog data values even if the alarms are disabled in the module configuration.

[2] For resistance ranges underflow detection is never enabled.

[3] When wire break alarm is disabled and an open wire condition exists in the sensor wiring, the module may report random values.

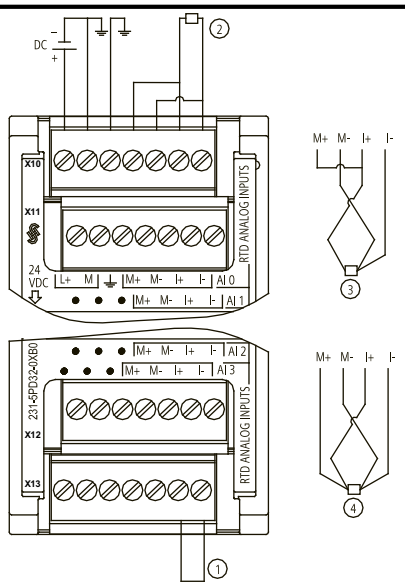
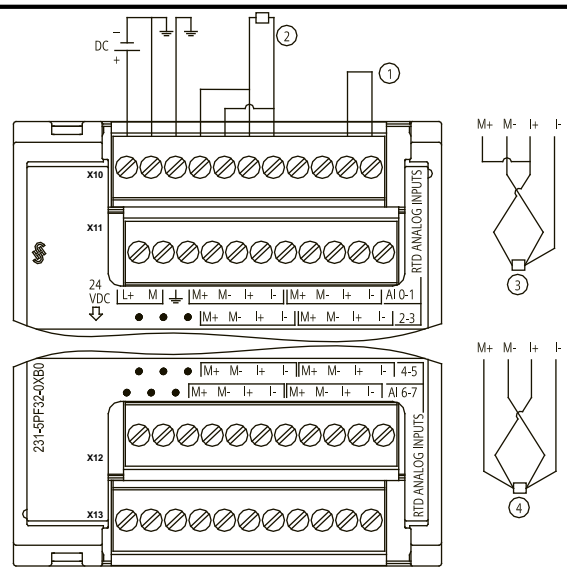
The SM 1231 RTD analog signal module measures the value of resistance connected to the module inputs. The measurement type can be selected as either "Resistor" or "Thermal resistor".

- "Resistor": The nominal range full scale value will be decimal 27648.
- "Thermal resistor": The value will be reported in degrees multiplied by ten (for example, 25.3 degrees will be reported as decimal 253). The climatic range values will be reported in degrees multiplied by one hundred (for example, 25.34 degrees will be reported as decimal 2534).

The SM 1231 RTD module uses a current to measure the resistance of the sensor. The amplitude of this current varies depending on the resistance being measured. The maximum value for the current is 0.48 mA with a zero ohm resistance. The minimum value for the current is 0.34 mA with a 4400 ohm RTD sensor. This current is pulsed depending on the number of active channels on the module. For two active channels, the duty cycle for one channel is 50%. If eight channels are active, the duty cycle for one channel is 12.5%. The maximum output voltage for an open circuit condition on the sensor is 5 V DC (measured between the I+ and I- terminals).

The SM 1231 RTD module supports measurements with 2-wire, 3-wire and 4-wire connections to the sensor resistor.

Table A-183 Wiring diagrams for the RTD SMs

SM 1231 RTD 4 x 16 bit (6ES7231-5PD32-0XB0)	SM 1231 RTD 8 x 16 bit (6ES7231-5PF32-0XB0)
	

① Loop-back unused RTD inputs

② 2-wire RTD ③ 3-wire RTD ④ 4-wire RTD

NOTE: Connectors must be gold. See Appendix C, Spare Parts for article number.

Table A-184 Connector Pin Locations for SM 1231 RTD 4 x 16 bit (6ES7231-5PD32-0XB0)

Pin	X10 (gold)	X11 (gold)	X12 (gold)	X13 (gold)
1	L+ / 24 V DC	No connection	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	Functional Earth	No connection	No connection	No connection
4	AI 0 M+ /RTD	AI 1 M+ /RTD	AI 2 M+ /RTD	AI 3 M+ /RTD
5	AI 0 M- /RTD	AI 1 M- /RTD	AI 2 M- /RTD	AI 3 M- /RTD
6	AI 0 I+ /RTD	AI 1 I+ /RTD	AI 2 I+ /RTD	AI 3 I+ /RTD
7	AI 0 I- /RTD	AI 1 I- /RTD	AI 2 I- /RTD	AI 3 I- /RTD

Table A-185 Connector Pin Locations for SM 1231 RTD 8 x 16 bit (6ES7231-5PF32-0XB0)

Pin	X10 (gold)	X11 (gold)	X12 (gold)	X13 (gold)
1	L+ / 24 V DC	No connection	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	Functional Earth	No connection	No connection	No connection
4	AI 0 M+ /RTD	AI 2 M+ /RTD	AI 4 M+ /RTD	AI 6 M+ /RTD
5	AI 0 M- /RTD	AI 2 M- /RTD	AI 4 M- /RTD	AI 6 M- /RTD
6	AI 0 I+ /RTD	AI 2 I+ /RTD	AI 4 I+ /RTD	AI 6 I+ /RTD

Pin	X10 (gold)	X11 (gold)	X12 (gold)	X13 (gold)
7	AI 0 I- /RTD	AI 2 I- /RTD	AI 4 I- /RTD	AI 6 I- /RTD
8	AI 1 M+ /RTD	AI 3 M+ /RTD	AI 5 M+ /RTD	A7 M+ /RTD
9	AI 1 M- /RTD	AI 3 M- /RTD	AI 5 M- /RTD	AI 7 M- /RTD
10	AI 1 I+ /RTD	AI 3 I+ /RTD	AI 5 I+ /RTD	AI 7 I+ /RTD
11	AI 1 I- /RTD	AI 3 I- /RTD	AI 5 I- /RTD	AI 7 I- /RTD

NOTE

The RTD unused channels can be deactivated. No error will occur if an unused channel is deactivated.

The RTD module needs to have the current loop continuous to eliminate extra stabilization time which is automatically added to an unused channel that is not deactivated. For consistency the RTD module should have a resistor connected (like the 2-wire RTD connection).

A.12.2.1 Selection tables for the SM 1231 RTD

Table A-186 Ranges and accuracy for the different sensors supported by the RTD modules

Temperature coefficient	RTD type	Under range minimum[1]	Nominal range low limit	Nominal range high limit	Over range maximum[2]	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
Pt 0.003850 ITS90 DIN EN 60751	Pt 100 cli-matic	-145.00 °C	-120.00 °C	145.00 °C	155.00 °C	±0.20 °C	±0.40 °C
	Pt 10	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	±1.0 °C	±2.0 °C
	Pt 50	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	±0.5 °C	±1.0 °C
	Pt 100						
	Pt 200						
	Pt 500						
	Pt 1000						
Pt 0.003902 Pt 0.003916 Pt 0.003920	Pt 100	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	± 0.5 °C	±1.0 °C
	Pt 200	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	± 0.5 °C	±1.0 °C
	Pt 500						
	Pt 1000						
Pt 0.003910	Pt 10	-273.2 °C	-240.0 °C	1100.0 °C	1295 °C	±1.0 °C	±2.0 °C
	Pt 50	-273.2 °C	-240.0 °C	1100.0 °C	1295 °C	±0.8 °C	±1.6 °C
	Pt 100						
	Pt 500						
Ni 0.006720 Ni 0.006180	Ni 100	-105.0 °C	-60.0 °C	250.0 °C	295.0 °C	±0.5 °C	±1.0 °C
	Ni 120						
	Ni 200						

1 RTD values below the under-range minimum value report -32768.

2 RTD values above the over-range maximum value report +32767.

Temperature coefficient	RTD type	Under range minimum[1]	Nominal range low limit	Nominal range high limit	Over range maximum[2]	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
Ni 0.006720 Ni 0.006180	Ni 500	-105.0 °C	-60.0 °C	250.0 °C	295.0 °C	±0.5 °C	±1.0 °C
	Ni 1000						
LG-Ni 0.005000	LG-Ni 1000	-105.0 °C	-60.0 °C	250.0 °C	295.0 °C	±0.5 °C	±1.0 °C
Ni 0.006170	Ni 100	-105.0 °C	-60.0 °C	180.0 °C	212.4 °C	±0.5 °C	±1.0 °C
Cu 0.004270	Cu 10	-240.0 °C	-200.0 °C	260.0 °C	312.0 °C	±1.0 °C	±2.0 °C
Cu 0.004260	Cu 10	-60.0 °C	-50.0 °C	200.0 °C	240.0 °C	±1.0 °C	±2.0 °C
	Cu 50	-60.0 °C	-50.0 °C	200.0 °C	240.0 °C	±0.6 °C	±1.2 °C
	Cu 100						
Cu 0.004280	Cu 10	-240.0 °C	-200.0 °C	200.0 °C	240.0 °C	±1.0 °C	±2.0 °C
	Cu 50	-240.0 °C	-200.0 °C	200.0 °C	240.0 °C	±0.7 °C	±1.4 °C
	Cu 100						

1 RTD values below the under-range minimum value report -32768.

2 RTD values above the over-range maximum value report +32767.

Table A-187 Resistance

Range	Under range minimum	Nominal range low limit	Nominal range high limit	Over range maximum[1]	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
150 Ω	n/a	0 (0 Ω)	27648 (150 Ω)	176.383 Ω	±0.05%	±0.1%
300 Ω	n/a	0 (0 Ω)	27648 (300 Ω)	352.767 Ω	±0.05%	±0.1%
600 Ω	n/a	0 (0 Ω)	27648 (600 Ω)	705.534 Ω	±0.05%	±0.1%

1 Resistance values above the over-range maximum value are reported as +32767.

NOTE

The module reports 32767 on any activated channel with no sensor connected. If open wire detection is also enabled, the module flashes the appropriate red LEDs.

When 500 Ω and 1000 Ω RTD ranges are used with other lower value resistors, the error may increase to two times the specified error.

Best accuracy will be achieved for the 10 Ω RTD ranges if 4 wire connections are used.

The resistance of the connection wires in 2 wire mode will cause an error in the sensor reading and therefore accuracy is not guaranteed.

Table A-188 Noise reduction and update times for the RTD modules

Rejection frequency selection	Integration time	Update time (seconds)	
		4-channel module	8-channel module
400 Hz (2.5 ms)	10 ms [1]	4-/2-wire: 0.142 3-wire: 0.285	4-/2-wire: 0.285 3-wire: 0.525
60 Hz (16.6 ms)	16.67 ms	4-/2-wire: 0.222 3-wire: 0.445	4-/2-wire: 0.445 3-wire: 0.845
50 Hz (20 ms)	20 ms	4-/2-wire: 0.262 3-wire: .505	4-/2-wire: 0.524 3-wire: 1.015
10 Hz (100 ms)	100 ms	4-/2-wire: 1.222 3-wire: 2.445	4-/2-wire: 2.425 3-wire: 4.845

[1] To maintain module resolution and accuracy when the 400 Hz filter is selected, the integration time is 10 ms. This selection also rejects 100 Hz and 200 Hz noise.

NOTE

After power is applied, the module performs internal calibration for the analog-to-digital converter. During this time the module reports a value of 32767 on each channel until valid data is available on that channel. Your user program may need to allow for this initialization time. Because the configuration of the module can vary the length of the initialization time, you should verify the behavior or the module in your configuration. If required, you can include logic in your user program to accommodate the initialization time of the module. You can implement this logic using a polling read in the "Startup OB" which blocks operation until the initialization is complete. You must implement the polling read using immediate access. If the value of the RTD polling read is 32767, then the read must be repeated until the value changes. For each module this polling only needs to be executed for the highest numbered used input point in the module (the module inputs are initialized in order from 0 to 7).

Representation of Analog values for RTDs

A representation of the digitized measured value for the RTD standard temperature range sensors are shown in the tables below.

Table A-189 Representation of analog values for resistance thermometers PT 100, 200, 500, 1000 and PT 10, 50, 100, 500 GOST (0.003850) standard

Pt x00 standard in °C (1 digit = 0.1 °C)	Units		Pt x00 standard in °F (1 digit = 0.1 °F)	Units		Range
	Decimal	Hexadecimal		Decimal	Hexadecimal	
> 1000.0	32767	7FFF	> 1832.0	32767	7FFF	Overflow
1000.0 : 850.1	10000 : 8501	2710 : 2135	1832.0 : 1562.1	18320 : 15621	4790 : 3D05	Overrange

Pt x00 standard in °C (1 digit = 0.1 °C)	Units		Pt x00 standard in °F (1 digit = 0.1 °F)	Units		Range
	Decimal	Hexadecimal		Decimal	Hexadecimal	
850.0 : -200.0	8500 : -2000	2134 : F830	1562.0 : -328.0	15620 : -3280	3D04 : F330	Rated range
-200.1 : -243.0	-2001 : -2430	F82F : F682	-328.1 : -405.4	-3281 : -4054	F32F : F02A	Underrange
< -243.0	-32768	8000	< -405.4	-32768	8000	Underflow

A.13 Technology modules

A.13.1 SM 1278 4xIO-Link Master SM

Table A-190 General specifications

Technical data		SM 1278 4xIO-Link Master signal module
Article number		6ES7278-4BD32-0XB0
Dimensions W x H x D (mm)		45 x 100 x 75
Weight		150 grams
General information		
	I&M data	Yes; IM0 to IM3
Supply voltage		
	Rated voltage (DC)	24 V DC
	Valid range low limit (DC)	19.2 V; 20.5 V if IO-Link is used (the supply voltage for IO-Link devices on the master must be at least 20 V)
	Valid range high limit (DC)	28.8 V DC
	Polarity reversal protection	Yes
Input current		
	Current consumption	65 mA; without load
Encoder supply		
	Number of outputs	4
	Output current, rated value	200 mA per channel
Power loss		
	Power loss, typ.	1 W, excluding port loading
Digital inputs/outputs		
	Cable length (meters)	20 m, unshielded, max.
SDLC		
	Cable length (meters)	20 m, unshielded, max.
IO-Link		
	Number of ports	4

Technical data			SM 1278 4xIO-Link Master signal module
	Number of ports which can be controlled at the same time		4
	IO-Link protocol 1.0		Yes
	IO-Link protocol 1.1		Yes
Operating mode			
	IO-Link		Yes
	DI		Yes
	DQ		Yes; max. 100 mA
Connection of IO-Link devices			
	Port type A		Yes
		Transmission rate	4.8 kBd (COM1)
			38.4 kBd (COM2)
			230.4 kBd (COM3)
	Cycle time, min.		2 ms, dynamic, dependent on the user data length
	Size of process data, input per port		32 bytes; max.
	Size of process data, input per module		32 bytes
	Size of process data, output per port		32 bytes; max.
	Size of process data, output per module		32 bytes
	Memory size for device parameters		2 Kbytes
	Cable length unshielded, max. (meters)		20 m
Interrupts/diagnostics/status information			
	Status display		Yes
Interrupts			
	Diagnostic interrupt		Yes; port diagnostics is only available in IO-Link mode
Diagnostic alarms			
	Diagnostics		
		Monitoring of supply voltage	Yes
		Short circuit	Yes
Diagnostic indicator LED			
	Monitoring of supply voltage		Yes; flashing red DIAG LED
	Channel status display		Yes; per channel one green LED for channel status Qn (SIO mode) and PORT status Cn (IO-Link mode)
	For channel diagnostics		Yes; red Fn LED
	For module diagnostics		Yes; green/red DIAG LED
Electrical isolation			
	Electrical isolation channels		
		Between the channels	No
		Between the channels and the backplane bus	Yes
Insulation			
	Insulation tested with		707 V DC (type test)

Technical data			SM 1278 4xIO-Link Master signal module
Ambient conditions			
	Operating temperature		
		Min.	-20 °C
		Max.	60 °C
		Horizontal installation, min.	-20 °C
		Horizontal installation, max.	60 °C
		Vertical installation, min.	-20 °C
		Vertical installation, max.	50 °C

Overview of the response time

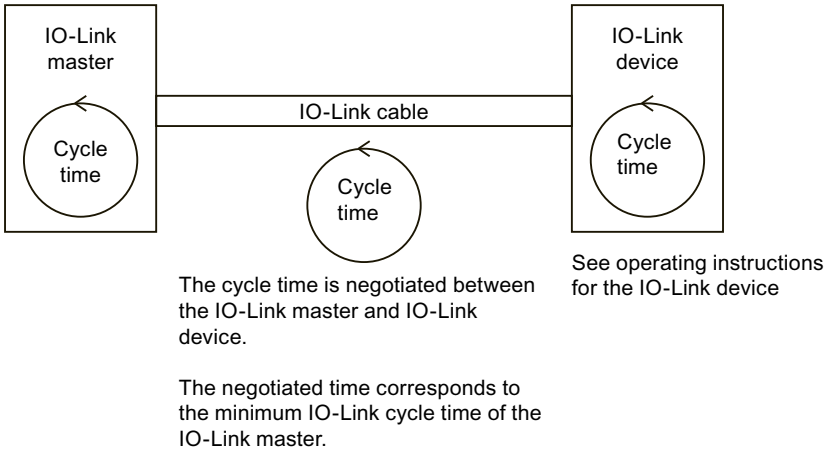


Table A-191 Wiring diagram for the SM 1278 IO-Link Master

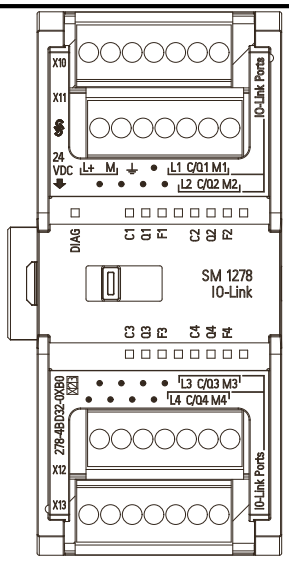
SM 1278 IO-Link Master (6ES7278-4BD32-0XB0)	
	

Table A-192 Connector pin locations for SM 1278 IO-Link Master (6ES7278-4BD32-0XB0)

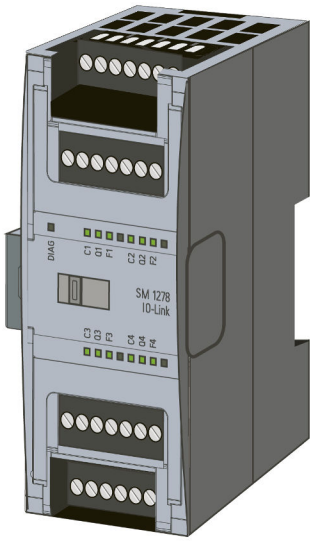
Pin	X10	X11	X12	X13
1	L+ / 24 V DC	No connection	No connection	No connection
2	M / 24 V DC	No connection	No connection	No connection
3	Functional Earth	No connection	No connection	No connection
4	No connection	No connection	No connection	No connection
5	L_1	L_2	L_3	L_4
6	C/Q_1	C/Q_2	C/Q_3	C/Q_4
7	M_1	M_2	M_3	M_4

A.13.1.1 SM 1278 4xIO-Link Master overview

The SM 1278 4xIO-Link Master is a 4-port module that functions as both a signal module and a communication module. Each port can operate in the IO-Link mode, single 24 V DC digital input or 24 V DC digital output.

The IO-Link master programs acyclic communication with an IO-Link device using the IO_LINK_DEVICE function block (FB) in your STEP 7 S7-1200 controller program. The IO_LINK_DEVICE FB indicates the IO-Link master your program uses, and which ports the master uses for data exchange.
Visit the Siemens Industry Online Support Web site (http://support.industry.siemens.com) for details on working with the IO-Link library. Enter "IO-Link" in the Web site's search box to access information about IO-Link products and their use.

View of the module



Properties

Technical properties

- IO-Link Master according to IO-Link specification V1.1 (see the IO-Link Consortium Web site (http://io-link.com/en/index.php) for details)
- Serial communication module with four ports (channels)
- Data transmission rate COM1 (4.8 kbaud), COM2 (38.4 kbaud), COM3 (230.4 kbaud)
- SIO mode (standard IO mode)
- Connection of up to four IO-Link devices (3-wire connection) or four standard actuators or standard encoders
- Programmable diagnostics function by port

Supported functions

- I&M (installation and maintenance) identification data
- Firmware update
- IO-Link parameter assignment by means of the S7-PCT port configuration tool, STEP 7 Professional, and an S7-1200 V4.x CPU. In STEP 7 Professional, IO-Link parameter assignment can be done using the TIA Portal with limited functionality.
- Port Qualifier Information (PQI) bits
- Backup and Restore using IO-Link library FBs

IO-Link is a point-to-point connection between a master and a device. Both conventional and intelligent sensors/actuators can be used as devices at the IO-Link via unshielded standard cables using proven 3-wire technology. IO-Link is backward compatible with conventional digital sensors and actuators. The circuit state and data channel are designed in proven 24 V DC technology.
For additional information about the SIMATIC-IO-Link technology, refer to the "IO-Link system Function Manual" on the Siemens Industry Online Support Web site (http://support.automation.siemens.com).

NOTE
IO-Link parameter data
When you replace the SM 4xIO-Link Master, the parameter data is not automatically assigned to it.

CAUTION
Removal and insertion of the SM 4xIO-Link Master
If you insert the SM 4xIO-Link Master with the load switched on, this can lead to dangerous conditions in your plant. Physical damage to the S7-1200 automation system might occur as a result.
Remove or insert the SM 4xIO-Link Master only when the load is switched off.
Injury can occur as a result of dangerous plant conditions or damage to the S7-1200 automation system.

Effects of resetting to the factory settings

Use the function "Reset to factory settings" to restore the parameter assignments you made with S7-PCT to the delivery state.
After a "Reset to factory settings", the parameters of the SM 1278 4xIO-Link module are assigned as follows:

- The ports are in DI mode
- The ports are mapped to the relative addresses 0.0 to 0.3
- The PortQualifier is disabled
- Maintenance data 1 to 3 is deleted

NOTE

When you reset to factory settings, the device parameters are deleted and the delivery state is restored.

If you remove an SM 1278 4xIO-Link signal module, reset it to factory settings before you put it into storage.

Procedure

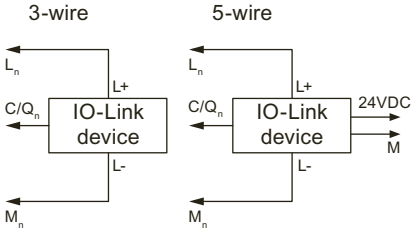
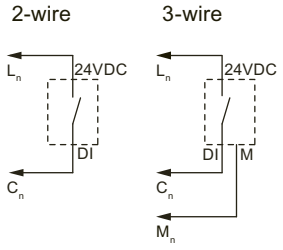
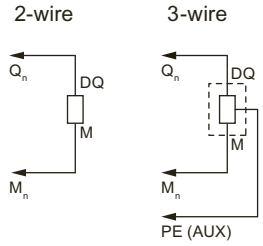
For "Reset to factory settings", proceed as described in the S7-PCT online help under "Master Configuration > 'Commands' tab".

A.13.1.2 Connecting

For details about pin assignment, see table, Connector pin locations for SM 1278 I/O-Link Master (6ES 278-4BD32-0XB0). (Page 1209)
The following table shows the terminal assignments for the SM 1278 4xIO-Link Master:

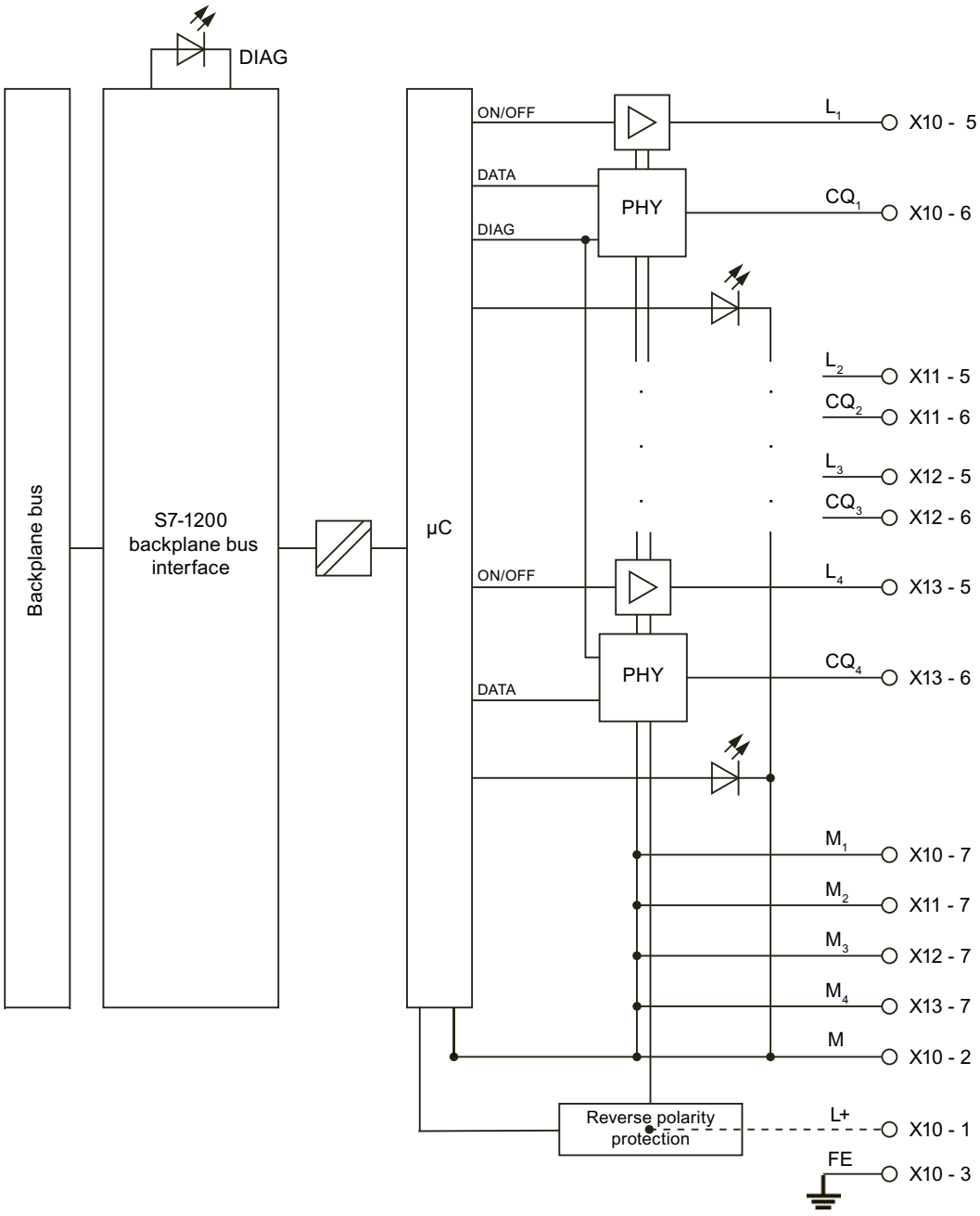
Pin	X10	X11	X12	X13	Notes	BaseUnits
7	M_1	M_2	M_3	M_4	• M_n: ground to slave • C/Q_n: SDLC, DI or DQ • L_n: 24 V DC to slave • M: ground • L+: 24 V DC to Master • RES: reserved; may not be assigned	A1
6	C/Q_1	C/Q_2	C/Q_3	C/Q_4		
5	L_1	L_2	L_3	L_4		
4	RES	RES	RES	RES		
3	⏚ (functional earth)	RES	RES	RES		
2	M	RES	RES	RES		
1	L+	RES	RES	RES		

The following table contains illustrations of connection examples, where n = port number:

IO-Link operating mode	Operating mode DI	Operating mode DQ
		

NOTE

Connected sensors must use the device supply provided by the Master module L_n connection.


DIAG
Backplane bus
S7-1200
backplane bus
interface
µC
ON/OFF
DATA
DIAG
PHY
L1
X10 - 5
CQ1
X10 - 6
L2
X11 - 5
CQ2
X11 - 6
L3
X12 - 5
CQ3
X12 - 6
ON/OFF
PHY
DATA
L4
X13 - 5
CQ4
X13 - 6
M1
X10 - 7
M2
X11 - 7
M3
X12 - 7
M4
X13 - 7
M
X10 - 2
Reverse polarity
protection
L+
X10 - 1
FE
X10 - 3

A.13.1.3 Parameters/address space

Configuring the SM 1278 4xIO-Link Master

For module integration, parameter assignment, and commissioning, you need STEP 7. For some features, you also need S7-PCT (Port Configuration Tool).
For additional information, refer to the SIMATIC IO-Link system manual (https://support.industry.siemens.com/cs/ww/en/view/65949252).

The following table shows the parameters for the SM 1278 4xIO-Link Master:

Parameters	Value range	Default	Configuration in RUN	Efficiency range
Diagnostics port 1	• Disable • Enable	Disable	Yes	Port (channel)
Diagnostics port 2	• Disable • Enable	Disable	Yes	Port (channel)
Diagnostics port 3	• Disable • Enable	Disable	Yes	Port (channel)
Diagnostics port 4	• Disable • Enable	Disable	Yes	Port (channel)

Enable diagnostics for port 1 to port 4 parameter

This parameter allows diagnostics to be enabled for specific ports of the four IO-Link ports.
The port assignments are as follows:
Port 1 → channel 1
Port 2 → channel 2
Port 3 → channel 3
Port 4 → channel 4

The maximum size of the input and output addresses of the SM 4xIO-Link Master is 32 bytes in each case. You assign address spaces using the S7-PCT port configuration tool by using the TIA Portal hardware configuration.

Parameter data record

Parameter assignment in the user program

You can configure the device in runtime.

Changing parameters in runtime

The module parameters are included in data record 128. You can transmit the modifiable parameters to the module with the WRREC instruction.
When you reset (power cycle) the CPU, the CPU overwrites the parameters that were sent to the module by the WRREC instruction during the parameterization process.

Instruction for parameter assignment

The following instruction is provided for assigning parameters to the I/O module in the user program:

Instruction	Application
SFB 53 WRREC	Transfer of the alterable parameters to the module.

Error message

The following return value is reported in the event of an error:

Error code	Meaning
$80B1_H$	Error in data length
$80E0_H$	Error in header information
$80E1_H$	Parameter error

Data record structure

The following table shows the IO-Link parameters:

Offset	Label	Type	Default	Description
0	Version	1 byte	0x02	Shows the structure of the record 0x02 for the IO-Link Master in accordance with IO-Link V1.1
1	Parameter length	1 byte	0x02	Parameter length (2 bytes + 2 headers)
IO-Link start parameters				
2	Port diagnostics (Port1 1 to n)	1 byte	0x00	Activating the diagnostics for port 1 to n
3	IOL properties	1 byte	0x00	Module properties

The following table shows the data record version:

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Reserved		Major version (00)		Minor version (0010)			

The following table shows the data record port diagnostics:

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Reserved				EN_Port4	EN_Port3	EN_Port2	EN_Port1

EN_Portx:

0 = Diagnostics deactivated

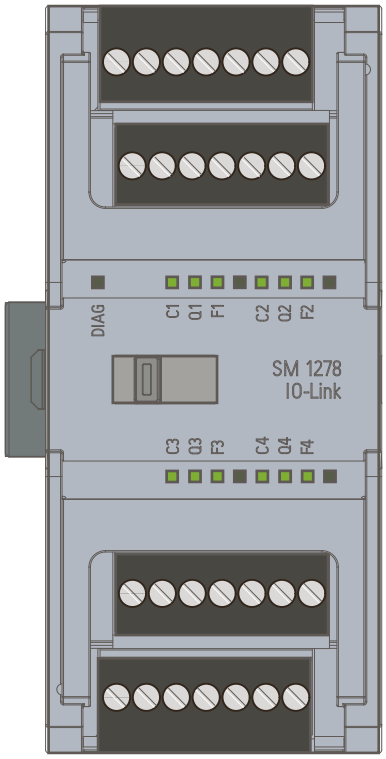
1 = Diagnostics activated

The following table shows the data record IOL properties:

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Reserved							

A.13.1.4 Interrupt, error, and system alarms

LED display



Meaning of the LED displays

The following table explains the meaning of the status and error displays. You can find remedial measures for diagnostic alarms in the "Diagnostic alarms" section.

LED DIAG

DIAG	Meaning
□ Off	Backplane bus supply of the S7-1200 not OK
☼ Flashes	Module is not configured
■ On	Module parameterized and no module diagnostics
☼ Flashes	Module parameterized and module diagnostics OR L+ power not connected

LED port status

Valid for IO-Link port which is in IO-Link port mode.

COM/1 ... COM/4	Meaning
□ Off	Port deactivated
☼ Flashes	Port activated, device not connected or Port is not connected to the configured device
■ On	Port activated, device connected

LED channel status

Valid for IO-Link port which is in DI/Q mode.

DI/Q1 ... DI/Q4	Meaning
□ Off	Process signal = 0
■ On	Process signal = 1

LED port error

F1 ... F4	Meaning
□ Off	No error
■ On	Error

Module errors are indicated as diagnostics (module status) only in IO-Link mode.

Diagnostic alarm	Error code (decimal)	STATUS (W#16#...)	Meaning (IO-Link error code)	IO-Link master	IO-Link device
Short-circuit	1	1804	Short-circuit at the process cables on the IO-Link device	X	
		7710	Short-circuit on IO device		X
Undervoltage	2	5111 5112	Supply voltage too low		X
Overvoltage	3	5110	Supply voltage too high		X
Overheating	5	1805	Temperature exceeded on master	X	
		4000 4210	Temperature exceeded on device		X
Wire break	6	1800	• No IO-Link device connected • There is a break on the signal line to the IO-Link device • IO-Link device cannot communicate due to a different error	X	
Overflow	7	8C10 8C20	Process tag range exceeded		X
		8C20	Measuring range exceeded		
Underflow	8	8C30	Process tag range too low		X
Error	9	---	All IO-Link error codes that are not listed here are mapped to this PROFIBUS DP error		X
Parameter assignment error	16	1882 1883	IO-Link master could not be configured	X	
		1802	Incorrect device		
		1886	Storage error		
		6320 6321 6350	Device was not configured correctly		X
Supply voltage missing	17	1806	L+ supply voltage for device missing	X	
		1807	L+ supply voltage for device too low (<20 V)		
Defective fuse	18	5101	Fuse on device is defective		X
Safety shutdown	25	1880	Serious error (master has to be replaced)	X	
External fault	26	1809 180A 180B 180C 180D	Error in data storage	X	
		1808	More than 6 errors are pending simultaneously on the IO-Link device		

A.14 Digital signal boards (SBs)

A.14.1 SB 1221 200 kHz digital input specifications

Table A-193 General specifications

Technical data	SB 1221 DI 4 x 24 V DC, 200 kHz	SB 1221 DI 4 x 5 V DC, 200 kHz
Article number	6ES7221-3BD30-0XB0	6ES7221-3AD30-0XB0
Dimensions W x H x D (mm)	38 x 62 x 21	
Weight	35 grams	
Power dissipation	1.5 W	1.0 W
Current consumption (SM Bus)	40 mA	
Current consumption (24 V DC)	7 mA / input + 20 mA	15 mA / input + 15 mA

Table A-194 Digital inputs

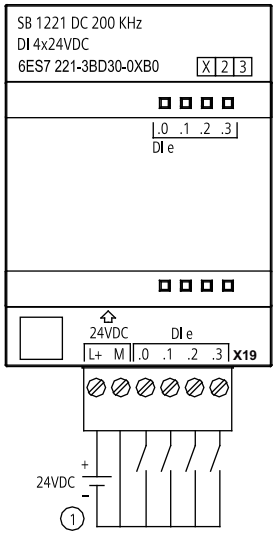
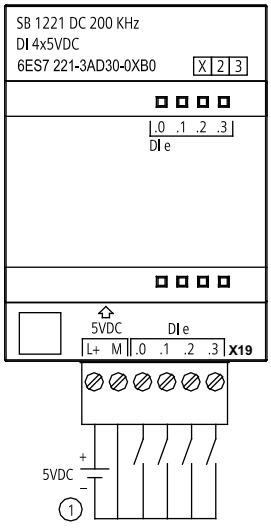
Technical data		SB 1221 DI 4 x 24 V DC, 200 kHz	SB 1221 DI 4 x 5 V DC, 200 kHz
Number of inputs		4	
Type		Source	
Rated voltage		24 V DC at 7 mA, nominal	5 V DC at 15 mA, nominal
Continuous permissible voltage		28.8 V DC	6 V DC
Surge voltage		35 V DC for 0.5 sec.	6 V
Logic 1 signal		0 V (10 mA) to L+ minus 10 V (2.9 mA)	0 V (20 mA) to L+ minus 2.0 V (5.1 mA)
Logic 0 signal		L+ minus 5 V (1.4 mA) to L+ (0 mA)	L+ minus 1.0 V (2.2 mA) to L + (0 mA)
HSC clock input rates (max.)		Single phase: 200 kHz Quadrature phase: 160 kHz	
Isolation (field side to logic)		707 V DC (type test)	
Isolation groups		1	
Filter times	us settings	0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0,12.8, 20.0	
	ms settings	0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
Number of inputs on simultaneously		• 2 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 4 at 55 °C horizontal or 45 °C vertical	4
Cable length (meters)		50 shielded twisted pair	

NOTE

When switching frequencies above 20 kHz, it is important that the digital inputs receive a square wave. Consider the following options to improve the signal quality to the inputs:

- Minimize the cable length
- Change a driver from a sink only driver to a sinking and sourcing driver
- Change to a higher quality cable
- Reduce the circuit/components from 24 V to 5 V
- Add an external load at the input

Table A-195 Wiring diagrams for the 200 kHz digital input SBs

SB 1221 DI 4 x 24 V DC, 200 kHz (6ES7221-3BD30-0XB0)	SB 1221 DI 4 x 5 V DC, 200 kHz (6ES7221-3AD30-0XB0)
	

① Supports sourcing inputs only

Table A-196 Connector pin locations for SB 1221 DI 4 x 24 V DC, 200 kHz (6ES7221-3BD30-0XB0)

Pin	X19
1	L+ / 24 V DC
2	M / 24 V DC
3	DI e.0
4	DI e.1
5	DI e.2
6	DI e.3

Table A-197 Connector pin locations for SB 1221 DI 4 x 5 V DC, 200 kHz (6ES7221-3AD30-0XB0)

Pin	X19
1	L+ / 5 V DC
2	M / 5 V DC
3	DI e.0
4	DI e.1
5	DI e.2
6	DI e.3

A.14.2 SB 1222 200 kHz digital output specifications

Table A-198 General specifications

Technical data	SB 1222 DQ 4 x 24 V DC, 200 kHz	SB 1222 DQ 4 x 5 V DC, 200 kHz
Article number	6ES7222-1BD30-0XB0	6ES7222-1AD30-0XB0
Dimensions W x H x D (mm)	38 x 62 x 21	
Weight	35 grams	
Power dissipation	0.5 W	
Current consumption (SM Bus)	35 mA	
Current consumption (24 V DC)	15 mA	

Table A-199 Digital outputs

Technical data	SB 1222 DQ 4 x 24 V DC, 200 kHz	SB 1222 DQ 4 x 5 V DC, 200 kHz
Number of outputs	4	
Output type	Solid state - MOSFET sink and source[1]	
Voltage range	20.4 to 28.8 V DC	4.25 to 6.0 V DC
Logic 1 signal at max. current	L+ minus 1.5 V	L+ minus 0.7 V
Logic 0 signal at max. current	1.0 V DC, max.	0.2 V DC, max.
Current (max.)	0.1 A	
Lamp load	--	
On state contact resistance	11 Ω max.	7 Ω max.
Off state resistance	6 Ω max.	0.2 Ω max.
Leakage current per point	--	
Pulse Train Output rate	200 kHz max., 2 Hz min.	
Surge current	0.11 A	
Overload protection	No	
Isolation (field side to logic)	707 V DC (type test)	
Isolation groups	1	
Currents per common	0.4 A	
Inductive clamp voltage	Non	
Switching delay	1.5 µs + 300 ns rise 1.5 µs + 300 ns fall	200 ns + 300 ns rise 200 ns + 300 ns fall
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Control of a digital input	Yes	
Parallel outputs for redundant load control	No	

[1] Because both sinking and sourcing configurations are supported by the same circuitry, the active state of a sourcing load is opposite that of a sinking load. A source output exhibits positive logic (Q bit and LED are ON when the load has current flow), while a sink output exhibits negative logic (Q bit and LED are OFF when the load has current flow). If the module is plugged in with no user program, the default for this module is 0 V, which means that a sinking load will be turned ON.

Technical data	SB 1222 DQ 4 x 24 V DC, 200 kHz	SB 1222 DQ 4 x 5 V DC, 200 kHz
Parallel outputs for increased load	No	
Number of outputs on simultaneously	• 2 (no adjacent points) at 60 °C horizontal or 50 °C vertical • 4 at 55 °C horizontal or 45 °C vertical	4
Cable length (meters)	50 shielded twisted pair	

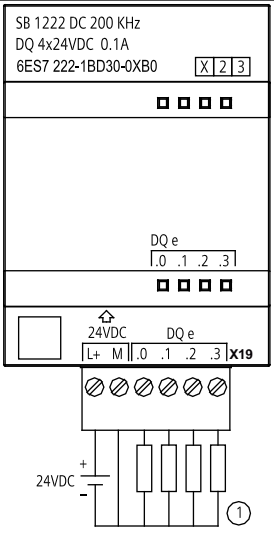
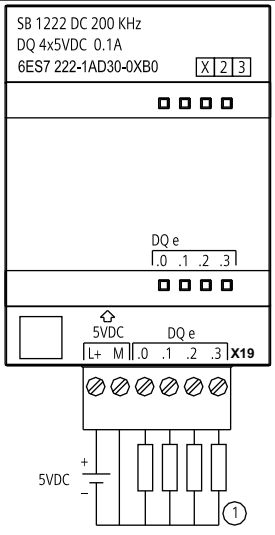
[1] Because both sinking and sourcing configurations are supported by the same circuitry, the active state of a sourcing load is opposite that of a sinking load. A source output exhibits positive logic (Q bit and LED are ON when the load has current flow), while a sink output exhibits negative logic (Q bit and LED are OFF when the load has current flow). If the module is plugged in with no user program, the default for this module is 0 V, which means that a sinking load will be turned ON.

NOTE

When switching frequencies above 20 kHz, it is important that the digital inputs receive a square wave. Consider the following options to improve the signal quality to the inputs:

- Minimize the cable length
- Change a driver from a sink only driver to a sinking and sourcing driver
- Change to a higher quality cable
- Reduce the circuit/components from 24 V to 5 V
- Add an external load at the input

Table A-200 Wiring diagrams for the 200 kHz digital output SBs

SB 1222 DQ 4 x 24 V DC, 200 kHz (6ES7222-1BD30-0XB0)	SB 1222 DQ 4 x 5 V DC, 200 kHz (6ES7222-1AD30-0XB0)
	

① For sourcing outputs, connect "Load" to "-" (shown). For sinking outputs, connect "Load" to "+". Because both sinking and sourcing configurations are supported by the same circuitry, the active state of a sourcing load is opposite that of a sinking load. A source output exhibits positive logic (Q bit and LED are ON when the load has current flow), while a sink output exhibits negative logic (Q bit and LED are OFF when the load has current flow). If the module is plugged in with no user program, the default for this module is 0 V, which means that a sinking load will be turned ON.

NOTE

Ensure that the M connection wire is securely grounded. Loss of the ground wire connection to the high-speed DQ SBs may allow enough leakage current to activate a DC load. If the outputs are used for critical DC load applications, extra caution should be exercised by using a redundant ground wire to the SB.

Table A-201 Connector pin locations for SB 1222 DQ 4 x 24 V DC, 200 kHz (6ES7222-1BD30-0XB0)

Pin	X19
1	L+ / 24 V DC
2	M / 24 V DC
3	DQ e.0
4	DQ e.1
5	DQ e.2
6	DQ e.3

Table A-202 Connector pin locations for SB 1222 DQ 4 x 5 V DC, 200 kHz (6ES7222-1AD30-0XB0)

Pin	X19
1	L+ / 5 V DC
2	M / 5 V DC
3	DQ e.0
4	DQ e.1
5	DQ e.2
6	DQ e.3

A.14.3 SB 1223 200 kHz digital input / output specifications

Table A-203 General specifications

Technical data	SB 1223 DI 2 x 24 V DC / DQ 2 x 24 V DC, 200 kHz	SB 1223 DI 2 x 5 V DC / DQ 2 x 5 V DC, 200 kHz
Article number	6ES7223-3BD30-0XB0	6ES7223-3AD30-0XB0
Dimensions W x H x D (mm)	38 x 62 x 21	
Weight	35 grams	
Power dissipation	1.0 W	0.5 W
Current consumption (SM Bus)	35 mA	
Current consumption (24 V DC)	7 mA / Input + 30 mA	15 mA / input + 15 mA

Table A-204 Digital inputs

Technical data		SB 1223 DI 2 x 24 V DC / DQ 2 x 24 V DC, 200 kHz	SB 1223 DI 2 x 5 V DC / DQ 2 x 5 V DC, 200 kHz
Number of inputs		2	
Type		Source	
Rated voltage		24 V DC at 7 mA, nominal	5 V DC at 15 mA, nominal
Continuous permissible voltage		28.8 V DC	6 V DC
Surge voltage		35 V DC for 0.5 sec.	6 V
Logic 1 signal		0 V (10 mA) to L+ minus 10 V (2.9 mA)	0 V (20 mA) to L+ minus 2.0 V (5.1 mA)
Logic 0 signal		L+ minus 5 V (1.4 mA) to L+ (0 mA)	L+ minus 1.0 V (2.2 mA) to L + (0 mA)
HSC clock input rates (max.)		Single phase: 200 kHz Quadrature phase: 160 kHz	
Isolation (field side to logic)		707 V DC (type test)	
Isolation groups		1 (no isolation to outputs)	
Filter times	us settings	0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
	ms settings	0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
Number of inputs on simultaneously		2	
Cable length (meters)		50 shielded twisted pair	

Table A-205 Digital outputs

Technical data	SB 1223 DI 2 x 24 V DC / DQ 2 x 24 V DC, 200 kHz	SB 1223 DI 2 x 5 V DC / DQ 2 x 5 V DC, 200 kHz
Number of outputs	2	
Output type	Solid state - MOSFET sink and source[1]	
Voltage range	20.4 to 28.8 V DC	4.25 to 6.0 V DC
Rated value	24 V DC	5 V DC
Logic 1 signal at max. current	L+ minus 1.5 V	L+ minus 0.7 V
Logic 0 signal at max. current	1.0 V DC, max.	0.2 V DC, max.
Current (max.)	0.1 A	
Lamp load	--	
On state contact resistance	11 Ω max.	7 Ω max.
Off state resistance	6 Ω max.	0.2 Ω max.
Leakage current per point	--	
Pulse Train Output rate	200 kHz max., 2 Hz min.	
Surge current	0.11 A	
Overload protection	No	
Isolation (field side to logic)	707 V DC (type test)	
Isolation groups	1 (no isolation to inputs)	
Currents per common	0.2 A	

[1] Because both sinking and sourcing configurations are supported by the same circuitry, the active state of a sourcing load is opposite that of a sinking load. A source output exhibits positive logic (Q bit and LED are ON when the load has current flow), while a sink output exhibits negative logic (Q bit and LED are OFF when the load has current flow). If the module is plugged in with no user program, the default for this module is 0 V, which means that a sinking load will be turned ON.

Technical data	SB 1223 DI 2 x 24 V DC / DQ 2 x 24 V DC, 200 kHz	SB 1223 DI 2 x 5 V DC / DQ 2 x 5 V DC, 200 kHz
Inductive clamp voltage	Non	
Switching delay	1.5 µs + 300 ns rise 1.5 µs + 300 ns fall	200 ns + 300 ns rise 200 ns + 300 ns fall
Behavior on RUN to STOP	Last value or substitute (default value 0)	
Control of a digital input	Yes	
Parallel outputs for redundant load control	No	
Parallel outputs for increased load	No	
Number of outputs on simultaneously	2	
Cable length (meters)	50 shielded twisted pair	

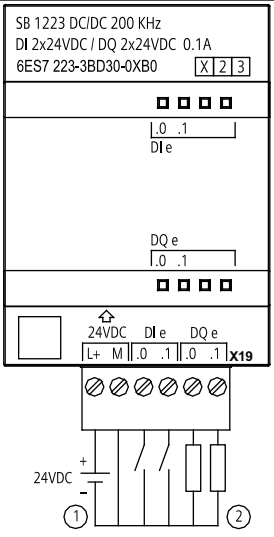
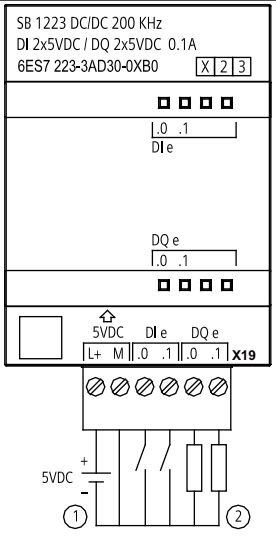
[1] Because both sinking and sourcing configurations are supported by the same circuitry, the active state of a sourcing load is opposite that of a sinking load. A source output exhibits positive logic (Q bit and LED are ON when the load has current flow), while a sink output exhibits negative logic (Q bit and LED are OFF when the load has current flow). If the module is plugged in with no user program, the default for this module is 0 V, which means that a sinking load will be turned ON.

NOTE

When switching frequencies above 20 kHz, it is important that the digital inputs receive a square wave. Consider the following options to improve the signal quality to the inputs:

- Minimize the cable length
- Change a driver from a sink only driver to a sinking and sourcing driver
- Change to a higher quality cable
- Reduce the circuit/components from 24 V to 5 V
- Add an external load at the input

Table A-206 Wiring diagrams for the 200 kHz digital input/output SBs

SB 1223 DI 2 x 24 V DC/DQ 2 x 24 V DC, 200 kHz (6ES7223-3BD30-0XB0)	SB 1223 DI 2 x 5 V DC / DQ 2 x 5 V DC, 200 kHz (6ES7223-3AD30-0XB0)
	

① Supports sourcing inputs only

[1] ② For sourcing outputs, connect "Load" to "-" (shown). For sinking outputs, connect "Load" to "+". Because both sinking and sourcing configurations are supported by the same circuitry, the active state of a sourcing load is opposite that of a sinking load. A source output exhibits positive logic (Q bit and LED are ON when the load has current flow), while a sink output exhibits negative logic (Q bit and LED are OFF when the load has current flow). If the module is plugged in with no user program, the default for this module is 0 V, which means that a sinking load will be turned ON.

NOTE

Ensure that the M connection wire is securely grounded. Loss of the ground wire connection to the high-speed DQ SBs may allow enough leakage current to activate a DC load. If the outputs are used for critical DC load applications, extra caution should be exercised by using a redundant ground wire to the SB.

Table A-207 Connector pin locations for SB 1223 DI 2 x 24 V DC/DQ 2 x 24 V DC, 200 kHz (6ES7223-3BD30-0XB0)

Pin	X19
1	L+ / 24 V DC
2	M / 24 V DC
3	DI e.0
4	DI e.1
5	DQ e.0
6	DQ e.1

Table A-208 Connector pin locations for SB 1223 DI 2 x 5 V DC / DQ 2 x 5 V DC, 200 kHz (6ES7223-3AD30-0XB0)

Pin	X19
1	L+ / 5 V DC
2	M / 5 V DC
3	DI e.0
4	DI e.1
5	DQ e.0
6	DQ e.1

A.14.4 SB 1223 2 X 24 V DC input / 2 X 24 V DC output specifications

Table A-209 General specifications

Technical Data	SB 1223 DI 2 x 24 V DC, DQ 2 x 24 V DC
Article number	6ES7223-0BD30-0XB0
Dimensions W x H x D (mm)	38 x 62 x 21
Weight	40 grams
Power dissipation	1.0 W
Current consumption (SM Bus)	50 mA
Current consumption (24 V DC)	4 mA / Input used

Table A-210 Digital inputs

Technical Data		SB 1223 DI 2 x 24 V DC, DQ 2 x 24 V DC
Number of inputs		2
Type		IEC Type 1 sink
Rated voltage		24 V DC at 4 mA, nominal
Continuous permissible voltage		30 V DC, max.
Surge voltage		35 V DC for 0.5 sec.
Logic 1 signal (min.)		15 V DC at 2.5 mA
Logic 0 signal (max.)		5 V DC at 1 mA
HSC clock input rates (max.)		Single phase: 30 kHz (15 to 26 V DC) Quadrature phase: 20 kHz (15 to 26 V DC)
Isolation (field side to logic)		707 V DC (type test)
Isolation groups		1
Filter times	us settings	0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4,10.0, 12.8, 20.0
	ms settings	0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0
Number of inputs on simultaneously		2
Cable length (meters)		500 shielded, 300 unshielded

Table A-211 Digital outputs

Technical Data	SB 1223 DI 2 x 24 V DC, DQ 2 x 24 V DC
Number of outputs	2
Output type	Solid state - MOSFET (sourcing)
Voltage range	20.4 to 28.8 V DC
Logic 1 signal at max. current	20 V DC min.
Logic 0 signal with 10K Ω load	0.1 V DC max.
Current (max.)	0.5 A
Lamp load	5 W
On state contact resistance	0.6 Ω max.
Leakage current per point	10 µA max.
Pulse Train Output (PTO) rate	20 kHz max., 2 Hz min.[1]
Surge current	5 A for 100 ms max.
Overload protection	No
Isolation (field side to logic)	707 V DC (type test)
Isolation groups	1
Currents per common	1 A
Inductive clamp voltage	L+ minus 48 V, 1 W dissipation
Switching delay	2 µs max. off to on 10 µs max. on to off
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes
Parallel outputs for redundant load control	No
Parallel outputs for increased load	No
Number of outputs on simultaneously	2
Cable length (meters)	500 m shielded, 150 m unshielded

[1] Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

Table A-212 Wiring diagram for the digital input/output SB

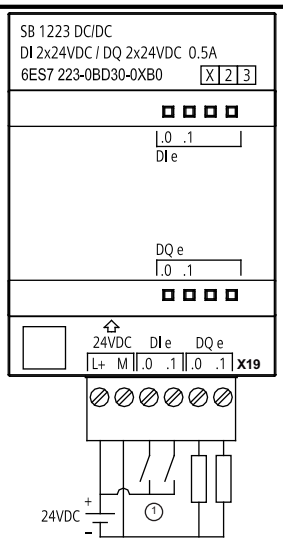
SB 1223 DI 2 x 24 V DC, DQ 2 x 24 V DC (6ES7223-0BD30-0XB0)	
	1 Supports sinking inputs only

Table A-213 Connector pin locations for SB 1223 DI 2 x 24 V DC, DQ 2 x 24 V DC (6ES7223-0BD30-0XB0)

Pin	X19
1	L+ / 24 V DC
2	M / 24 V DC
3	DI e.0
4	DI e.1
5	DQ e.0
6	DQ e.1

A.15 Analog signal boards (SBs)

A.15.1 SB 1231 1 analog input specifications

Table A-214 General specifications

Technical data	SB 1231 AI 1 x 12 bit
Article number	6ES7231-4HA30-0XB0
Dimensions W x H x D (mm)	38 x 62 x 21
Weight	35 grams
Power dissipation	0.4 W
Current consumption (SM Bus)	55 mA
Current consumption (24 V DC)	none

Table A-215 Analog inputs

Technical data	SB 1231 AI 1x12 bit
Number of inputs	1
Type	Voltage or current (differential)
Range	±10 V, ±5 V, ±2.5 or 0 to 20 mA
Resolution	11 bits + sign bit
Full scale range (data word)	-27648 to 27648
Over/Under range (data word)	Voltage: 32511 to 27649 / -27649 to -32512 Current: 32511 to 27649 / 0 to -4864 (Refer to Analog input representation for voltage and Analog input representation for current (Page 1237).)
Overflow/Underflow (data word)	Voltage: 32767 to 32512 / -32513 to -32768 Current: 32767 to 32512 / -4865 to -32768 (Refer to Analog input representation for voltage and Analog input representation for current (Page 1237).)
Maximum withstand voltage / current	±35 V / ±40 mA
Smoothing	None, weak, medium, or strong (refer to Analog input response times for step response time (Page 1236).)
Noise rejection	400, 60, 50, or 10 Hz (refer to Analog input response times for sample rates (Page 1237).)
Accuracy (25 °C / -20 to 60 °C)	±0.3% / ±0.6% of full scale
Input impedance	Voltage: 150 kΩ; Current: 250 Ω
Measuring principle	Actual value conversion
Common mode rejection	40 dB, DC to 60 Hz
Operational signal range	Signal plus common mode voltage must be less than +35 V and greater than -35 V
Isolation (field side to logic)	None
Cable length (meters)	100 m, twisted and shielded

Table A-216 Diagnostics

Technical data	SB 1231 AI 1 x 12 bit
Overflow/underflow	Yes
24 V DC low voltage	no

SB 1231 wiring current transducers

Wiring current transducers are available as 2-wire transducers and 4-wire transducers as shown below.

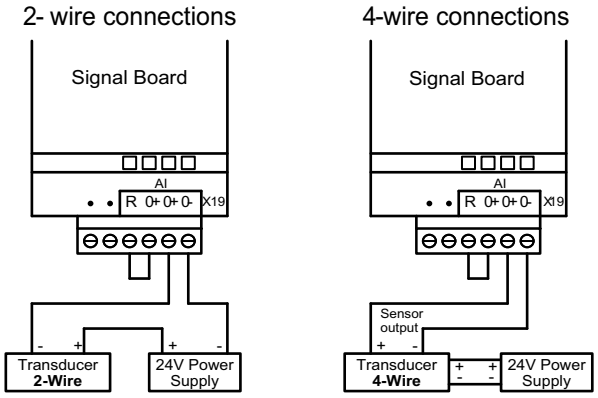


Table A-217 Wiring diagram for the analog input SB

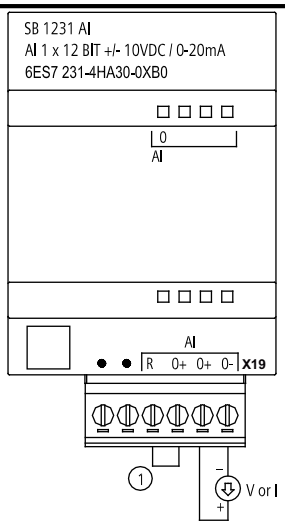
SB 1231 AI x 12 bit (6ES7231-4HA30-0XB0)	
	① Connect "R" and "0+" for current input. Do not connect for voltage input. Note: Connectors must be gold. See Appendix C, Spare Parts for article number.

Table A-218 Connector pin locations for SB 1231 AI x 12 bit (6ES7231-4HA30-0XB0)

Pin	X19 (gold)
1	No connection
2	No connection
3	AI R
4	AI 0+
5	AI 0+
6	AI 0-

A.15.2 SB 1232 1 analog output specifications

Table A-219 General specifications

Technical data	SB 1232 AQ 1 x 12 bit
Article number	6ES7232-4HA30-0XB0
Dimensions W x H x D (mm)	38 x 62 x 21
Weight	40 grams
Power dissipation	1.5 W
Current consumption (SM Bus)	15 mA
Current consumption (24 V DC)	40 mA (no load)

Table A-220 Analog outputs

Technical data	SB 1232 AQ 1 x 12 bit
Number of outputs	1
Type	Voltage or current
Range	±10 V or 0 to 20 mA
Resolution	Voltage: 12 bits Current: 11 bits
Full scale range (data word) Refer to the output ranges for voltage and current (Page 1238).	Voltage: -27648 to 27648 Current: 0 to 27648
Accuracy (25 °C / -20 to 60 °C)	±0.5% / ±1% of full scale
Settling time (95% of new value)	Voltage: 300 µs (R), 750 µs (1 uF) Current: 600 µs (1 mH), 2 ms (10 mH)
Load impedance	Voltage: ≥ 1000 Ω Current: ≤ 600 Ω
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Isolation (field side to logic)	None
Cable length (meters)	100 m, twisted and shielded

Table A-221 Diagnostics

Technical data	SB 1232 AQ 1 x 12 bit
Overflow/underflow	Yes
Short to ground (voltage mode only)	Yes
Wire break (current mode only)	Yes

Table A-222 Wiring diagram for the SB 1232 AQ 1 x 12 bit

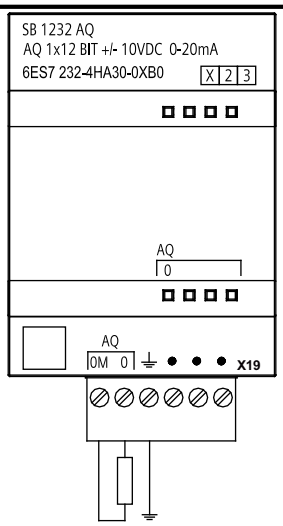
SB 1232 AQ 1 x 12 bit (6ES7232-4HA30-0XB0)	
	
Note: Connectors must be gold. See Appendix C, Spare Parts for article number.	

Table A-223 Connector pin locations for SB 1232 AQ 1 x 12 bit (6ES7232-4HA30-0XB0)

Pin	X19 (gold)
1	AQ 0M
2	AQ 0
3	Functional Earth
4	No connection
5	No connection
6	No connection

A.15.3 Measurement ranges for analog inputs and outputs

A.15.3.1 Step response of the analog inputs

Table A-224 Step response (ms), 0 V to 10 V measured at 95%

Smoothing selection (sample averaging)	Integration time selection			
	400 Hz (2.5 ms)	60 Hz (16.6 ms)	50 Hz (20 ms)	10 Hz (100 ms)
None (1 cycle): No averaging	4.5 ms	18.7 ms	22.0 ms	102 ms
Weak (4 cycles): 4 samples	10.6 ms	59.3 ms	70.8 ms	346 ms
Medium (16 cycles): 16 samples	33.0 ms	208 ms	250 ms	1240 ms
Strong (32 cycles): 32 samples	63.0 ms	408 ms	490 ms	2440 ms
Sample time	**0.156 ms**	**1.042 ms**	**1.250 ms**	**6.250 ms**

A.15.3.2 Sample time and update times for the analog inputs

Table A-225 Sample time and update time

Selection	Sample time	SB update time
400 Hz (2.5 ms)	0.156 ms	0.156 ms
60 Hz (16.6 ms)	1.042 ms	1.042 ms
50 Hz (20 ms)	1.250 ms	1.25 ms
10 Hz (100 ms)	6.250 ms	6.25 ms

A.15.3.3 Measurement ranges of the analog inputs for voltage and current (SB and SM)

Table A-226 Analog input representation for voltage (SB and SM)

System		Voltage Measuring Range				
Decimal	**Hexadecimal**	**±10 V**	**±5 V**	**±2.5 V**	**±1.25 V**	
32767	7FFF[1]	11.851 V	5.926 V	2.963 V	1.481 V	Overflow
32512	7F00					
32511	7EFF	11.759 V	5.879 V	2.940 V	1.470 V	Overshoot range
27649	6C01					
27648	6C00	10 V	5 V	2.5 V	1.250 V	Rated range
20736	5100	7.5 V	3.75 V	1.875 V	0.938 V	
1	1	361.7 µV	180.8 µV	90.4 µV	45.2 µV	
0	0	0 V	0 V	0 V	0 V	
-1	FFFF					
-20736	AF00	-7.5 V	-3.75 V	-1.875 V	-0.938 V	
-27648	9400	-10 V	-5 V	-2.5 V	-1.250 V	
-27649	93FF					Undershoot range
-32512	8100	-11.759 V	-5.879 V	-2.940 V	-1.470 V	
-32513	80FF					Underflow
-32768	8000	-11.851 V	-5.926 V	-2.963 V	-1.481 V	

[1] 7FFF can be returned for one of the following reasons: overflow (as noted in this table), before valid values are available (for example immediately upon a power up), or if a wire break is detected.

Table A-227 Analog input representation for current (SB and SM)

System		Current measuring range		
Decimal	**Hexadecimal**	**0 mA to 20 mA**	**4 mA to 20 mA**	
32767	7FFF	> 23.52 mA	> 22.81 mA	Overflow
32511	7EFF	23.52 mA	22.81 mA	Overshoot range
27649	6C01			
27648	6C00	20 mA	20 mA	Nominal range
20736	5100	15 mA	16 mA	

[1] The wire break value of 32767 (16#7FFF) is always returned regardless of the state of the wire break alarm.

System		Current measuring range		
Decimal	**Hexadecimal**	**0 mA to 20 mA**	**4 mA to 20 mA**	
1	1	723.4 nA	4 mA + 578.7 nA	Nominal range
0	0	0 mA	4 mA	
-1	FFFF			Undershoot range
-4864	ED00	-3.52 mA	1.185 mA	
32767[1]	7FFF		< 1.185 mA	Wire break (4 to 20 mA) (Page 1083)
-32768	8000	< -3.52 mA		Underflow (0 to 20 mA)

[1] The wire break value of 32767 (16#7FFF) is always returned regardless of the state of the wire break alarm.

A.15.3.4 Measurement ranges of the analog outputs for voltage and current (SB and SM)

Table A-228 Analog output representation for voltage (SB and SM)

System		Voltage Output Range	
Decimal	**Hexadecimal**	**± 10 V**	
32767	7FFF	See note 1	Overflow
32512	7F00	See note 1	
32511	7EFF	11.76 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range
20736	5100	7.5 V	
1	1	361.7 µ V	
0	0	0 V	
-1	FFFF	-361.7 µ V	
-20736	AF00	-7.5 V	
-27648	9400	-10 V	
-27649	93FF		Undershoot range
-32512	8100	-11.76 V	
-32513	80FF	See note 1	Underflow
-32768	8000	See note 1	

[1] In an overflow or underflow condition, analog outputs will take on the substitute value of the STOP mode.

Table A-229 Analog output representation for current (SB and SM)

System		Current output range		
Decimal	**Hexadecimal**	**0 mA to 20 mA**	**4 mA to 20 mA**	
32767	7FFF	See note 1	See note 1	Overflow
32512	7F00	See note 1	See note 1	
32511	7EFF	23.52 mA	22.81 mA	Overshoot range
27649	6C01			

[1] In an overflow or underflow condition, analog outputs will take on the substitute value of the STOP mode.

System		Current output range		
Decimal	**Hexadecimal**	**0 mA to 20 mA**	**4 mA to 20 mA**	
27648	6C00	20 mA	20 mA	Rated range
20736	5100	15 mA	16 mA	
1	1	723.4 nA	4 mA + 578.7 nA	
0	0	0 mA	4mA	
-1	FFFF		4 mA to 578.7 nA	Undershoot range
-6912	E500		0 mA	
-6913	E4FF			Not possible. Output value limited to 0 mA.
-32512	8100			
-32513	80FF	See note 1	See note 1	Underflow
-32768	8000	See note 1	See note 1	

[1] In an overflow or underflow condition, analog outputs will take on the substitute value of the STOP mode.

A.15.4 Thermocouple signal boards (SBs)

A.15.4.1 SB 1231 1 analog thermocouple input specifications

NOTE

To use this SB, your CPU firmware must be V2.0 or higher.

Table A-230 General specifications

Technical data	SB 1231 AI 1 x 16 bit Thermocouple
Article number	6ES7231-5QA30-0XB0
Dimensions W x H x D (mm)	38 x 62 x 21
Weight	35 grams
Power dissipation	0.5 W
Current consumption (SM Bus)	5 mA
Current consumption (24 V DC)	20 mA

Table A-231 Analog inputs

Technical data		SB 1231 AI 1x16 bit Thermocouple
Number of inputs		1
Type		Floating TC and mV
Range • Nominal range (data word) • Overrange/underrange (data word) • Overflow/underflow (data word)		See Thermocouple filter selection table (Page 1240).
Resolution	Temperature	0.1° C / 0.1° F
	Voltage	15 bits plus sign
Maximum withstand voltage		±35 V

Technical data	SB 1231 AI 1x16 bit Thermocouple
Noise rejection	85 dB for the selected filter setting (10 Hz, 50 Hz, 60 Hz, 400 Hz)
Common mode rejection	> 120 dB at 120 V AC
Impedance	≥ 10 M Ω
Accuracy	See Thermocouple selection table (Page 1240).
Repeatability	±0.05% FS
Measuring principle	Integrating
Module update time	See Thermocouple filter selection table (Page 1240).
Cold junction error	±1.5° C
Isolation (field side to logic)	707 V DC (type test)
Cable length (meters)	100 m to sensor max.
Wire resistance	100 Ω max.

Table A-232 Diagnostics

Technical data	SB 1231 AI 1 x 16 bit Thermocouple
Overflow/underflow[1]	Yes
Wire break[2, 3]	Yes

1 The overflow and underflow diagnostic alarm information will be reported in the analog data values even if the alarms are disabled in the module configuration.

2 When wire break alarm is disabled and an open wire condition exists in the sensor wiring, the module may report random values.

3 The module performs wire break testing every 6 seconds, which extends the update time by 9 ms for each enable channel once every 6 seconds.

The SM 1231 Thermocouple (TC) analog signal module measures the value of voltage connected to the module inputs.

The SB 1231 Thermocouple analog signal board measures the value of voltage connected to the signal board inputs. The temperature measurement type can be either "Thermocouple" or "Voltage".

- "Thermocouple": The value will be reported in degrees multiplied by ten (for example, 25.3 degrees will be reported as decimal 253).
- "Voltage": The nominal range full scale value will be decimal 27648.

A.15.4.2 Basic operation for a thermocouple

Thermocouples are formed whenever two dissimilar metals are electrically bonded to each other. A voltage is generated that is proportional to the junction temperature. This voltage is small; one microvolt could represent many degrees. Measuring the voltage from a thermocouple, compensating for extra junctions, and then linearizing the result forms the basis of temperature measurement using thermocouples.

When you connect a thermocouple to the SM 1231 Thermocouple module, the two dissimilar metal wires are attached to the module at the module signal connector. The place where the two dissimilar wires are attached to each other forms the sensor thermocouple.

Two more thermocouples are formed where the two dissimilar wires are attached to the signal connector. The connector temperature causes a voltage that adds to the voltage from

the sensor thermocouple. If this voltage is not corrected, then the temperature reported will deviate from the sensor temperature.

Cold junction compensation is used to compensate for the connector thermocouple. Thermocouple tables are based on a reference junction temperature, usually zero degrees Celsius. The cold junction compensation compensates the connector to zero degrees Celsius. The cold junction compensation restores the voltage added by the connector thermocouples. The temperature of the module is measured internally, and then converted to a value to be added to the sensor conversion. The corrected sensor conversion is then linearized using the thermocouple tables.

For optimum operation of the cold junction compensation, the thermocouple module must be located in a thermally stable environment. Slow variation (less than 0.1 °C/minute) in ambient module temperature is correctly compensated within the module specifications. Air movement across the module will also cause cold junction compensation errors.

If better cold junction error compensation is needed, an external iso-thermal terminal block may be used. The thermocouple module provides for use of a 0 °C referenced or 50 °C referenced terminal block.

Selection table for the SB 1231 thermocouple

The ranges and accuracy for the different thermocouple types supported by the SB 1231 Thermocouple signal board are shown in the table below.

Table A-233 Thermocouple selection table

Type	Under-range minimum[1]	Nominal range low limit	Nominal range high limit	Over-range maximum[2]	Normal range [3, 4] accuracy @ 25 °C	Normal range [1, 2,6] accuracy -20 °C to 60 °C
J	-210.0 °C	-150.0 °C	1200.0 °C	1450.0 °C	±0.3 °C	±0.6 °C
	-346.0 °F	-238.0 °F	2192.0 °F	2642.0 °F	±0.5 °F	±1.1 °F
K	-270.0 °C	-200.0 °C	1372.0 °C	1622.0 °C	±0.4 °C	±1.0 °C
	-454.0 °F	-328.0 °F	2501.6 °F	2951.6 °F	±0.7 °F	±1.8 °F
T	-270.0 °C	-200.0 °C	400.0 °C	540.0 °C	±0.5 °C	±1.0 °C
	-454.0 °F	-328.0 °F	752.0 °F	1004.0 °F	±0.9 °F	±1.8 °F
E	-270.0 °C	-200.0 °C	1000.0 °C	1200.0 °C	±0.3 °C	±0.6 °C
	-454.0 °F	-328.0 °F	1832.0 °F	2192.0 °F	±0.5 °F	±1.1 °F
R & S	-50.0 °C	100.0 °C	1768.0 °C	2019.0 °C	±1.0 °C	±2.5 °C
	-58.0 °C	212.0 °F	3214.4 °F	3276.6 °F [5]	±1.8 °F	±4.5 °F
B	0.0 °C	200.0 °C	800.0 °C	--	±2.0 °C	±2.5 °C
	32.0 °F	392.0 °F	1472.0 °F	--	±3.6 °F	±4.5 °F

[1] Thermocouple values below the under-range minimum value are reported as -32768.

[2] Thermocouple values above the over-range maximum value are reported as 32767.

[3] Internal cold junction error is ±1.5 °C for all ranges. This adds to the error in this table. The module requires at least 30 minutes of warm-up time to meet this specification.

[4] In the presence of radiated radio frequency of 970 MHz to 990 MHz, the accuracy of the SM 1231 AI 4 x 16 bit TC may be degraded.

[5] Lower limit of 3276.6 °F with °F reporting

[6] Cold junction compensation error has not been characterized for module ambient temperatures below 0 °C and may exceed the specified value.

Type	Under-range minimum[1]	Nominal range low limit	Nominal range high limit	Over-range maximum[2]	Normal range [3, 4] accuracy @ 25 °C	Normal range [1, 2,6] accuracy -20 °C to 60 °C
B	--	800.0 °C	1820.0 °C	1820.0 °C	±1.0 °C	±2.3 °C
	--	1472.0 °F	3276.6 °F [5]	3276.6 °F [5]	±1.8 °F	±4.1 °F
N	-270.0 °C	-200.0 °C	1300.0 °C	1550.0 °C	±1.0 °C	±1.6 °C
	-454.0 °F	-328.0 °F	2372.0 °F	2822.0 °F	±1.8 °F	±2.9 °F
C	0.0 °C	100.0 °C	2315.0 °C	2500.0 °C	±0.7 °C	±2.7 °C
	32.0 °F	212.0 °F	3276.6 °F [5]	3276.6 °F [5]	±1.3 °F	±4.9 °F
TXK/XK (L)	-200.0 °C	-150.0 °C	800.0 °C	1050.0 °C	±0.6 °C	±1.2 °C
	-328.0 °F	302.0 °F	1472.0 °F	1922.0 °F	±1.1 °F	±2.2 °F
Voltage	-32512	-27648 -80mV	27648 80mV	32511	±0.05%	±0.1%

1 Thermocouple values below the under-range minimum value are reported as -32768.

2 Thermocouple values above the over-range maximum value are reported as 32767.

3 Internal cold junction error is ±1.5 °C for all ranges. This adds to the error in this table. The module requires at least 30 minutes of warm-up time to meet this specification.

4 In the presence of radiated radio frequency of 970 MHz to 990 MHz, the accuracy of the SM 1231 AI 4 x 16 bit TC may be degraded.

5 Lower limit of 3276.6 °F with °F reporting

6 Cold junction compensation error has not been characterized for module ambient temperatures below 0 °C and may exceed the specified value.

Table A-234 Filter selection table for the SB 1231 Thermocouple

Rejection frequency (Hz)	Integration time (ms)	Signal board update time (seconds)
10	100	0.306
50	20	0.066
60	16.67	0.056
400[1]	10	0.036

1 To maintain module resolution and accuracy when 400 Hz rejection is selected, the integration time is 10 ms. This selection also rejects 100 Hz and 200 Hz noise.

It is recommended for measuring thermocouples that a 100 ms integration time be used. The use of smaller integration times will increase the repeatability error of the temperature readings.

NOTE

After power is applied, the module performs internal calibration for the analog-to-digital converter. During this time the module reports a value of 32767 on each channel until valid data is available on that channel. Your user program may need to allow for this initialization time. Because the configuration of the module can vary the length of the initialization time, you should verify the behavior or the module in your configuration. If required, you can include logic in your user program to accommodate the initialization time of the module. You can implement this logic using a polling read in the "Startup OB" which blocks operation until the initialization is complete. You must implement the polling read using immediate access. If the value of the thermocouple polling read is 32767, then the read must be repeated until the value changes. For each module this polling only needs to be executed for the highest numbered used input point in the module (the module inputs are initialized in order from 0 to 7).

Table A-235 Wiring diagram for SB 1231 AI 1 x 16 thermocouple

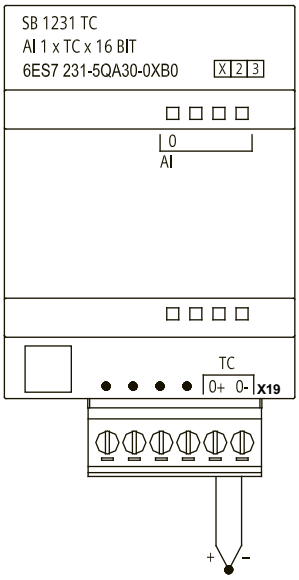
SB 1231 AI 1 x 16 bit thermocouple (6ES7231-5QA30-0XB0)	
	
Note: Connectors must be gold. See Appendix C, Spare Parts for article number.	

Table A-236 Connector pin locations for SB 1231 AI 1 x 16 bit thermocouple (6ES7231-5QA30-0XB0)

Pin	X19 (gold)
1	No connection
2	No connection
3	No connection
4	No connection
5	AI 0- /TC
6	AI 0+ /TC

A.15.5 RTD signal boards (SBs)

A.15.5.1 SB 1231 1 analog RTD input specifications

NOTE
To use this SB, your CPU firmware must be V2.0 or higher.

Table A-237 General specifications

Technical data	SB 1231 AI 1 x 16 bit RTD
Article number	6ES7231-5PA30-0XB0
Dimensions W x H x D (mm)	38 x 62 x 2
Weight	35 grams
Power dissipation	0.7 W
Current consumption (SM Bus)	5 mA
Current consumption (24 V DC)	25 mA

Table A-238 Analog inputs

Technical data		SB 1231 AI 1 x 16 bit RTD
Number of inputs		1
Type		Module referenced RTD and Ohms
Range • Nominal range (data word) • Overrange/underrange (data word) • Overflow/underflow (data word)		See Selection tables (Page 1246).
Resolution	Temperature	0.1 °C/ 0.1 °F
	Voltage	
Maximum withstand voltage		±35 V
Noise rejection		85 dB (10 Hz, 50 Hz, 60 Hz, 400 Hz)
Common mode rejection		> 120 dB
Impedance		≥ 10 MΩ
Accuracy		See Selection tables (Page 1246).
Repeatability		±0.05% FS
Maximum sensor dissipation		0.5 m W
Measuring principle		Integrating
Module update time		See Selection tables (Page 1246).
Isolation (field side to logic)		707 V DC (type test)
Cable length (meters)		100 m to sensor max.
Wire resistance		20 Ω, 2.7 for 10 Ω RTD max.

Table A-239 Diagnostics

Technical data	SB 1231 AI 1 x 16 bit RTD
Overflow/underflow[1, 2]	Yes
Wire break [3]	Yes

[1] The overflow and underflow diagnostic alarm information will be reported in the analog data values even if the alarms are disabled in the module configuration.

[2] For resistance ranges underflow detection is never enabled.

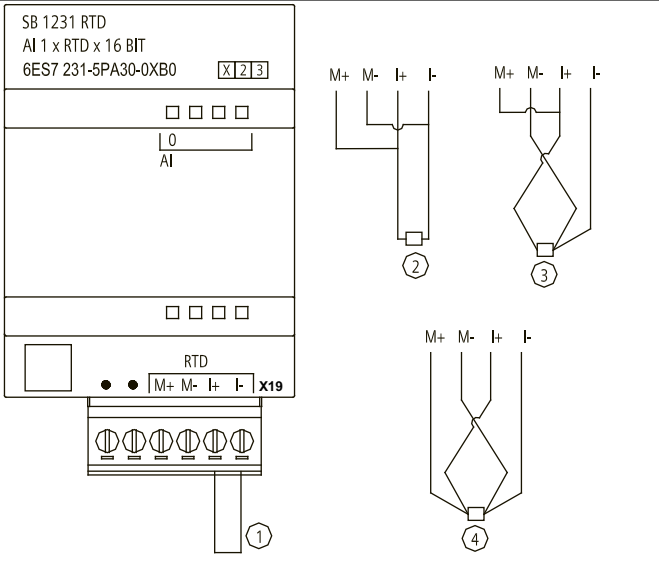
[3] When wire break alarm is disabled and an open wire condition exists in the sensor wiring, the module may report random values.

The SM 1231 RTD analog signal board measures the value of resistance connected to the signal board inputs. The measurement type can be selected as either "Resistor" or "Thermal resistor".

- "Resistor": The nominal range full scale value will be decimal 27648.
- "Thermal resistor": The value will be reported in degrees multiplied by ten (for example, 25.3 degrees will be reported as decimal 253). The climatic range values will be reported in degrees multiplied by one hundred (for example, 25.34 degrees will be reported as decimal 2534).

The SB 1231 RTD signal board supports measurements with 2-wire, 3-wire and 4-wire connections to the sensor resistor.

Table A-240 Wiring diagram for SB 1231 AI 1 x 16 bit RTD

SB 1231 AI 1 x 16 bit RTD (6ES7231-5PA30-0XB0)	
	① Loop-back unused RTD input ② 2-wire RTD ③ 3-wire RTD ④ 4-wire RTD

Note: Connectors must be gold. See Appendix C, Spare Parts for article number.

Table A-241 Connector pin locations for SB 1231 AI 1 x 16 bit RTD (6ES7231-5PA30-0XB0)

Pin	X19 (gold)
1	No connection
2	No connection
3	AI 0 M+ /RTD
4	AI 0 M- /RTD
5	AI 0 I+ /RTD
6	AI 0 I- /RTD

A.15.5.2 Selection tables for the SB 1231 RTD

Table A-242 Ranges and accuracy for the different sensors supported by the RTD modules

Temperature coefficient	RTD type	Under range minimum[1]	Nominal range low limit	Nominal range high limit	Over range maximum[2]	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
Pt 0.003850 ITS90 DIN EN 60751	Pt 100 climatic	-145.00 °C	-120.00 °C	-145.00 °C	-155.00 °C	±0.20 °C	±0.40 °C
	Pt 10	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	±1.0 °C	±2.0 °C
	Pt 50	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	±0.5 °C	±1.0 °C
	Pt 100						
	Pt 200						
	Pt 500						
	Pt 1000						
Pt 0.003902 Pt 0.003916 Pt 0.003920	Pt 100	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	± 0.5 °C	±1.0 °C
	Pt 200						
	Pt 500						
	Pt 1000						
Pt 0.003910	Pt 10	-273.2 °C	-240.0 °C	1100.0 °C	1295 °C	±1.0 °C	±2.0 °C
	Pt 50	-273.2 °C	-240.0 °C	1100.0 °C	1295 °C	±0.8 °C	±1.6 °C
	Pt 100						
	Pt 500						
Ni 0.006720 Ni 0.006180	Ni 100	-105.0 °C	-60.0 °C	250.0 °C	295.0 °C	±0.5 °C	±1.0 °C
	Ni 120						
	Ni 200						
	Ni 500						
	Ni 1000						
LG-Ni 0.005000	LG-Ni 1000	-105.0 °C	-60.0 °C	250.0 °C	295.0 °C	±0.5 °C	±1.0 °C
Ni 0.006170	Ni 100	-105.0 °C	-60.0 °C	180.0 °C	212.4 °C	±0.5 °C	±1.0 °C
Cu 0.004270	Cu 10	-240.0 °C	-200.0 °C	260.0 °C	312.0 °C	±1.0 °	±2.0 °C

1 RTD values below the under-range minimum value are reported as -32768.

2 RTD values above the over-range maximum value are reported as +32768.

Temperature coefficient	RTD type	Under range minimum[1]	Nominal range low limit	Nominal range high limit	Over range maximum[2]	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
Cu 0.004260	Cu 10	-60.0 °C	-50.0 °C	200.0 °C	240.0 °C	±1.0 °C	±2.0 °C
	Cu 50	-60.0 °C	-50.0 °C	200.0 °C	240.0 °C	±0.6 °C	±1.2 °C
	Cu 100						
Cu 0.004280	Cu 10	-240.0 °C	-200.0 °C	200.0 °C	240.0 °C	±1.0 °C	±2.0 °C
	Cu 50	-240.0 °C	-200.0 °C	200.0 °C	240.0 °C	±0.7 °C	±1.4 °C
	Cu 100						

1 RTD values below the under-range minimum value are reported as -32768.

2 RTD values above the over-range maximum value are reported as +32768.

Table A-243 Resistance

Range	Under range minimum	Nominal range low limit	Nominal range high limit	Over range maximum[1]	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
150 Ω	n/a	0 (0 Ω)	27648 (150 Ω)	176.383 Ω	±0.05%	±0.1%
300 Ω	n/a	0 (0 Ω)	27648 (300 Ω)	352.767 Ω	±0.05%	±0.1%
600 Ω	n/a	0 (0 Ω)	27648 (600 Ω)	705.534 Ω	±0.05%	±0.1%

1 Resistance values above the over-range maximum value are reported as 32767.

NOTE

The module reports 32767 on any activated channel with no sensor connected. If open wire detection is also enabled, the module flashes the appropriate red LEDs.

Best accuracy will be achieved for the 10 Ω RTD ranges if 4 wire connections are used.

The resistance of the connection wires in 2 wire mode will cause an error in the sensor reading and therefore accuracy is not guaranteed.

Table A-244 Noise reduction and update times for the RTD modules

Rejection frequency selection	Integration time	4-/2-wire, 1-channel module Update time (seconds)	3-wire, 1-channel module Update time (seconds)
400 Hz (2.5 ms)	10 ms [1]	0.036	0.071
60 Hz (16.6 ms)	16.67 ms	0.056	0.111
50 Hz (20 ms)	20 ms	0.066	1.086
10 Hz (100 ms)	100 ms	0.306	0.611

1 To maintain module resolution and accuracy when the 400 Hz filter is selected, the integration time is 10 ms. This selection also rejects 100 Hz and 200 Hz noise.

NOTE

After power is applied, the module performs internal calibration for the analog-to-digital converter. During this time the module reports a value of 32767 on each channel until valid data is available on that channel. Your user program may need to allow for this initialization time. Because the configuration of the module can vary the length of the initialization time, you should verify the behavior or the module in your configuration. If required, you can include logic in your user program to accommodate the initialization time of the module. You can implement this logic using a polling read in the "Startup OB" which blocks operation until the initialization is complete. You must implement the polling read using immediate access. If the value of the RTD polling read is 32767, then the read must be repeated until the value changes. For each module this polling only needs to be executed for the highest numbered used input point in the module (the module inputs are initialized in order from 0 to 7).

A.16 BB 1297 Battery board

BB 1297 Battery Board

The S7-1200 BB 1297 Battery Board is designed for long-term backup of the Real-time clock. It is pluggable in the signal board slot of the S7-1200 CPU (firmware 3.0 and later versions). You must add the BB 1297 to the device configuration and download the hardware configuration to the CPU for the BB to be functional.

The battery (type CR1025) is not included with the BB 1297 and must be purchased by the user.

NOTE

The BB 1297 is mechanically designed to fit the CPUs with the firmware 3.0 and later versions.

Do not use the BB 1297 with earlier version CPUs as the BB 1297 connector will not plug into the CPU.

WARNING

Risks when installing or connecting an unspecified battery in the BB 1297

Installing an unspecified battery in the BB 1297, or otherwise connecting an unspecified battery to the circuit can result in fire or component damage and unpredictable operation of machinery.

Use only the specified CR1025 battery for backup of the Real-time clock.

Fire or unpredictable operation of machinery can result in death, severe personal injury, or property damage.

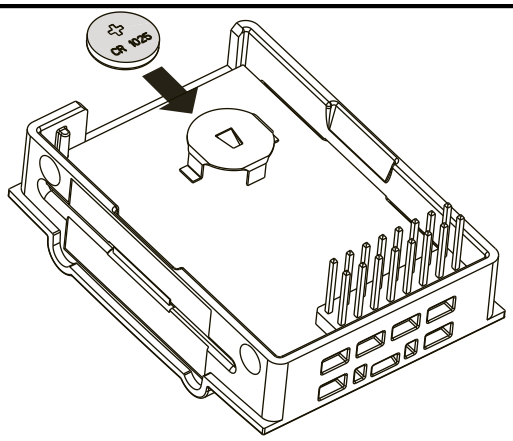
Table A-245 General specifications

Technical data	BB 1297 Battery Board
Article number	6ES7297-0AX30-0XA0
Dimensions W x H x D (mm)	38 x 62 x 21
Weight	28 grams
Power dissipation	0.5 W
Current consumption (SM Bus)	11 mA
Current consumption (24 V DC)	none

Battery (not included)	BB 1297 Battery Board
Hold up time	Approximately 1 year
Battery type	CR1025 Refer to Installing or replacing a battery in the BB 1297 battery board (Page 49)
Nominal voltage	3 V
Nominal capacity	At least 30 mAH

Diagnostics	BB 1297 Battery Board
Critical battery level	< 2.5 V
Battery diagnostic	Low voltage indicator: • Low battery voltage causes the CPU MAINT LED to illuminate with the amber light continuously ON. • Diagnostics Buffer Event: 16#06:2700 "Submodule maintenance demanded: At least one battery exhausted (BATTF)"
Battery status	Battery status bit provided 0 = Battery OK 1 = Battery low
Battery status update	Battery status is updated at power up and then once per day while CPU is in RUN mode.

Table A-246 Insertion diagram for the BB 1297 battery board

BB 1297 battery board (6ES7297-0AX30-0XA0)	
	

A.17 Communication interfaces

A.17.1 PROFIBUS

A.17.1.1 CM 1242-5 PROFIBUS DP SLAVE

Table A-247 Technical specifications of the CM 1242-5

Technical specifications	
Article number	6GK7242-5DX30-0XE0
Interfaces	
Connection to PROFIBUS	9-pin D-sub female connector
Maximum current consumption on the PROFIBUS interface when connecting network components (for example optical network components)	15 mA at 5 V (only for bus termination) *)
Permitted ambient conditions	
Ambient temperature • during storage • during transportation • during operation with a vertical installation (DIN rail horizontal) • during operation with a horizontal installation (DIN rail vertical)	 • -40 °C to 70 °C • -40 °C to 70 °C • 0 °C to 55 °C • 0 °C to 45 °C
Relative humidity at 25 °C during operation, without condensation, maximum	95 %
Degree of protection	IP20
Power supply, current consumption and power loss	
Type of power supply	DC
Power supply from the backplane bus	5 V
Current consumption (typical)	150 mA
Effective power loss (typical)	0.75 W
Electrical isolation • PROFIBUS interface to ground • PROFIBUS interface to internal circuit	710 V DC for 1 minute
Dimensions and weights	
• Width • Height • Depth	• 30 mm • 100 mm • 75 mm
Weight • Net weight • Weight including packaging	 • 115 g • 152 g

A.17.1.2 Pinout of the D-sub socket of the CM 1242-5

PROFIBUS interface

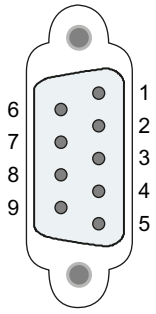


Table A-248 Pinout of the D-sub socket

Pin	Description	Pin	Description
1	- not used -	6	P5V2: +5V power supply
2	- not used -	7	- not used -
3	RxD/TxD-P: Data line B	8	RxD/TxD-N: Data line A
4	RTS	9	- not used -
5	M5V2: Data reference potential (ground DGND)	Housing	Ground connector

A.17.1.3 CM 1243-5 PROFIBUS DP Master

Table A-249 Technical specifications of the CM 1243-5

Technical specifications	
Article number	6GK7243-5DX30-0XE0
Interfaces	
Connection to PROFIBUS	9-pin D-sub female connector
Maximum current consumption on the PROFIBUS interface when connecting network components (for example optical network components)	15 mA at 5 V (only for bus termination) *)
Permitted ambient conditions	
Ambient temperature • during storage • during transportation • during operation with a vertical installation (DIN rail horizontal) • during operation with a horizontal installation (DIN rail vertical)	 • -40 °C to 70 °C • -40 °C to 70 °C • 0 °C to 55 °C • 0 °C to 45 °C
Relative humidity at 25 °C during operation, without condensation, maximum	95 %

Technical specifications	
Degree of protection	IP20
Power supply, current consumption and power loss	
Type of power supply	DC
Power supply / external • minimum • maximum	24 V • 19.2 V • 28.8 V
Current consumption (typical) • from 24 V DC • from the S7-1200 backplane bus	 • 100 mA • 0 mA
Effective power loss (typical) • from 24 V DC • from the S7-1200 backplane bus	 • 2.4 W • 0 W
Power supply 24 V DC / external • Min. cable cross section • Max. cable cross section • Tightening torque of the screw terminals	 • min.: 0.14 mm^2 (AWG 25) • max.: 1.5 mm^2 (AWG 15) • 0.45 Nm (4 lb-in)
Electrical isolation • PROFIBUS interface to ground • PROFIBUS interface to internal circuit	710 V DC for 1 minute
Dimensions and weights	
• Width • Height • Depth	• 30 mm • 100 mm • 75 mm
Weight • Net weight • Weight including packaging	 • 134 g • 171 g

NOTE

The CM 1243-5 (PROFIBUS master module) must receive power from the 24 V DC sensor supply of the CPU.

A.17.1.4 Pinout of the D-sub socket of the CM 1243-5

PROFIBUS interface

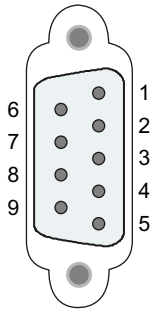


Table A-250 Pinout of the D-sub socket

Pin	Description	Pin	Description
1	- not used -	6	VP: Power supply +5 V only for bus terminating resistors; not for supplying external devices
2	- not used -	7	- not used -
3	RxD/TxD-P: Data line B	8	RxD/TxD-N: Data line A
4	CNTR-P: RTS	9	- not used -
5	DGND: Ground for data signals and VP	Housing	Ground connector

PROFIBUS cable

NOTE

Contacting the shield of the PROFIBUS cable

The shield of the PROFIBUS cable must be contacted.

To do this, strip the insulation from the end of the PROFIBUS cable and connect the shield to functional earth.

A.17.2 CP 1243-7 LTE

NOTE

The CP 1243-7 LTE is not approved for Maritime applications.

NOTE

To use these modules, your CPU firmware must be V2.0 or higher.

Table A-251 Technical specifications of the CP 1243-7 LTE (EU and US versions)

Technical specifications	
Article number • EU version • US version	 6GK7243-7KX30-0XE0 6GK7243-7SX30-0XE0
Transfer rate	
LTE transmission transfer rate • with downlink / maximum • with uplink / maximum	 42 Mbit/s 5.76 Mbit/s
Interfaces	
Number of interfaces / according to Industrial Ethernet	0
Number of electrical connections • for external antenna(s) • for power supply	 1 1
Number of SIM card slots	1
Type of electrical connection • for external antenna(s) • for power supply	 SMA socket (50 ohms) 3-pole terminal block
SIM card slot version	Standard
Wireless technology	
Supported wireless services	• SMS • GPRS Note: GPRS (Multislot Class 10)
Supported wireless networks and operating frequency for transmission	• GSM • UMTS • LTE
Operating frequency for EU version • GSM • UMTS • LTE	 900 MHz, 1800 MHz 900 MHz, 2100 MHz 800 MHz, 1800 MHz, 2600 MHz
Operating frequency for US version • GSM/UMTS • LTE	 850 MHz, 1900 MHz 700 MHz, 1700 MHz
Supply voltage, current consumption, and power loss	
Type of voltage / of the supply voltage	DC
Supply voltage / external	24 V
Supply voltage / external / at DC / rated value	24 V
Relative positive tolerance / at DC / at 24 V	20 %
Relative negative tolerance / at DC / at 24 V	20 %
Consumed current from external supply voltage / at DC / at 24 V • Typical • Maximum	 0.1 A 0.22 A
Ambient conditions	

Technical specifications	
Ambient temperature • For vertical installation / during operation • For horizontally arranged busbars / during operation • During storage • During transport	 -20 ... +60 °C -20 ... +70 °C -40 ... +70 °C -40 ... +70 °C
Relative humidity at 25 °C / without condensation / during operation / maximum	95 %
Protection class	IP20
Design, dimensions, and weights	
Module format	Compact module S7-1200 single width
Width	30 mm
Height	100 mm
Depth	75 mm
Net weight	0.133 kg
Fastening method • 35 mm top hat DIN rail mounting • S7-300 rail mounting • Wall mounting	 Yes No Yes
Product features, product functions, product components / general	
Number of units per CPU / maximum	3
Performance data	
Number of users / telephone numbers / definable / maximum	10
Performance data / open communication	
Number of possible connections / for open communication by means of T blocks / maximum	Like CPU
Performance data / IT functions	
Number of possible connections as email client / maximum	1
Performance data / telecontrol	
Suitable for substation use	Yes
Supported control center connection	Telecontrol Server Basic • through permanent connection • through demand-oriented connection Note: Connects to SCADA system using OPC interface
Supported protocols	• DNP3 • IEC 60870-5
Product function / data buffering if connection is aborted	Yes, 64,000 events
Number of stations / for direct communication / with Telecontrol Server Basic • in send direction / maximum • in receive direction / maximum	 3 15
Performance data / teleservice	
Diagnostics function / online diagnostics with SIMATIC STEP 7	Yes
Supported product functions	• Program download with SIMATIC STEP 7 • Remote firmware update

Technical specifications	
Product functions / managements, configuration, engineering	
Required configuration software	STEP 7 Basic/Professional
Product functions / diagnostics	
Product function / web-based diagnostics	Yes
Product functions / security	
Firewall version	Stateful inspection
Product function / with VPN connection	IPsec, SINEMA RC
Type of encryption algorithms / with VPN connection	AEs-256, AES-192, AES-128, 3DES-168, DES-56
Type of authentication / with VPN connection	Preshared key (PSK), x.509v3 certificates
Type of hashing algorithms / with VPN connection	MD5, SHA-1
Number of possible connections / with VPN connection	1
Supported product functions	• Password protection for teleservice access • Encrypted data transmission
Product functions / time	
Supported protocol	NTP
Supported time synchronization	From control center
Standards, specifications, approvals / hazardous environments	
Certification marking for suitability / CCC / for hazardous zone according to GB standard (GB3836.1, GB3836.8)	Ex nA IIC T4 Gc

NOTE

Preventing CPU interference from antennas

CPU interference can occur if antenna proximity is too close, or if you do not use recommended antennas. For recommended antennas, refer to the SIMATIC NET Operating Instructions ANT896-4ME (Omni-Antenna 0.7 / 1/7 GHz) (https://support.industry.siemens.com/cs/ww/en/view/100699507). Instructions are available in English and German.

A.17.3 CM 1243-2 AS-i master

A.17.3.1 Technical data for the AS-i master CM 1243-2

Table A-252 Technical data for the AS-i master CM 1243-2

Technical data	
Article number	3RK7243-2AA30-0XB0
Firmware version	V1.0
Date	01.12.2011
Interfaces	
Maximum current consumption From the S7-1200 backplane bus From the AS-i cable	 Max. 250 mA, supply voltage S7-1200 communication bus 5 V DC Max. 100 mA
Maximum current carrying capacity between the ASI+/ASI- terminals	8 A
Pin assignment	See section Electrical connections of the AS-i master (Page 1258)
Conductor cross-section	0.2 mm² (AWG 24) ... 3.3 mm² (AWG 12)
ASI connector tightening torque	0.56 Nm
Permissible ambient conditions	
Ambient temperature During storage During transport During the operating phase, with vertical installation (horizontal standard mounting rail) During the operating phase, with horizontal installation (vertical standard mounting rail)	 -40 °C ... 70 °C -40 °C ... 70 °C 0 °C ... 55 °C 0 °C ... 45 °C
Relative humidity at 25 °C during operating phase, no condensation, maximum	95 %
Degree of protection	IP20
Power supply, current consumption, power loss	
Type of power supply	DC
Current consumption (typically) From the S7-1200 backplane bus	 200 mA
Total power loss (typical): • From the S7-1200 backplane bus • From AS-i cable	 1 W 2.4 W
Dimensions and weights	
Width Height Depth	30 mm 100 mm 75 mm
Weight Net weight Weight including packaging	 122 g 159 g

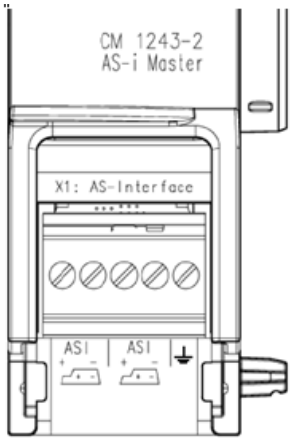
A.17.3.2 Electrical connections of the AS-i master

Power supply of the AS-i master CM 1243-2

The AS-i master CM 1243-2 is supplied over the communications bus of the S7-1200. This means that a diagnostics message can still be sent to the S7-1200 following failure of the AS-i supply voltage. The connection to the communications bus is on the right-hand side of the AS-i master CM 1243-2.

AS-Interface terminals

The removable terminal for connecting the AS-i cable is located behind the lower cover on the front of the AS-i master CM 1243-2.



If the AS-i shaped cable is used, you can recognize the correct polarity of the cable by means of the symbol

Information on how to remove and re-install the terminal block can be found in the Installation chapter (Page 52).

NOTE

Maximum current carrying capacity of the terminal contacts

The current carrying capacity of the connection contacts is max. 8 A. If this value is exceeded on the AS-i cable, the AS-i master CM 1243-2 must not be "looped in" to the AS-i cable, but must instead be connected via a spur line (only one connection pair assigned on the AS-i master CM 1243-2).

Please also ensure that the cables used are suitable for operating temperatures of at least 75 °C if current is being conducted via the AS-i master and currents of greater than 4 amperes are present.

You will find additional information on connecting the AS-i cable in the section "Installation, connection and commissioning of the modules" in the manual "AS-i Master CM 1243-2 and AS-i data decoupling unit DCM 1271 for SIMATIC S7-1200".

Terminal assignment

Label	Meaning
ASI+	AS-i connection – positive polarity
ASI–	AS-i connection – negative polarity
⏚	Functional ground

A.17.4 RS232, RS422, and RS485

A.17.4.1 CB 1241 RS485 specifications

NOTE
To use this CB, your CPU firmware must be V2.0 or higher.

Table A-253 General specifications

Technical data	CB 1241 RS485
Article number	6ES7241-1CH30-1XB0
Dimensions W x H x D (mm)	38 x 62 x 21
Weight	40 grams

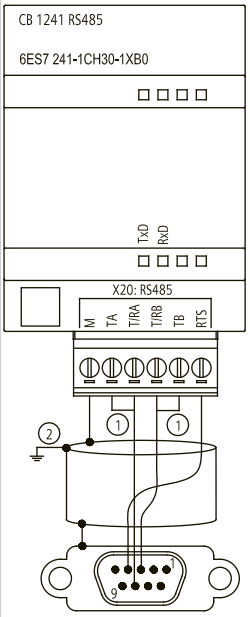
Table A-254 Transmitter and receiver

Technical data	CB 1241 RS485
Type	RS485 (2-wire half-duplex)
Common mode voltage range	-7 V to +12 V, 1 second, 3 VRMS continuous
Transmitter differential output voltage	2 V min. at R_L = 100 Ω 1.5 V min. at R_L = 54 Ω
Termination and bias	10K to +5 V on B, RS485 Pin 3 10K to GND on A, RS485 Pin 4
Optional termination	Short Pin TB to Pin T/RB, effective termination impedance is 127 Ω, connects to RS485 Pin 3 Short Pin TA to Pin T/RA, effective termination impedance is 127 Ω, connects to RS485 Pin 4
Receiver input impedance	5.4K Ω min. including termination
Receiver threshold/sensitivity	+/- 0.2 V min., 60 mV typical hysteresis
Isolation RS485 signal to chassis ground RS485 signal to CPU logic common	707 V DC (type test)
Cable length, shielded	1000 m max.
Baud rate	300 baud, 600 baud, 1.2 kbits, 2.4 kbits, 4.8 kbits, 9.6 kbits (default), 19.2 kbits, 38.4 kbits, 57.6 kbits, 76.8 kbits, 115.2 kbits
Parity	No parity (default), even, odd, Mark (parity bit always set to 1), Space (parity bit always set to 0)

Technical data	CB 1241 RS485
Number of stop bits	1 (default), 2
Flow control	Not supported
Wait time	0 to 65535 ms

Table A-255 Power supply

Technical data	CB 1241 RS485
Power loss (dissipation)	1.5 W
Current consumption (SM Bus), max.	50 mA
Current consumption (24 V DC) max.	80 mA

CB 1241 RS485 (6ES7241-1CH30-1XB0)	
	
① Connect "TA" and TB" as shown to terminate the network. (Terminate only the end devices on the RS485 network.)	
② Use shielded twisted pair cable and connect the cable shield to ground.	

You terminate only the two ends of the RS485 network. The devices in between the two end devices are not terminated or biased. See the topic "Biasing and terminating an RS485 network connector" (Page 838)

Table A-256 Connector pin locations for CB 1241 RS485 (6ES7241-1CH30-1XB0)

Pin	9-Pin connector	X20
1	RS485 / Logic GND	--
2	RS485 / Not Used	--
3	RS485 / TxD+	4 - T/RB
4	RS485 / RTS	6 - RTS
5	RS485 / Logic GND	--
6	RS485 / 5 V Power	--
7	RS485 / Not used	--
8	RS485 / TxD-	3 - T/RA
9	RS485 / Not Used	--
Shell		1 - M

A.17.4.2 CM 1241 RS232 specifications

Table A-257 General specifications

Technical data	CM 1241 RS232
Article number	6ES7241-1AH32-0XB0
Dimensions (mm)	30 x 100 x 75
Weight	150 grams

Table A-258 Transmitter and receiver

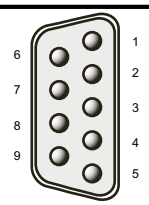
Technical data	CM 1241 RS232
Type	RS232 (full-duplex)
Transmitter output voltage	+/- 5 V min. at R_L = 3K Ω
Transmit output voltage	+/- 15 V DC max.
Receiver input impedance	3 K Ω min.
Receiver threshold/sensitivity	0.8 V min. low, 2.4 max. high 0.5 V typical hysteresis
Receiver input voltage	+/- 30 V DC max.
Isolation RS 232 signal to chassis ground RS 232 signal to CPU logic common	707 V DC (type test)
Cable length, shielded	10 m max.
Baud rate	300 baud, 600 baud, 1.2 kbits, 2.4 kbits, 4.8 kbits, 9.6 kbits (default), 19.2 kbits, 38.4 kbits, 57.6 kbits, 76.8 kbits, 115.2 kbits
Parity	No parity (default), even, odd, Mark (parity bit always set to 1), Space (parity bit always set to 0)

Technical data	CM 1241 RS232
Number of stop bits	1 (default), 2
Flow control	Hardware, software
Wait time	0 to 65535 ms

Table A-259 Power supply

Technical data	CM 1241 RS232
Power loss (dissipation)	1 W
From +5 V DC	200 mA

Table A-260 RS232 connector (male)

Pin	Description	Connector (male)	Pin	Description
1 DCD	Data carrier detect: Input		6 DSR	Data set ready: Input
2 RxD	Received data from DCE: Input		7 RTS	Request to send: Output
3 TxD	Transmitted data to DCE: Output		8 CTS	Clear to send: Input
4 DTR	Data terminal ready: Output		9 RI	Ring indicator (not used)
5 GND	Logic ground		SHELL	Chassis ground

A.17.4.3 CM 1241 RS422/485 specifications

CM 1241 RS422/485 Specifications

Table A-261 General specifications

Technical data	CM 1241 RS422/485
Article number	6ES7241-1CH32-0XB0
Dimensions W x H x H (mm)	30 x 100 x 75
Weight	155 grams

Table A-262 Transmitter and receiver

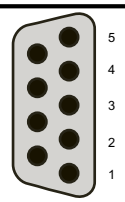
Technical data	CM 1241 RS422/485
Type	RS422 or RS485, 9-pin sub D female connector
Common mode voltage range	-7 V to +12 V, 1 second, 3 VRMS continuous
Transmitter differential output voltage	2 V min. at R_L = 100 Ω 1.5 V min. at R_L = 54 Ω
Termination and bias	10K Ω to +5 V on B, PROFIBUS Pin 3 10K Ω to GND on A, PROFIBUS Pin 8 Internal bias options provided, or no internal bias. In all cases, external termination is required, see Biasing and terminating an RS485 network connector (Page 838) and Configuring the RS422 and RS485 in the S7-1200 Programmable Controller System Manual (Page 885)
Receiver input impedance	5.4K Ω min. including termination
Receiver threshold/sensitivity	+/- 0.2 V min., 60 mV typical hysteresis

Technical data	CM 1241 RS422/485
Isolation RS485 signal to chassis ground RS485 signal to CPU logic common	707 V DC (type test)
Cable length, shielded	1000 m max. (baud rate dependent)
Baud rate	300 baud, 600 baud, 1.2 kbits, 2.4 kbits, 4.8 kbits, 9.6 kbits (default), 19.2 kbits, 38.4 kbits, 57.6 kbits, 76.8 kbits, 115.2 kbits
Parity	No parity (default), even, odd, Mark (parity bit always set to 1), Space (parity bit always set to 0)
Number of stop bits	1 (default), 2
Flow control	XON/XOFF supported for the RS422 mode
Wait time	0 to 65535 ms

Table A-263 Power supply

Technical data	CM 1241 RS422/485
Power loss (dissipation)	1.1 W
From +5 V DC	220 mA

Table A-264 RS485 or RS422 connector (female)

Pin	Description	Connector (female)	Pin	Description
1	Logic or communication ground	 Figure	6 PWR	+5 V with 100 ohm series resistor: Output
2 TxD+ [1]	Connected for RS422 Not used for RS485: Output		7	Not connected
3 TxD+ [2]	Signal B (RxD/TxD+): Input/Output		8 TXD- [2]	Signal A (RxD/TxD-): Input/Output
4 RTS [3]	Request to send (TTL level) Output		9 TXD- [1]	Connected for RS422 Not used for RS485: Output
5 GND	Logic or communication ground		SHELL	Chassis ground

[1] Pin 2 (TxD+) and Pin 9 (TxD-) are the RS422 transmit signals.

[2] Pin 3 (RxD/Tx+) and Pin 8 (RxD/TxD-) are RS485 transmit and receive signals. For RS422, Pin 3 is RxD+ and Pin 8 is RxD-.

[3] The RTS is a TTL level signal and can be used to control another half duplex device based on this signal. It is active when you transmit and is inactive all other times.

A.18 SIMATIC memory cards

Capacity	Article Number
32 GB	6ES7954-8LT04-0AA0
2 GB	6ES7954-8LP04-0AA0
256 MB	6ES7954-8LL04-0AA0
24 MB	6ES7954-8LF04-0AA0
12 MB	6ES7954-8LE04-0AA0
4 MB	6ES7954-8LC04-0AA0

A.19 Input simulators

Table A-265 General specifications

Technical data	8 Position Simulator	14 Position Simulator	CPU 1217C Simulator
Article number	6ES7274-1XF30-0XA0	6ES7274-1XH30-0XA0	6ES7274-1XK30-0XA0
Dimensions W x H x D (mm)	43 x 35 x 23	67 x 35 x 23	93 x 40 x 23
Weight	20 grams	30 grams	43 grams
Points	8	14	14
Used with CPU	CPU 1211C, CPU 1212C	CPU 1214C, CPU 1215C	CPU 1217C

WARNING

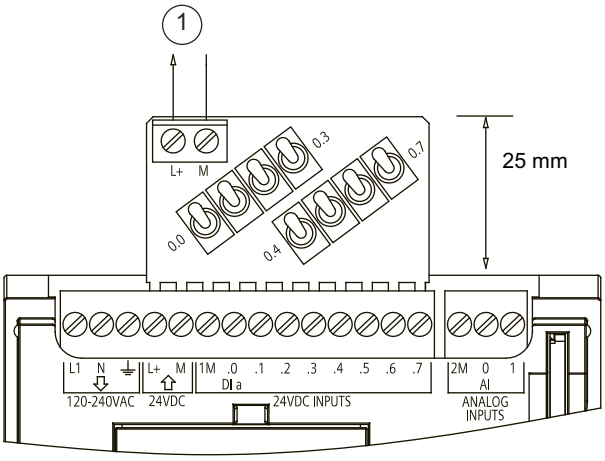
Safe use of input simulators

These input simulators are not approved for use in Class I DIV 2 or Class I Zone 2 hazardous locations. The switches present a potential spark hazard/explosion hazard if used in a Class I DIV 2 or Class I Zone 2 location.

Use these input simulators only in non-hazardous locations. Do not use in Class I DIV 2 or Class I Zone 2 hazardous locations.

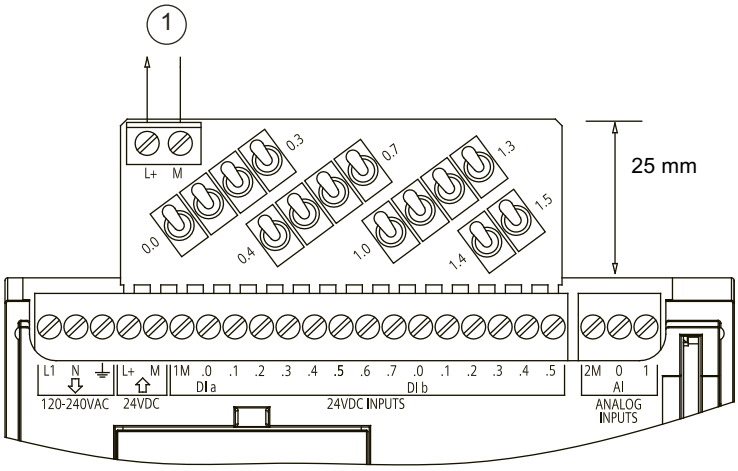
Unapproved use can result in death or serious injury to personnel, and/or damage to equipment.

8 Position Simulator (6ES7274-1XF30-0XA0)



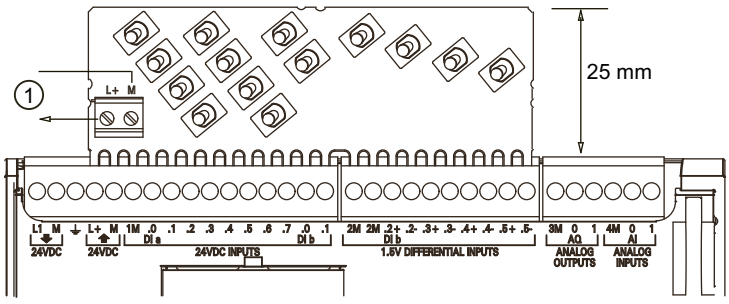
① 24 V DC sensor power out

14 Position Simulator (6ES7274-1XF30-0XA0)



① 24 V DC sensor power out

CPU 1217C Simulator (6ES7274-1XK30-0XA0)



① 24 V DC sensor power out

A.20 S7-1200 Potentiometer module

The S7-1200 Potentiometer module is an accessory for S7-1200 CPU. Each potentiometer creates an output voltage proportional to the position of the potentiometer to drive each of the two CPU analog inputs 0 V DC to 10 V DC. To install the potentiometer:

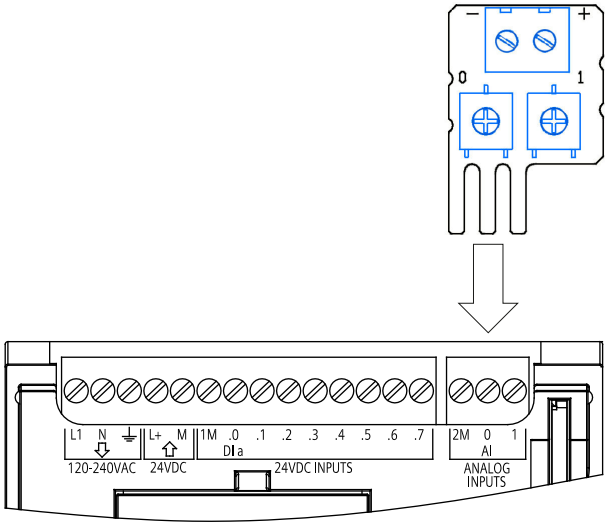
1. Insert the circuit board ‘fingers’ into any S7-1200 CPU analog input terminal block, and connect an external DC power supply to the 2-position connector on the potentiometer module.
2. Use a small screwdriver to make the adjustments: turn the potentiometer clockwise (to the right) to increase the voltage output, and counterclockwise (to the left) to decrease the voltage output.

NOTE

Follow ESD guidelines when handling the S7-1200 Potentiometer module.

Technical data	S7-1200 Potentiometer module
Article number	6ES7274-1XA30-0XA0
Used with CPU	All S7-1200 CPUs
Number of potentiometers	2
Dimensions W x H x D (mm)	20 x 33 x 14
Weight	26 grams
User-supplied voltage input at 2-position connector[1] (Class 2, Limited Power, or sensor power from PLC)	16.4 V DC to 28.8 V DC
Cable length (meters)/type	<30 m, shielded twisted pair
Input current consumption	10 mA max.
Potentiometer voltage output to S7-1200 CPU analog inputs[1]	0 V DC to 10.5 V DC min.
Isolation	Not isolated
Ambient temperature range	-20 °C to 60 °C

[1] Potentiometer module output voltage stability depends on the quality of the user-supplied voltage input at the 2-position connector - consider it as an analog input voltage.

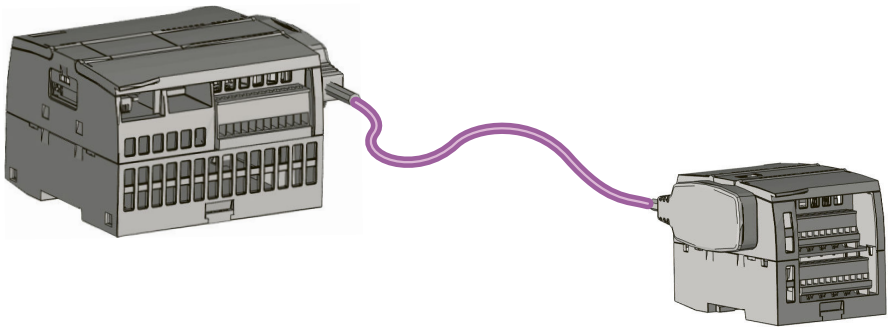


A.21 I/O expansion cable

Table A-266 Expansion cables

Technical Data	
Article number	6ES7290-6AA30-0XA0
Cable length	2 m
Weight	200 g

Refer to the installation section (Page 53) for information about installing and removing the S7-1200 expansion cable.



A.22 Companion products

A.22.1 PM 1207 power module

The PM 1207 is a power supply module for the SIMATIC S7-1200. It provides the following features:

- Input 120/230 V AC, output 24 V DC/2.5A

For more information about this product and for the product documentation, refer to the product catalog for the PM 1207 (https://mall.industry.siemens.com/mall/en/de/Catalog/Product/6EP1332-1SH71).

A.22.2 CSM 1277 compact switch module

The CSM1277 is an Industrial Ethernet compact switch module. It can be used to multiply the Ethernet interface of the S7-1200 to allow simultaneous communication with operator panels, programming devices, or other controllers. It provides the following features:

- 4 x RJ45 sockets for connecting to Industrial Ethernet
- 3 pole plug in terminal strip for connection of the external 24 V DC supply on top
- LEDs for diagnostics and status display of Industrial Ethernet ports
- Article number 6GK7277-1AA00-0AA0

For more information about this product and for the product documentation, refer to the product catalog for the CSM 1277 (https://eb.automation.siemens.com/mall/en/de/Catalog/Search?searchTerm=csm%201277&tab=).

A.22.3 CM CANopen module

The CM CANopen module is a plug-in module between the SIMATIC S7-1200 PLC and any device running CANopen. The CM CANopen can be configured to be both master or slave. There are two CM CANopen modules: the CANopen module (article number 021620-B), and the CANopen (Ruggedized) module (article number 021730-B).

The CANopen module provides the following features:

- Able to connect 3 modules per CPU
- Connects up to 16 CANopen slave nodes
- 256 byte input and 256 byte output per module

- 3 LEDs provide diagnostic information on module, network, and I/O status
- Supports storage of CANopen network configuration in the PLC
- Able to integrate the module in the hardware catalogue of the TIA Portal configuration suite
- CANopen configuration via included CANopen Configuration Studio (included) or via any other external CANopen configuration tool
- Complies to the CANopen communication profiles CiA 301 rev. 4.2 and the CiA 302 rev. 4.1
- Supports transparent CAN 2.0A for custom protocol handling
- Pre-made function blocks available for each PLC programming in TIA portal
- CM CANopen modules include; DSUB with screw terminals for subnetwork. CM CANopen configuration studio CD, and USB configuration cable

For more information about this product and for the product documentation, refer to the product catalog for the CM CANopen module (https://sieportal.siemens.com/su/bjuP8).

A.22.4 RF120C communications module

The RF10C allows Siemens RFID and code reading systems to be connected directly and easily to an S7-1200. The reader is connected to the RF120C via a point-to-point connection. Up to three communications modules can be connected to an S7-1200 to the left of the CPU. The RF120C communications module is configured via the TIA Portal. The article number for the RF120C communications module is 6GT2002-0LA00.

For more information about this product and for the product documentation, refer to the product catalog for the RF120C (https://support.industry.siemens.com/cs/us/en/pv/6GT2002-0LA00/pi?dl=en).

A.22.5 SM 1238 Energy meter module

The SM 1238 Energy Meter 480 V AC is designed for machine-level deployment in an S7-1200 system. It records over 200 different electrical measurement and energy values. It lets you create transparency about the energy requirements of individual components of a production plant down to the machine level. Using the measured values provided by the SM 1238 Energy meter module, you can determine energy consumption and power demand.

For more information about this product and for the product documentation and specifications, refer to the Siemens Industry Online Support Web site (https://support.industry.siemens.com/cs/ww/en/view/109483435).

A.22.6 SIWAREX electronic weighing systems

SIWAREX WP231, WP241, and WP251

The SIWAREX WP231, WP241, and WP251 electronic weighing systems can be used in the S7-1200. These modules use all the features of a modern automation system, such as integrated communication, operation and monitoring, the diagnostic system as well as the configuration tools in the TIA Portal.

- The SIWAREX WP231 (https://support.industry.siemens.com/cs/us/en/view/109780855), calibrator weighing electronic (1 channel) for strain gauge load cells / full bridges (1-4 MV/V) for SIMATIC S7-1200, RS485 and Ethernet - interface, onboard I/O: 4 DI / 4 DO, 1 AO (0/4...20 MA)
- The SIWAREX WP241 (https://support.industry.siemens.com/cs/ww/en/view/109750452), belt weigher electronic (1 channel) for strain gauge load cells / full bridges (1-4 M/V) for SIMATIC S7-1200, RS485 and Ethernet-interface, onboard I/O: 4 DI / 4 DO, 1 AO (0/4...20 MA)
- The SIWAREX WP251 (https://support.industry.siemens.com/cs/ww/en/view/109762579), weighing electronic for batching and filling processes (1 channel) for strain gauge load cells / full bridges (1-4 MV/V) for SIMATIC S7-1200, RS485 and Ethernet - interface, onboard I/O: 4 DI / 4 DO, 1 AO (0/4...20 MA),

Calculating a power budget

B

All S7-1200 CPUs have an internal power supply that provides power to the CPU, any expansion modules, and the 24 V DC Sensor power output.

There are five types of expansion modules: signal modules, communication modules, signal boards, communication boards, and battery boards.

Signal modules (SM) are installed on the right-side of the CPU. You can connect the maximum number of signal modules to your CPU.

The following table shows the maximum number of signal modules you can connect to each CPU model:

CPU model	Maximum number of signal modules allowed
1211C	0
1212C	2
1214C	8
1215C	8
1217C	8

Communication modules (CM) are installed on the left-side of the CPU. You can connect a maximum of 3 communication modules to any CPU.

Signal boards (SB), communications boards (CB), and battery boards (BB) are installed on top of the CPU. You can connect a maximum of 1 signal board, communication board, or battery board to any CPU.

WARNING

Risks with exceeding the power budget

Exceeding either power budget can cause unpredictable behavior.

Use the following information as a guide for determining how much power (or current) the CPU can provide for your configuration.

Unpredictable operation can result in death, severe personal injury, and/or property damage.

Each CPU supplies both 5 V DC and 24 V DC power:

- The CPU provides 5 V DC power for the expansion modules when an expansion module is connected. If you exceed the 5 V DC power budget, connecting the maximum number of expansion modules to your CPU might not be possible. You must remove the expansion modules until the requirement is within the power budget.
- Each CPU has a 24 V DC sensor supply that can supply 24 V DC for local input points, for relay coils on the expansion modules, or for other requirements. If your 24 V DC power requirements exceed the budget of the sensor supply, you can add an external 24 V DC power supply to your system. You must manually connect the external 24 V DC supply to the input points or relay coils on the expansion modules.

WARNING

Risks with parallel connections

Connecting an external 24 V DC power supply in parallel with the DC sensor supply can result in a conflict between the two supplies as each seeks to establish its own preferred output voltage level. The result of this conflict can be shortened lifetime or immediate failure of one or both power supplies, with consequent unpredictable operation of the PLC system.

The DC sensor supply on the CPU and any external power supply should provide power to different points.

Unpredictable operation can result in death, severe personal injury, and/or property damage.

Some of the 24 V DC power input ports in the PLC system are interconnected, with a logic common circuit connecting multiple M terminals. The CPU 24 V DC power supply input, the SM relay coil power input, and a non-isolated analog power supply input are examples of circuits that are interconnected when designated as not isolated in the data sheets. All non-isolated M terminals must connect to the same external reference potential.

WARNING

Risks with connecting non-isolated M terminals to different reference potentials

Connecting non-isolated M terminals to different reference potentials causes unpredictable current flows. Unpredictable current flows can cause PLC damage or abnormal PLC and equipment operation.

Always be sure that all non-isolated M terminals in a PLC system are connected to the same reference potential.

PLC damage or abnormal PLC and equipment operation can cause death, severe personal injury, and/or property damage.

Information about the power budgets of the CPUs and the power requirements of the signal modules is provided in the technical specifications (Page 1090).

Example power budget

The following example shows a sample calculation of the power requirements for a configuration that includes one CPU 1214C AC/DC/Relay, one SB 1223 2 x 24 V DC Input/ 2 x 24 V DC Output, one CM 1241, three SM 1223 8 DC In/8 Relay Out, and one SM 1221 8 DC In. This example has a total of 48 inputs and 36 outputs.

NOTE

The CPU has already allocated the power required to drive the internal relay coils. You do not need to include the internal relay coil power requirements in a power budget calculation.

The CPU in this example provides sufficient 5 V DC current for the SMs, but does not provide enough 24 V DC current from the sensor supply for all of the inputs and expansion relay coils. The I/O requires 456 mA and the CPU provides only 400 mA. This installation requires an additional source of at least 56 mA at 24 V DC power to operate all the included 24 V DC inputs and outputs.

Table B-1 Sample power budget

CPU power budget	**5 V DC**	**24 V DC**
CPU 1214C AC/DC/Relay	1600 mA	400 mA
	Minus	
System requirements	**5 V DC**	**24 V DC**
CPU 1214C, 14 inputs	-	14 * 4 mA = 56 mA
1 SB 1223 2 x 24 V DC Input/ 2 x 24 V DC Output	50 mA	2 * 4 mA = 8 mA
1 CM 1241 RS422/485, 5 V power	220 mA	
3 SM 1223, 5 V power	3 * 145 mA = 435 mA	-
1 SM 1221, 5 V power	1 * 105 mA = 105 mA	-
3 SM 1223, 8 inputs each	-	3 * 8 * 4 mA = 96 mA
3 SM 1223, 8 relay coils each	-	3 * 8 * 11 mA = 264 mA
1 SM 1221, 8 inputs each	-	8 * 4 mA = 32 mA
Total requirements	810 mA	456 mA
	Equals	
Current balance	**5 V DC**	**24 V DC**
Current balance total	790 mA	(56 mA)

Form for calculating your power budget

Use the following table to determine how much power (or current) the S7-1200 CPU can provide for your configuration. Refer to the technical specifications (Page 1090) for the power budgets of your CPU model and the power requirements of your signal modules.

Table B-2 Calculations for a power budget

CPU power budget	**5 V DC**	**24 V DC**
	Minus	
System requirements	**5 V DC**	**24 V DC**
Total requirements		

CPU power budget	**5 V DC**	**24 V DC**
	Equals	
Current balance	**5 V DC**	**24 V DC**
Current balance total		

Ordering Information

C

C.1 CPU modules

Table C-1 S7-1200 CPUs

CPU models		Article number
CPU 1211C	CPU 1211C DC/DC/DC	6ES7211-1AE40-0XB0
	CPU 1211C AC/DC/Relay	6ES7211-1BE40-0XB0
	CPU 1211C DC/DC/Relay	6ES7211-1HE40-0XB0
CPU 1212C	CPU 1212C DC/DC/DC	6ES7212-1AE40-0XB0
	CPU 1212C AC/DC/Relay	6ES7212-1BE40-0XB0
	CPU 1212C DC/DC/Relay	6ES7212-1HE40-0XB0
CPU 1214C	CPU 1214C DC/DC/DC	6ES7214-1AG40-0XB0
	CPU 1214C AC/DC/Relay	6ES7214-1BG40-0XB0
	CPU 1214C DC/DC/Relay	6ES7214-1HG40-0XB0
CPU 1215C	CPU 1215C DC/DC/DC	6ES7215-1AG40-0XB0
	CPU 1215C AC/DC/Relay	6ES7215-1BG40-0XB0
	CPU 1215C DC/DC/Relay	6ES7215-1HG40-0XB0
CPU 1217C	CPU 1217C DC/DC/DC	6ES7217-1AG40-0XB0

C.2 Signal modules (SMs), signal boards (SBs), and battery boards (BBs)

Table C-2 Signal modules (SMs)

Signal modules		Article number
Digital input	SM 1221 8 x 24 V DC Input (Sink/Source)	6ES7221-1BF32-0XB0
	SM 1221 16 x 24 V DC Input (Sink/Source)	6ES7221-1BH32-0XB0
Digital output	SM 1222 8 x 24 V DC Output (Source)	6ES7222-1BF32-0XB0
	SM 1222 16 x 24 V DC Output (Source)	6ES7222-1BH32-0XB0
	SM 1222 16 x 24 V DC Output (Sinking)	6ES7222-1BH32-1XB0
	SM 1222 8 x Relay Output	6ES7222-1HF32-0XB0
	SM 1222 8 x Relay Output (Changeover)	6ES7222-1XF32-0XB0
	SM 1222 16 x Relay Output	6ES7222-1HH32-0XB0
Digital input / output	SM 1223 8 x 24 V DC Input (Sink/Source) / 8 x 24 V DC Output (Source)	6ES7223-1BH32-0XB0
	SM 1223 16 x 24 V DC Input (Sink/Source) / 16 x 24 V DC Output (Source)	6ES7223-1BL32-0XB0
	SM 1223 16 x 24 V DC Input / 16 x 24 V DC Output (Sinking)	6ES7223-1BL32-1XB0
	SM 1223 8 x 24 V DC Input (Sink/Source) / 8 x Relay Output	6ES7223-1PH32-0XB0
	SM 1223 16 x 24 V DC Input (Sink/Source) / 16 x Relay Output	6ES7223-1PL32-0XB0

Signal modules		Article number
Digital input / output	SM 1223 8 x 120/230 V AC Input (Sink/Source) / 8 x Relay Outputs	6ES7223-1QH32-0XB0
Analog input	SM 1231 4 x Analog Input	6ES7231-4HD32-0XB0
	SM 1231 8 x Analog Input	6ES7231-4HF32-0XB0
	SM 1231 4 x Analog Input x 16 bit (high feature)	6ES7231-5ND32-0XB0
	SM 1238 Energy Meter 480 V AC	6ES7238-5XA32-0XB0
Analog output	SM 1232 2 x Analog Output	6ES7232-4HB32-0XB0
	SM 1232 4 x Analog Output	6ES7232-4HD32-0XB0
Analog input / output	SM 1234 4 x Analog Input / 2 x Analog Output	6ES7234-4HE32-0XB0
RTD and thermocouple	SM 1231 TC 4 x 16 bit	6ES7231-5QD32-0XB0
	SM 1231 TC 8 x 16 bit	6ES7231-5QF32-0XB0
	SM 1231 RTD 4 x 16 bit	6ES7231-5PD32-0XB0
	SM 1231 RTD 8 x 16 bit	6ES7231-5PF32-0XB0
Technology modules	SM 1278 4xIO-Link Master	6ES7278-4BD32-0XB0
	SIWAREX WP231, calibrator weighing electronic (1 channel) for strain gauge load cells / full bridges (1-4 MV/V) for SIMATIC S7-1200, RS485 and Ethernet - interface, onboard I/O: 4 DI / 4 DO, 1 AO (0/4...20 MA)	7MH4960-2AA01
	SIWAREX WP241, belt weigher electronic (1 channel) for strain gauge load cells / full bridges (1-4 M/V) for SIMATIC S7-1200, RS485 and Ethernet-interface, onboard I/O: 4 DI / 4 DO, 1 AO (0/4...20 MA)	7MH4960-4AA01
	SIWAREX WP251, weighing electronic for batching and filling processes (1 channel) for strain gauge load cells / full bridges (1-4 MV/V) for SIMATIC S7-1200, RS485 and Ethernet - interface, onboard I/O: 4 DI / 4 DO, 1 AO (0/4...20MA),	7MH4960-6AA01

Table C-3 Signal boards (SB) and battery boards (BBs)

Signal and battery boards		Article number
Digital input	SB 1221 200 kHz 4 x 24 V DC Input (Source)	6ES7221-3BD30-0XB0
	SB 1221 200 kHz 4 x 5 V DC Input (Source)	6ES7221-3AD30-0XB0
Digital output	SB 1222 200 kHz 4 x 24 V DC Output (Sink/Source)	6ES7222-1BD30-0XB0
	SB 1222 200 kHz 4 x 5 V DC Output (Sink/Source)	6ES7222-1AD30-0XB0
Digital input / output	SB 1223 2 x 24 V DC Input (Sink) / 2 x 24 V DC Output (Source)	6ES7223-0BD30-0XB0
	SB 1223 200 kHz 2 x 24 V DC Input (Source) / 2 x 24 V DC Output (Sink/Source)	6ES7223-3BD30-0XB0
	SB 1223 200 kHz 2 x 5 V DC Input (Source) / 2 x 5 V DC Output (Sink/Source)	6ES7223-3AD30-0XB0
Analog	SB 1232 1 Analog Output	6ES7232-4HA30-0XB0
	SB 1231 1 Analog Input	6ES7231-4HA30-0XB0
	SB 1231 1 Analog Input Thermocouple	6ES7231-5QA30-0XB0
	SB 1231 1 Analog Input RTD	6ES7231-5PA30-0XB0
Battery	BB 1297 Battery Board (battery type CR1025 not included)	6ES7297-0AX30-0XA0

C.3 Communication

Table C-4 Communication module (CM)

Communication module (CM)			Article number
RS232, RS422, and RS485	CM 1241 RS232	RS232	6ES7241-1AH32-0XB0
	CM 1241 RS422/485	RS422/485	6ES7241-1CH32-0XB0
PROFIBUS	CM 1243-5	PROFIBUS Master	6GK7243-5DX30-0XE0
	CM 1242-5	PROFIBUS Slave	6GK7242-5DX30-0XE0
AS-i Master	CM 1243-2	AS-i Master	3RK7243-2AA30-0XB0

Table C-5 Communication board (CB)

Communication board (CB)			Article number
RS485	CB 1241 RS485	RS485	6ES7241-1CH30-1XB0

Table C-6 Communication Processor (CP)

CP	Interface	Article number
CP 1243-7 LTE-US	LTE	6GK7243-7SX30-0XE0
CP 1243-7 LTE-EU	LTE	6GK7243-7KX30-0XE0
CP 1243-1	IE-interface	6GK7243-1BX30-0XE0
CP 1243-8 IRC	IE-interface	6GK7243-8RX30-0XE0

Table C-7 Accessories

Accessory			Article number
Antenna	ANT896-4ME	wireless	6GK5896-4ME00-0AA0

Table C-8 Connectors

Type of Connector		Article number
RS485	35-degree cable output, screw-terminal connection	6ES7972-0BA42-0XA0
	35-degree cable output, FastConnect connection	6ES7972-0BA60-0XA0

C.4 Fail-safe CPUs and signal modules

Table C-9 Fail-safe CPUs

Fail-safe CPU models		Article number
CPU 1212FC	CPU 1212FC DC/DC/DC	6ES7212-1AF40-0XB0
	CPU 1212FC DC/DC/Relay	6ES7212-1HF40-0XB0
CPU 1214FC	CPU 1214FC DC/DC/DC	6ES7214-1AF40-0XB0
	CPU 1214FC DC/DC/Relay	6ES7214-1HF40-0XB0
CPU 1215FC	CPU 1215FC DC/DC/DC	6ES7215-1AF40-0XB0
	CPU 1215FC DC/DC/Relay	6ES7215-1HF40-0XB0

Table C-10 Fail-safe signal modules

Functional Safety signal modules		Article number
Digital input	SM 1226 F-DI 16 x 24 V DC	6ES7226-6BA32-0XB0
Digital output	SM 1226 F-DQ 4 x 24 V DC	6ES7226-6DA32-0XB0
	SM 1226 F-DQ 2 x Relay	6ES7226-6RA32-0XB0

C.5 Other modules

Table C-11 Companion products

Item		Article number
Power supply	PM 1207 power supply	6EP1332-1SH71
Ethernet switch	CSM 1277 Ethernet switch - 4 ports	6GK7277-1AA10-0AA0
CM CANopen	CANopen for SIMATIC S7-1200	021620-B
	CANopen (Ruggedized) for SIMATIC S7-1200	021730-B
RF120C	RF120C communications module	6GT2002-0LA00

C.6 Memory cards

Table C-12 Memory cards

SIMATIC memory cards	Article number
SIMATIC MC 32 GB	6ES7954-8LT04-0AA0
SIMATIC MC 2 GB	6ES7954-8LP04-0AA0
SIMATIC MC 256 MB	6ES7954-8LL04-0AA0
SIMATIC MC 24 MB	6ES7954-8LF04-0AA0
SIMATIC MC 12 MB	6ES7954-8LE04-0AA0
SIMATIC MC 4 MB	6ES7954-8LC04-0AA0

C.7 Spare parts and other hardware

Table C-13 Expansion cables, simulators, and end retainers

Item		Article number
I/O expansion cable	I/O Expansion cable, 2 m	6ES7290-6AA30-0XA0
I/O simulator	Simulator (1211C/1212C - 8 position)	6ES7274-1XF30-0XA0
	Simulator (1214C/1215C - 14 position)	6ES7274-1XH30-0XA0
	Simulator, CPU 1217C	6ES7274-1XK30-0XA0
Potentiometer module	S7-1200 Potentiometer module	6ES7274-1XA30-0XA0
Ethernet strain relief	Single port RJ45 strain relief, 10/100 Mbit/sec	6ES7290-3AA30-0XA0
	Dual port RJ45 strain relief, 10/100 Mbit/sec	6ES7290-3AB30-0XA0
Spare door kit	CPU 1211C/1212C	6ES7291-1AA30-0XA0
	CPU 1214C	6ES7291-1AB30-0XA0

Item		Article number
Spare door kit	CPU 1215C	6ES7291-1AC30-0XA0
	CPU 1217C	6ES7291-1AD30-0XA0
	Signal module, 45 mm	6ES7291-1BA30-0XA0
	Signal module, 70 mm	6ES7291-1BB30-0XA0
	Communication module (for use with 6ES72xx-xxx32-0XB0 and 6ES72xx-xxx30-0XB0 modules)	6ES7291-1CC30-0XA0
End Retainer	End Retainer Thermoplastic, 10 MM	8WH9150-0CA00
	End Retainer Steel, 10.3 MM	8WA1805

Replacing the terminal block connector

It is important to use the correct terminal block for your module. Refer to the tables below and your module specifications to determine the correct terminal block replacement.

NOTE

Keyed removable terminal blocks

PLCs always require correct wiring to ensure safety and proper operation.

When replacing the terminal block in your CPU or SM, it is important that you use the correct terminal block and correct wiring source for your module.

The keyed feature helps prevent you from accidentally placing a high voltage wired terminal block into a low voltage module, or from placing a special voltage wired terminal block into a normal voltage module. Some terminal blocks are specifically keyed at left, at right or at middle.

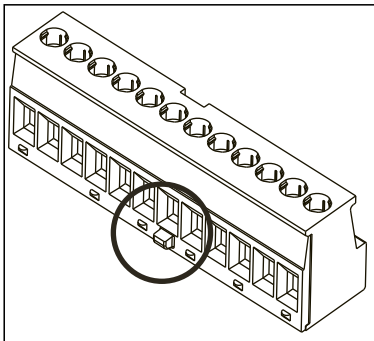
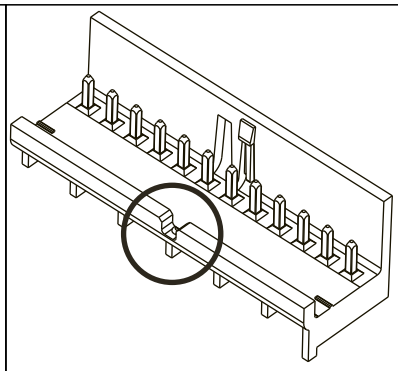
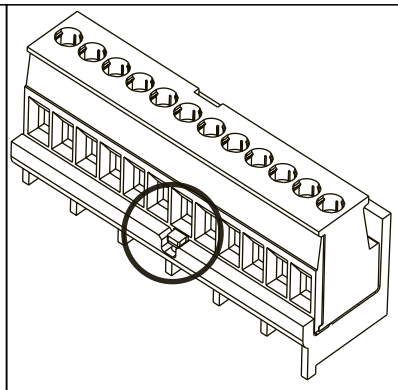
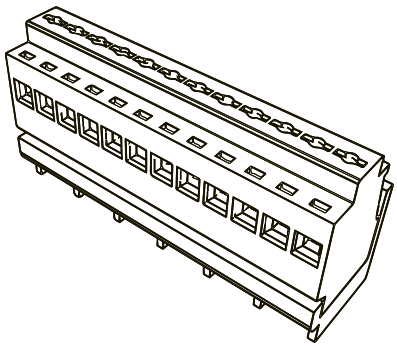
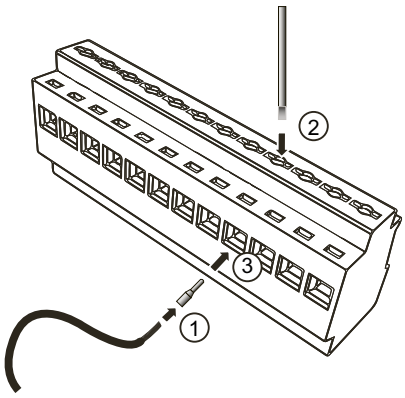
		
Removable terminal block (keyed example shown	Key on device	Key on device only fits appropriate removable terminal block
		
Push-in terminal block	Follow these steps: 1. Insert wire and crimp connector. 2. Depress the membrane using a small screwdriver to open slot. 3. Insert crimped connector into opened slot on terminal block.	

Table C-14 S7-1200 CPU V4.0 and later - Terminal block spare kits

If you have S7-1200 CPU V4.0 and later (article number)	Use this terminal block spare kit (4/pk)		
	Terminal block (screw-type) article number	Equivalent Push-in terminal block article number	Terminal block description
CPU 1211C DC/DC/DC (6ES7211-1AE40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AH30-0XA0	6ES7292-2AH30-0XA0	8 pin, tin-plated
	6ES7292-1AP30-0XA0	6ES7292-2AP30-0XA0	14 pin, tin-plated
CPU 1211C DC/DC/Relay (6ES7211-1HE40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AH40-0XA0	6ES7292-2AH40-0XA0	8 pin, tin-plated, keyed
	6ES7292-1AP30-0XA0	6ES7292-2AP30-0XA0	14 pin, tin-plated
CPU 1211C AC/DC/Relay (6ES7211-1BE40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AH40-0XA0	6ES7292-2AH40-0XA0	8 pin, tin-plated, keyed
	6ES7292-1AP40-0XA0	6ES7292-2AP40-0XA0	14 pin, tin-plated, keyed
CPU 1212C DC/DC/DC (6ES7212-1AE40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AH30-0XA0	6ES7292-2AH30-0XA0	8 pin, tin-plated

If you have S7-1200 CPU V4.0 and later (article number)	Use this terminal block spare kit (4/pk)		
	Terminal block (screw-type) article number	Equivalent Push-in terminal block article number	Terminal block description
CPU 1212C DC/DC/DC (6ES7212-1AE40-0XB0)	6ES7292-1AP30-0XA0	6ES7292-2AP30-0XA0	14 pin, tin-plated
CPU 1212C DC/DC/Relay (6ES7212-1HE40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AH40-0XA0	6ES7292-2AH40-0XA0	8 pin, tin-plated, keyed
	6ES7292-1AP30-0XA0	6ES7292-2AP30-0XA0	14 pin, tin-plated
CPU 1212C AC/DC/Relay (6ES7212-1BE40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AH40-0XA0	6ES7292-2AH40-0XA0	8 pin, tin-plated, keyed
	6ES7292-1AP40-0XA0	6ES7292-2AP40-0XA0	14 pin, tin-plated, keyed
CPU 1214C DC/DC/DC (6ES7214-1AG40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AM30-0XA0	6ES7292-2AM30-0XA0	12 pin, tin-plated
	6ES7292-1AV30-0XA0	6ES7292-2AV30-0XA0	20 pin, tin-plated
CPU 1214C DC/DC/Relay (6ES7214-1HG40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AM40-0XA0	6ES7292-2AM40-0XA0	12 pin, tin-plated, keyed
	6ES7292-1AV30-0XA0	6ES7292-2AV30-0XA0	20 pin, tin-plated
CPU 1214C AC/DC/Relay (6ES7214-1BG40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AM40-0XA0	6ES7292-2AM40-0XA0	12 pin, tin-plated, keyed
	6ES7292-1AV40-0XA0	6ES7292-2AV40-0XA0	20 pin, tin-plated, keyed
CPU 1215C DC/DC/DC (6ES7215-1AG40-0XB0)	6ES7292-1BF30-0XB0	6ES7292-2BF30-0XB0	6 pin, gold-plated
	6ES7292-1AM30-0XA0	6ES7292-2AM30-0XA0	12 pin, tin-plated
	6ES7292-1AV30-0XA0	6ES7292-2AV30-0XA0	20 pin, tin-plated
CPU 1215C DC/DC/Relay (6ES7215-1HG40-0XB0)	6ES7292-1BF30-0XB0	6ES7292-2BF30-0XB0	6 pin, gold-plated
	6ES7292-1AM40-0XA0	6ES7292-2AM40-0XA0	12 pin, tin-plated, keyed
	6ES7292-1AV30-0XA0	6ES7292-2AV30-0XA0	20 pin, tin-plated
CPU 1215C AC/DC/Relay (6ES7215-1BG40-0XB0)	6ES7292-1BF30-0XB0	6ES7292-2BF30-0XB0	6 pin, gold-plated
	6ES7292-1AM40-0XA0	6ES7292-2AM40-0XA0	12 pin, tin-plated, keyed
	6ES7292-1AV40-0XA0	6ES7292-2AV40-0XA0	20 pin, tin-plated, keyed
CPU 1217C DC/DC/DC (6ES7217-1AG40-0XB0)	6ES7292-1BF30-0XB0	6ES7292-2BF30-0XB0	6 pin, gold-plated
	6ES7292-1AK30-0XA0	6ES7292-2AK30-0XA0	10 pin, pin-plated
	6ES7292-1AR30-0XA0	6ES7292-2AR30-0XA0	16 pin, pin-plated
	6ES7292-1AT30-0XA0	6ES7292-2AT30-0XA0	18 pin, tin-plated

Table C-15 S7-1200 SMs V3.2 and later - Terminal block spare kits

If you have S7-1200 SMs V3.2 and later (article number)	Use this terminal block spare kit (4/pk)		
	Terminal block (screw-type) article number	Equivalent Push-in terminal block article number	Terminal block description
SM 1221 DI 8 x DC (6ES7221-1BF32-0XB0)	6ES7292-1AG30-0XA0	6ES7292-2AG30-0XA0	7 pin, tin-plated
SM 1222 DQ 8 x DC (6ES7222-1BF32-0XB0)	6ES7292-1AG30-0XA0	6ES7292-2AG30-0XA0	7 pin, tin-plated
SM 1222 DQ 8 x Relay (6ES7222-1HF32-0XB0)	6ES7292-1AG40-0XA1	6ES7292-2AG40-0XA1	7 pin, tin-plated, keyed-left

If you have S7-1200 SMs V3.2 and later (article number)	Use this terminal block spare kit (4/pk)		
	Terminal block (screw-type) article number	Equivalent Push-in terminal block article number	Terminal block description
SM 1238 Energy Meter 480 V AC (6ES7238-5XA32-0XB0) for voltage input (top)	6ES7292-1AG40-0XA2	6ES7292-2AG40-0XA2	7-pin, tin-plated, keyed-middle
SM 1238 Energy Meter 480 V AC (6ES7238-5XA32-0XB0) for current input (bottom)	6ES7292-1AG30-0XA0	6ES7292-2AG30-0XA0	7-pin, tin-plated
SM 1231 AI 4 x 13 bit (6ES7231-4HD32-0XB0)	6ES7292-1BG30-0XA0	6ES7292-2BG30-0XA0	7 pin, gold-plated
SM 1232 AQ 2 x 14 bit (6ES7232-4HB32-0XB0)	6ES7292-1BG30-0XA0	6ES7292-2BG30-0XA0	7 pin, gold-plated
SM 1231 AI 4 x TC (6ES7231-5QD32-0XB0)	6ES7292-1BG30-0XA0	6ES7292-2BG30-0XA0	7 pin, gold-plated
SM 1231 AI 4 x 16 bit (6ES7231-5ND32-0XB0)	6ES7292-1BG30-0XA0	6ES7292-2BG30-0XA0	7 pin, gold-plated
SM 1221 DI 16 x DC (6ES7221-1BH32-0XB0)	6ES7292-1AG30-0XA0	6ES7292-2AG30-0XA0	7 pin, tin-plated
SM 1222 DQ 16 x DC (6ES7222-1BH32-0XB0)	6ES7292-1AG30-0XA0	6ES7292-2AG30-0XA0	7 pin, tin-plated
SM 1222 DQ 16 x Relay (6ES7222-1HH32-0XB0)	6ES7292-1AG40-0XA0	6ES7292-2AG40-0XA0	7 pin, tin-plated, keyed-right
SM 1223 DI 8 x DC/DQ 8 x DC (6ES7223-1BH32-0XB0)	6ES7292-1AG30-0XA0	6ES7292-2AG30-0XA0	7 pin, tin-plated
SM 1223 8 x DC/8 x Relay (6ES7223-1PH32-0XB0)	6ES7292-1AG30-0XA0	6ES7292-2AG30-0XA0	7 pin, tin-plated
	6ES7292-1AG40-0XA0	6ES7292-2AG40-0XA0	7 pin, tin-plated, keyed-right
SM 1223 8 x AC/8 x Relay (6ES7223-1QH32-0XB0)	6ES7292-1AG40-0XA0	6ES7292-2AG40-0XA0	7 pin, tin-plated, keyed-right
SM 1234 AI 4 / AQ 2 (6ES7234-4HE32-0XB0)	6ES7292-1BG30-0XA0	6ES7292-2BG30-0XA0	7 pin, gold-plated
SM 1231 AI 8 x 13 BIT (6ES7231-4HF32-0XB0)	6ES7292-1BG30-0XA0	6ES7292-2BG30-0XA0	7 pin, gold-plated
SM 1232 AQ 4 x 14 bit (6ES7232-4HD32-0XB0)	6ES7292-1BG30-0XA0	6ES7292-2BG30-0XA0	7 pin, gold-plated
SM 1231 AI 4 x RTD (6ES7231-5PD32-0XB0)	6ES7292-1BG30-0XA0	6ES7292-2BG30-0XA0	7 pin, gold-plated
SM 1231 AI 8 x TC (6ES7231-5QF32-0XB0)	6ES7292-1BG30-0XA0	6ES7292-2BG30-0XA0	7 pin, gold-plated
SM 1278 IO LINK (6ES7278-4BD32 0XB0)	6ES7292-1AG30-0XA0	6ES7292-2AG30-0XA0	7 pin, tin-plated
SM 1222 DQ 8 x Relay (Changeover) (6ES7222-1XF32-0XB0)	6ES7292-1AL40-0XA0	6ES7292-2AL40-0XA0	11 pin, tin-plated, keyed
SM 1223 DI 16 x DC/DQ 16 x DC (6ES7223-1BL32-0XB0)	6ES7292-1AL30-0XA0	6ES7292-2AL30-0XA0	11 pin, tin-plated

If you have S7-1200 SMs V3.2 and later (article number)	Use this terminal block spare kit (4/pk)		
	Terminal block (screw-type) article number	Equivalent Push-in terminal block article number	Terminal block description
SM 1223 DI 16 x DC/DQ 16 x Relay (6ES7223-1PL32-0XB0)	6ES7292-1AL30-0XA0	6ES7292-2AL30-0XA0	11 pin, tin-plated
	6ES7292-1AL40-0XA0	6ES7292-2AL40-0XA0	11 pin, tin-plated, keyed
SM 1231 AI 8 x RTD (6ES7231-5PF32-0XB0)	6ES7292-1BL30-0XA0	6ES7292-2BL30-0XA0	11 pin, gold-plated

Table C-16 S7-1200 SBs, CBs, and BBs - Terminal block spare kits

If you have S7-1200 SB, CB, or BB (article number)	Use this terminal block spare kit (4/pk)	
	Terminal block (screw-type) article number	Terminal block description
SB 1221 DI 4 x 5 V DC (6ES7221-3AD30-0XB0)	6ES7292-1BF30-0XA0	6-pin
SB 1221 DI 4 x 5 V DC (6ES7221-3AD30-0XB0)		
SB 1221 DI 4 x 24 V DC (6ES7221-3BD30-0XB0)		
SB 1222 DQ 4 x 5 V DC (6ES7222-1AD30-0XB0)		
SB 1222 DQ 4 x 24 V DC (6ES7222-1BD30-0XB0)		
SB 1223 DI 2x24 V DC/DQ 2x24 V DC (6ES7223-0BD30-0XB0)		
SB 1223 DI 2x5 V DC / DQ 2x5 V DC (6ES7223-3AD30-0XB0)		
SB 1223 DI 2x24 V DC / DQ 2x24 V DC (6ES7223-3BD30-0XB0)		
SB 1231 AI 1 x 12 BIT (6ES7231-4HA30-0XB0)		
SB 1231 AI 1 x RTD (6ES7231-5PA30-0XB0)		
SB 1231 AI 1 x TC (6ES7231-5QA30-0XB0)		
SB 1232 AQ 1x12 BIT (6ES7232-4HA30-0XB0)		
CB 1231 RS485 (6ES7241-1CH30-1XB0)		
BB 1297 Battery (6ES7297-0AX30-0XA0)		

Table C-17 Fail-safe CPUs - Terminal block spare kit

If you have Fail-safe CPU (article number)	Use this terminal block spare kit (4/pk)		
	Terminal block article number	Equivalent Push-in terminal block article number	Terminal block description
CPU 1212FC DC/DC/DC (6ES7212-1AF40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AH30-0XA0	6ES7292-2AH30-0XA0	12 pin, tin-plated
	6ES7292-1AP30-0XA0	6ES7292-2AP30-0XA0	20 pin, tin-plated
CPU 1212FC DC/DC/Relay (6ES7212-1HF40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AH40-0XA0	6ES7292-2AH40-0XA0	3 pin, gold-plated
	6ES7292-1AP30-0XA0	6ES7292-2AP30-0XA0	12 pin, tin-plated, keyed
CPU 1214FC DC/DC/DC (6ES7214-1AF40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AM30-0XA0	6ES7292-2AM30-0XA0	12 pin, tin-plated
	6ES7292-1AV30-0XA0	6ES7292-2AV30-0XA0	20 pin, tin-plated
CPU 1214FC DC/DC/Relay (6ES7214-1HF40-0XB0)	6ES7292-1BC30-0XA0	6ES7292-2BC30-0XA0	3 pin, gold-plated
	6ES7292-1AM40-0XA0	6ES7292-2AM40-0XA0	12 pin, tin-plated, keyed
	6ES7292-1AV30-0XA0	6ES7292-2AV30-0XA0	20 pin, tin-plated

If you have Fail-safe CPU (article number)	Use this terminal block spare kit (4/pk)		
	Terminal block article number	Equivalent Push-in terminal block article number	Terminal block description
CPU 1215FC DC/DC/DC (6ES7215-1AF40 0XB0)	6ES7292-1BF30-0XB0	6ES7292-2BF30-0XB0	6 pin, gold-plate
	6ES7292-1AM30-0XA0	6ES7292-2AM30-0XA0	12 pin, tin-plated
	6ES7292-1AV30-0XA0	6ES7292-2AV30-0XA0	20 pin, tin-plated
CPU 1215FC DC/DC/Relay (6ES7215-1HF40 0XB0)	6ES7292-1BF30-0XB0	6ES7292-2BF30-0XB0	6 pin, gold-plated
	6ES7292-1AM40-0XA0	6ES7292-2AM40-0XA0	2 pin, tin-plated, keyed
	6ES7292-1AV30-0XA0	6ES7292-2AV30-0XA0	20 pin, tin-plated

Table C-18 Fail-safe signal modules - Terminal block spare kit

If you have Fail-safe signal module (article number)	Use this Terminal block spare kit (4/pk)		
	Terminal block article number	Equivalent Push-in terminal block article number	Terminal block description
SM 1226 F-DI (6ES7226-6BA32-0XB0)	6ES7292-1AL30-0XA0	6ES7292-2AL30-0XA0	11 pin, tin-plated
SM 1226 F-DQ (6ES7226-6DA32-0XB0)	6ES7292-1AL30-0XA0	6ES7292-2AL30-0XA0	11 pin, tin-plated
SM 1226 F-Relay (6ES7226-6RA32-0XB0)	6ES7292-1AL40-0XA0	6ES7292-2AL40-0XA0	11 pin, tin-plated, keyed

C.8 Programming software

Table C-19 Programming software

SIMATIC software		Article number
Programming software	STEP 7 Basic V20	6ES7822-0AE24-0YA5
	STEP 7 Professional V20	6ES7822-1AE24-0YA5

C.9 OPC UA Licenses

Table C-20 OPC UA Licenses for S7-1200

OPU UA licenses		Article number
SIMATIC license	SIMATIC OPC UA S7-1200 Basic DVD	6ES7823-0BA00-2BA0
	SIMATIC OPC UA S7-1200 Basic DL	6ES7823-0BE00-2BA0

Device exchange and spare parts compatibility D

D.1 Replacing a CPU that has protection of confidential configuration data

The assignment of passwords to protect confidential PLC configuration data also has an impact on the replacement parts scenario.

Rules for the replacement parts scenario

Observe the following rules for the replacement parts scenario:

Configuration of the replacement CPU via TIA Portal

- If possible, use a CPU that does not have a project configuration or a configured password for protection of confidential PLC configuration data as the replacement CPU.
  Advantage: You can load the project into the replacement CPU without any further preparation.
- If the replacement CPU has already been configured, you must reset the CPU to the factory settings (Page 1057) and select these options:
  - Delete password for protection of confidential PLC configuration data
  - Format memory card, if the CPU has a memory card

Replacing a CPU with configuration data on a SIMATIC memory card

- If you have **not** assigned a password to a CPU in your project to protect confidential PLC configuration data, you can insert the memory card of the CPU to be replaced into a new, unused CPU without any further action.
- If the replacement CPU has already been configured with a password, you must first reset this CPU to the factory settings (Page 1057) using the option "Delete password for protection of confidential PLC configuration data".
- If you have assigned the same password for protection of confidential PLC configuration data to a group of CPUs, you can also assign the group password to the replacement CPU from the device configuration (Page 145) in the TIA Portal. In this case you can, for example, insert a memory card with the current project into the CPU and put it into operation without any further password handling.
- If you assign different passwords to each CPU in your project, go online (Page 1051) and set the password for protection of confidential data for the replacement CPU with the online and diagnostics tools. Select "Set password to protect confidential PLC configuration data" from the online functions. (Page 1056)

D.2 Exchanging a V3.0 CPU for a V4.x CPU

To upgrade a V3.0 CPU to a V4.x CPU, you must replace the CPU hardware. You cannot upgrade a V3.0 CPU to a V4.x CPU by firmware update.

Then in your STEP 7 project, you can replace your V3.0 CPU with a V4.x CPU (Page 136) and use your existing STEP 7 project that you designed for the V3.0 CPU.

When you replace a V3.0 CPU with a V4.x CPU, you might also want to check for and apply firmware updates (Page 117) to your connected signal and communication modules.

NOTE

No device exchange possible in STEP 7 from V4.x to V3.0

You can exchange a V3.0 CPU for a V4.x CPU, but you cannot exchange a V4.x CPU for a V3.0 CPU after you download the configuration. If you want to view or otherwise use your existing STEP 7 project for a V3.0 CPU, make an archive of your project prior to the device exchange.

Note that if you have not downloaded the exchanged device configuration, you can undo it. After downloading, however, you cannot undo the device exchange from V3.0 to V4.x.

You need to be aware of some configuration and operational changes between the two CPU versions.

Upgrading STEP 7 projects

To work with a STEP 7 project that is STEP 7 V13 or older, you must first upgrade the project to STEP 7 V13 SP1 or SP2. Then you can upgrade the STEP 7 V13 SPx project to the current STEP 7 version.

⚠ WARNING

Risks with editing and executing program logic from older versions of STEP 7

You cannot upgrade a project that is STEP 7 V13 or older to the current version by copying program logic.

You must upgrade your STEP 7 project as defined above.

Executing STEP 7 program logic that you copied from an older version to a newer version can cause unpredictable program behavior and can result in death or severe personal injury.

Organization blocks

You can configure OB execution to be interruptible or non-interruptible (Page 77). In projects from V3.0 CPUs, STEP 7 set all OBs by default to be non-interruptible.

STEP 7 sets all OB priorities (Page 77) to the values they were in the V3.0 CPU STEP 7 project.

You can subsequently change the interruption or priority settings if you choose.

The Diagnostic error interrupt OB (Page 71) start information references the submodule as a whole if no diagnostics event is pending.

CPU password protection

STEP 7 sets the password protection level (Page 151) for the V4.x CPU to be the equivalent password protection level that was set for the V3.0 CPU, and assigns the V3.0 password to the "Full access (no protection)" password for the V4.x CPU:

V3.0 protection level	V4.x access level
No protection	Full access (no protection)
Write protection	Read access
Write/read protection	HMI access

Note that the V4.x access level "No access (complete protection)" did not exist for V3.0.

Web server

If you use user-defined Web pages in your V3.0 project, store them in your project installation folder under the subfolder "UserFiles\Webserver" prior to upgrading your project. If you store your user-defined pages at this location, saving the STEP 7 project will also save the user-defined Web pages.

If you exchange a V3.0 CPU for a V4.x CPU, your Web server project setting (Page 755) for activating the Web server and HTTPS setting will be the same as it was in V3.0. You can then configure users, privileges, passwords (Page 757), and languages (Page 755) as needed to use the Web server. If you do not configure users with additional privileges, then you are limited as to what you can view from the standard Web pages (Page 768). The S7-1200 V4.x CPU does not support the former pre-configured "admin" user and password.

The S7-1200 V3.0 Web server Data log page provided a "Download and Clear" operation. The V4.x Web server File browser page (Page 794), from which you access data logs, no longer provides this feature. Instead, the Web server provides the ability to download and delete data log files.

Transfer card incompatibility

You cannot use a V3.0 transfer card (Page 106) to transfer a V3.0 program to a V4.x CPU. You must open the V3.0 project in STEP 7, change the device to a V4.x CPU (Page 136), and download the STEP 7 project to your V4.x CPU. After you have changed your project to a V4.x project, you can then make a V4.x transfer card for subsequent program transfers.

GET/PUT communication

By default, S7-1200 V3.0 CPUs enabled GET/PUT communication. When you replace your V3.0 CPU with a V4.x CPU (Page 136), you see a message in the compatibility information section stating that GET/PUT is enabled.

Motion control support

S7-1200 V4.x CPUs do not support the V1.0 and V2.0 motion libraries. If you perform a device exchange for a STEP 7 project with V1.0 or V2.0 motion libraries, the device exchange substitutes compatible V3.0 motion control instructions (Page 509) for the V1.0 or V2.0 motion library instructions at compile.

If you perform a device exchange from a V3.0 CPU to a V4.x CPU for a STEP 7 project that contains two different motion control instruction versions (V3.0 and V5.0), the device exchange substitutes compatible V5.0 motion control instructions (Page 509) at compile.

During a device exchange from a V3.0 CPU to a V4.x CPU, the motion control Technological Object (TO) version does not automatically change from V3.0 to V5.0. If you want to upgrade to the later versions, you must go to the Instruction tree and select the required S7-1200 Motion Control version for your project.

The S7-1200 V4.x CPU allows the following motion control versions:

- V3.0
- V4.0
- V5.0
- V6.0

The TO structure is different between motion control versions V3.0 and V5.0. All associated blocks change as well. Block interfaces, watch tables, and traces update to the new motion control V5.0 structure. You can find the differences between the V3.0 CPU and V4.x CPU motion control axis parameters in the following two tables:

V3.0 CPU (Motion control V3.0)	V4.x CPU (Motion control V5.0)
Config.General.LengthUnit	Units.LengthUnit
Config.Mechanics.PulsesPerDriveRevolution	Actor.DriveParameter.PulsesPerDriveRevolution
Config.Mechanics.LeadScrew	Mechanics.LeadScrew
Config.Mechanics.InverseDirection	Actor.InverseDirection
Config.DynamicLimits.MinVelocity	DynamicLimits.MinVelocity
Config.DynamicLimits.MaxVelocity	DynamicLimits.MaxVelocity
Config.DynamicDefaults.Acceleration	DynamicDefaults.Acceleration
Config.DynamicDefaults.Deceleration	DynamicDefaults.Deceleration
Config.DynamicDefaults.EmergencyDeceleration	DynamicDefaults.EmergencyDeceleration
Config.DynamicDefaults.Jerk	DynamicDefaults.Jerk
Config.PositionLimits_SW.Active	PositionLimitsSW.Active
Config.PositionLimits_SW.MinPosition	PositionLimitsSW.MinPosition
Config.PositionLimits_SW.MaxPosition	PositionLimitsSW.MaxPosition
Config.PositionLimits_HW.Active	PositionLimitsHW.Active
Config.PositionLimits_HW.MinSwitchedLevel	PositionLimitsHW.MinSwitchLevel
Config.PositionLimits_HW.MaxSwitchedLevel	PositionLimitsHW.MaxSwitchLevel
Config.Homing.AutoReversal	Homing.AutoReversal
Config.Homing.Direction	Homing.ApproachDirection
Config.Homing.SideActiveHoming	Sensor[1].ActiveHoming.SideInput
Config.Homing.SidePassiveHoming	Sensor[1].PassiveHoming.SideInput
Config.Homing.Offset	Sensor[1].ActiveHoming.HomePositionOffset
Config.Homing.FastVelocity	Homing.ApproachVelocity
Config.Homing.SlowVelocity	Homing.ReferencingVelocity
MotionStatus.Position	Position

V3.0 CPU (Motion control V3.0)	V4.x CPU (Motion control V5.0)
MotionStatus.Velocity	Velocity
MotionStatus.Distance	StatusPositioning.Distance
MotionStatus.TargetPosition	StatusPositioning.TargetPosition
StatusBits.SpeedCommand	StatusBits.VelocityCommand
StatusBits.Homing	StatusBits.HomingCommand

The only "commandtable" parameter that is renamed is the array with the commands:

V3.0	V4.x
Config.Command[]	Command[]

Note: The array "Command[]" is a UDT of the type "TO_CmdTab_Config_Command" in V3.0 and "TO_Struct_Command" in V4.x.

Instruction changes

The following instructions have changes in parameters or behavior:

- RDREC and WRREC (Page 330)
- CONV (Page 258)

HMI panel communication

If you had one or more HMI panels (Page 36) connected to your S7-1200 V3.0 CPU, the communication to the S7-1200 V4.x CPU depends on the type of communication you use and the firmware version of the HMI panel. Recompile and download your project to the CPU and the HMI and/or update your HMI firmware.

Requirement to recompile program blocks

After exchanging a V3.0 CPU for a V4.x CPU, you must recompile all program blocks before you can download them to the V4.x CPU. Additionally, if any of the blocks have know-how protection (Page 159) or copy protection bound to a PLC serial number (Page 160), you must remove the protection before you compile and download the blocks. (You do not, however, need to deactivate copy protection bound to a memory card.) After a successful compile, you can reconfigure the know-how protection and/or PLC serial number copy protection. Note that if your project includes any blocks with know-how protection that an OEM (Original Equipment Manufacturer) provided, you must contact the OEM to provide V4.x versions of those blocks.

In general, Siemens recommends that you recompile the hardware configuration and software in STEP 7 and download to all devices in your project after the device exchange. Correct any errors that compiling the project finds, and recompile until you have no errors. Then, you can download the project to the V4.x CPU.

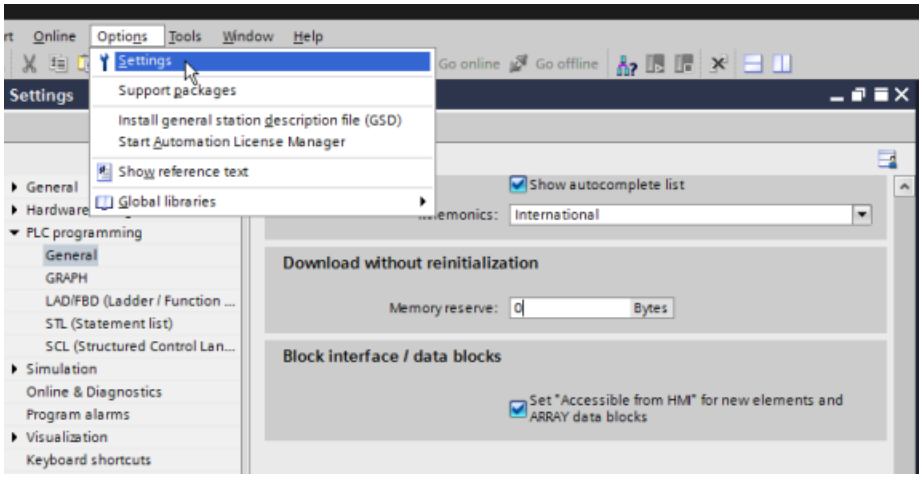
S7-1200 V3.0 projects might not fit in S7-1200 V4.x CPUs

S7-1200 V4.0 and later added a reserve area of 100 bytes to each DB to support download without reinitialization.

You can remove the 100-byte reserve area from DBs prior to attempting to download a V3.0 project to a V4.x CPU.

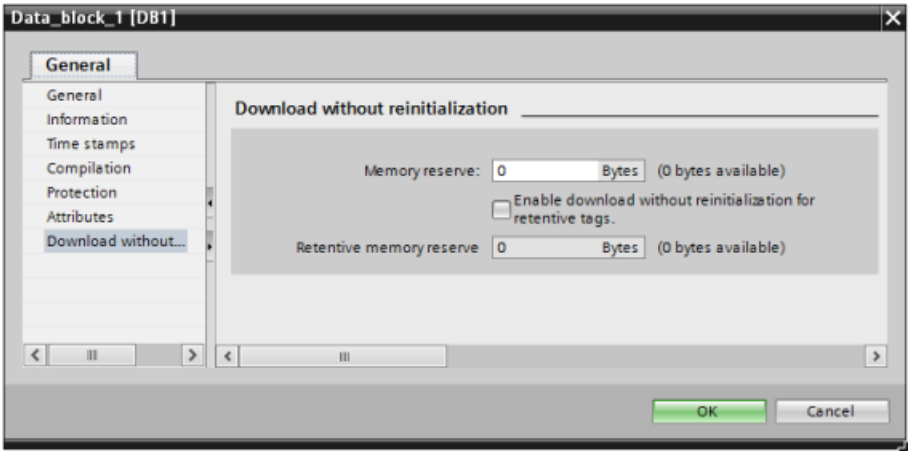
To remove the 100-byte reserve area, follow these steps before you perform the device exchange:

1. From the TIA Portal main menu, select the Options > Settings menu command.
2. From the navigation tree, open the PLC programming > General node.
3. In the "Download without reinitialization" area, set the memory reserve to 0 bytes.



If you have already performed the device exchange, you must remove the 100-byte reserve from each block individually:

1. From the project tree, right-click a data block from the Program blocks folder and select Properties from the shortcut menu.
2. In the Data block properties dialog, select the "Download without reinitialization" node.
3. Set the memory reserve to 0 bytes.
4. Repeat for each data block in your project.



D.3 S7-1200 V3.0 and earlier terminal block spare kits

Table D-1 S7-1200 CPU V3.0 and earlier - Terminal Block spare kits

If you have S7-1200 CPU V3.0 and earlier (article number)	Use this terminal block spare kit (4/pk)	
	Terminal block article number	Terminal block description
CPU 1211C DC/DC/DC (6ES7211-1AE31-0XB0)	6ES7292-1BC30-0XA0 6ES7292-1AH30-0XA0 6ES7292-1AP30-0XA0	3 pin, gold-plated 8 pin, gold-plated 14 pin, tin-plated
CPU 1211C AC/DC/Relay (6ES7211-1BE31-0XB0)		
CPU 1211C DC/DC/Relay (6ES7211-1HE31-0XB0)		
CPU 1212C DC/DC/DC (6ES7212-1AE31-0XB0)		
CPU 1212C AC/DC/Relay (6ES7212-1BE31-0XB0)		
CPU 1212C DC/DC/Relay (6ES7212-1HE31-0XB0)		
CPU 1214C DC/DC/DC (6ES7214-1AG31-0XB0)	6ES7292-1BC30-0XA0 6ES7292-1AM30-0XA0 6ES7292-1AV30-0XA0	3 pin, gold-plated 12 pin, tin-plated 20 pin, tin-plated
CPU 1214C AC/DC/Relay (6ES7214-1BG31-0XB0)		
CPU 1214C DC/DC/Relay (6ES7214-1HG31-0XB0)		
CPU 1215C DC/DC/DC (6ES7215-1AG31-0XB0)	6ES7292-1BF30-0XB0 6ES7292-1AM30-0XA0 6ES7292-1AV30-0XA0	6 pin, gold-plated 12 pin, tin-plated 20 pin, tin-plated
CPU 1215C AC/DC/Relay (6ES7215-1BG31-0XB0)		
CPU 1215C DC/DC/Relay (6ES7215-1HG31-0XB0)		

Table D-2 S7-1200 SMs V3.0 and earlier - Terminal Block spare kits

If you have S7-1200 SM V3.0 and earlier (article number)	Use this terminal block spare kit (4/pk)	
	Terminal block article number	Terminal block description
SM 1221 DI 8 x DC (6ES7221-1BF30-0XB0)	6ES7292-1AG30-0XA0	7 pin, tin-plated
SM 1222 DQ 8 x DC (6ES7222-1BF30-0XB0)		
SM 1222 DQ 8 x Relay (6ES7222-1HF30-0XB0)		
SM 1231 AI 4 x 13 bit (6ES7231-4HD30-0XB0)	6ES7292-1BG30-0XA0	7 pin, gold-plated
SM 1232 AQ 2 x 14 bit (6ES7232-4HB30-0XB0)		
SM 1231 AI 4 x TC (6ES7231-5QD30-0XB0)		
SM 1231 AI 4 x 16 bit (6ES7231-5ND30-0XB0)		
SM 1221 DI 16 x DC (6ES7221-1BH30-0XB0)	6ES7292-1AG30-0XA0	7 pin, tin-plated
SM 1222 DQ 16 x DC (6ES7222-1BH30-0XB0)		
SM 1222 DQ 16 x Relay (6ES7222-1HH30-0XB0)		
SM 1223 DI 8 x DC/DQ 8x DC (6ES7223-1BH30-0XB0)		
SM 1223 8 x DC/8 x Relay (6ES7223-1PH30-0XB0)		
SM 1223 8 x AC/8 x Relay (6ES7223-1QH30-0XB0)		
SM 1234 AI 4 / AQ 2 (6ES7234-4HE30-0XB0)	6ES7292-1BG30-0XA0	7 pin, gold-plated
SM 1231 AI 8 x 13 bit (6ES7231-4HF30-0XB0)		
SM 1232 AQ 4 x 14 bit (6ES7232-4HD30-0XB0)		
SM 1231 AI 4 x RTD (6ES7231-5PD30-0XB0)		
SM 1231 AI 8 x TC (6ES7231-5QF30-0XB0)		
SM 1222 DQ 8 x Relay (Changeover) (6ES7222-1XF30-0XB0)	6ES7292-1AL30-0XA0	11 pin, tin-plated

If you have S7-1200 SM V3.0 and earlier (article number)	Use this terminal block spare kit (4/pk)	
	Terminal block article number	Terminal block description
SM 1223 DI 16 x DC/DQ 16 x DC (6ES7223-1BL30-0XB0)	6ES7292-1AL30-0XA0	11 pin, tin-plated
SM 1223 16 x DC/16 x Relay (6ES7223-1PL30-0XB0)		
SM 1231 AI 8 x RTD (6ES7231-5PF30-0XB0)	6ES7292-1BL30-0XA0	11 pin, gold-plated

Index

&

& box (FBD AND logic operation), 198

/

/= box (FBD negate assignment), 199

=

== box (FBD compare operation), 215

= box (FBD assignment), 199

>

>=1 box (FBD OR logic operation), 198

A

ABS (form absolute value), 223

AC
- wiring and grounding prerequisites, 55
- isolation guidelines, 56
- grounding guidelines, 56
- wiring guidelines, 57

Accessible devices
- updating firmware, 1056
- formatting a memory card, 1060

Accessing
- user-defined Web pages, 814

Access protection, CPU, 151

ACOS (form arccosine value), 225

ACT_TINT (activate time of day interrupt), 366

Active/passive communication
- configuring the partners, 533
- connection IDs, 549
- parameters, 551
- configuring the partners, 711

ADD (add), 220

Add new device
- CPU, 124
- unspecific CPU, 125
- detect existing hardware, 125

Addresses, getting station information, 390

Addressing
- memory areas and I/O in the PLC, 89

Ad hoc mode, TCP and ISO on TCP, 548

Air flow, 42

Aliases in user-defined Web pages, 804

Analog I/O
- conversion to engineering units, 94
- configuration, 138
- conversion to engineering units, 264
- status indicators, 1048
- step response times (CPU), 1112
- step response times (CPU), 1123
- step response times (CPU), 1135
- step response times (CPU), 1147
- step response times (CPU), 1163
- step response times (SM), 1195
- voltage (inputs), 1195
- current (inputs), 1196
- current and voltage (outputs), 1196
- step response times (SB), 1236
- voltage (inputs), 1237
- current (inputs), 1237-1238
- current and voltage (outputs), 1238

Analog signal boards
- SB 1231, 1232
- SB 1232, 1235
- SB 1231 Thermocouple, 1239
- SB 1231 RTD, 1244

Analog signal modules
- SM 1231, 1186
- SM 1232, 1190
- SM 1234, 1192
- SM 1231 Thermocouple, 1197
- SM 1231 RTD, 1203

AND (logic operation), 287

Approvals
CE, 1090
cULus, 1091
FM, 1092
ATEX, 1093
CCCEx approval, 1094
Australia and New Zealand - RCM Mark, 1094
Korea Certification, 1094
Maritime, 1094

Arrays, accessing members, 258

Article numbers
CPUs, 1274
signal modules, 1274
signal boards, battery boards, 1275
communication interfaces (CM, CB and CP, 1276
connectors and terminal connections, 1276
CPU 1214FC, CPU 1215FC, 1276
FS signal modules, 1277
CSM 1277 Ethernet switch, 1277
PM 1207 power supply, 1277
memory cards, 1277
expansion cables, 1277
simulators, 1277
connector blocks, 1277
end retainer, 1277
programming software, 1283
STEP 7, 1283

AS-i
instructions, RDREC and WRREC (read/write data record), 330
AS-i master CM 1243-2, 696
add AS-i master CM1243-2 module, 698
add AS-i slave, 698
network connection, 698
AS-i master device configuration, 699
assign the AS-i slave address, 700
AS-i slave configuration without STEP 7, 702
system assignment of AS-i slave addresses, 702
system assignment, 702
AS-i slave configuration with STEP 7, 703
transferring digital values, 703
transferring analog values, 703

ASIN (form arcsinevalue), 225

Assigning enum types, user-defined Web pages, 806

Assigning online device names, PROFINET IO, 1053

ATEX approval, 1093

ATH (convert ASCII string to hexadecimal number), 311

ATTACH (attach an OB to an interrupt event), 358

AT tag overlay, 104

ATTR_DB (Read data block attribute), 464

Australia and New Zealand - RCM Mark approval, 1094

Autonegotiation, 541

AWP_Enum_Def, 805

AWP_Import_Fragment, 808

AWP_In_Variable, 800, 803

AWP_Out_Variable, 802

AWP_Start_Fragment, 807

AWP commands, 798
writing variables, 800
reading special variables, 802
writing special variables, 803
using an alias, 804
defining an enum type, 805
referencing an enum type, 806
generating fragments, 807
importing fragments, 808
combining definitions, 809

B

Backing up
options, contents, and special considerations, 1085
an online CPU, 1086
saving files, 1088
Restoring a backup, 1089

Basic panels (HMI), 36

Battery board (BB)
BB 1297, 1249
inserting battery, 1249

Baud rate, 844

BB 1297, 1249

Binding to a CPU, memory card, or password, 160

Bit logic
normally open and closed contacts, 197
AND, OR, and XOR instructions, 198
NOT instruction (invert RLO), 198
normally open and closed coils, 199
set and reset instructions, 200
positive and negative edge instructions, 202

Blocks
types of, 61
types of, 61
function (FC), 61
function block (FB), 61
organization blocks (OBs), 66
organization blocks (OBs), 77
know-how protection (password protection), 159
copy protection, 160
linear and structured programs, 168
calling, 169
organization blocks (OBs), 170
function (FC), 172
function block (FB), 172
data block (DB), 172
data block (DB), 174
calling, 182
download to device, 189
copying blocks from an online CPU, 193
consistency check, 196
CPU 1211C specifications, 1106
CPU 1212C specifications, 1117
CPU 1214C specifications, 1129
CPU 1215C specifications, 1141
CPU 1217C specifications, 1155

Boolean or bit value access, 90

Break, 846, 848

Browsers supported for Web server, 754

BUFFER parameter, SEND_P2P, 872

Bus connector, 36

C

Cable
Network communication, 838
expansion, 1266

CALCULATE (calculate), 219

Calendar, 293

Calling code blocks within the user program, 169

Call structure, 196

Call structure local memory allocation, 92

CAN_DINT (cancel time-delay interrupt), 368

CAN_TINT (cancel time of day interrupt), 366

CANopen modules
021620-B, 021630-B, 1267

Capturing values from an online DB, 1066

CB 1241
termination and bias, 839
RS485, 1260

CE approval, 1090

CEIL (generate next higher integer from floating-point number), 263

Certificate parameters, 529

Certificates, TLS, 557

Change device, 136

Char (character data type), 100

Character position, message length, 853

Character sequence
message start , 848
message end, 852

Chars_TO_Strg (convert array of CHAR to character string), 310

Checking the connection, 601

Clearance, airflow, and cooling, 42

Clock
memory bits, 86
CPU time-of-day clock, 87
instructions for reading and setting), 296

Coils, 197

Cold junction compensation, thermocouple, 1200, 1241

Communication
loss, pull or plug of modules, 72
communication load, 82
cycle time configuration, 82
PROFINET and PROFIBUS, 520
secure vs. legacy, 521
number of connections (PROFINET/PROFIBUS), 527
secure, 529
certificates (recommended), 529
between CPUs and other devices, 530
network connection, 531
active/passive, configuring the partners, 533
IP address, 538
MAC address, 538
time synchronization property (PROFINET), 545
protocols, 548
connection IDs, 549
active/passive, configuring the partners, 551
TCON_Param, 551
network, 640
hardware connection, 640
PROFIBUS address assignment, 695
AS-i slave address assignment, 700
active/passive, configuring the partners, 711
flow control, 844
send and receive parameters, 846
polling architecture, 881
Communication board (CB)
comparison chart, 35
overview, 35
removal, 49
installation, 49
device configuration, 121
adding modules, 127
configuration of parameters, 138
configuration of parameters, 162
RS485, 837
LED indicators, 837
programming, 880
LED indicators, 1047
CB 1241 RS485, 1260
Communication interfaces
comparison chart of the modules, 35
device configuration, 121
adding modules, 127
RS232 and RS485, 837
configuration, 842
3964(R), 854
programming, 880
LED indicators, 1047
CB 1241 RS485, 1260
CM 1241 RS232, 1261
Communication module (CM)
comparison chart, 35
overview, 36
removal, 51
installation, 51
device configuration, 121
adding modules, 127
configuration of parameters, 138
configuration of parameters, 162
add CM 1243-5 (DP master) module, 694
add AS-i master CM1243-2 module, 698
RS232 and RS485, 837
LED indicators, 837
data reception, 873
programming, 880
configuration for PtP example program, 882
data reception, 999
LED indicators, 1047
CM 1241 RS232, 1261
CM 1241 RS422/RS485, 1262
power requirements, 1270
Communication processor (CP)
comparison chart, 35
overview, 36
device configuration, 121
adding modules, 127
configuration of parameters, 138
configuration of parameters, 162
Communication standard Web page, 781
Compact switch module, CSM 1277, 1267
Comparing and synchronizing code blocks for online/offline CPUs, 1063
Comparing values, 215
Comparison chart
CPU models, 33
modules, 35

Compatibility, 39
CONCAT (combine character strings), 314
Configuration
cycle time , 81
communication load, 82
startup parameters, 109
discover, 125
adding modules, 127
CPU parameters, 136
modules, 138
modules, 162
HSC (high-speed counter), 495
network connection, 531
PROFINET port, 538
Ethernet port, 538
IP address, 538
MAC address, 538
PLC to PLC communication, 644
PROFIBUS address assignment, 695
AS-i master device, 699
AS-i slave device, 699
ports, 842
communication interfaces, 842
receive message, 847
3964(R), communication interfaces/ports, 854
RS422, operating modes, 885
RS485 operating modes, 887
Configuration, 3964(R)
priority and protocol parameters, 855
Configuration, user-defined Web pages
STEP 7 configuration, 811
setting up multiple languages, 829
Configuration control (option handling), 127
control data record, 131
example, 133
Configuration of transmitted message, 846
Connection contacts
Maximum current carrying capacity, 1258
Connections
types of communication, 520
number of connections (PROFINET/PROFIBUS), 527
partners, 533
connection IDs , 549
configuration, 551
Ethernet protocols, 710
S7 connection, 710
types, multi-node connections, 710
partners, 711
Web server, 834
Connector, installation and removal, 52
Consistency check, 196
Constraints
user-defined Web pages, 814
Web server, 834
Contact information, 27, 136
Contacts, 197
Contamination level/overvoltage category, 1097
CONTINUE, SCL, 285
Control DB for user-defined Web pages
parameter to WWW instruction, 812
request commands and states, 829
global commands, 829
CONV (convert value), 259
Conversion (SCL instructions), 259
Cookie, siemens_automation_language, 826
Cookie restrictions, standard Web pages, 835
Cooling, 42
Copying, cutting, and pasting in STEP 7, 39
Copying blocks from an online CPU, 193
Copy protection
binding to a CPU, memory card, or password, 160
COS (form cosine value), 225
Counters
CTU (count up), 211
CTD (count down), 211
CTUD (count up and down), 211
operation (standard counters), 212
CTRL_HSC_EXT (Control high-speed counter, extended), 481
HSC configuration, 495
CTRL_HSC (control high-speed counter), 504
quantity, 1107
size, 1107
Counting modes, high-speed counter, 496
CountOfElements (Get number of ARRAY elements), 253
CP module
access to Web server, 766
Web server Start page, 773

CPU configuration
cycle time monitoring, 81
operational parameters, 136
pulse channels, 421
communication to HMI, 642
multiple CPUs, 644
CPU memory card
inserting, 107
transfer card, 109
program card, 113
CPU properties, user-defined Web pages
STEP 7 configuration, 811
setting up multiple languages, 829
CPUs
CPU 1211C, 1105
CPU 1212C, 1116
CPU 1214C, 1127
CPU 1215C, 1139
CPU 1217C, 1153
CREATE_DB (Create data block), 459
Creating a network connection
between PLCs, 531
Cross-reference to show usage, 195
CSM 1277 compact switch module, 1267
CTD (count down), 211
CTRL_HSC_EXT (Control high-speed counter, extended)
instruction overview, 481
example, 482
CTRL_HSC (control high-speed counter), 504
CTS (Hardware flow control, PtP), 844-845
CTU (count up), 211
CTUD (count up and down), 211
cULus approval, 1091
Current consumption, 42, 1270
Cycle time
overview, 81
configuration, 82
monitoring, 1061
Cyclic interrupt OB, 68

D

D_ACT_DP, 340
Data block
overview, 61
organization blocks (OBs), 66
difference between global and instance, 89
organization blocks (OBs), 170
overview, 174
global data block, 174
optimized access, 174
standard access, 174
creating with CREATE_DB, 459
reading and writing data blocks from load memory, 462
reading attributes with ATTR_DB, 464
deleting with DELETE_DB, 466
CONF_DATA, 632
importing fragments in user-defined Web pages, 808
capturing and resetting values, 1066
Data block
synchronizing online and offline start values, 192
Data exchange between IO systems, 654
Data handling block (DHB), 174
Data log
data log overview, 435
data record structure, 435
creating, 436
opening, 440
writing, 441
emptying, 443
closing, 445
deleting, 446
creating a new file, 447
viewing Data logs, 449
size limit and calculating size, 451
example program, 453
DataLogClear, 443
DataLogDelete, 446
Data transmission, initiating, 870, 997

Data types
overview, 95
Bool, Byte, Word, and DWord, 96
USInt, SInt, UInt, Int, UDInt, Dint (integer), 97
Real, LReal (floating-point real), 97
Time, Date, TOD (time of day), DTL (date and time long), 98
characters and strings, 100
arrays, 101
Struct, 102
PLC data type editor, 102
Variant (pointer), 103
Date
Date data type, 98
DTL (date and time long data type), 99
T_CONV (convert times and extract), 293
T_ADD (add times), 294
T_SUB (subtract times), 294
T_DIFF (time difference), 294
T_COMBINE (combine times), 295
SET_TIMEZONE (set time zone), 297
Daylight saving time TimeTransformationRule, 298
DB_ANY_TO_VARIANT (Convert DB_ANY to VARIANT, 267
DB (data block), 174
DC
wiring and grounding prerequisites, 55
isolation guidelines, 56
grounding guidelines, 56
wiring guidelines, 57
inductive loads guidelines, 59
outputs, 1099
Debugging in RUN mode, 1072, 1080
DEC (decrement), 222
DECO (decode), 288
Defining enum types, user-defined Web pages, 805
Degree of protection, 1098
DELETE_DB (Delete data block), 466
DELETE (delete characters in a character string), 316
DEMUX (demultiplex), 290
Deserialize, 229
Designing a PLC system, 167, 168
DETACH (detach an OB from an interrupt even)t, 358
Device
PROFINET IO, 648
PROFINET IO device names, 648
shared, 662
Device configuration, 121
add new device, 124
discover, 125
adding modules, 127
changing a device type, 136
configuring the CPU, 136
configuring the modules, 138
configuring the modules, 162
network connection, 531
PROFINET port, 538
Ethernet port, 538
time synchronization property (PROFINET), 545
PROFIBUS, 695
AS-i slave, 699
Device exchange
procedure, 136
V3.0 CPU for a V4.x CPU, 1285
DeviceStates, examples, 398
DeviceStates (read module status of an I/O system), 397
Diagnostic error interrupt OB, 71
Diagnostics
reducing security events, 87
viewing with standard Web pages, 773
status LED indicators, 1047
monitoring cycle time and memory usage, 1061
Diagnostics, instructions
LED (read LED status), 382
Get_IM_Data (read the identification and maintenance data), 383
Get_name, 384
DeviceStates (read module status of an I/O system), 397
ModuleStates (read module status information of a module), 402
GET_DIAG (read diagnostic information), 406
Diagnostics buffer
overview, 86
viewing in standard Web pages, 776
display events, 1062
Digital I/O
configuration, 138
pulse catch, 138
status indicators, 1048

Digital input filter time, 139
Digital signal boards
SB 1221, 1222
SB 1222, 1224
SB 1223, 1226
SB 1223, 1230
Digital signal modules
SM 1221, 1169
SM 1222 DQ 8, 1171
SM 1222 DQ 16, 1172
SM 1223 DI and DQ, 1177-1178
SM 1223, 1184
DIN rail, 46
Directories, languages for user-defined Web pages, 826
DIS_AIRT (disable execution of higher priority interrupts and asynchronous error events), 370
Discover to upload an online CPU, 125
Displaying the MAC and IP addresses, 542
DIV (divide), 220
Documentation, 27
Downloading
firmware update, 117
project to device, 189
displaying the MAC and IP addresses, 542
Siemens security certificate to PC, 772
user-defined Web page DBs, 814
Download in RUN mode
overview, 1072
prerequisites, 1073
initiating from STEP 7, 1074
downloading selected blocks, 1075
compile errors, 1076
extended block interface, 1077
download without reinitialization, 1077
memory reserve and retentive memory reserve, 1077
global memory reserve settings, 1079
restrictions, 1079
failed download, 1079
considerations, 1080
DPNRM_DG, 355
DPRD_DAT (read consistent data of a DP standard slave), 348
DP standard slaves
Reading all inputs with GETIO, 333
Writing all outputs with SETIO, 334
Reading a portion of the inputs with GETIO_PART, 335
Writing a part of the outputs with SETIO_PART, 336
DPWR_DAT (write consistent data of a DP standard slave), 348
Drives, setting up MM4 drive, 901
Dynamic binding, 160

E

Edge instructions, positive and negative, 202
Edit in RUN mode, 1072
Electromagnetic compatibility, 1096
Electromagnetic compatibility (EMC), 1095
E-mail, sending with TMAIL_C, 604
EN_AIRT (enable execution of higher priority interrupts and asynchronous error events), 370
EN and ENO (power flow), 187
ENCO (encode), 288
End conditions, message, 850
Endian format, 250
ENDIS_PW (enable disable passwords), 272
End message character, 852
Enum types in user-defined Web pages, 805, 806
Environmental
operating conditions, 1097
transport and storage conditions, 1097
EQ_ElemType (Compare data type of an ARRAY element for UNEQUAL with the data type of a tag), 218
EQ_Type (Compare data type for EQUAL with the data type of a tag), 218
Errors
time errors, 70
diagnostic errors, 71
common errors for extended instructions, 473

Ethernet
types of communication, 520
number of communication connections, 527
switching, 530
network connection, 531
IP address, 538
MAC address, 538
overview, 546
ad hoc mode, 548
connection IDs, 549
CSM 1277 compact switch module, 1267
Ethernet, instructions
RDREC and WRREC (read/write data record), 330
RALRM (receive interrupt), 337
DPWR_DAT (write consistent data of a DP standard slave) and DPRD_DAT (read consistent data of a DP standard slave), 348
RCVREC (receive data record), 351
PRVREC (make data record available), 353
DPNRM_DG (read diagnostic data from a DP slave), 355
TSEND_C and TRCV_C, 562
TCON, TDISCON, TSEND, and TRCV, 578
TUSEND and TURCV, 624
T_CONFIG (configure interface), 629
GET (read data from a remote CPU) and PUT (write data to a remote CPU), 706
Ethernet, legacy instructions
TSEND_C and TRCV_C, 572
TCON, TDISCON, TSEND, and TRCV, 592
Ethernet protocols, 546
multi-node connections, 710
Event execution and queueing, 77
Examples, communication
PROFINET communication protocols, 546
CPU communication with separate send and receive connections, 549
CPU communication with a common send and receive connection, 550
CPU communication over TSEND_C or TRCV_C connections, 551
T_CONFIG, changing IP parameters, 635
T_CONFIG, changing IP parameters and PROFINET IO device names, 636
T_CONFIG, changing IP parameters of the NTP servers, 638
I-device as IO device and IO controller, 654
shared device, 662
shared I-device, 667
AS-i slave addressing, 700
configuring a PROFINET S7 connection, 715
configuring a PROFIBUS S7 connection, 716
Examples, instructions
PEEK and POKE variations, 185
timer coils, 206
LIMIT (set limit value), 224
Deserialize, 230
Serialize, 233
SWAP (swap bytes), 248
PEEK and POKE variations, 249
RUNTIME (Measure program runtime), 279
CONTINUE, SCL, 285
EXIT, SCL, 286
GOTO (SCL), 286
RETURN, SCL, 287
DECO (Decode), 289
SHL (Shift left), SCL, 292
ROR (Rotate right), SCL, 292
S_CONV (convert character string), 307
STRG_VAL (convert string to numerical value), 308
VAL_STRG (convert numerical value to string), 309
ATH (ASCII to hexadecimal), 312
HTA (Hexadecimal to ASCII), 312
SET_CINT cyclic interrupt execution and time parameter, 362
DeviceStates, PROFIBUS and PROFINET, 398
ModuleStates, PROFIBUS and PROFINET, 403
GET_DIAG and modes, 411
CTRL_PWM, 423
CTRL_HSC_EXT, 482

Examples, legacy Modbus RTU
MB_HOLD_REG parameter, 1037
holding register addressing, 1039
master program, 1042
slave program, 1044
Examples, legacy Modbus TCP
MB_HOLD_REG parameter, 1020
holding register addressing, 1022
MB_SERVER multiple Modbus TCP connections, 1024
MB_CLIENT: multiple requests with common Modbus TCP connection, 1024
MB_CLIENT multiple requests with different Modbus TCP connections, 1025
MB_CLIENT output image write request, 1027
MB_CLIENT coordinating multiple Modbus TCP requests, 1027
Examples, Modbus
Modbus TCP, MB_CLIENT connection parameters, 911
Modbus TCP, MB_SERVER connection parameters, 915
Modbus TCP, MB_HOLD_REG parameter examples, 917
Modbus TCP, holding register addressing, 921
MB_SERVER multiple Modbus TCP connections, 962
MB_CLIENT multiple requests with common Modbus TCP connection, 963
MB_CLIENT multiple requests with different Modbus TCP connections, 964
Modbus TCP MB_CLIENT ourput image write request, 965
Modbus TCP MB_CLIENT coordinating multiple requests, 965
Modbus RTU master program, 987
Modbus RTU slave program, 989
Examples, PtP communication
start message condition, 849
end message condition, 852
message length within message, 853
Receive_Config, 865
terminal emulator, 882
configuration, 882
STEP 7 programming, 887
terminal emulator, 889
running the terminal emulator example, 889
Legacy PtP communication, RCV_CFG, 995
Examples, runtime string instructions
GetSymbolName, 321
GetSymbolPath, 323
GetInstanceName, 325
GetInstancePath, 327
GetBlockName, 329
Examples, USS communication
USS communication error reporting, 899
legacy USS communication errors reporting, 1011-1012
Examples, various
analog value processing, 94
slice of tagged data type, 104
AT tag overlay, 105
configuration control (option handling), 133
ENO evaluation in SCL, 188
accessing array elements, 258
analog value processing, 264
nested CASE statements, SCL, 282
recipe, 426
recipe, 432
data log program, 453
high-speed counter, 493
trace and logic analyzer function, 1082
CPU 1217C Differential input and application, 1167
CPU 1217C differential output and appplication, 1168
S7-1200 IO-Link Master connection, 1215
power budget calculation, 1271

Examples, Web server
access from mobile device, 766
reading variables, 799
aliases, 799
writing variables, 801
reading special variables, 803
writing special variables, 804
aliases, 804
enum types, 805
enum types, 806
fragment DBs, 808
combining AWP declarations, 809
special characters in AWP commands, 810
user-defined Web page, 816
reading variables, 818
enum types, 819
writing variables, 819
writing special variables, 820
user-defined Web page, 820
user-defined Web page to switch languages, 826-827
STEP 7 program to check fragments, 832

Exchanging a V3.0 CPU for a V4.x CPU, 1285

Execution speeds of instructions, 1106, 1117, 1128, 1140, 1154

EXIT, SCL, 286

EXP (form exponential value), 225

Expanding the capabilities of the S7-1200, 35

Expansion cable, 53
installation, 53
removal, 53

EXPT (exponentiate), 225

Extended block interface
download in RUN mode, 1077

F

F_TRIG (set tag on negative signal edge), 203

Factory settings reset, 1057

FB (function block), 61

FBD (function block diagram), 180

FC (function), 61, 172

Features, new, 37

FieldRead (read field), 257

FieldWrite (write field), 257

FileDelete (Delete file on the memory card), 478

FileReadC (Read file from the memory card), 473

FileWriteC (Write file on the memory card), 476

FILL_BLK (fill block), 234

Filter time, 139

FIND (find characters in a character string), 319

Firmware update
with a memory card, 117
from Web server, 780
from the SIMATIC Automation Tool, 780
from STEP 7, 1055

First scan indicator, 85

Fixed length, 852

Flexible machines (configuration control), 128

FLOOR (generate next lower integer from floating-point number), 263

Flow control, 844
configuration, 844
managing, 844

FM approval, 1092

Folders, languages for user-defined Web pages, 826

FOR, SCL, 283

Forcing values, 1070, 1071

Formatting a memory card, 1060

FRAC (return fraction), 225

Fragment DBs (user-defined Web pages)
creating from AWP command, 807
importing with AWP command, 808
generating, 811

Freeport protocol, 840

Frequency, clock bits, 86

Function (FC)
overview, 61
know-how protection, 159
linear and structured programs, 168
calling code blocks within the user program, 169
overview, 172

Functionality, I-device, 650

Function block (FB)
overview, 61
know-how protection, 159
linear and structured programs, 168
calling code blocks within the user program, 169
overview, 172

G

GATHER, 241

GATHER_BLK, 245

Gen_UsrMsg (Generate user diagnostic alarms), 371

Generating user-defined Web page DBs, 811

GEO2LOG (Determine the hardware identifier based upon slot information), 467

GEOADDR, 472

GET_DIAG (read diagnostic information), 406

GET_ERROR_ID (get error ID locally), 277

GET_ERROR (get error locally), 276

Get_Features (get advanced features), 878

Get_IM_Data (read the identification and maintenance data), 383

Get_name, 384

GET (read data from a remote CPU), 534
configuring the connection, 534

GetBlockName (Read out name of the block), 328

GetInstanceName (Read out name of block instance), 324

GetInstancePath (Query composite global name of the block instance), 326

GETIO, 333

GETIO_PART, 335

GETSMCInfo, 412

GetSMCinfo (Reading out information about the memory card), 412

GetStationInfo, 390

GetSymbolName (Read out a tag on the input parameter), 319

GetSymbolPath (Query composite global name of the input parameter assignment), 322

Global data block, 89, 174

Global library
USS protocol overview, 889
legacy USS protocol overview, 1004

GOTO, SCL, 286

GSD file, 659

Guidelines
installation, 41
installation procedures, 46
CPU installation, 47
wiring and grounding prerequisites, 55
isolation, 56
grounding, 56
wiring, 57
lamp loads, 58
inductive loads, 59

H

Hardware configuration, 121
add new device, 124
discover, 125
adding modules, 127
configuring the CPU, 136
configuring the modules, 138
configuring the modules, 162
network connection, 531
PROFINET port, 538
Ethernet port, 538
PROFIBUS, 695
AS-i slave device, 699

Hardware flow control, 844-845

Hardware interrupt OB, 69

High-speed counter
CTRL_HSC_EXT (Control high-speed counter, extended), 481
synchronization, 489
gate function, 490
capture function, 491
compare function, 493
application, 493
configuration, 495
counting modes, 496
operating phase, 497
CTRL_HSC (Control high-speed counter, extended), 504
cannot be forced, 1072

HMI devices
overview, 36
network connection, 531
configuring PROFINET communication, 642

HSC_Count (system data type), 485
HSC_Frequency (system data type), 488
HSC_Period (system data type), 487
HSC (high-speed counter)
  configuration, 495
  counting modes, 496
  operating phase, 497
HTA (convert hexadecimal number to ASCII string), 311
HTML pages, user-defined, 796
  developing, 797
  refreshing, 797
  accessing S7-1200 data, 798
  page locations, 811
  web page example, 820
  language locations, 829
HTTP connections, Web server, 834

I

I/O
  inductive loads guidelines, 59
  addressing, 93
  digital status indicators, 1048
  analog status indicators, 1048
  monitoring status in program editor, 1066
  monitoring with a watch table, 1068
  forcing values, 1070
  forcing values operation, 1071
  step response times (CPU), 1112
  step response times (CPU), 1123
  step response times (CPU), 1135
  step response times (CPU), 1147
  step response times (CPU), 1163
  step response times (SM), 1195
  analog input voltage, 1195
  analog input current, 1196
  analog output current and voltage, 1196
  step response times (SB), 1236
  analog input voltage, 1237
  analog input current, 1237-1238
  analog output current and voltage, 1238
Identification of CPU, viewing with Web server, 773
I-device (intelligent IO device)
  functionality, 650
  Properties, 651
  lower-level PN IO system, 652
  configuring, 657
  configuring with GSD file, 659
  shared, 667
Idle line, 847, 848
IF-THEN, SCL, 281
I memory
  monitoring in watch table, 1065
IN_Range (value within range), 216
INC (increment), 222
Incompatible CPU version error, 1051
Indexing arrays with variables, 258
Inductive loads guidelines, 59
Industrial environments, approvals, 1095
Information resources, 27
Input filter time, 139
Inputs and outputs
  pulse catch bits, 140
  monitoring, 1065
Input simulators, 1264
INSERT (insert characters in a character string), 317
Inserting a device
  unspecific CPU, 125
Inserting the memory card into CPU, 107

Installation
signal modules (SM), 36
overview, 41
guidelines, 41
cooling, 42
air flow, 42
clearance, 42
thermal zone, 42
power budget, 42
thermal zone, 45
mounting dimensions, 45
overview, 46
CPU, 47
signal board (SB), 49
communication board (CB), 49
signal module (SM), 50
communication module (CM), 51
terminal block connector, 52
wiring and grounding prerequisites, 55
isolation guidelines, 56
grounding guidelines, 56
wiring guidelines, 57
lamp loads guidelines, 58
inductive loads guidelines, 59

Instance data block, 89, 173

Instruction execution speeds, 1106, 1117, 1128, 1140, 1154

Instructions
bit logic, 198
set and reset instructions, 200
timer, 204
counter, 211
comparing values, 215
range evaluation, 216
checking for valid or invalid real numbers, 217
equality and non-equality comparison), 218
null comparison, 218
array check, 219
move instructions, 226
conversion), 259
rounding and truncating real numbers), 262
jump instructions, 268
program control (SCL), 280
logic operations, 287
shift and rotate instructions, 291
date, time, and clock functions, 293
string and character, 301
common parameters, 639
legacy USS status codes, 1011

Instructions, legacy
PORT_CFG (configure communication parameters dynamically), 990
SEND_CFG (configure serial transmission parameters dynamically), 992
RCV_CFG (configure serial receive parameters dynamically), 993
SEND_PTP (transmit send buffer data), 997
RCV_PTP (enable receive messages), 999
RCV_RST (delete receive buffer), 1001
SGN_GET (Query RS232 signals), 1002
SGN_SET (set RS-232 signals), 1003
USS_PORT (Edit communication via USS network), 1005
USS_DRV (Swap data with drive), 1006
USS_RPM (readout parameters from the drive), 1008
USS_WPM (change parameters in the drive), 1010
MB_CLIENT (communicate via PROFINET as Modbus TCP client), 1013
MB_SERVER (communicate via PROFINET as Modbus TCP server), 1019
MB_COMM_LOAD (configure port on the PtP module for Modbus RTU), 1028
MB_MASTER (communicate via the PtP port as Modbus master), 1031
MB_SLAVE (communicate via the PtP port as Modbus slave), 1036

Instructions, positive and negative edge signals, 202

Inter-character gap, 851

Interrupts
  overview, 67
  interrupt latency, 77
  ATTACH (attach an OB to an interrupt event), 358
  DETACH (detach an OB from an interrupt event, 358
  time delay interrupt instructions, 368

Intro standard Web page, 772

INV (create ones complement), 288

IO2MOD (Determine the hardware identifier from an I/O address, 470

IO-Link
  signal module (Link Master), 1209
  device profile, 1212
  properties, 1212
  functions, 1213
  replacing, 1213
  reset to factory settings, 1214
  pin assignment, 1214
  diagram, 1216
  configuring, 1217
  parameters, 1217
  address space, 1217
  parameters, 1217
  LED status, 1219
  diagnostic alarms, 1221

IO system, data exchange, 654

IP address, 136
  device configuration, 136
  Assigning, 535
  assigning to an online CPU, 537
  configuring, 538
  MAC address, 538
  assigning, 542
  displaying and downloading, 542
  configuring the online CPU, 1054

IP address, emergency (temporary), 719

IP router, 538

IS_ARRAY (Check for ARRAY), 219

IS_NULL (Query for EQUALS ZERO pointer), 218

Isolation guidelines, 56

ISO on TCP
  ad hoc mode, 548

ISO-on-TCP
  connection configuration, 533
  connection IDs, 549
  parameters, 551

ISO on TCP protocol, 546

J

JavaScript, standard Web pages, 835

JMP_LIST (define jump list), 269

JMP (jump if RLO = 1), 268

JMPN (jump if RLO = 0), 268

K

Know-how protection
  password protection, 159
  viewing with Web server, 773

Korea Certification approval, 1094

L

Label (jump label), 268

LAD (ladder logic)
  overview, 179
  program editor and online status, 1066
  monitoring online status, 1066
  status, 1070

Lamp loads guidelines, 58

Languages, user-defined Web pages, 826

Latency, 77

LED (read LED status), 382

LED indicators
  communication interfaces, 837
  CPU status, 1047
  communication interface, 1047

LEFT (read the left characters of a character string), 315

Legacy communication, 521

Legacy TCON, TDISCON, TSEND, and TRCV instructions, 592

Legacy TRCV_C and TSEND_C, 572

Legacy USS protocol library
overview, 1004
instruction versions, 1004
requirements for using, 1004
USS_PORT (Edit communication via USS network), 1005
USS_DRV (Swap data with drive), 1006
USS_RPM (readout parameters from the drive), 1008
USS_WPM (change parameters in the drive), 1010
status codes, 1011

LEN (determine the length of a character string), 313

Length, PtP message, 853

LENGTH parameter, SEND_P2P, 872

Licenses, OPC UA, 1283

LIMIT (set limit value), 224

Linear programming, 168

LN (form natural logarithm), 225

Load memory, 33
user-defined Web pages, 814
CPU 1211C, 1105
CPU 1212C, 1116
CPU 1214C, 1127
CPU 1215C, 1139
CPU 1217C, 1153

Local/Partner connection, 532

Local memory
maximum per OB priority level, 92
usage by blocks, 92

Local time
instructions for reading and setting, 296

LOG2GEO (Determine the slot from the hardware identifier), 469

Logging in/out, standard Web pages, 770

Logic analyzer, 1081

Loss of CPU communication to modules, 72

Lost password, 119

LOWER_BOUND (read out ARRAY low limit), 254

M

MAC address
configuration, 538
displaying and downloading, 542
locating, 543

Manual fragment DB control, 829

Manuals, 27

Maritime approval, 1094

Master polling architecture, 881

Math, 219, 220

MAX_LEN (maximum length of a character string), 313

MAX (get maximum), 223

Maximum Web server connections, 834

MB_CLIENT, 906

MB_CLIENT (communicate via PROFINET as Modbus TCP client), legacy, 1013

MB_COMM_LOAD (configure port on the PtP module for Modbus RTU), legacy, 1028

MB_MASTER (communicate via the PtP port as Modbus master), legacy, 1031

MB_RED_CLIENT, 924

MB_RED_SERVER, 942

MB_SERVER, 914

MB_SERVER (communicate via PROFINET as Modbus TCP server), legacy, 1019

MB_SLAVE (communicate via the PtP port as Modbus slave), legacy, 1036

MC_ChangeDynamic (change dynamic settings for the axis), 516

MC_CommandTable, 514

MC_Halt (pause axis), 512

MC_Home (home axis), 511

MC_MoveAbsolute (position axis absolutely), 512

MC_MoveJog (move axis in jog mode), 514

MC_MoveRelative (position axis relatively), 513

MC_MoveVelocity (move axis at predefined velocity), 513

MC_Power (release/block axis), 510

MC_ReadParam (read parameters of a technology object), 515

MC_Reset (confirm error), 511

MC_WriteParam (write to parameters of a technology object), 515

MC-PostServo OB, 77

MC-PreServo OB, 76

Measurements, trace jobs, 1082
Media redundancy
  Functions in ring topology, 677
  Configuring, 681
Memory
  load, work, and retentive, 83
  system and clock memory, 84
  L (local memory), 89
  I (process image input), 91
  Q (process image output), 91
  M (bit memory), 92
  temp memory, 92
  monitoring usage, 1061
Memory areas
  process image and physical access, 89
  addressing Boolean or bit values, 90
Memory areas, viewing with Web server, 773
Memory card, 106
  overview, 106
  inserting into CPU, 107
  configure the startup parameters, 109
  transfer card, 109
  program card, 113
  Protection of confidential PLC configuration data, 115
  firmware update, 117
  empty transfer card for a lost password, 119
  reading information, 412
  incompatibility error, 1051
Memory card service life, 114
Memory location access, 89
Memory locations, 91
Message conditions
  start, 848
  end, 850
Message configuration
  transmit (send) parameters, 846
  receive parameters, 847
  instructions, 880
Message length, maximum, 852
MicroMaster drive, connecting, 900
MID (read the middle characters of a character string), 315
MIN (get minimum), 223
Miscellaneous PtP parameter errors, 858
Mobile device
  accessing Web server, 765
  Web page layout, 769
MOD (return remainder of division), 221
Modbus
  function codes, 902
  network station addresses, 903
  memory addresses, 904
Modbus_Comm_Load (Configure SIPLUS I/O or port on the PtP module for Modbus RTU) instruction, 968
Modbus_Master (Communicate using SIPLUS I/O or the PtP port as Modbus RTU master), 972
Modbus_Slave (Communicate using SIPLUS I/O or the PtP port as Modbus RTU slave), 978
Modbus example programs
  Modbus RTU master, 987
  Modbus RTU slave, 989
Modbus RTU
  overview, 966
  maximum Modbus slaves, 968
Modbus RTU, instructions
  versions, 968
  Modbus_Comm_Load, 968
  Modbus_Master, 972
  Modbus_Slave, 978
Modbus RTU, legacy instructions
  MB_COMM_LOAD (configure port on the PtP module for Modbus RTU), 1028
  MB_MASTER (communicate via the PtP port as Modbus master), 1031
  MB_SLAVE (communicate via the PtP port as Modbus slave), 1036
Modbus TCP
  overview, 904
  maximum number of connections, 904
Modbus TCP, instructions
  versions, 905
  MB_CLIENT, 906
  MB_SERVER, 914
  MB_RED_CLIENT, 924
  MB_RED_SERVER, 942
Modbus TCP, legacy instructions
  MB_CLIENT (communicate via PROFINET as Modbus TCP client), 1013
  MB_SERVER (communicate via PROFINET as Modbus TCP server), 1019
Mode for PG/PC and HMI communication, 144

Modifying
variables from Web server, 784
watch table, 1068

Module information standard Web page, 777

Modules
comparison chart, 35
signal board (SB), 35
communication boards (CB), 35
signal modules (SM), 36
communication processor (CP), 36
communication module (CM), 36
thermal zone, 42
thermal zone, 45
configuring parameters, 138
configuring parameters, 162

ModuleStates, 402

ModuleStates example, 403

Monitoring
cycle time and memory usage, 1061
watch table, 1065
program status in editor, 1066
capturing and resetting DB values, 1066
watch table, 1068
force table, 1070
forcing values, 1071

Monitoring the program, 194

Monitoring variables from Web server, 784

Motion control
overview, 507
instructions, 509

Mounting
guidelines, 41
airflow, clearance, cooling, and thermal zone, 42
airflow, clearance, cooling, and thermal zone, 45
dimensions, 45
overview, 46
CPU, 47
board, communication (CB) and signal (SB), 49
module, communication (CM) and signal (SM), 50
module, communication (CM) and signal (SM), 51
terminal block connector, 52
expansion cable, 53
wiring and grounding prerequisites, 55
isolation guidelines, 56
grounding guidelines, 56
wiring guidelines, 57
lamp loads guidelines, 58
inductive loads guidelines, 59

MOVE_BLK (move block), 226

MOVE (move value), 226

Movement sequence (MC_CommandTable), 514

MRP (Media Redundancy Protocol), 675

MUL (multiply), 220

Multi-node connections, 710

Multiple AWP variable definitions, 809

MUX (multiplex), 290

N

N_TRIG (scan RLO for negative signal edge), 203

N (scan operand for negative signal edge), 202

N= box and N coil (set operand on negative signal edge), 202

NE_ElemType (Compare data type for UNEQUAL with the data type of a tag), 218

NE_Type (Compare data type for UNEQUAL with the data type of a tag), 218

NEG (create twos complement), 222

Nesting depth, 61

Network communication, 640
bias and terminate cable, 838

Network connection
connecting devices, 531
between two devices, 643
between two devices, 645
multiple CPUs, 648
multiple CPUs, 694
multiple CPUs, 698

Network time protocol (NTP), 544

New features, 37

No restart, 62

NORM_X (normalize), 263

Normalizing analog values, 264

Normally open/closed"; "coil, 199

Normally open/closed"; "contact, 197

NOT_NULL (Query for UNEQUALS ZERO pointer), 218

NOT_OK (check invalidity), 217

NOT (invert RLO), 198

Numbers
binary, 96
integer, 97
real, 97

O

OBs, 67

OK (check validity), 217

On-delay and off-delay timers, 204

Online
assigning an IP address to a CPU, 537
going online with PLC, 1051
IP address, 1054
time of day, 1055
operating panel, 1061
monitoring cycle time and memory usage, 1061
diagnostics buffer, 1062
comparing and synchronizing code blocks, 1063
tools, 1065
use of watch table, 1065
status, 1066
capturing and resetting DB values, 1066
watch table, 1068
forcing values, 1070
forcing values, 1071
downloading in RUN mode, 1072
backing up a CPU, 1086

OPC UA
certificates (recommended), 529
user rights, 728
Method calls, 748

OPC UA Method calls, 748

OPC UA server
activating, 720
configuration settings, 723
security overview, 725
supported security policies, 726
trusted clients, 727
define server interface, 734
data types and node types, 734
PLC nodes, 735
interfaces, 736
companion specifications, 736

Open User Communication
certificates (recommended), 529
establishing a connection and reading data with TRCV_C, 562
establishing a connection and sending data with TSEND_C, 562
establishing a connection and reading data with legacy TRCV_C, 572
establishing a connection and sending data with legacy TSEND_C, 572

Open User Communication instructions return values, 639

Operating mode
operating modes of the CPU, 62
changing STOP/RUN, 1061

Operating phase
HSC (high-speed counter), 497

operator control block, 36

Operator panel, CPU, 1061

Optimized data blocks, 174

Option handling (configuration control), 127

OPU UA licenses, 1283

OR (logic operation), 287

Organization block
overview, 61
startup processing, 65
processing, 66
priority classes, 67
calling and functionality, 67
cyclic interrupt, 68
temp memory allocation, 92
know-how protection, 159
linear and structured programming, 168
calling code blocks within the user program, 169
processing, 170
creating, 171
multiple cyclic, 171
configuring operation, 172
Reading start information with RD_SINFO, 373

OUT_Range (value outside range), 216

Outputs
pulse, 419
configuring pulse channels, 421

Overvoltage category, 1097

P

P_TRIG (scan RLO for positive signal edge), 202

P (scan operand for positive signal edge) , 202

P= box and P coil (set operand on positive signal edge), 202

P3964_Config (Configuring the 3964(R) protocol), 868
errors, 869

Panels (HMI), 36

Parameters configuration
transmit, 646
receive, 648
LENGH and BUFFER for SEND_P2P, 872

Parity, 844

Passive/active communication
configuring the partners, 533
connection IDs, 549
parameters, 551
configuring the partners, 711

Password enable/disable, 272

Password protection
empty transfer card, 119
lost password, 119
access to the CPU, 151
code block, 159
binding to a CPU, memory card, or password, 160
copy protection, 160
ENDIS_PW (enable disable passwords), 272

PEEK, PEEK_WORD, PEEK_BOOL, PEEK_DWORD, PEEK_BLK, 185, 249

Performance times, 1106, 1117, 1128, 1140, 1154

Phase shift, cyclic interrupt OBs, 68

PID
PID_Compact (universal PID controller with integrated tuning), 517
PID_3STEP (PID controller with tuning for valves), 518
PID_Temp (universal PID controller that allows handling of temperature control), 519

PLC
overview of features, 32
cycle time , 81
cycle time configuration, 82
communication load, 82
tag table, 89
adding modules, 127
system design, 167
using blocks, 168
assigning an IP address to an online CPU, 537
going online, 1051

PM 1207 power module, 1267

PN slave
Activating and deactivating with D_ACT_DP, 340

Pointers
Variant data type, 103

Point-to-Point communication
Freeport, 840
programming, 880

POKE, POKE_BOOL, POKE_BLK, 185, 249

Polling architecture, 881

Pollution degree, 1097

PORT_CFG (configure communication parameters dynamically), legacy, 990

Port_Config (port configuration), 859

Portal view, 38

Port configuration, 842
3964(R), 854
errors, 861
instructions, 880
PtP example program, 882
errors, 992
Port numbers
assigning to communication partners, 546
restricted, 640
Potentiometer module, 1266
Power budget, 42
overview, 1270
example, 1271
form for calculations, 1272
Power supply module
PM1207, 1267
Priority class for OBs
overview, 67
event execution and queuing, 79
Process image
Reading inputs with GETIO, 333
Writing outputs with SETIO, 334
Reading the process image area with GETIO_PART, 335
Transferring the process image area with SETIO_PART, 336
forcing values, 1070
force operation, 1071
PROFIBUS
DPNRM_DG (read diagnostic data from a DP slave), 355
DeviceStates example, 398
ModuleStates example, 403
number of communication connections, 527
network connection, 531
master and slave, 691
CM 1242-5, DP slave and master usage, 691
add CM 1243-5 (DP master) module, 694
add DP slave, 694
network connection, 694
address assignment, 695
S7 connection, 710
PROFIBUS, instructions
RDREC and WRREC (read/write data record), 330
RALRM (receive interrupt), 337
DPWR_DAT (write consistent data of a DP standard slave) and DPRD_DAT (read consistent data of a standard DP slave) , 348
GET (read data from a remote CPU) and PUT (write data to a remote CPU), 706
PROFIenergy, 357
Profile OB, 75
PROFINET
configuring the IP address, 136
time synchronization, 136
DeviceStates example, 400
ModuleStates example, 405
types of communication, 520
number of communication connections, 527
network connection, 531
IP address, 538
MAC address, 538
Ethernet address properties, 539
testing a network, 542
time synchronization property, 545
system start-up time, 545
device naming and addressing, 546
IP address assignment, 546
overview, 546
ad hoc mode, 548
connection IDs, 549
resetting a connection, 599
configuring communication between CPU and HMI device, 642
network connection between two devices, 643
PLC-to-PLC communication, 644
CPU-to-CPU communication, 644
network connection between two devices, 645
network connection, 648
S7 connection, 710

PROFINET, instructions
RDREC and WRREC (read/write data record), 330
RALRM (receive interrupt), 337
DPWR_DAT (write consistent data of a DP standard slave) and DPRD_DAT (read consistent data of a standard DP slave), 348
RCVREC (receive data record), 351
PRVREC (make data record available), 353
TSEND_C and TRCV_C (send and receive data using Ethernet), 562
TCON, TDISCON, TSEND, and TRCV, 578
T_RESET, 599
T_DIAG, 601
TUSEND and TURCV, 624
T_CONFIG (configure interface), 629
TRCV_C, 647
GET (read data from a remote CPU) and PUT (write data to a remote CPU), 706
PROFINET, legacy instructions
TSEND_C and TRCV_C, 572
legacy TCON, TDISCON, TSEND, and TRCV instructions, 592
PROFINET IO
adding a device, 648
assigning a CPU and device names, 648
assigning device names online, 1053
PROFINET IO devices
Writing all outputs with SETIO, 334
Reading a portion of the inputs with GETIO_PART, 335
Writing a part of the outputs with SETIO_PART, 336
PROFINET port
autonegotiation, 541
PROFINET RT, 546
Program
organization blocks (OBs), 66
priority class, 67
memory card, 106
password protection, 159
binding to a CPU, memory card, or password, 160
linear and structured programs, 168
calling code blocks within the user program, 169
organization blocks (OBs), 170
download to device, 189
copying blocks from an online CPU, 193
Program card
overview, 106
inserting into CPU, 107
configure the startup parameters, 109
creating, 113
Program control (SCL), 280
IF-THEN, 281
CASE, 282
FOR, 283
WHILE, 284
REPEAT, 284
CONTINUE, 285
EXIT, 286
GO TO, 286
RETURN, 287
Program cycle OB, 67
Program editor
monitoring status, 1066
Program execution, 61
Program information
In the call structure, 196
Programming
operating modes of the CPU, 62
priority class, 67
unspecific CPU, 125
binding to a CPU, memory card, or password, 160
linear program, 168
structured program, 168
calling code blocks within the user program, 169
function (FC), 172
LAD (ladder), 179
FBD (function block diagram), 180
SCL (Structured Control Language), 181
SCL (Structured Control Language), 181
SCL (Structured Control Language), 182
power flow (EN and ENO), 187
system time, 296
RTM (runtime meters), 299
PID_Compact (universal PID controller with integrated tuning), 517
PID_3STEP (PID controller with tuning for valves), 518
PID_Temp (universal PID controller that allows handling of temperature control), 519
PtP instructions, 880
comparing and synchronizing code blocks, 1063

Programming user-defined Web page language switch, 826

Program structure, 169

Project
  transfer card, 109
  program card, 113
  access protection, 151
  protecting a code block, 159
  binding to a CPU, memory card, or password, 160
  download to device, 189
  comparing and synchronizing code blocks, 1063

Project view, 38, 39

Protection class, 1097

Protection level
  lost password, 119
  CPU, 151
  code block, 159
  binding to a CPU, memory card, or password, 160

Protection of confidential PLC configuration data
  SIMATIC memory card, 115
  security wizard, 144
  functionality, 145

Protocol
  PROFINET RT, 546
  TCP and ISO on TCP, 546
  UDP, 546
  communication, 840
  Freeport, 840
  Modbus, 840
  USS, 840

Protocols, communication, 548

PRVREC (make data record available), 353

PTO (pulse train output)
  CTRL_PWM (pulse width modulation), 415
  CTRL_PTO (pulse train output), 416
  operation, 419
  configuring pulse channels, 421
  cannot be forced, 1072

PtP communication, 840
  configuring ports, 842
  configuring parameters, 846
  instruction return values, 857
  error classes, 858
  programming, 880
  legacy conditon/error classes, 990

PtP communication, 3864(R)
  configuring ports, 854

PtP communication, 3964(R)
  configuring priority and protocol parameters, 855

PtP communication example program, 882
  configuration, 882
  STEP 7 programming, 887
  terminal emulator, 889
  running, 889

Pull or plug of modules OB, 72

Pulse
  catch bits, digital input configuration, 140
  outputs, 419

Pulse
  delay (TP), 204

Pulse catch, 138

PUT (write data to a remote CPU), 534
  configuring the connection, 534

PWM (pulse width modulation)
  CTRL_PWM (pulse width modulation), 415
  CTRL_PTO (pulse train output), 416
  operation, 419
  configuring pulse channels, 421
  cycle time and pulse duration, 422
  I/O addresses, 424
  changing the Pulse duration, 424
  changing the Cycle time, 424
  cannot be forced, 1072

Q

Q memory
  pulse outputs, 419
  configuring pulse channels, 421

QRY_CINT (query cyclic interrupt parameters), 363

QRY_DINT (query time-delay interrupt status), 368

QRY_TINT (query status of time of day interrupt), 367

Queueing, 77

Quotation mark conventions, Web server, 809

R

R_TRIG (set tag on positive signal edge), 203

R (reset ouput), 200

Rack or station failure OB, 73

RALRM (receive interrupt), 337

Rated voltages, 1098, 1098

RCV_CFG (configure serial receive parameters dynamically), legacy, 993
RCV_PTP (enable receive messages), legacy, 999
RCV_RST (delete receive buffer), legacy, 1001
RCVREC (receive data record), 351
RD_ADDR (determine the IO addresses from the hardware identifier), 471
RD_LOC_T (read local time), 296
RD_SINFO (Read current OB start information), 373
RD_SYS_T (read time-of-day), 296
RDREC (read data record), 330, 345
RE_TRIGR (restart cycle monitoring time), 274
READ_BIG (Read data in big endian format), 250
READ_DBL (read from data block in load memory), 462
READ_LITTLE (Read data in little endian format), 250
Reading
  from DBs, I/O, or memory, 185
  from DBs, I/O, or memory, 249
  HTTP variables, 802
Receive
  parameters configuration, 648
  configuration errors, 867
  runtime return values, 873
  configuration errors, 997
  runtime return values, 999
Receive_Config (receive configuration), 863
Receive_P2P (receive Point-to-Point), 873
Receive_Reset (receiver reset), 875
Receive message configuration
  PtP device configuration, 847
  PtP example program, 883
Recipe
  overview, 425
  DB structure, 426
  RecipeExport (recipe export), 429
  RecipeImport (recipe import), 431
  example program, 433
Redundancy
  MRP, 675
  clients, 677
  domains, 678
Referencing enum types, user-defined Web pages, 806
Refreshing (updating) user-defined Web pages, 797
Relay electrical service life, 1099
REPEAT, SCL, 284
REPLACE (replace characters in a character string), 318
RESET_BF (reset bit field), 200
Reset timer (RT), 204
Resetting the values of a DB, 1066
Reset to factory settings, 1057
Restoring a backup, 1089
Restricted TSAPs and port numbers, 640
RET (return), 271
Retentive block tags
  download in RUN mode, 1078
Retentive memory, 33
  CPU 1211C, 1105
  CPU 1212C, 1116
  CPU 1214C, 1127
  CPU 1215C, 1139
  CPU 1217C, 1153
RETURN, SCL, 287
Return values
  Open User Communication instructions, 639
  PtP instructions, 857
Reverse voltage protection, 1098
RIGHT (read the right characters of a character string), 315
Ring
  topology, 677
  port, 683
ROL (rotate left) and ROR (rotate right), 292
ROUND (round numerical value), 262
Router IP address, 539
RS (reset/set flip-flop), 201
RS232 and RS485 communication modules, 837
RS485 connector
  termination and bias, 838
RT (reset timer), 204
RTS (Hardware flow control, PtP), 844-845
RTS On delay, Off delay, 846
Run axis commands as movement sequence (MC_CommandTable), 514

RUN mode, 62
transition to STOP, 88
force operation, 1071
RUNTIME(Measure program runtime), 279
Runtime meters (RTM), 299

S

S_CONV (convert character string), 302
S_MOV (move chracter string), 301
S (set ouput), 200
S7 communication (configuring the connection), 534
S7 routing, 684
Saving backup files, 1088
SCALE_X (scale), 263
Scaling analog values, 264
Scan cycle
overview, 81
force operation, 1071
SCATTER, 235
SCATTER_BLK, 238
SCL (Structured Control Language)
calling blocks, 169
overview, 181
program editor, 181
Var section, 181
calling an FB or FC, 182
priority of operators, 182
addressing, 182
control statements, 182
conditions, 182
operators, 182
expressions, 182
EN and ENO (power flow), 187
bit logic, 197
timers, 204
comparing values, 215
Conversion instructions, 259
program control, 280
control statements, 280
Secure communication, 521, 529
Secure PG/PC and HMI communication, certificates (recommended), 529
Security
reducing events in diagnostic buffer, 87
lost password, 119
using the security wizard, 144
protection of confidential PLC configuration data, 145
CPU access protection, 151
know-how protection for a code block, 159
binding to a CPU, memory card, or password, 160
copy protection, 160
secure vs. legacy communication, 521
SEL (select), 289
SEND_CFG (configure serial transmission parameters dynamically), legacy, 992
Send_Config (send configuration), 861
Send_P2P (send Point-to-Point data), 870
SEND_P2P (send Point-to-Point data)
LENGH and BUFFER parameters, 872
SEND_PTP (transmit send buffer data), legacy, 997
Send message configuration, 846
Send parameters configuration, 533, 646, 711
Serial communication, 840
Serialize, 232
Service and support, 27
SET_BF (set bit field), 200
SET_CINT (set cyclic interrupt parameters), 361
Set_Features (set advanced features), 879
SET_TIMEZONE (set time zone), 297
SET_TINTL (set date and time of day interrupt), 364
SETIO, 334
SETIO_PART, 336
SGN_GET (get RS232 signals), 876
SGN_GET (Query RS232 signals), legacy, 1002
SGN_SET (set RS-232 signals), legacy, 1003
Shared device
concept, 659
configuration, 662
Shared I-device, configuration, 667
Shielded connections, grounding guidelines, 56
SHL (shift left) and SHR (shift right), 291

siemens_automation_language cookie, 826
Siemens security certificate, Web pages, 772
Signal_Set (set RS232 signals), 877
Signal boards (SB)
  overview, 35
  removal, 49
  installation, 49
  adding modules, 127
  configuration of parameters, 138
  configuration of parameters, 162
  SB 1221 DI 4 x 24 V DC, 200 kHz, 1222
  SB 1221 DI 4 x 5 V DC, 200 kHz, 1222
  SB 1222 DQ 4 x 24 V DC, 200 kHz, 1224
  SB 1222 DQ 4 x 5 V DC, 200 kHz, 1224
  SB 1223 DI 2 x 24 V DC/DQ 2 x 24 V DC, 200 kHz, 1226
  SB 1223 DI 2 x 5 V DC/DQ 2 x 5 V DC, 200 kHz, 1226
  SB 1223 DI 2 x 24 V DC, DQ 2 x 24 V DC, 1230
  SB 1231 AI 1 x 12 bit, 1232
  SB 1232 AQ 1 x 12 bit, 1235
  SB 1231 AI 1 x 16 bit Thermocouple, 1239
  SB 1231 AI 1 x 16 bit RTD, 1244
  power requirements, 1270
Signal boards (SBs) and signal modules (SMs)
  analog input voltage, 1195
  analog input current, 1196
  analog output current and voltage, 1196
  analog input voltage, 1237
  analog input current, 1237-1238
  analog output current and voltage, 1238
Signal handling errors, 876, 877, 1002, 1003
Signal modules (SM), general
  CPU expansion, 36
  installation and removal, 50
  expansion cable, 53
  adding modules, 127
  configuration of parameters, 138
  configuration of parameters, 162
  step response times, 1195
  power requirements, 1270
Signal modules (SM), types
  SM 1221, 1169
  SM 1222, 1171
  SM 1222, 1172
  SM 1223, 1177-1178
  SM 1223, 1184
  SM 1231, 1186
  SM 1232, 1190
  SM 1234, 1192
  SM 1231, 1197
  SM 1231, 1203
  SM 1278, 1209
Simulators, 1264
SIN (form sine value), 225
Single FB with multiple instance DBs, 173
Slave polling architecture, 881
Slice (of a tagged data type), 103
SM 1231 RTD
  selection tables, 1206-1207
  selection tables, 1246-1247
SM and SB
  comparison chart, 35
  device configuration, 121
Smart phone, accessing Web server, 765
Snapshot of DB values, 1066
SNMP, enabling and disabling, 687
Snubber circuits for inductive loads, 59
Software flow control, 845
Special characters
  User-defined Web pages, 809

Specifications
general technical specifications, 1090
approvals, 1090
industrial environments, 1095
electromagnetic compatibility (EMC), 1095
environmental conditions, 1097
rated voltages, 1098
CPU 1211C, 1105
step response times (CPU), 1112
CPU 1212C, 1116
step response times (CPU), 1123
CPU 1214C, 1127
step response times (CPU), 1135
CPU 1215C, 1139
step response times (CPU), 1147
CPU 1217C, 1153
step response times (CPU), 1163
SM 1221 DI 8 x 24 V DC, 1169
SM 1221 DI 16 x 24 V DC, 1169
SM 1222 DQ 8, 1171
SM 1222 DQ 16, 1172
SM 1223 DI and DQ, 1177-1178
SM 1223 DI 8 x 120/230 V AC/DQ 8 x Relay, 1184
SM 1231 AI 4 x 13 bit, 1186
SM 1231 AI 8 x 13 bit, 1186
SM 1231 AI 4 x 16 bit, 1186
SM 1232 AQ 2 x 14 bit, 1190
SM 1232 AQ 4 x 14 bit, 1190
SM 1234 AI 4 x 13 bit/AQ 2 x 14 bit, 1192
step response times (SM), 1195
analog input voltage, 1195
analog input current, 1196
analog output current and voltage, 1196
SM 1231 AI 4 x 16 bit TC, 1197
SM 1231 AI 8 x 16 bit TC, 1197
SM 1231 AI 4 x RTD x 16 bit signal module, 1203
SM 1231 AI 8 x RTD x 16 bit signal module, 1203
SM 1278 4xIO-Link Master, 1209
SB 1221 DI 4 x 24 V DC, 200 kHz, 1222
SB 1221 DI 4 x 5 V DC, 200 kHz, 1222
SB 1222 DQ 4 x 24 V DC, 200 kHz, 1224
SB 1222 DQ 4 x 5 V DC, 200 kHz, 1224
SB 1223 DI 2 x 24 V DC/DQ 2 x 24 V DC, 200 kHz, 1226
SB 1223 DI 2 x 5 V DC/DQ 2 x 5 V DC, 200 kHz, 1226
SB 1223 DI 2 x 24 V DC, DQ 2 x 24 V DC, 1230
SB 1231 AI 1 x 12 bit, 1232
SB 1232 AQ 1 x 12 bit, 1235
step response times (SB), 1236
analog input voltage, 1237
analog input current, 1237-1238
analog output current and voltage, 1238
SB 1231 AI 1 x 16 bit Thermocouple, 1239
SB 1231 AI 1 x 16 bit RTD, 1244
BB 1297, 1249
CB 1241 RS485, 1260
CM 1241 RS232, 1261
CM 1241 RS422/485, 1262
memory cards, 1263
input simulators, 1264
potentiometer module, 1266

SQR (form square), 225

SQRT (form square root), 225

SR (set/reset flip-flop), 201

SRT_DINT (start time-delay interrupt), 368

Standard data blocks, 174

Standard machine projects (configuration control), 128

Standard Web pages, 753
accessing from PC, 764
secure access, 765
layout, 768
logging in and out, 770
Intro, 772
Start, 773
changing operating mode, 773
Diagnostics, 773
Diagnostics Buffer, 776
Module information, 777
communication, 781
Tag status, 784
JavaScript, 835
cookie restrictions, 835

Start conditions, message, 848

Start message character, 848

Start standard Web page, 773

Startup
startup processing, 65
force operation, 1071

Startup after POWER ON, 62

Startup OB, 67

Startup parameters, 109

Station
Read information with GetStationInfo, 390

STATUS, RDREC, WRREC, RALARM, 345
Status LEDs
communication interfaces, 837
CPU, 1047
Status OB, 74
STEP 7
view (Portal and Project), 38
version compatibility, 39
code blocks, 61
operating modes of the CPU, 62
priority class, 67
cycle time , 81
cycle time configuration, 82
communication load, 82
configuring devices, 121
adding devices, 124
adding devices, 127
configuring devices, 136
configuring devices, 138
password protection, 159
configuring devices, 162
linear and structured programs, 168
code blocks, 169
function (FC), 172
download project to device , 189
copying blocks from an online CPU, 193
network connection, 531
assigning an IP address to an online CPU, 537
PROFINET port, 538
Ethernet port, 538
adding devices, 648
PROFIBUS configuration, 695
AS-i master device configuration, 699
entering the AS-i slave address, 700
going online with PLC, 1051
comparing and synchronizing code blocks, 1063
watch table, 1065
monitoring status in program editor, 1066
forcing values, 1070
STEP 7 programming
user-defined Web pages, 812
PtP example program, 887
Stop bits, 844
STOP mode, 62
enable outputs, 1070
force operation, 1071
STP (exit program), 275
Strg_TO_Chars (convert character string to array of CHAR), 310
STRG_VAL (convert character string to numerical value), 302
String
data type, 100
data overview, 301
S_MOVE (move character string), 301
Structured programming, block structure, 168
SUB (subtract), 220
Subnet mask, 539
Support, 27
Suppressor circuits for inductive loads, 59
Surge immunity, 1096
SWAP (swap bytes), 248
SWITCH (jump distributor), 269
Switching languages, user-defined Web pages, 826
Synchronization
time-of-day clock, 165
offline and online CPU, 192
high-speed counter (HSC), 489
time, Network Time Protocol (NTP), 545
System clock
instructions for reading and setting, 296
System memory byte, 85

T

T_ADD (add times), 294
T_COMBINE (combine times), 295
T_CONFIG (configure interface), 629
T_CONV (convert times and extract), 293
T_DIAG, 601
T_DIFF (time difference), 294
T_RESET, 599
T_SUB (subtract times), 294
Tablet, accessing Web server, 765
Tag
slice, 103
overlay, 104
monitoring status or value, 1065
force operation, 1071
Tag status standard Web page, 784
TAN (form tangent value), 225

TCON
configuration, 533
connection IDs, 549
connection parameters, 551

TCON_Param, 551

TCON, TDISCON, TSEND, and TRCV, 578

TCP
connection configuration, 533
connection configuration, 533
protocol, 546
ad hoc mode, 548
connection IDs, 549
parameters, 551

TCP/IP communication, 546

Technical specifications, 1090

Technology instructions, 481

Technology module, SM 1278 4xIO-Link Master, 1209

TeleControl
communication processors, 1045

Temp memory
maximum per OB priority level, 92
usage by blocks, 92

Terminal block connector, 52, 1278

Terminal emulator for PtP example program, 889

Testing the program, 194

Thermal zone, 42, 45

Thermocouple
basic operation, 1200
cold junction compensation, 1200
SM 1231 selection table, 1201
SB 1231 AI 1 x 16 bit, 1239
basic operation, 1241
cold junction compensation, 1241
SB 1231 selection table, 1241
SB 1231 Filter selection table, 1242

TIA Portal, Portal view and Project view, 38

Time
Time data type, 98
TOD (time of day data type), 98
DTL (date and time long data type), 99
T_CONV (convert times and extract), 293
T_ADD (add times), 294
T_SUB (subtract times), 294
T_DIFF (time difference), 294
T_COMBINE (combine times), 295
instructions for reading and setting, 296
SET_TIMEZONE (set time zone), 297
configuring the online CPU, 1055

Time delay Interrupt OB, 68

Time delay interrupts (programming), 368

Time error interrupt OB, 70

Time of day OB, 73

Timers
instructions, 204
operation, 207
size, 1107
quantity, 1107

Time synchronization
setting the time-of-day clock, 165
network time protocol (NTP), 545

TimeTransformationRule for daylight saving time, 298

TLS certificates, 557

TMAIL_C, 604

Topology
view, 39
ring, 677

Trace feature, 1081

Transfer (program) cards, 1263

Transfer card, 106
overview, 106
inserting into CPU, 107
configure the startup parameters, 109
empty transfer card for a lost password, 119

Transmission block (T-block), 645

Transmit
configuration errors, 863
runtime errors, 871
configuration errors, 993
runtime errors, 999

Transmit message configuration
PtP device configuration, 846
PtP example program, 883
TRCV_C (receive data via Ethernet, TCP), 548
ad hoc mode, 548
connection IDs, 549
connection parameters, 551
TRCV_C (receive data via Ethernet, TCP)
configuration, 533
TRCV (receive data via Ethernet, TCP)
ad hoc mode, 548
connection IDs, 549
parameter configuration, 648
Triggering
values in the watch table, 1069
trace, 1081
Trigonometric instructions, 225
Troubleshooting
LED indicators, 1047
diagnostics buffer, 1062
TRUNC (truncate numerical value) , 262
TS Adapter, 35
TSAP (transport service access points), 535
instructions for assigning to devices, 546
definition, 547
restricted TSAPs and port numbers, 640
configuring general parameters, 645
configuring general parameters, 710
TSEND_C (send data via Ethernet, TCP), 533
configuration, 533
connection IDs, 549
connection parameters, 551
TSEND_C (send data via Ethernet (TCP)
instruction configuration, 646
TSEND (send data via Ethernet, TCP)
connection IDs, 549
TURCV (receive data via Ethernet, UDP), 533
configuration, 533
connection parameters, 551
TUSEND (send data via Ethernet, UDP), 533
configuration, 533
parameters, 551

U

UDP
connection configuration, 533
protocol, 546
parameters, 551
UFILL_BLK (fill block uninterruptible), 234
UMOVE_BLK (move block uninterruptible), 226
Unknown CPU version error, 1051
Unspecific CPU, 125
Update OB, 74
Updating firmware
with a memory card, 117
from Web server, 780
from the SIMATIC Automation Tool, 780
from STEP 7, 1055
Upgrading a V3.0 CPU to V4.x, 1285
Uploading
copying blocks from an online CPU, 193
UPPER_BOUND (read out ARRAY high limit), 255
User configuration, Web server, 757

User-defined Web pages
overview, 796
creating with HTML editor, 797
refreshing, 797
AWP commands for accessing S7-1200 data, 798
reading variables, 799
writing variables, 800
reading special variables, 802
writing special variables, 803
creating fragments, 807
importing fragments, 808
handling special characters, 809
configuring, 811
generating program blocks, 811
deleting program blocks, 812
enabling with WWW instruction, 812
programming in STEP 7, 812
downloading corresponding DBs, 814
accessing from PC, 814
load memory constraints, 814
example, 816
HTML listing, 820
multiple languages, 826
multiple language configuration, 829
manual fragment DB control, 829
activating and deactivating from control DB, 829

User interface of STEP 7, 38

User program
organization blocks (OBs), 66
password protection, 159
binding to a CPU, memory card, or password, 160
linear and structured programs, 168
calling code blocks within the user program, 169
organization blocks (OBs), 170
download to device , 189
copying blocks from an online CPU, 193

User rights, OPC UA, 728

USS protocol library
overview, 889
instruction versions, 891
requirements for using, 891
USS_Port_Scan (Edit communication via USS network), 892
USS_Drive_Control (Swap data with drive), 893
USS_Read_Param (readout parameters from the drive), 895
USS_Write_Param (change parameters in the drive), 897
status codes, 898

V

VAL_STRG (convert numerical value to character string), 302

Valve PID tuning, 518

Variable (tag) status Web page, 784

Variable index for an array, 258

VARIANT_TO_DB_ANY (Convert VARIANT to DB_ANY), 266

VariantGet (Read VARIANT tag value), 252

VariantPut (Write VARIANT tag value), 252

Visualization, HMI devices, 36

W

Wait time, 844

Warm restart, 62

Watchdog timer (RE_TRIGR instruction), 274

Watch table
force, 194
monitoring, 1065
using, 1068
trigger values, 1069
enable outputs in STOP mode, 1070

WChar (word character data type), 100

Web server
certificates (recommended), 529
browser support, 754
update rate, 755
enabling, 755
user configuration, 757
standard Web pages, 764
mobile device access, 765
access through CP module, 766
appearance on mobile device, 769
user-defined Web pages, 796
quotation mark conventions, 809
constraints, 834
maximum HTTP connections, 834

WHILE, SCL, 284

Wireless connection to Web server, 765

Wiring diagrams
CPU 1211C, 1113
CPU 1212C, 1124
CPU 1214C, 1136
CPU 1215C, 1149
CPU 1217C, 1165
SM 1221, 1170
SM 1222, 1174
SM 1223, 1180
SM 1223, 1186
SM 1231, 1188
SM 1232, 1191
SM 1234, 1194
SM 1231 thermocouple, 1199
SM 1231 RTD, 1205
SM 1278 IO-Link Master, 1211
SB 1221, 1223
SB 1222, 1225
SB 1223, 1229
SB 1223, 1232
SB 1231, 1234
SB 1232, 1236
SB 1231 thermocouple, 1243
SB 1231 RTD, 1245
CB 1241 RS 485, 1260

Wiring guidelines, 42
clearance for airflow and cooling, 42
prerequisites, 55
grounding, 56

Work memory, 33
CPU 1211C, 1105
CPU 1212C, 1116
CPU 1214C, 1127
CPU 1215C, 1139
CPU 1217C, 1153

WR_LOC_T (set local time), 296

WR_SYS_T (set time-of-day), 296

WRIT_DBL (write to data block in load memory), 462

WRITE_BIG (Write data in big endian format), 250

WRITE_LITTLE (Write data in little endian format), 250

Writing
to DBs, I/O, or memory, 185
to DBs, I/O, or memory, 249
HTTP variables, 803

WRREC (write data record), 330, 345

WString (word string data type), 100

WWW (synchronizing user-defined Web pages), 812

X

x box (FBD EXCLUSIVE OR logic operation), 198

XON / XOFF, 845

XOR (logic operation), 287