SIEMENS

Ingenuity for life

TIA-SAFETY

SITRAIN
Training for Industry

SIMATIC safety related programming with STEP 7 Safety in the TIA Portal

siemens.com/sitrain

SIEMENS

SITRAIN
Training for Industry

SIMATIC S7

Configuring and Programming with TIA Safety Advanced

Course TIA-SAFETY

Name: ______________________

Course from: ____________ to: ____________

Instructor: ______________________

Location: ______________________

SITRAIN course offer on the Internet: www.siemens.de/sitrain

Training Document Version: V15.00.00.
(for STEP7 V15 Safety Advanced)

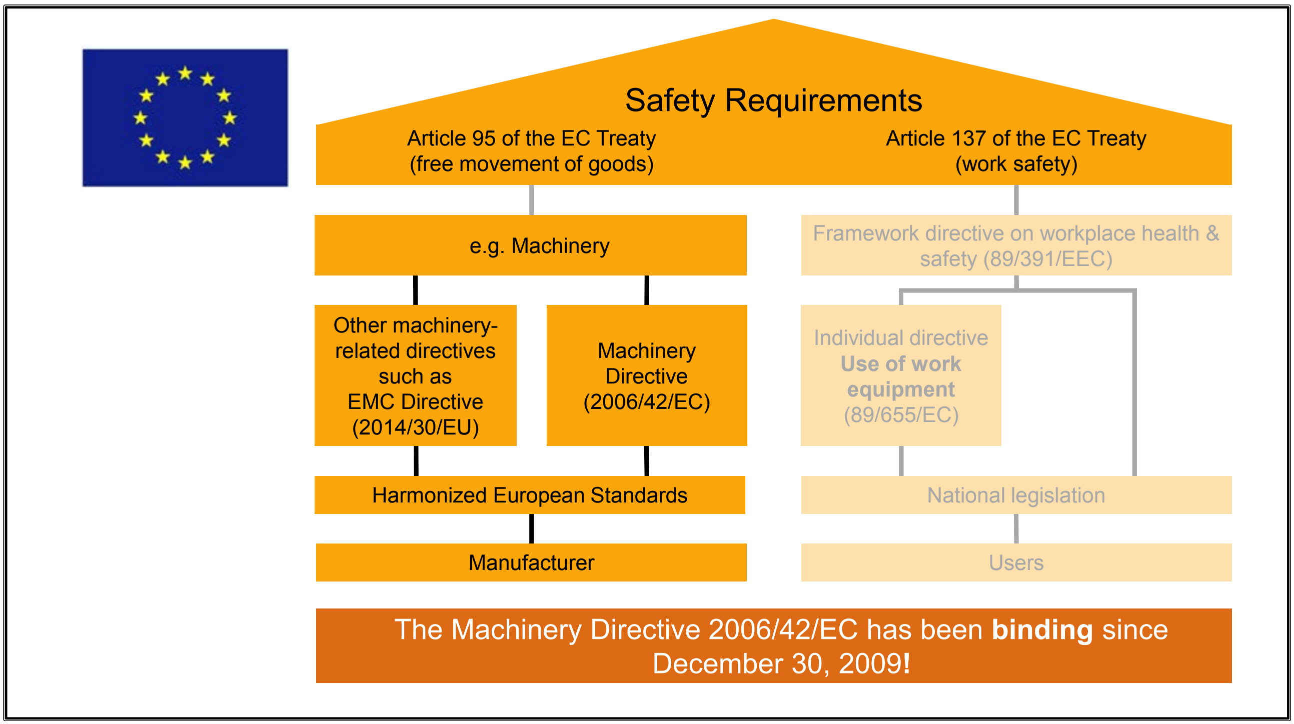
Contents 1

1. Overview of Standards and Directives

At the end of the chapter the participant will ...

… be familiar with the necessary steps for a safe machine

1.1. EU Legal Structure



Legally, two topic complexes need to be considered with regard to operation of machinery: work safety and the internal market.

Work Safety (dimmed text):

Employers must ensure the necessary prerequisites for operator control and operation of machinery:

- Sufficient lighting
- Suction
- Slip-proof floor
- Operator training courses
- Work safety, for example protective clothing

This course does not cover this topic area.

Internal Market:

When machinery is put into circulation in Europe via the internal market, such machinery must fulfill the Machinery Directive. The Machinery Directive 2006/42/EC currently applies. It superseded the previous MD 98/37/EC.
The EFTA states and also Switzerland and Turkey apply the Machinery Directive.
The current Machinery Directive focuses more on machines. The current Machinery Directive does not consider technical facilities such as (aerial) cableways or medical equipment.

Harmonized Standards:
Harmonized standards are European standards and are drawn up by the organizations CEN, CENELEC and ETSI by order of the European Commission and EFTA, that is, they have a standardization mandate. Harmonization of standards is announced in the Official Journal of the European Union.
Important: when applying harmonized standards, machine manufacturers only need to prove that they have fulfilled the requirements of the harmonized standards, in which case conformity is presumed.

1.2. Who is a Manufacturer?

A manufacturer is whoever ...

1 ... has the responsibility for the design and manufacture of machinery that falls under the directive, and who places the machinery on the market in his own name. This is generally the **mechanical equipment manufacturer and plant builder**.

2 ... changes the purpose of use of the machinery or carries out a functional expansion. This can be the **plant operator** or a company mandated by the plant operator that carries out **modernization work**.

3 ... imports machinery from a third country and is therefore legally obliged to assume the manufacturer's obligations defined in the directive. This is generally the **importer**.

As one might possibly assume, the manufacturer is not only the one who builds the machine. The machinery operator or anyone carrying out modernization work is also regarded as the manufacturer if they change the machinery or extend its range of functions.

An example will clarify this: features are added to a machine or the originally intended throughput of a machine is increased. New hazards can arise as a result. The importer introducing machinery to Europe from Asia, for example, must also ensure that the machinery complies with national legislation. The importer therefore also assumes the legal responsibility of the manufacturer.

1.3. What are Directives?

CE Directives

They are passed by the EC and must be implemented by the Member States into national laws. CE is basically a technical passport (mandatory for export within the EC)

Examples of Relevant Directives

- Machinery Directive
- Low Voltage Directory
- EMC
- Pressure Equipment Directive
- Toy Safety Directive
- etc.

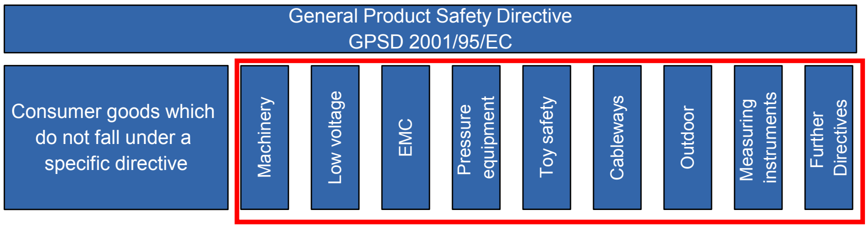
CE

CE is the symbol for the free movement of products within the European Union. Formerly, it was the abbreviation for Communauté Européenne, Comunidad Europea, Comunidade Europeia and Comunità Europea.

1.4. Selecting the Directive(s)

A directive is to be applied for a certain product, if …

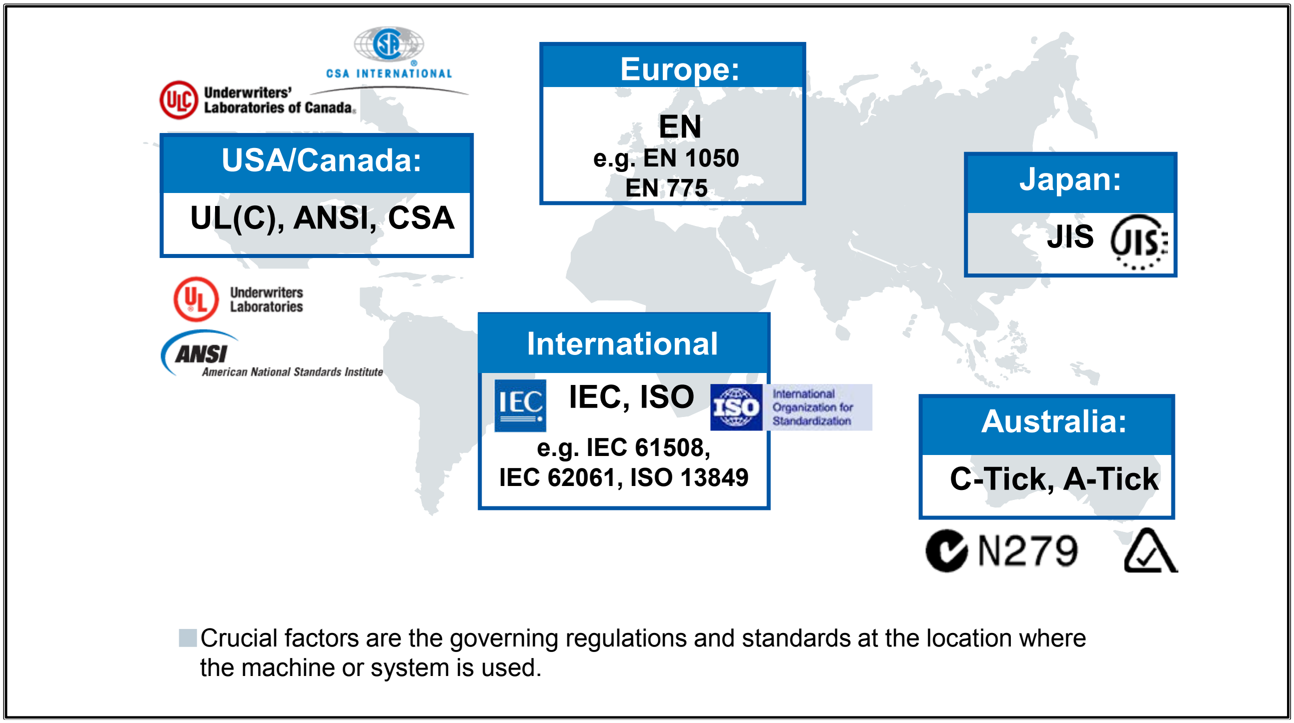
- the product formally falls within the area of validity of this directive
- the product entails risks which are described in the basic requirements of this directive
- information regarding the allocation to a directive can also be obtained from knowing under which directive an associated product standard is listed as harmonized standard
- Sector-specific rules have priority over general rules



Directives are based on a Global Concept:

- The purpose of the EC Directives is to ensure free movement of goods in the European economic area. The goal is to remove all technical trade barriers that exist for technical products and their use due to different technical requirements of Member States.
- EC Directives contain only general safety goals and specify basic safety requirements.
- Technical details can be defined in standards by standardization organizations that have a corresponding mandate of the EU Commission (CEN, CENELEC). These standards, which all Member States must adopt unchanged as national standards, are listed in the Official Journal of the EU and are thereby harmonized under a specific Directive.
- The legislative body does not stipulate compliance with specific standards. However, it "may be presumed" that when the harmonized standards are complied with, the relevant safety requirements of the Directives are met.

1.5. International Safety Standards



UL

Underwriters Laboratories: Certification organization for product safety in the USA and Canada

ANSI

American National Standards Institute: (US) American agency for industrial procedure standards

CSA

Canadian Standards Association: issues a product mark of conformity which proclaims the compliance, for example, with ISO, ANSI, ULC

IEC

International Electrotechnical Commission: is an international standardization committee situated in Geneva for electrotechnical and electronics standards. Several standards are developed together with ISO.

ISO

International Organization for Standardization: is the international association of standardization organizations

EN

European standards

JIS

Japan Industrial Standard: Japanese industrial standard (comparable to DIN)

C-Tick

Marking of the ACA (Australian Communications Authority), somewhat comparable to the CE-marking

A-Tick

Marking of the Australian Telecommunication Standards, comparable to the EMC Directive

CEN

European Committee for Standardization, Brussels

CENELEC

European Committee for Electrotechnical Standardization, Brussels (→ EN = European standards)

DIN

German Institute for Standardization, Berlin

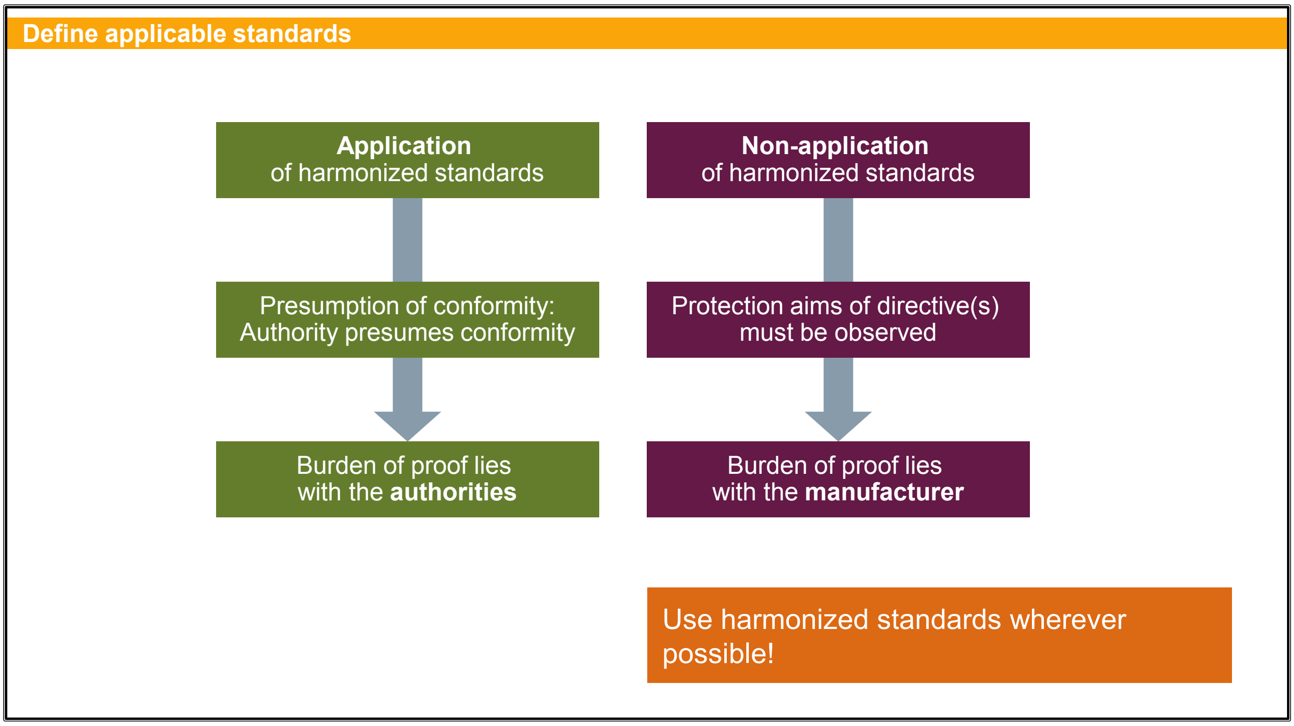
VDE

Association for Electrical, Electronic and Information Technologies, Frankfurt am Main

Examples (Germany):

- DIN EN IEC 62061
- DIN EN ISO 13849

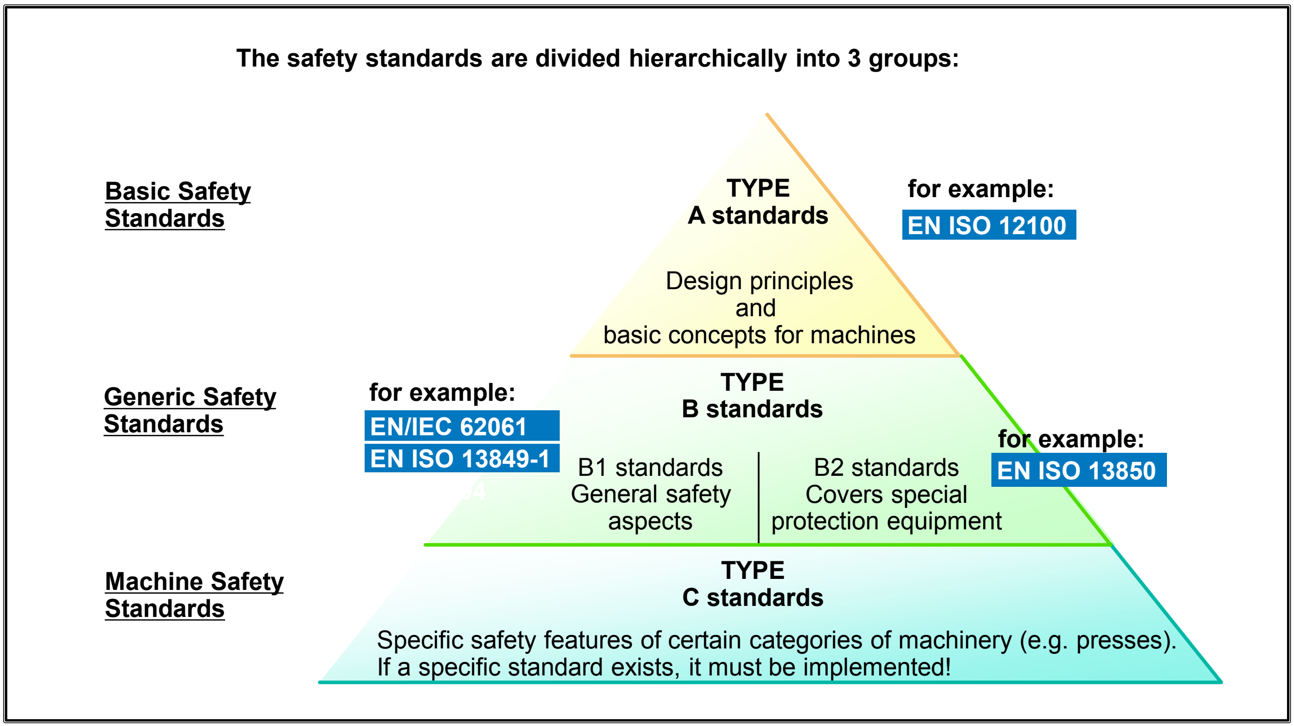
1.5.1. Harmonized Standards



Harmonized Standards

- The application of harmonized standards is voluntary!
- They are published in the Official Journal of the European Union under at least one directive
- All Member States transpose them into national standards without change
- They document the current state of the art
- They clarify the abstractly formulated protection aims of the directives
- They facilitate proof of conformity
- They have a precisely defined scope of application which describes the application area and the environment.

1.5.2. The Hierarchy of Safety Standards



Basic Safety Standards / A Standards

Basic safety standards; apply to all machinery; are directed towards the standard makers for B and C standards; are only then considered by the manufacturer if no B/C standard exists. They deal with basic concepts, design principles and general aspects which can be applied to machinery.

Generic Safety Standards / B Standards

They deal with a safety aspect or a type of protection equipment which can be applied to a whole series of machinery.

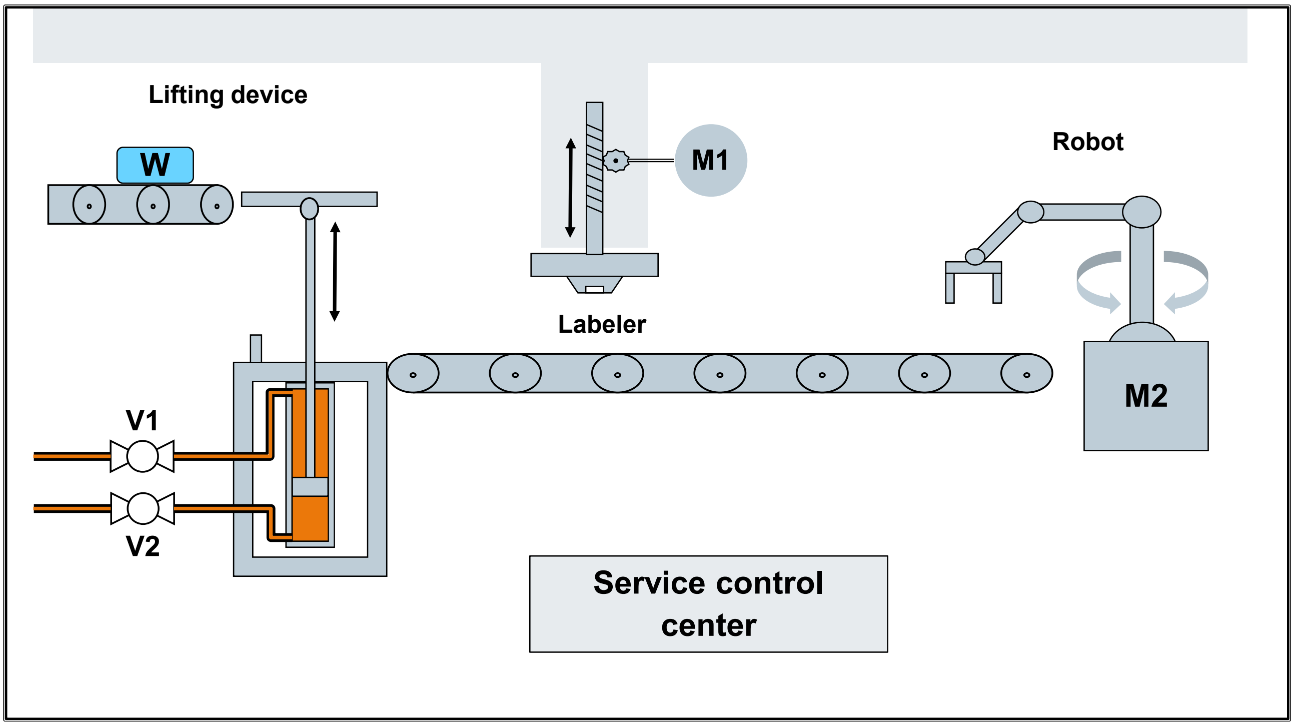
B1 standards: for certain safety aspects (ergonomic principles, safety clearances, noise, surface temperature ...) are not device-specific.

B2 standards: for protection equipment (for example E-STOP, two-hand control devices, guard (isolating protective equipment ...) are device-specific.

Machine Safety Standards / C Standards

They deal with detailed safety requirements for a specific machine or a group of machines. Machine safety standards (for example for machine tools, woodworking machinery ...) include machine-specific requirements which may differ from the A and B standards and have the highest priority for the machine manufacturer.

1.6. "Labeler" Example Machine



"Labeler" Example Machine

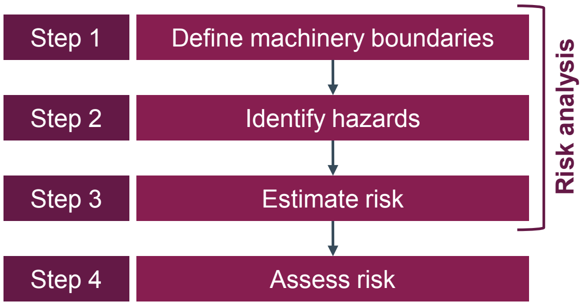
The machine labels the workpiece “W” via an electric spindle press. The workpiece is fed-in by a hydraulic lifting device. After the workpiece is labeled, it is removed using a gripper robot. The labeling process is monitored in a service control center.

1.7. Implementing the Machinery Directive for the "Labeler"

The necessary phases on the way to a safe machine can be shown with a process chain.

1.8. Risk Assessment according to EN ISO 12100

Risk assessment



The risk assessment is the complete process that encompasses a risk analysis and risk evaluation.

1.8.1. Step 1: Define Machinery Boundaries

Risk assessment

Define boundaries of the machinery according to EN ISO 12100 Chapter 5.3

Step 1 — Define machinery boundaries
Step 2 — Identify hazards
Step 3 — Estimate risk
Step 4 — Assess risk

Physical boundaries

- Application boundaries
- Human/machine interface
- Power supply

Time boundaries

- Service life
- Maintenance intervals
- Operating phases

User groups

- Training, experience, skills
- Other persons on the machinery

Physical Boundaries

- Dimensions of the machinery
- Interfaces
  - to the power supply
  - to upstream and downstream machines (if the machinery has been conceived for operation in combination with other machinery)
  - to cleaning systems
  - to humans, etc.
- Intended workplaces and motion spaces
- Properties such as the dimensions and mass of the machinery

Time Boundaries

- Presumable service life
- Total number of revolutions
- Number of load cycles
- Filling or discharge operations
- Work cycles or operating hours, etc.

Note:

Data is needed when defining testing and maintenance measures and intervals.

1.8.1.1. Boundaries of the Example Machine "Labeler"

Risk assessment

Example excerpt from the machine's description:

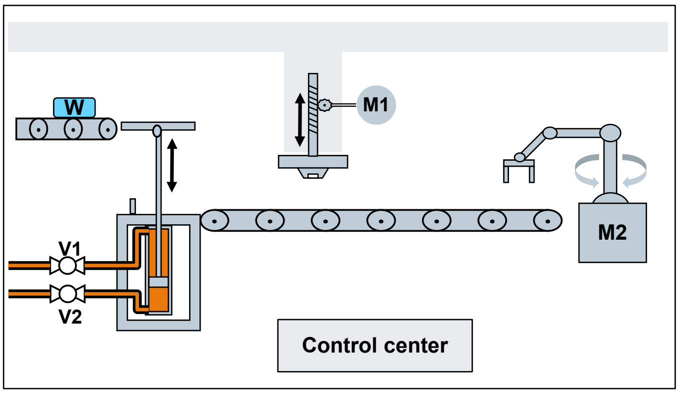
Intended use
- Machine for labeling a package up to a maximum 500 mm x 500 mm and maximum 10kg
- Feed-in a workpiece using a hydraulic lifting device
- Removal using a 360° rotatable robot with gripping device

Application boundaries
- Power supply: 400 V 3~ 50 Hz
- Indoor use (IP54)
- Temperature range: -15° to +50° C
- Labeler: max. 50Nm
- Lifting device: max. 10kg
- Robot: radius 2x2m

User groups
- Only specialist personnel, no laypersons
- Trainees only under supervision by specialists

Time boundaries
150,000 operating hours

Physical boundaries
- The machine does not include loading aids
- Space required by persons handling the machine



Application Boundaries

- Use for the intended purpose
- Reasonably foreseeable incorrect use
- For example, properties and quantities of substances, materials, consumables or workpieces
- Operating parameters such as pressure, temperature, speed, power, etc.
- Intended or foreseeable areas of use (industry, household, etc.)
- Ambient conditions

Group of Persons

- Non-technical person
- Operator
- Maintenance personnel
- Machine setter

Note:

A certain qualification level must not be used as justification for a possibly lower technical protection level.

Note:

Not all boundaries of the machine can be defined in the first assessment of the machine, e.g., the question as to presumable useful life of safety-related parts does not arise until appropriate measures for their use have been determined. The boundaries of the machine must be specified in the operating instructions. To avoid foreseeable incorrect use, it is advisable to use exclusive formulations if no technical measures can be taken against them.

1.8.2. Step 2: Identify Hazards

Risk assessment

Systematically identify hazards and/or hazard situations in all lifecycle phases and operating modes of the machine:

Step 1	Define machinery boundaries
Step 2	Identify hazards
Step 3	Estimate risk
Step 4	Assess risk

- Assembly
- Transport
- Installation
- Commissioning
- Application
- Decommissioning, disassembly
- Disposal

Systematically identify **all reasonably foreseeable hazards** in all lifecycle phases and operating modes of the machine.

1.8.2.1. Possible Hazards

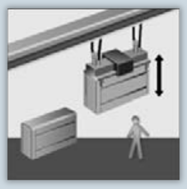
Risk assessment

Possible hazards according to EN ISO 12100

Cutting

- Cutting into
- Cutting off

Dropping



- Crushing
- Pushing

Motion

- Crushing
- Pushing
- Shearing

Gravity

- Crushing
- Pushing
- Compressing

Approach

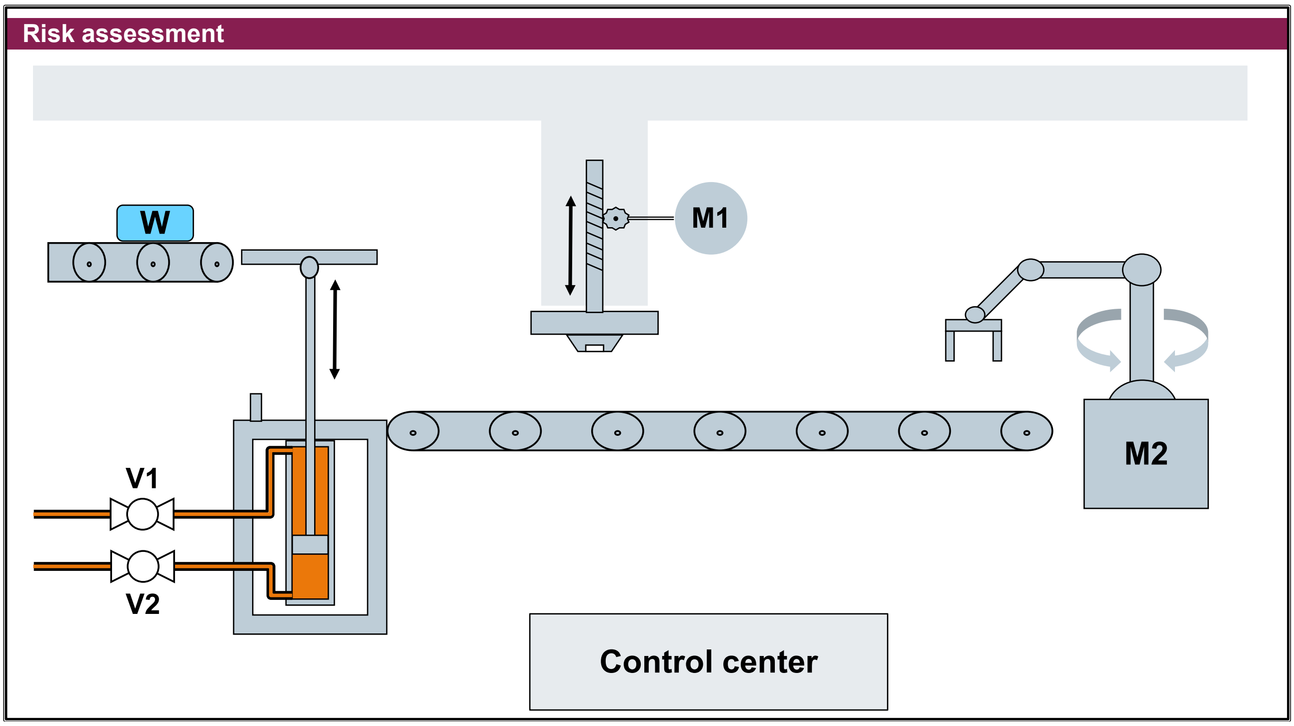
- Crushing
- Pushing

Rotation

- Pulling in
- Rubbing
- Abrading
- Crushing

When identifying hazardous locations, you must always consider the lifecycle phases and operating modes of a machine. Example: in the **series production** lifecycle phase, hazards in the **manual** and **automatic** modes can differ because the machine is operated at different speeds depending on the mode of operation.

1.8.2.2. Exercise 1: Identifying Hazards on the Machine



1.8.3. Step 3: Estimate the Risk

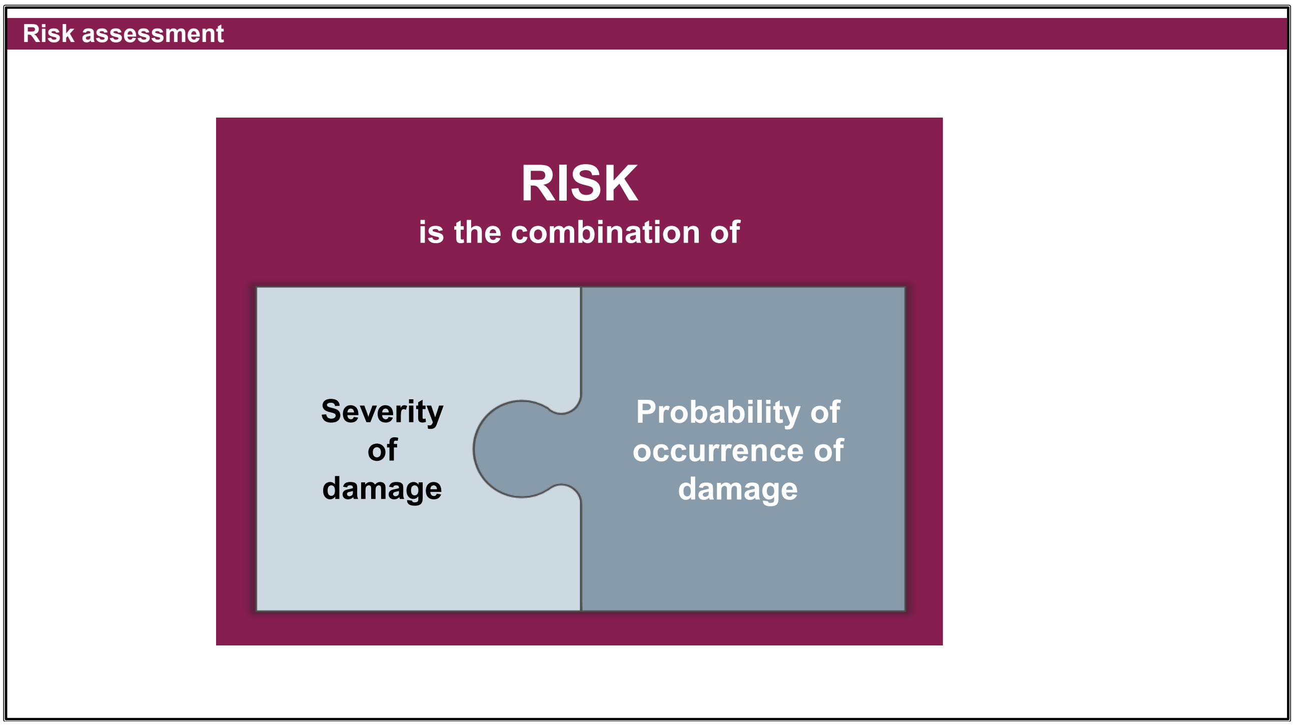
Risk assessment

Extensive estimation of the probability and the extent of damage caused by the hazard situations determined:

Step 1	Define machinery boundaries
Step 2	Identify hazards
Step 3	**Estimate risk**
Step 4	Assess risk

- The associated risk is estimated for every hazard.
- The machine is considered without taking account of countermeasures.
- The result of the first evaluation of a hazard is the original risk.

1.8.3.1. Risk


Risk assessment
RISK
is the combination of
Severity of damage
Probability of occurrence of damage

1.8.3.2. Severity

Risk assessment

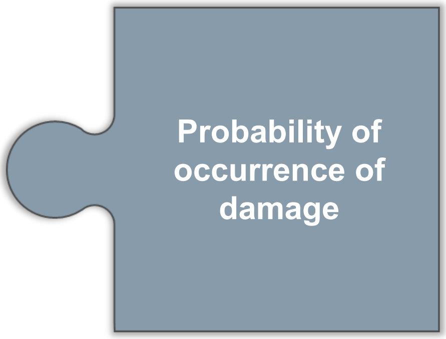
The severity of damage that can be caused by the hazard

- Reversible, first aid necessary
- Reversible, treatment by a doctor necessary
- Broken limbs, loss of fingers
- Irreversible, death, loss of an eye or an arm

When evaluating the extent of damage, you must generally distinguish between reversible and irreversible damage.

1.8.3.3. Possibility of Occurrence

Risk assessment



Frequency and duration of the exposure to danger

- Need for access to the hazardous area
- Type of access and exposure time
- Number of persons, frequency of access

Probability of a hazardous event

- Low
- Medium
- High

Possibility of avoiding or limiting damage

- Type of movement: sudden, fast or slow
- Qualification of persons
- Risk awareness
- Reflexes, practical experience
- Mobility, possibility of escape

Three factors crucially influence the probability of damage occurring:

- Frequency and duration of the exposure to danger
- Probability of a hazardous event
- Possibility of avoiding or limiting damage

1.8.4. Step 4: Assess the Risk

Risk assessment

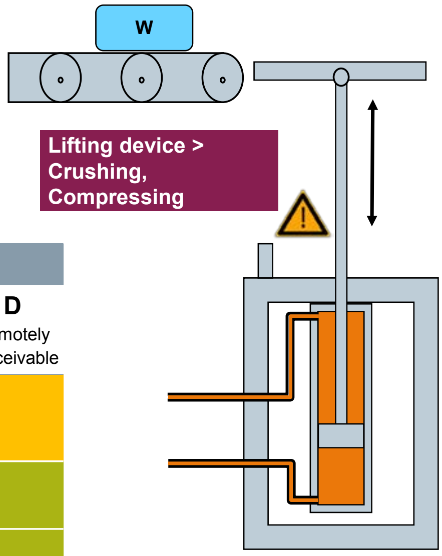
The key question: Is the (original) risk of each hazardous location justifiable or do measures have to be taken?

Step 1	Define machinery boundaries
Step 2	Identify hazards
Step 3	Estimate risk
Step 4	Assess risk

1.8.4.1. Exercise 2: Assessing the Risk (Lifting Device)

Risk assessment

Severity	Probability



Severity of harm		Probability of occurrence A Very likely	B Likely	C Improbable	D Remotely conceivable
4	Irreversible: - Death - Loss of an eye - Loss of an arm				
3	Irreversible: - Broken limbs - Loss of fingers				
2	Reversible: Treatment by a doctor necessary				
1	Reversible: First aid necessary				

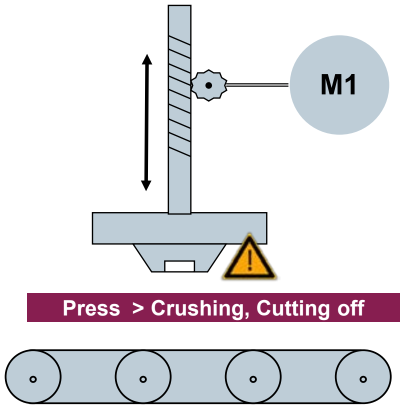
With the risk detected on the example machine, you can determine a defined value for the risk in the risk graph. By means of suitable measures, the risk should optimally be shifted from the red area to the green area.

1.8.4.2. Exercise 3: Assessing the Risk (Labeler)

Risk assessment

Severity	Probability

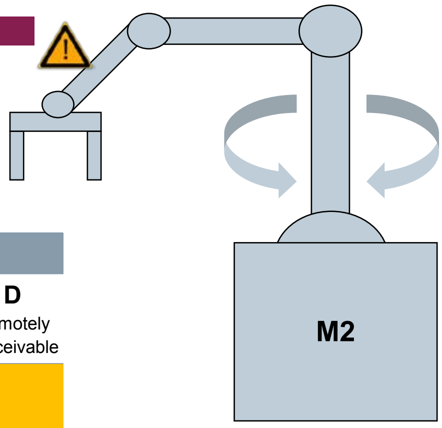
Severity of harm		Probability of occurrence **A** Very likely	 **B** Likely	 **C** Improbable	 **D** Remotely conceivable
4	Irreversible: - Death - Loss of an eye - Loss of an arm				
3	Irreversible: - Broken limbs - Loss of fingers				
2	Reversible: Treatment by a doctor necessary				
1	Reversible: First aid necessary				



1.8.4.3. Exercise 4: Assessing the Risk (Robot)

Risk assessment

Robot > Pushing, Crushing



Severity	Probability

	Probability of occurrence			
Severity of harm	**A** Very likely	**B** Likely	**C** Improbable	**D** Remotely conceivable
4 Irreversible: - Death - Loss of an eye - Loss of an arm				
3 Irreversible: - Broken limbs - Loss of fingers				
2 Reversible: Treatment by a doctor necessary				
1 Reversible: First aid necessary				

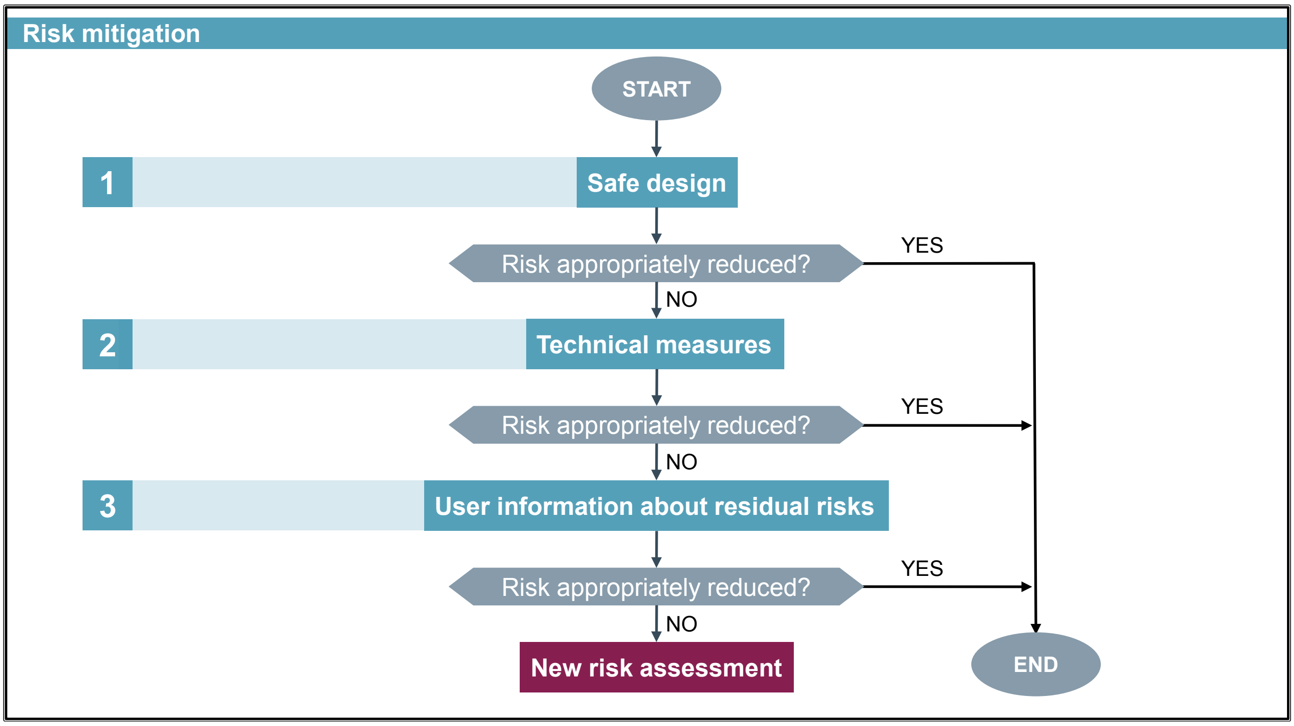
1.8.5. Summary

Risk assessment

- The machine and the risks ensuing from it have been described and evaluated.
- The result of the risk assessment is the basis for the safety concept for risk mitigation.
- By means of a correct risk assessment, the claim of negligence can be rejected in the event of damage occurring.

With the risk detected on the example machine, you can determine a defined value for the risk in the risk graph. Suitable measures should be used to shift the risk from the red area to the green area.

1.9. Risk Mitigation according to EN ISO 12100



Use the 3-step method in accordance with the harmonized EN ISO 12100 standard for definition and evaluation of the safety measures. This method can be visualized with a decision-making graph.

You begin by defining design-based safety measures. If these measures produce an accepted residual risk, no further measures are necessary.

Purely design-based measures can often be circumvented by operating personnel and so these measures do not yet produce an accepted residual risk on their own. Additional technical safety measures are required in this case.

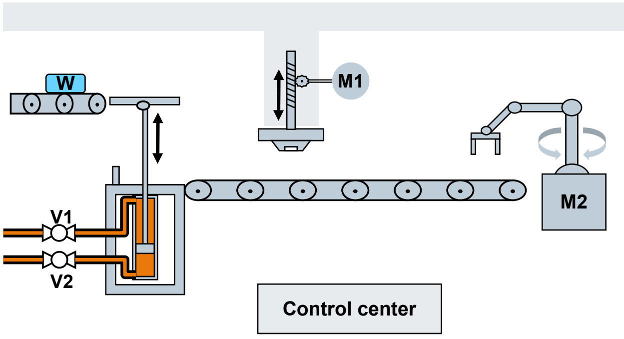
Residual risks remaining after technical safety measures can generally be mitigated by information for the user and operating specifications. Examples: wearing protective clothing, observing safety clearances, following a prescribed operating sequence, etc.

1.9.1. Step 1: Safe Design

Risk mitigation

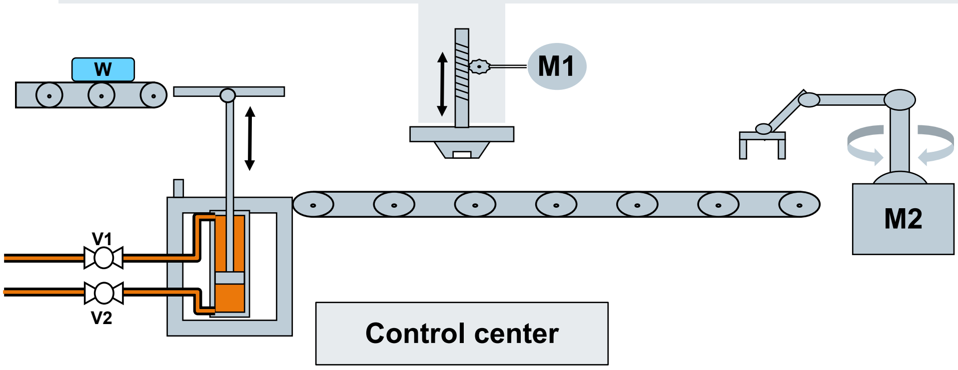
Safe machinery design has highest priority when it comes to risk mitigation!

- Integration of safety in the machine's design
- Safe operation and maintenance of the machine through design measures
- Easiest possibility of reducing the severity of harm
- Notes on safe design can be found in EN ISO 12100 Para. 6.2



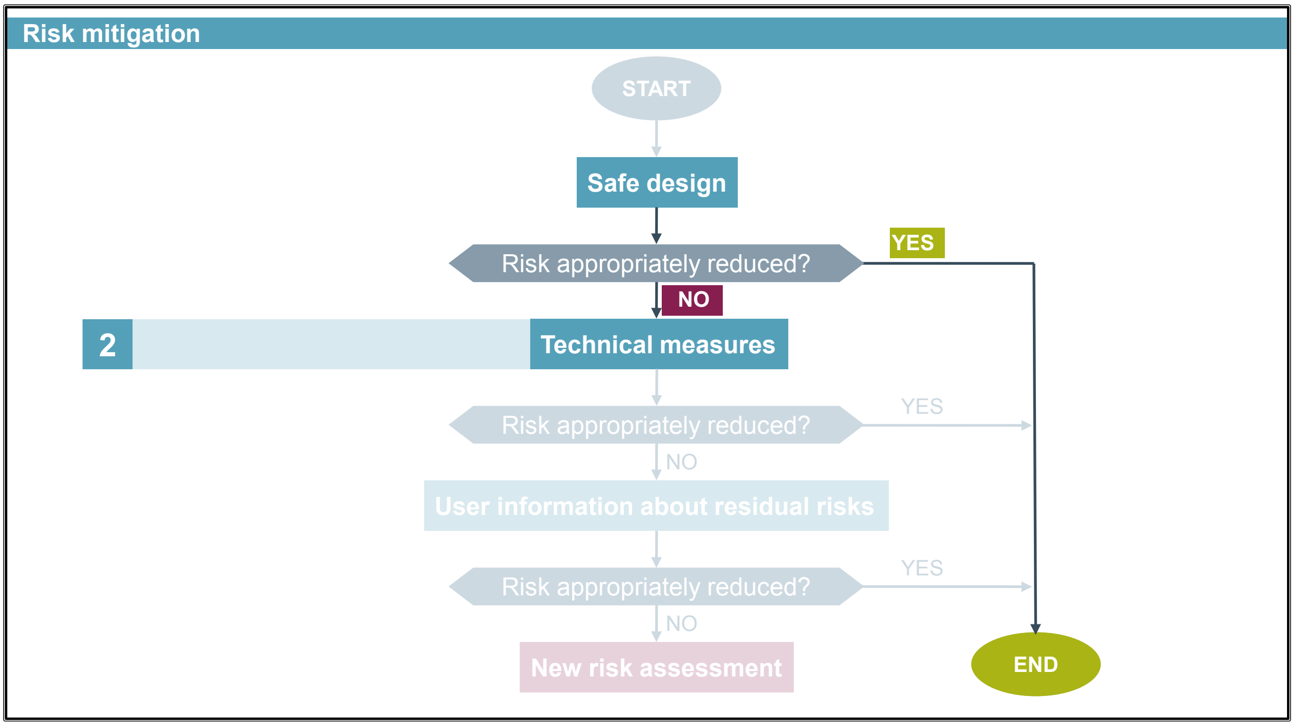
1.9.1.1. Exercise 5: Measures for Safe Design

Risk mitigation



Severity of harm	A Very likely	B Likely	C Improbable	D Remotely conceivable
4 Irreversible: - Death - Loss of an eye - Loss of an arm	**4A** **(Robot)**			
3 Irreversible: - Broken limbs - Loss of fingers	**3A** **(Labeler)**	**3B** **(Lifting device)**		

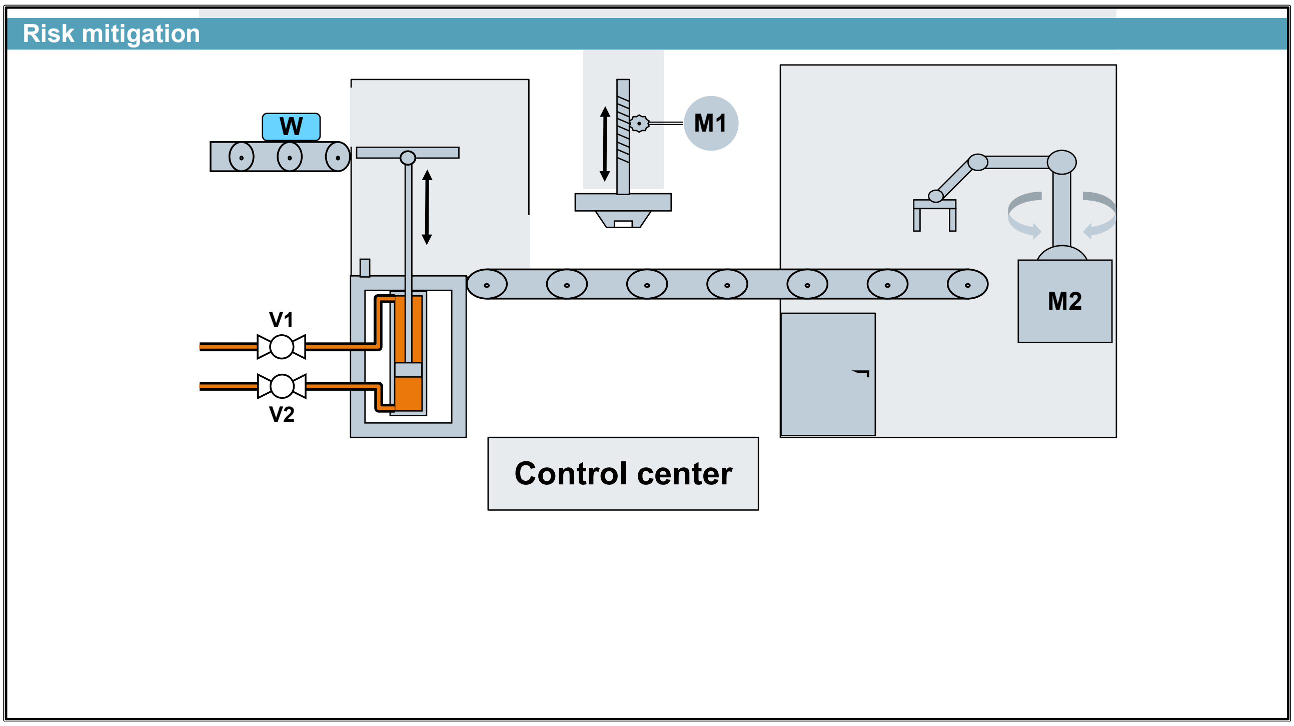
1.9.2. Step 2: Technical Protective Measures



If the design of the machine is safe, according to the 3-step method no further measures would be necessary.

In the example, the design does not yet offer adequate safety, and you must take additional technical measures.

1.9.2.1. Exercise 6: Possible Technical Protective Measures



1.9.2.2. Exercise 7: Evaluating Technical Measures

Risk mitigation

Evaluate technical measures

		Probability of occurrence			
Severity of harm		**A** Very likely	**B** Likely	**C** Improbable	**D** Remotely conceivable
4	Irreversible: - Death - Loss of an eye - Loss of an arm			**4C** **(Robot)**	
3	Irreversible: - Broken limbs - Loss of fingers	**3A** **(Labeler)**			
2	Reversible: Treatment by a doctor necessary				
1	Reversible: First aid necessary				

Current residual risks:

Are further <u>technical</u> measures necessary?

1.9.2.3. Designing the Architecture of the Safety Functions Grading Risks by means of Safety Levels

Risk mitigation

Safety levels define the quality of the technical protective measures

- **Depending on the level of the risk, a certain level of safety is required**
- Determining the risk and the resulting safety levels differ according to the standard used

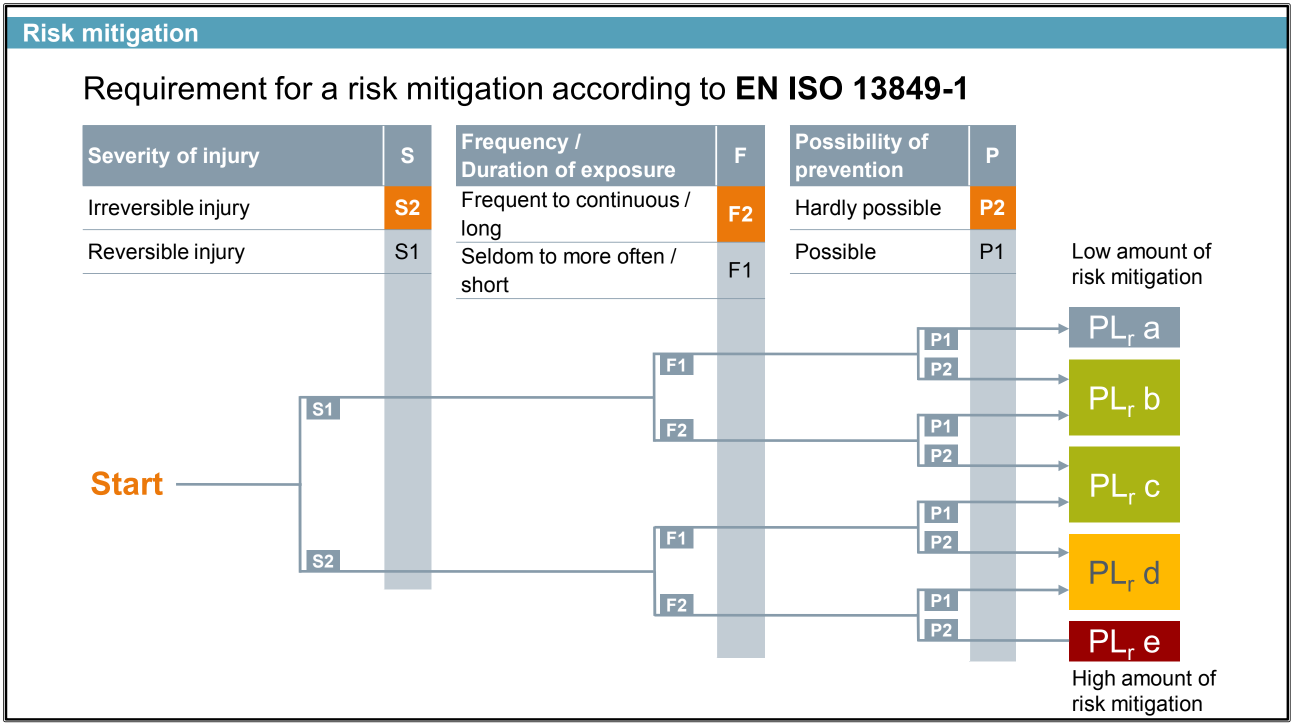
For the functional safety (safety of machines), there are 2 standards with different safety levels

- EN ISO 13849-1 Performance Levels PL a to PL e
- IEC 62061 Safety Integrity Levels SIL 1 to SIL 3

Grading Risks by means of Safety Levels

Depending on the level of risk, you must select a specific safety level. You can apply two different standards here.

1.9.2.4. Requirements according to EN ISO 13849-1



Performance level (PL) reduction on the basis of a lower probability of the hazard occurring (Section A.2.3.2)

There are several changes in Annex A. First, the informative nature of the process of PL_r determination presented in Annex A is highlighted more clearly: It is not binding and only represents an estimation of the risk mitigation. Due to the normative compromise reached in the circle of experts, taking into account reasons that may also lie outside the parameters of the risk graph, type C standards can deviate in terms of their PL_r definitions from the PL_r that would transpire from the risk graph.

The note on distinction of F1 and F2 is now formulated as follows:

- If no other justification exists, F2 should be chosen if the frequency is more than once every 15 minutes.
- F1 may be chosen if the total exposure time does not exceed 1/20 of the total service life and the frequency is not more than once every 15 minutes.

The probability of a hazardous event has now been added. If it can be evaluated as low, the PL_r may be reduced by one level. A further reduction of ‘PL_r a’ is not provided for.

1.9.2.5. Meaning of the Safety Levels

Risk mitigation

- The safety levels SIL and PL specify how high the reliability of a safety system must be:

Safety Level **SIL**	**PL**	**Required reliability of the safety system** (in failures/hour)		**Measures for increasing the reliability**
-	PL a	10^{-5} to 10^{-4}	Reliability	
SIL 1	PL b	$3x10^{-6}$ to 10^{-5}		Use “proven components”,
SIL 1	PL c	10^{-6} to $3x10^{-6}$		Regular functional tests, Automatic error detection,
SIL 2	PL d	10^{-7} to 10^{-6}		Redundant design,
SIL 3	PL e	10^{-8} to 10^{-7}		Redundancy + Error detection

- With the correct use of a safety system, its probability of failure is equivalent to the **probability of a hazard**.
- EN 62061 and EN ISO 13849-1 therefore define a **quantitative** risk and go further than EN 954-1.

Both assessments provide a result in which the failure rate allows an explicit statement about the risk. It defines how high the probability of a hazard may be.

With the help of device-specific parameters, this failure rate can be calculated according to both standards, thus allowing a statement of whether implementation of the safety function is sufficient for the required safety level.

PL and SIL are comparable but cannot be equated.

Additional measures are required to achieve the other certificate in each case, e.g., from SIL2 to SIL3.

EN 62061 and EN ISO 13849-1 regard safety functions as follows:

- A defined safety function can be assigned to a particular hazard (posed by the machine)
- The required safety level can be determined for a defined safety function

A safety function must be defined for each hazard that cannot be eliminated by structural measures. This can be implemented using a safety system. Safety systems must have a certain effectiveness, based on the examined hazard and the estimated risk.

- EN 62061: Safety Integrity Level (SIL)
- EN ISO 13849: Performance Level (PL)

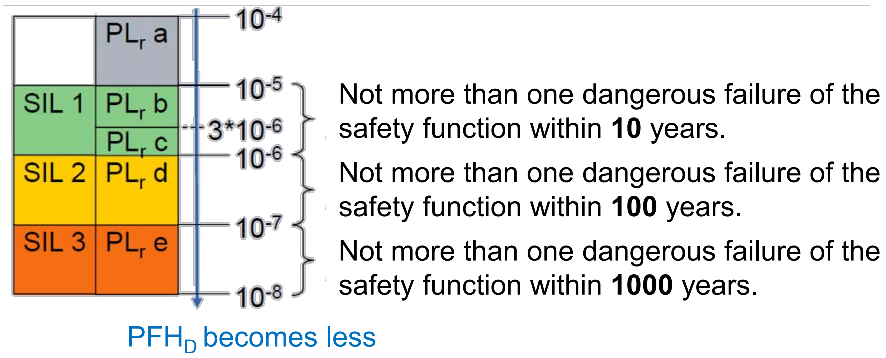
1.9.2.6. What does a Safety Level say?

Risk mitigation

Requirements relating to safety levels: Probability of failure

EN 62061 and EN ISO 13849-1 describe requirements for the maximum permissible probability of failure of the safety function:

- Probability of a dangerous failure per hour PFH_D
- The higher the safety level, the lower the PFH_D must be



Statistical Values

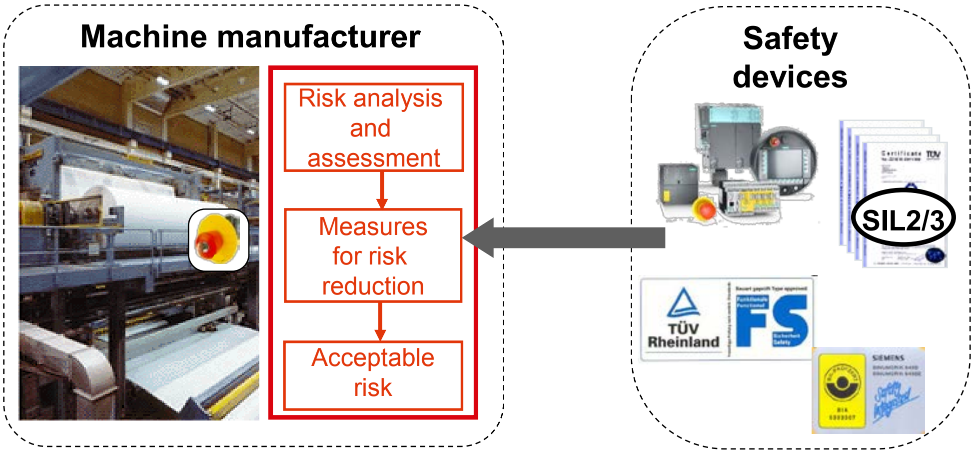
Calculated and achieved safety levels that represent "dangerous failures per unit time" are always statistical values. In other words: If a safety level SIL1 achieves a value of 2.7 x 10^{-5}, this means that 1.1826 dangerous failures could theoretically occur within 5 years. It does not mean that such a failure will necessarily occur after almost 5 years; likewise, you cannot be sure that "nothing will happen" for 4 years.

If a failure occurs, this also does not mean that nothing will now "happen" for the next 4 years. Likewise, it is also possible (and probable) that nothing "will go wrong" for 12 years.

1.9.2.7. "Safe" Machine, Certificates for Safety Devices

Risk mitigation

- An efficient measure for achieving an acceptable risk is the use of **certified** safety devices:



- The **safety devices** must be tested according to the respective relevant standards.
- They receive a **certificate** regarding the safety level that was achieved, e.g. SIL 2/3.
- The tests / acceptances are conducted by TÜV (German Technical Inspectorate), BG / BGIA (BG-Institute for Occupational Safety and Health) or similar test centers.

Certified safety devices facilitate acceptance testing.

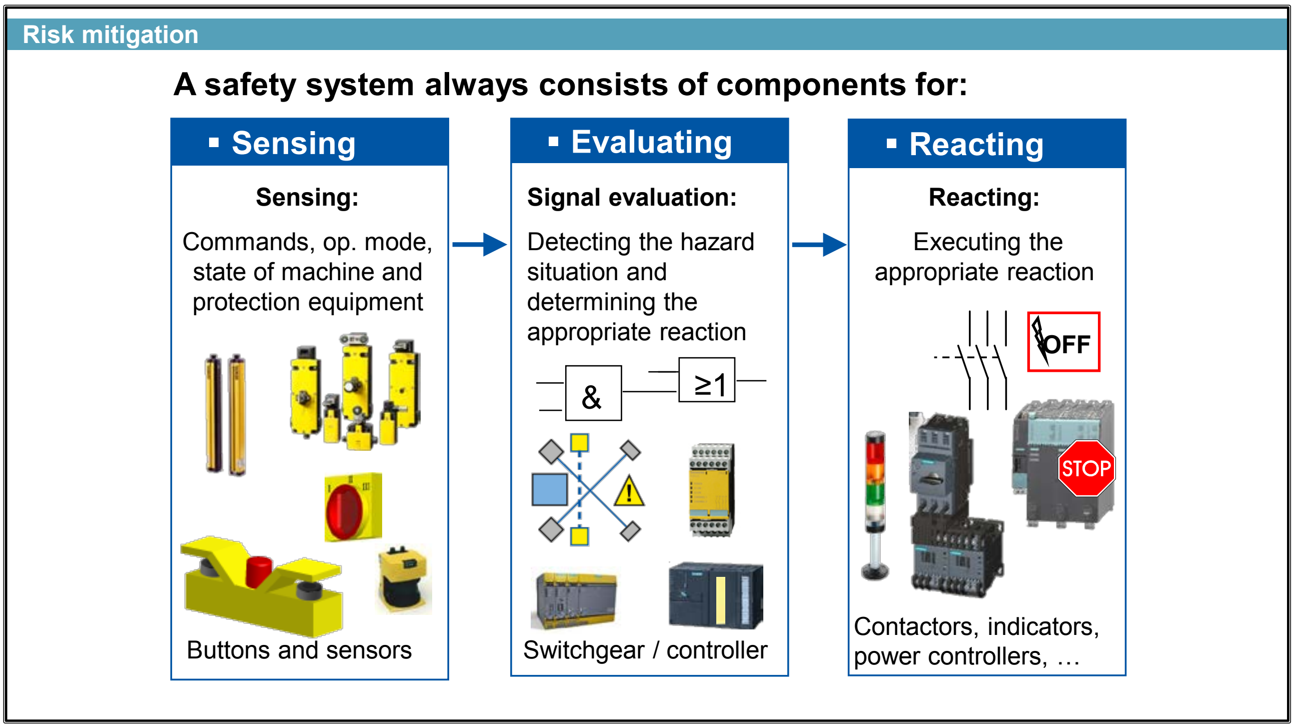
Siemens drives are certified; for example, G120 (SIL2), S120 (SIL2, PL d)

Other components for acquisition and processing (logic) also have certificates.

Certified components do not ensure that a required PL or SIL is also actually achieved. The components for the subsystems can ensure that with a corresponding interface. However, in the SENSING-EVALUATING-REACTING interaction, this is not guaranteed. This means:

- Sensor SIL3
- Logic SIL3
- Actuator SIL3 does not mean that the safety function also automatically fulfills SIL3.

1.9.2.8. The Principle of Safety Systems



3-part Systems: Sensing, Evaluating and Reacting

Sensing

Sensing can be divided into two subareas: optical sensors (light barriers, light curtains, laser scanners, etc.) and switch technology (Emergency Stop buttons, position switches, etc.).

Evaluating

This includes safety relays (3TK28) and controllers with the associated I/O components (DIs, DOs and bus systems); the logic operation between "sensing" and "reacting" takes place here.

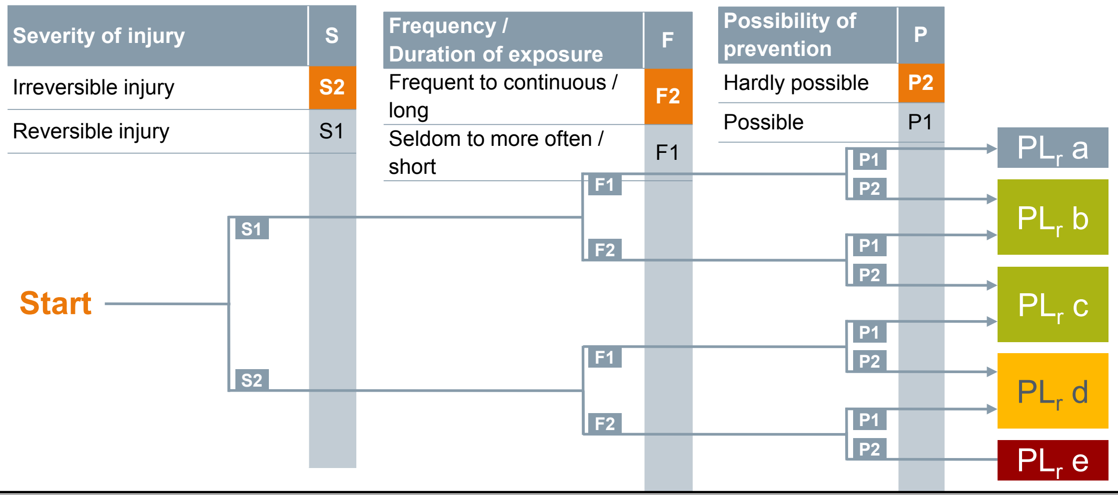
Reacting

The actuators carry out the reaction. In the simplest case, these are lights or contactors, but also include complex devices such as frequency converters (among others S120).

1.9.2.9. Exercise 8: Requirements of the Safety Functions

Risk mitigation

Lifting device	Labeler	Robot	Control unit
E-Stop	Two-hand contr.dev	Door monitoring	E-Stop
	E-Stop	E-Stop	

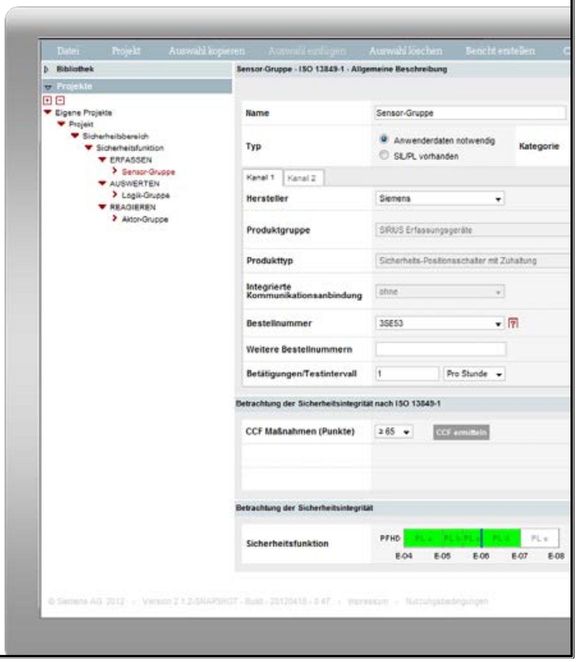


1.9.2.10. Checking Safety Functions

Risk mitigation

The checking of safety functions
is a MUST!

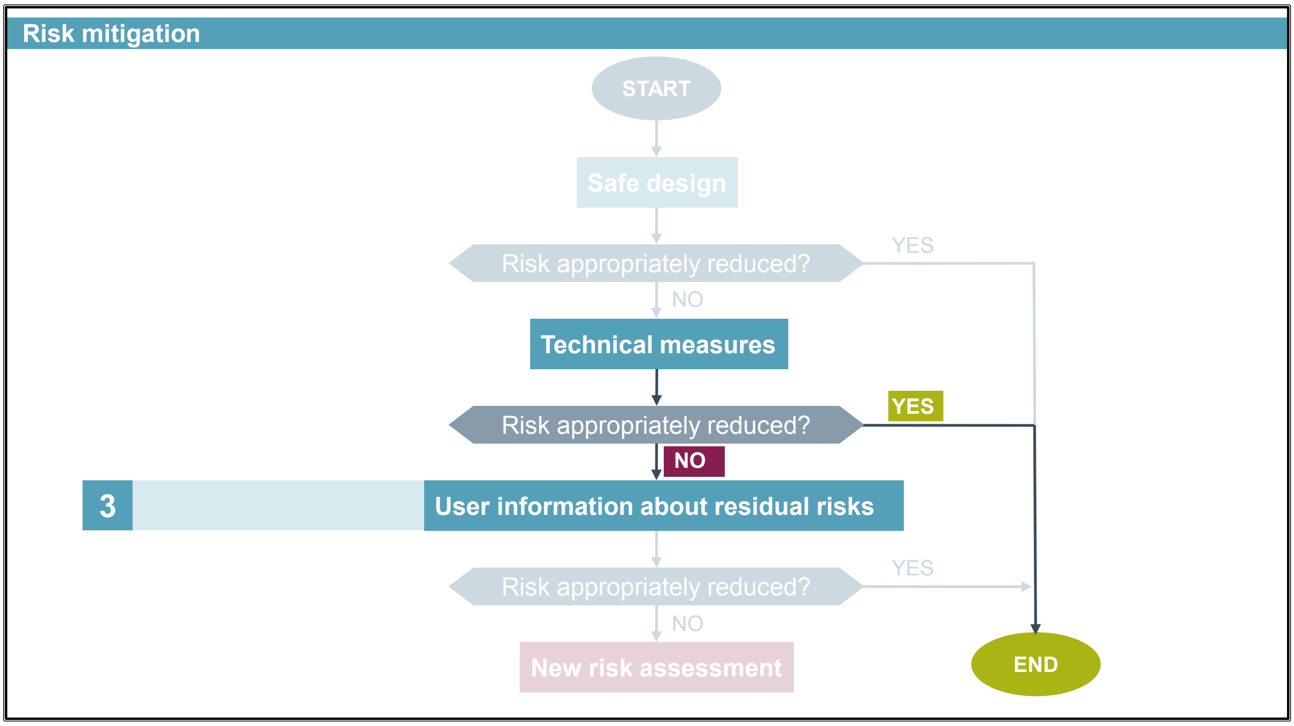
- Prescribed by the standards EN ISO 13849 and EN 62061
- Safety concept must be evaluated and documented by way of the failure probability calculation
- Evaluation possible with SET: Safety Evaluation Tool
- Free use of the online tool: www.siemens.com/safety-evaluation-tool



How can you check whether you are achieving the determined safety level by means of your safety functions? The best thing is to use the free Safety Evaluation Tool **SET** from Siemens.

More information at www.siemens.com/safety-evaluation-tool

1.9.3. Step 3: User Information about Residual Risks



In the example case, the additional technical measures offer sufficient certainty of arriving at an accepted residual risk. This is why you do not need to take any additional technical measures.

If the technical measures do not lead to an accepted residual risk, according to the 3-step method, user information about residual risks is necessary.

1.9.4. Summary

Risk mitigation

- The implemented design and technical measures have minimized the risk to such an extent that no further technical measures are necessary.
- The current state of the art used ensures legal certainty.
- Further residual risks must be pointed out through user information, such as, warning signs and training.

1.10. Verification

Verification

The manufacturer drafts the technical documents as proof of conformity. The Machinery Directive, Annex VII, prescribes the relevant contents of the technical documents.

The documentation should include, among other things:

- Risk assessment
- Project documentation including the requirement specification, the safety plan, the verification plan, the validation plan
- Development documentation including test plans and test reports
- Manuals

Documentation is essential for clarification of liability in the event of personal injury!

1.10.1. Conformity Assessment

Verification

To prove the compatibility of the machine to the provisions of the Directive(s), the manufacturer or his authorized representative carries out a conformity assessment procedure.

Possible procedures according to MRL 2006/42/EC

- Internal production check
- Type test
- Quality assurance system

1.10.2. Contents of the EC Declaration of Conformity

Verification

The EC Declaration of Conformity for machinery must include the following information:

- Name and address of the manufacturer or his authorized representative established within the Community
- Description of the machinery, all relevant provisions to which the machinery complies
- Where appropriate, name and address of the notified body and the number of the EC type-examination certificate
- Where appropriate, name and address of the notified body to which the files have been forwarded in accordance with Article 12, Paragraph 3
- Where appropriate, name and address of the notified body which has carried out the verification in accordance with Article 12, Paragraph 3, where appropriate, the publication references of the harmonized standards
- Where appropriate, national technical standards and specifications which have been applied
- Particulars of the signatory authorized to sign the legally binding declaration for the manufacturer or his authorized representative established in the Community

In the **declaration of incorporation** (not a complete machine, but a part for mounting in other machines or systems…), you also have to declare the machine parts for incorporation and include a statement that the machine must not be commissioned until the machine into which it will be incorporated meets the provisions of the Directive.

Verification / Contents of the EC Declaration of Conformity

In the new version of the Machinery Directive (2006/42/EC of May 17, 2006), the (earlier) manufacturer declaration has been legally superseded by a declaration of incorporation since December 29, 2009.

In contrast to the old "manufacturer declaration", the declaration of incorporation contains safety-related information. The specific contents of the declaration of incorporation are stated in a check list in Annex II 1 B of the Machinery Directive.

A declaration of incorporation is issued for a partly completed machine by the manufacturer or an authorized representative. In accordance with Annex II B of the Directive, it must contain a statement that the commissioning of a machine or system in which this component is incorporated is prohibited until conformity with the directive has been established. Furthermore, the declaration must contain the following information (in addition to the information required for the previous directive):

- Business name and address of the manufacturer; in addition to the description also information for identification (generic denomination, function, model, type, serial number and commercial name);
- Name and address of the person responsible for the documentation; he/she must be a resident of the EU;
- A declaration of which requirements of the Machinery Directive are applied and a declaration that the technical documents are prepared in accordance with Annex VII B;
- A declaration of commitment to transmit, in response to a reasoned request, documents to national authorities; also the method of transmission must be specified;
- Information about the person who issues the declaration of incorporation.

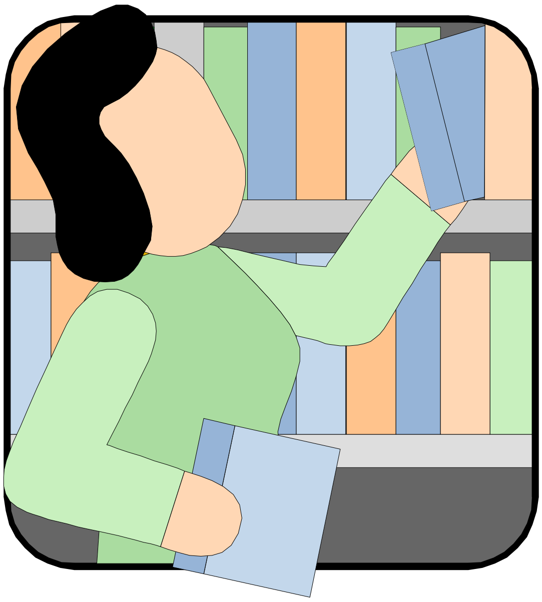
A CE-marking is not permitted for partly completed machinery according to the Machinery Directive.

1.11. Summary

- The Machinery Directive has the status of a law!
- The Machinery Directive is binding for all machine manufacturers and applies to all safety solutions used.
- Due to the presumption of conformity, application of harmonized standards reduces liability risk.
- The use of certified products for applications in accordance with EN 62061 and EN ISO 13849 facilitates the implementation of safety solutions.

On the safe side: safe machine, cost savings, legal certainty!

1.12. Additional Information



1.12.1. The European Machinery Directive

The EU Machinery Directive 2006/42/EC

http://www.newapproach.org // http://eur-lex.europa.eu

- Describes basic safety and health protection requirements for machinery
- Complying with the Machinery Directive MRL 2006/42/EC is one prerequisite for the CE-marking.
- The European Machinery Directive is implemented in national legislation and is therefore binding.

1.12.2. Help on Standards

Courses at SITRAIN

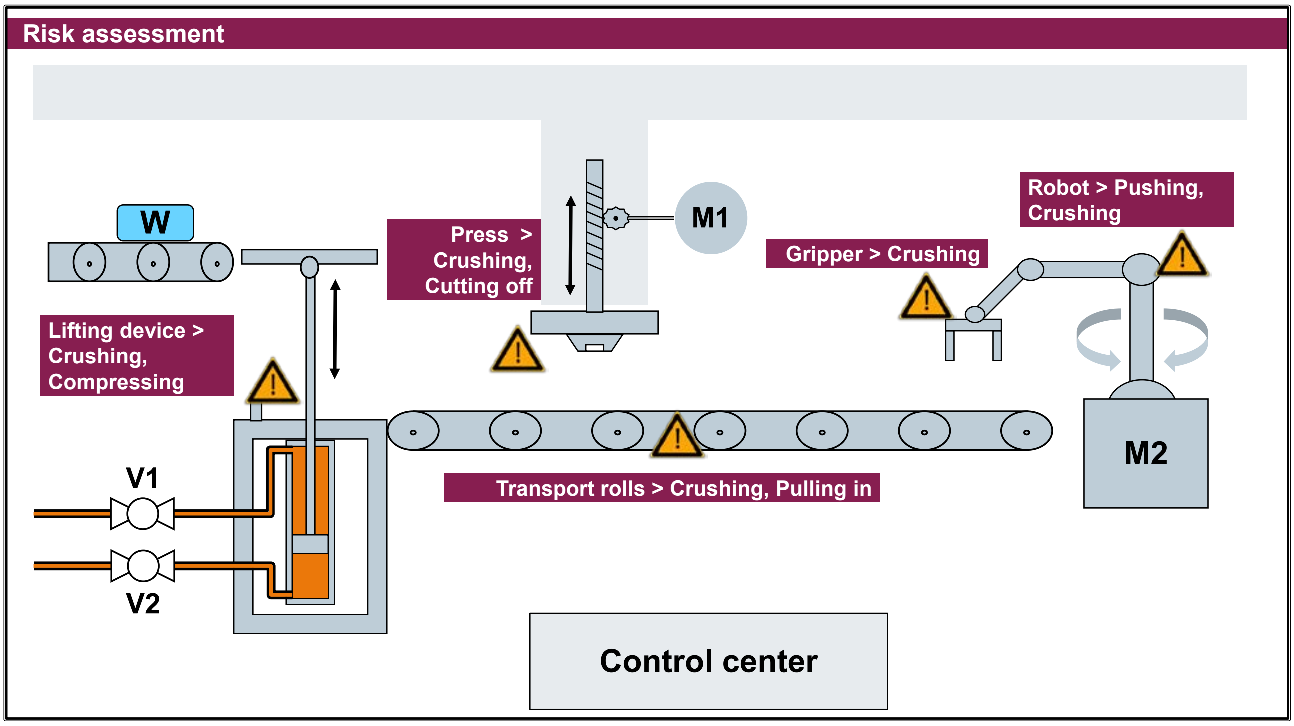
http://sitrain.automation.siemens.com/sitrainworld/

ST-FASAFN
CE-Marking & Functional Safety in Machine and System Manufacturing

1.13. Possible Solutions for Exercises 1-8

The solutions are not binding but a possibility. In principle, there is no “one” correct solution for the topics Risk assessment and Risk mitigation.

1.13.1. Exercise 1

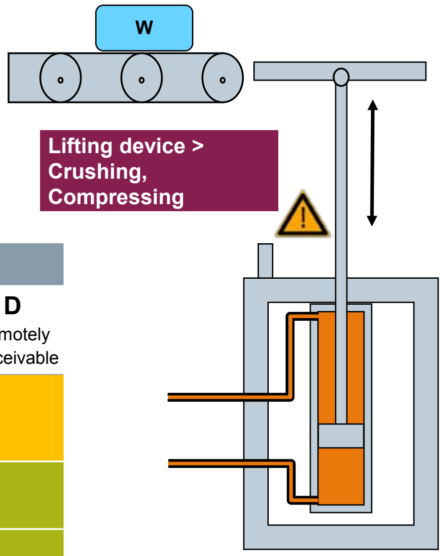


1.13.2. Exercise 2

Risk assessment

Severity
Irreversible:
- Broken limbs
- Loss of fingers

Probability
It is likely that an injury occurs.



		Probability of occurrence			
Severity of harm		**A** Very likely	**B** Likely	**C** Improbable	**D** Remotely conceivable
4	Irreversible: - Death - Loss of an eye - Loss of an arm				
3	Irreversible: - Broken limbs - Loss of fingers		3B		
2	Reversible: Treatment by a doctor necessary				
1	Reversible: First aid necessary				

Risk evaluation by the team

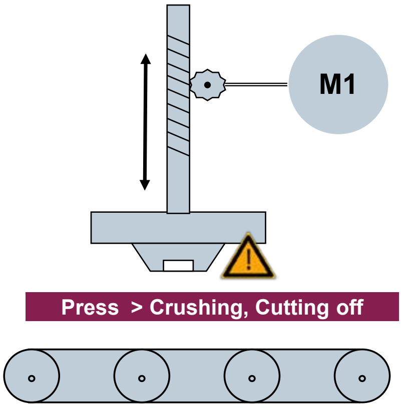
1.13.3. Exercise 3

Risk assessment

Severity	Probability
Irreversible: - Broken limbs - Loss of fingers	It is very likely that an injury occurs.

Severity of harm	Probability of occurrence A Very likely	B Likely	C Improbable	D Remotely conceivable
4 Irreversible: - Death - Loss of an eye - Loss of an arm				
3 Irreversible: - Broken limbs - Loss of fingers	3A			
2 Reversible: Treatment by a doctor necessary				
1 Reversible: First aid necessary				

Risk evaluation by the team



1.13.4. Exercise 4

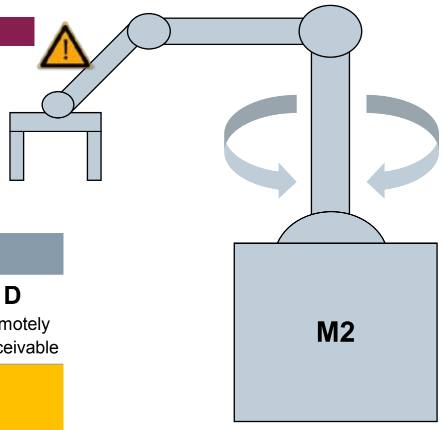
Risk assessment

Robot > Pushing, Crushing

Severity	Probability
Irreversible: - Death - Loss of an eye/arm	It is very likely that an injury occurs.

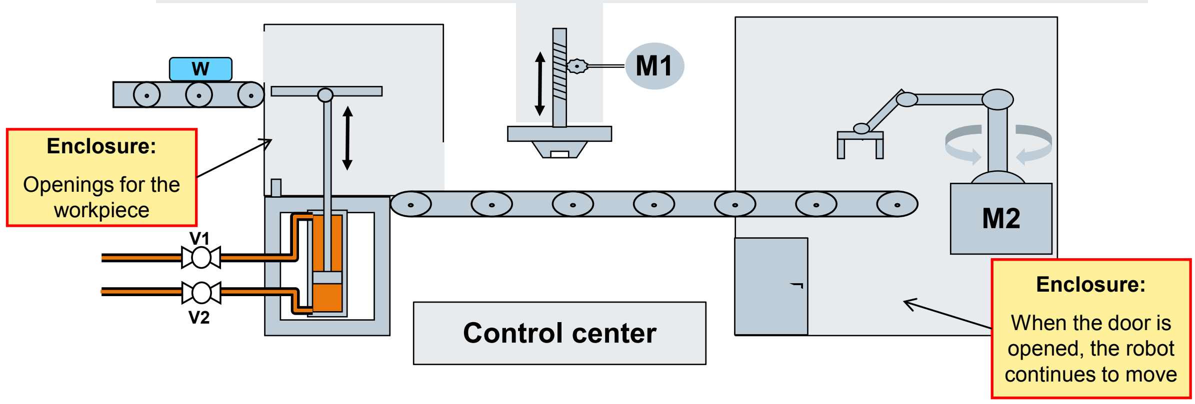
		Probability of occurrence			
Severity of harm		**A** Very likely	**B** Likely	**C** Improbable	**D** Remotely conceivable
4	Irreversible: - Death - Loss of an eye - Loss of an arm	**4A**			
3	Irreversible: - Broken limbs - Loss of fingers				
2	Reversible: Treatment by a doctor necessary				
1	Reversible: First aid necessary				

Risk evaluation by the team



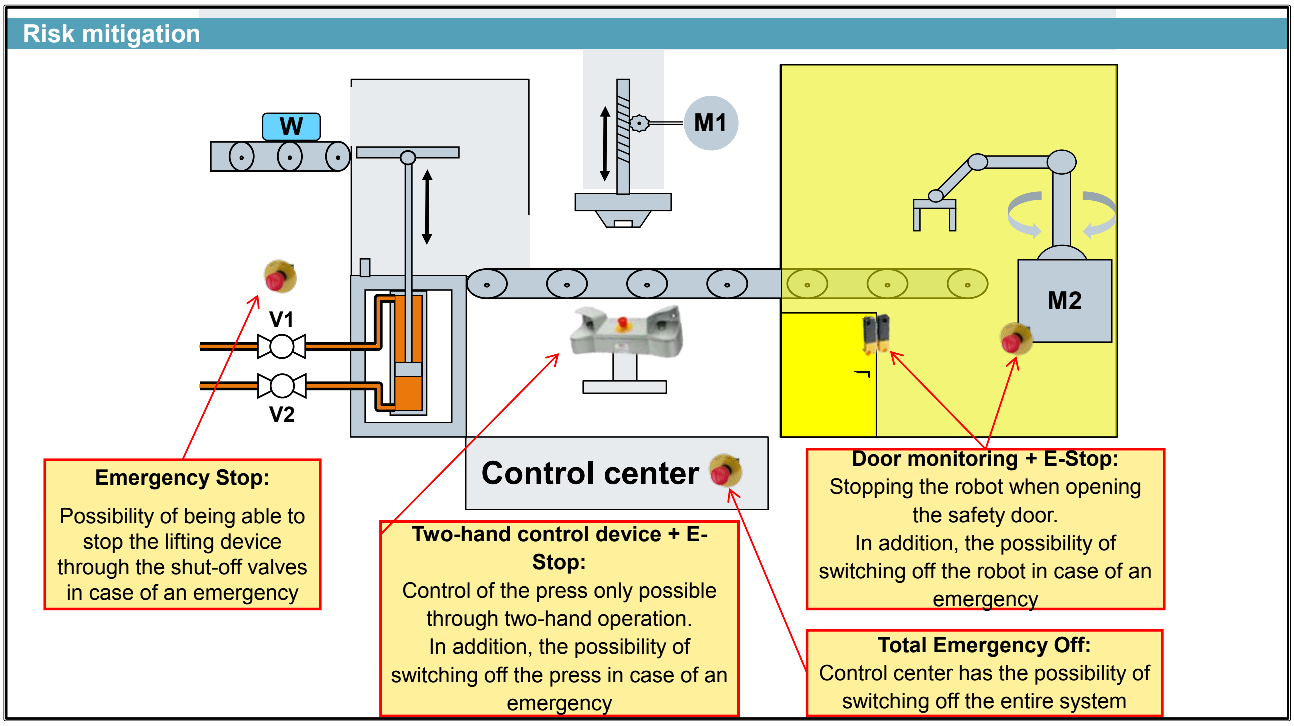
1.13.5. Exercise 5

Risk mitigation

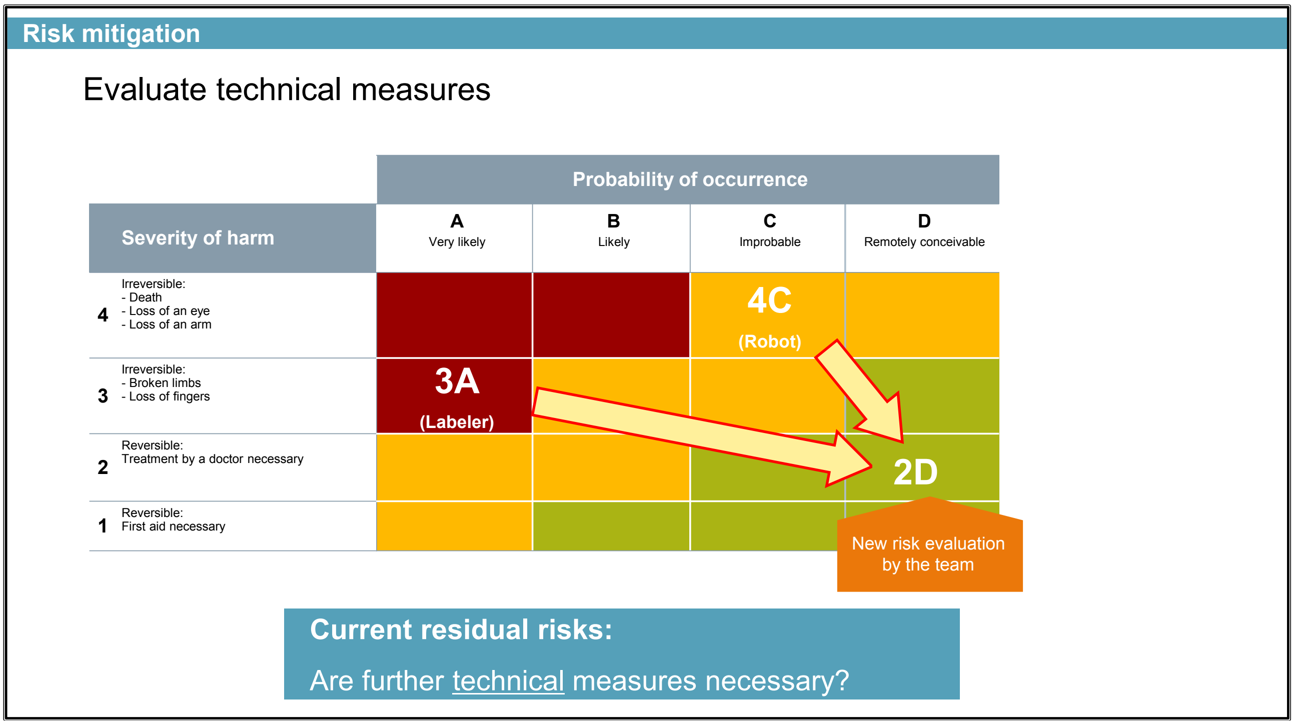


	Severity of harm	A Very likely	B Likely	C Improbable	D Remotely conceivable
4	Irreversible: - Death - Loss of an eye - Loss of an arm	4A (Robot)			
3	Irreversible: - Broken limbs - Loss of fingers	3A (Labeler)	3B (Lifting device)		

1.13.6. Exercise 6



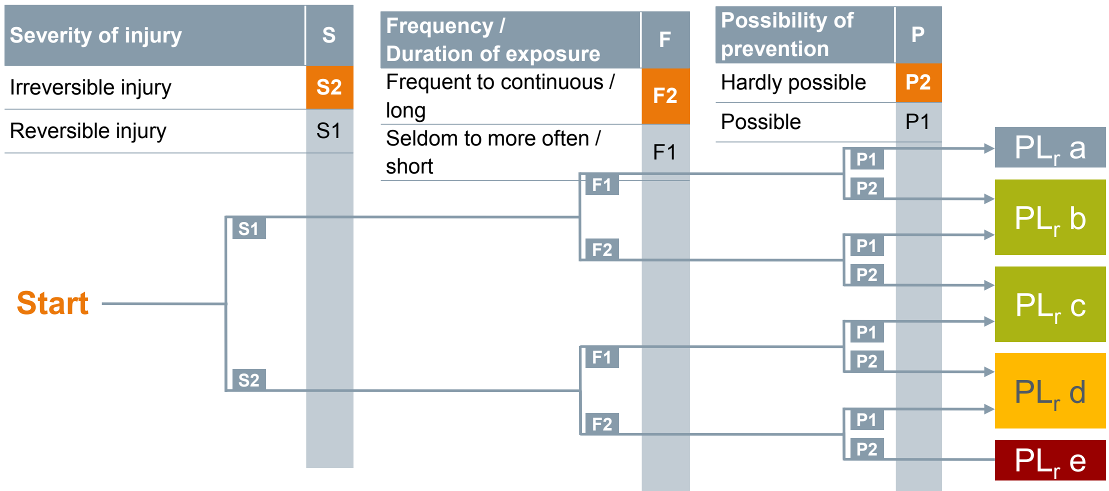
1.13.7. Exercise 7



1.13.8. Exercise 8

Risk mitigation

Lifting device		Labeler		Robot		Control unit	
E-Stop	**PLc**	Two-hand contr.dev	**PLd**	Door monitoring	**PLd**	E-Stop	**PLd**
		E-Stop	**PLd**	E-Stop	**PLd**		



Contents

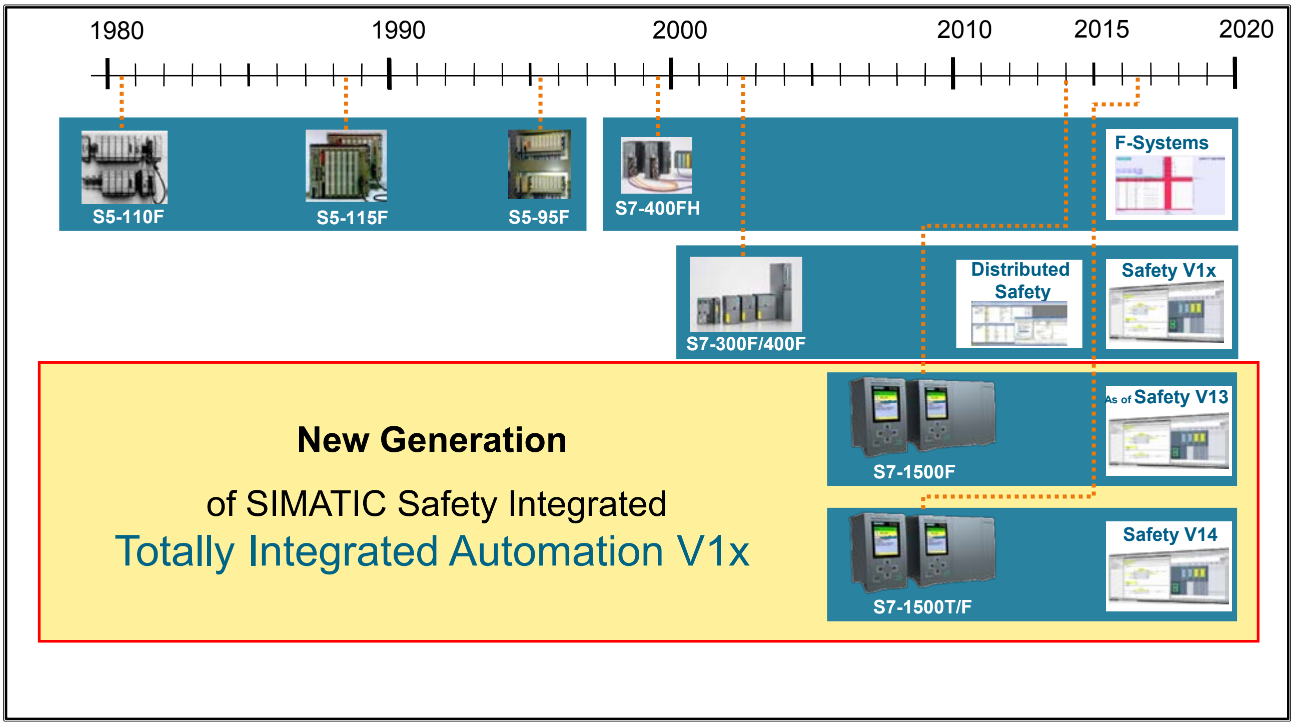
2

2. Product Overview

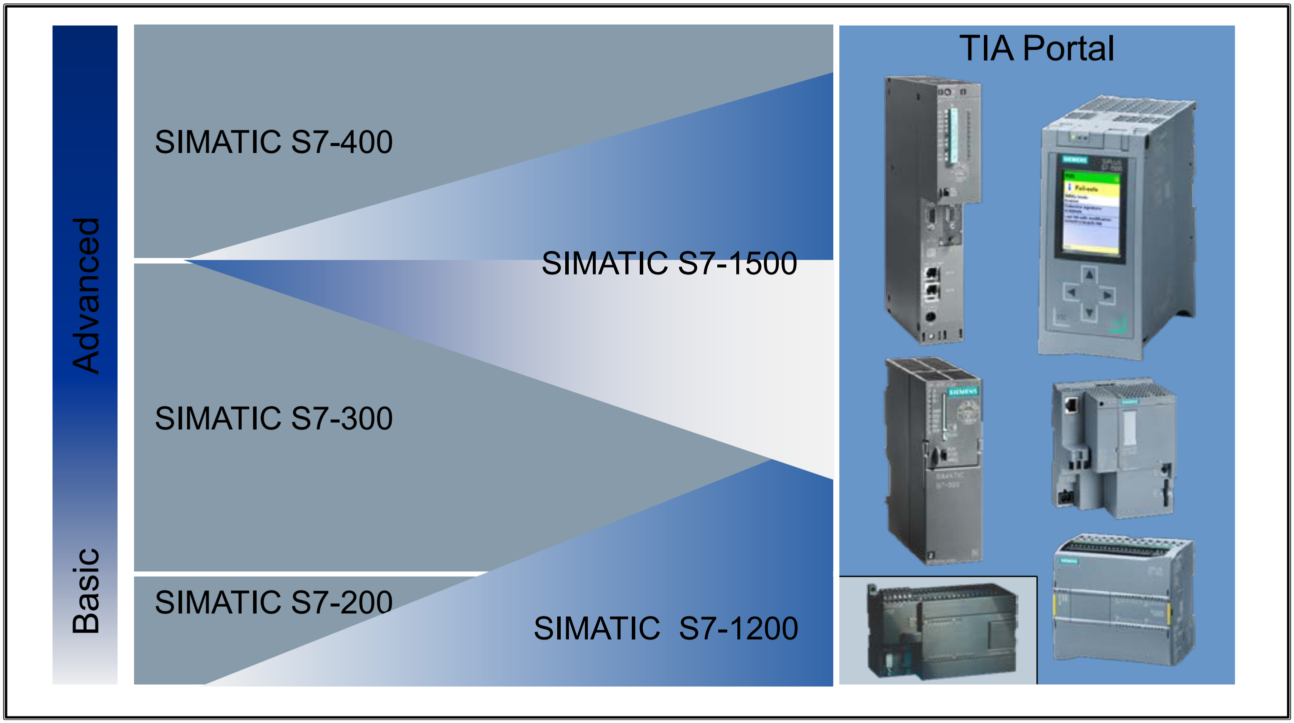
At the end of the chapter the participant will ...

… gain an initial overview of the fail-safe components portfolio in the TIA Portal

2.1. History of SIMATIC Safety



2.2. Positioning the Modular S7 Controllers

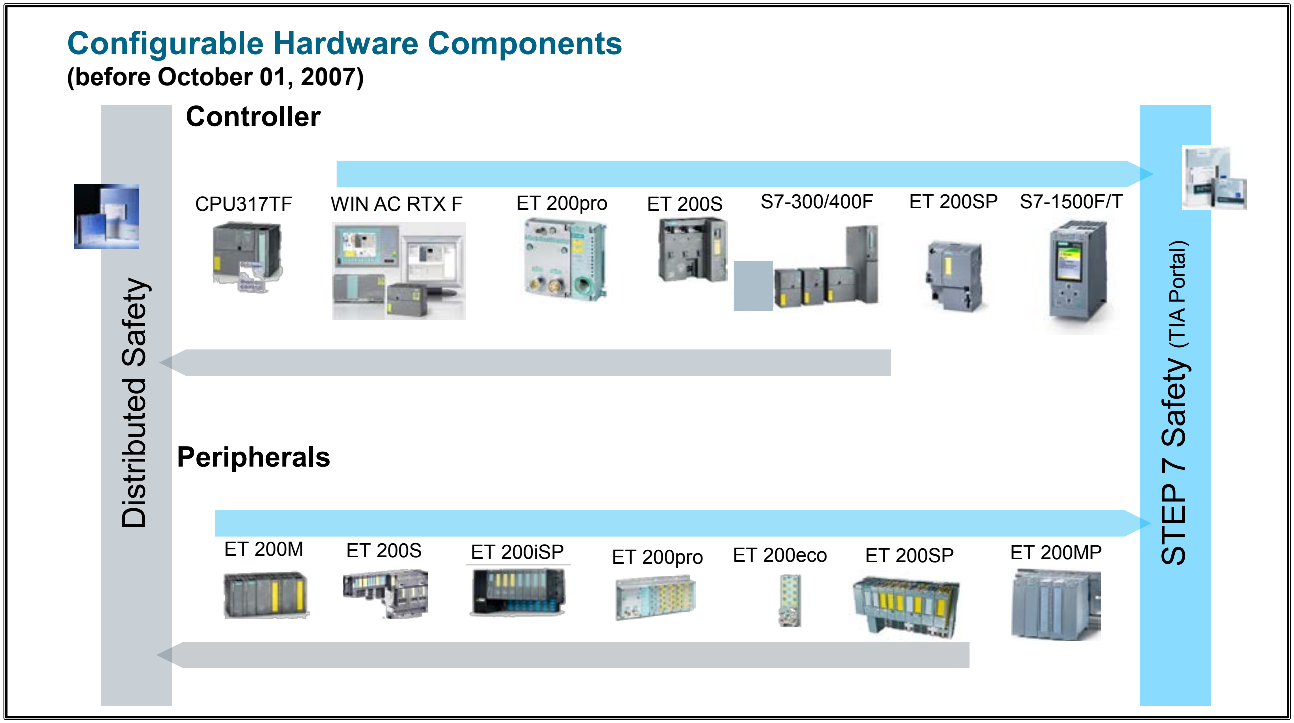


SIMATIC S7

The programmable logic controllers can be divided into the performance ranges Basic (S7-1200) and Advanced (S7-1500).

The product range of the S7-1200 and S7-1500 will be expanded in the next few years such that the S7-200, S7-300 and even the S7-400 can be completely replaced.

2.3. Configurable Hardware



2.4. SIMATIC S7-1200

	1200-CPUs				
CPU Types	**1211C**	**1212FC**	**1214FC**	**1215FC**	**1217C**
Interfaces	1	1	1	1 1	1 1
Program / Data memory	50KB 4 MB	75/100KB 4 MB	100/125KB 4 MB	125/150KB 4 MB	150KB 4 MB
Bit Performance	85 ns	85 ns	85 ns	85 ns	85 ns
Width	90 mm	90 mm	110 mm	130 mm	150 mm

Features

- Modular compact control system for the low-end performance range
- Scaled CPU range
- Extensive range of modules
- Can be expanded to up to 11 modules (depends on the CPU)
- Can be networked with PROFIBUS or PROFINET
- Slot
  - Communication modules are placed to the left of the CPU (number depends on the CPU)
  - Signal modules are placed to the right of the CPU (number depends on the CPU)
- "Total package" with CPU and I/O in one device
  - integrated digital and analog I/O
  - an expansion with signal board
- "Micro PLC" with integrated functions

2.4.1. S7-1214FC / 1215FC

CPU 1214FC / 1215FC

(DC/DC/DC; DC/DC/Rly)

- Safety program and standard applications
- Work memory 125 / 150 KB, 4 MB load memory
- Performance: 85-ns bit performance
- 110 /130 mm widths
- PROFINET interface
- Integrated technology such as Motion, controlling, counting, measuring
- **No F-I/Os on Board!**
- **Profisafe (as of V4.1)**

Failsafe S7-1200 IO-Modules

- SM 1226 F-DI 16 x 24VDC
- SM 1226 F-DQ 4 x 24VDC
- SM 1226 F-DQ 2 x Relay

Slot Rules

- Communication modules are placed to the left of the CPU (number depends on the CPU)
- Signal modules (digital, analog) are placed to the right of the CPU (number depends on the CPU)

Signal Modules

- Digital input, output or mixed modules (24VDC, relay)
- Analog input, output or mixed modules (voltage, current, resistance, thermocouple)

Communication Modules (CM - Communication Module, CP - Communication Processor)

- Point-to-point connection (RS232, RS485)
- PROFIBUS
- ASi-Master
- Telecontrol (GPRS functionality)

Expansion Board

- The CPU can be expanded by the addition of one signal board for I/O or one communication board.
- Optionally, a battery board can be installed to provide long-term battery backup for the CPU’s real-time clock

2.5. SIMATIC S7-1500

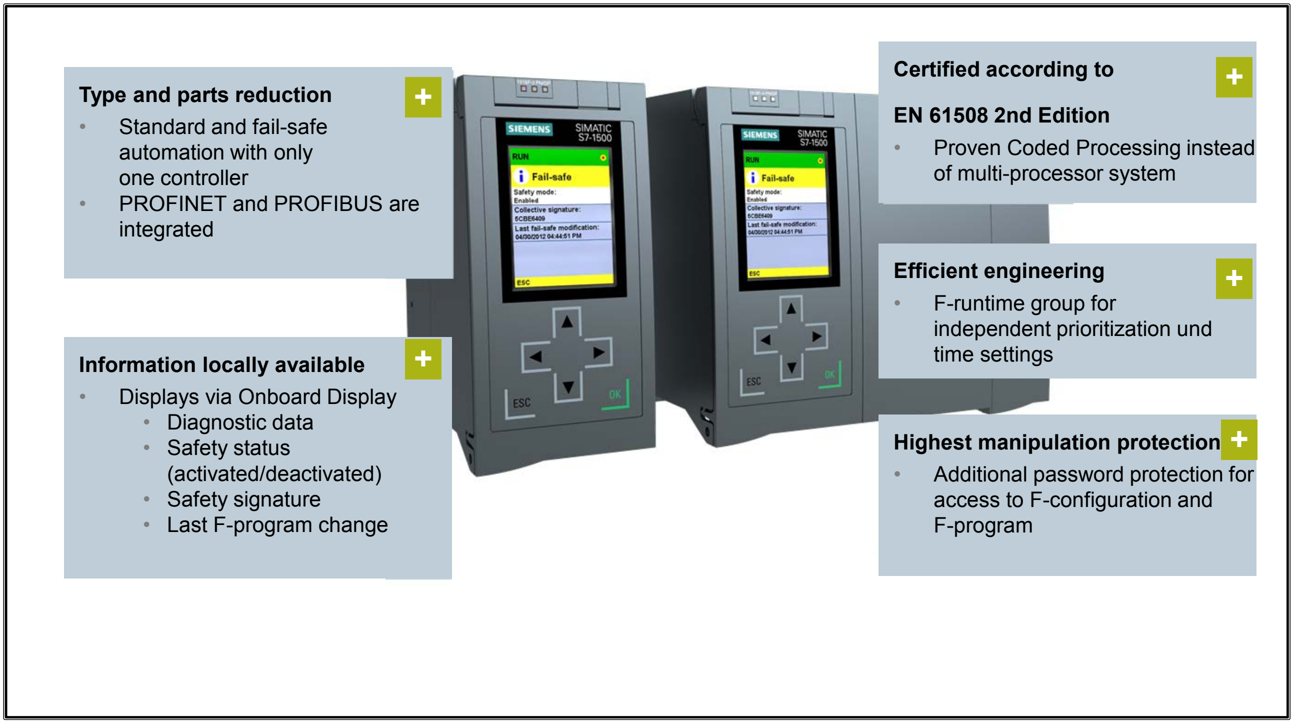
	ET 200SP		1500 CPUs						T-CPUs	MFP CPU
CPU Types	**1510SP F-1PN**	**1512SPF-1PN**	**1511F-1PN**	**1513F-1PN**	**1515F-2PN**	**1516F-3PN/DP**	**1517F-3PN/DP**	**1518F-4PN/DP**	**1511TF 1515TF 1516TF 1517TF**	**1518F-4PN/DP MFP**
Interfaces	1 1 1	1 1 1	1 1	1 1	1 2 1	1 2 1	1 2 1	1 2 1 3	As Standard	1 2 1 3
Program / Data memory	100/150KB 750KB	200/300KB 1MB	150/225KB 1MB	300/450KB 1.5 MB	500/750KB 3 MB	1/1.5 MB 5 MB	2/3 MB 8 MB	4/6 MB 20 MB	50% more Program memory	4/6 MB 20 MB 50 MB[1)]
Bit Performance	72ns	48ns	60 ns	40 ns	30 ns	10 ns	2 ns	1 ns	As Standard	1 ns
Width	100mm	100mm	35 mm	35 mm	70 mm	70 mm	175 mm	175 mm	As Standard	175 mm

1) additional 50 MB memory for ODK applications

Highlights of the SIMATIC S7-1500 System

- Highest performance of the entire system (terminal-terminal)
  - High performance program execution in the CPU
  - High performance backplane bus
  - PROFINET interface with PROFINET IO IRT on every CPU
  - Automatically activated system diagnostics, right down to the IO channel
- Trace for all CPU tags
- CPU - Display for:
  - Access to MLFB, FW version and serial number
  - Commissioning (e.g. Setting the IP address, station name)
  - Backup/Restore
  - Diagnostics
- Simplified programming through user-friendly instructions in LAD/FBD/STL

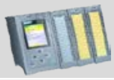
2.5.1. SIMATIC S7-1500F CPUs



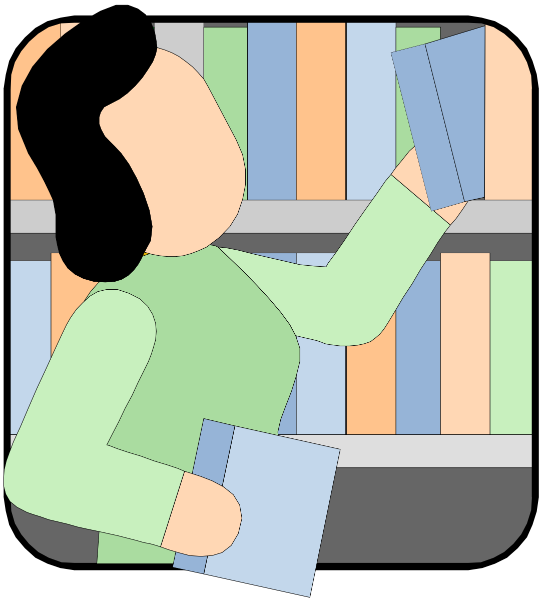
CPU 1510SP F-1 PN to CPU 1518F-4 PN/DP

The CPU 1510SP F-1 PN to CPU 1518F-4 PN/DP are the fail-safe CPUs for standard and fail-safe applications that contain distributed automation structures in addition to central I/O. They can be used as a PROFINET IO Controller or as distributed intelligence (PROFINET I-Device). The integrated PROFINET IO IRT interface is designed as a switch so that a linear topology (structure) can be set up in the system. In addition, the CPU offers comprehensive closed-loop control functionalities as well as the ability to connect drives via standardized PLCopen blocks. The S7-151xF fail-safe controllers are certified according to EN 61508 (2010) for functional safety and are suitable for use in safety-relevant applications up to SIL 3 according to IEC 62061 and PL e according to ISO 13849. For IT security, an additional password protection has been set up for F-configuration and F-program.

2.6. Fail-safe I/Os

Fail-safe I/Os		F-DI	F-DO	F-DI/DO	F-AI	F-PM	F-RO	Properties	
IP20	ET 200M	X	X	-	X	-	-	Modular I/O for high-channel applications with up to 24 channels per module	
	ET 200MP	X	X	-	-	-	-	Modular I/O for high-channel applications with up to 24 channels per module	
	ET 200S	X	X	X	-	X	X	Fine-modular I/O with up to 8 channels per module	
	ET 200SP	X	X	-	-	X	X	Fine-modular I/O with up to 8 channels per module	
	ET 200iSP	X	X	-	X	-	-	Fine-modular I/O with up to 8 channels per module suitable for the hazardous area	
IP 65/67	ET 200pro	X	-	X	-	-	X	Modular, multifunctional I/O in high degree of protection	
	ET 200eco	X	-	-	-	-	-	Economical Block I/O in high degree of protection	

2.8. Additional Information



2.8.1. ET 200SP and ET 200pro Controller

- **SIMATIC S7-1500 with the design of a SIMATIC ET 200SP or ET 200pro**
- **For machines with distributed architecture and serial machines with limited space**
- **Transfer of the intelligence from the central control cabinet to Distributed Controller**
- **Available in standard and fail-safe version**

Further Information under the Link:

TIA Portal Information Center **>** Product information **>** Controllers **>** SIMATIC controllers in general > Distributed Controllers

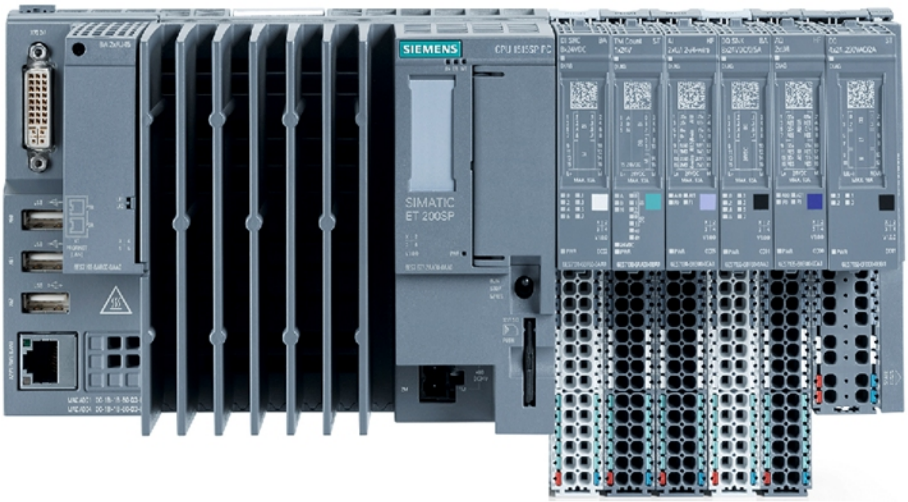
2.8.2. Software Controller

- **Use with industry-suitable SIMATIC IPCs**
- **Runs completely independently of the Windows system (even with restart or failure of Windows)**
- **Flexible controller for special-purpose machines with high performance and functional requirements**
- **Integration of user-specific functions via open interfaces (for example C++ / Matlab)**

Further Information under the Link:

TIA Portal Information Center **>** Product information **>** PC-Based Automation **>** SIMATIC Software Controller

2.8.3. ET 200SP Open Controller "All in one"



- **Controller with central, modular I/Os**
- **Visualization and Windows applications**
- **PC interfaces for monitor, mouse and keyboard**
- **Gigabit Ethernet**

Further Information under the Link:

TIA Portal Information Center **>** First steps **>** Getting Started **>** SIMATIC Open Controller - Getting Started

2.8.4. Overview Safety Functions SINAMICS S/G

Drive	Basic Functions			Extended Functions								
ET 200 S/PRO FC F-Version	STO	SS1		SLS								
SINAMICS G120/G120C/G120D-2	STO											
SINAMICS G120 F-Version	STO	SS1		SLS	SDI	SSM						
SINAMICS G120D-2 F-Version	STO	SS1		SLS	SDI	SSM						
SINAMICS S110	STO	SS1	SBC	SLS	SDI	SSM	SS2	SOS				
SINAMICS S120 Booksize & Blocksize	STO	SS1	SBC	SLS	SDI	SSM	SS2	SOS	SLP	SP	SBT	SGS
SINAMICS S120 Chassis & Cabinet Modules	STO	SS1	SBC	SLS	SDI	SSM	SS2	SOS	SLP	SP	SBT	SGS
SINAMICS G130/150	STO	SS1	SBC	SLS	SDI	SSM	SS2	SOS	SLP	SP	SBT	SGS
SINAMICS S150	STO	SS1	SBC	SLS	SDI	SSM	SS2	SOS	SLP	SP	SBT	SGS

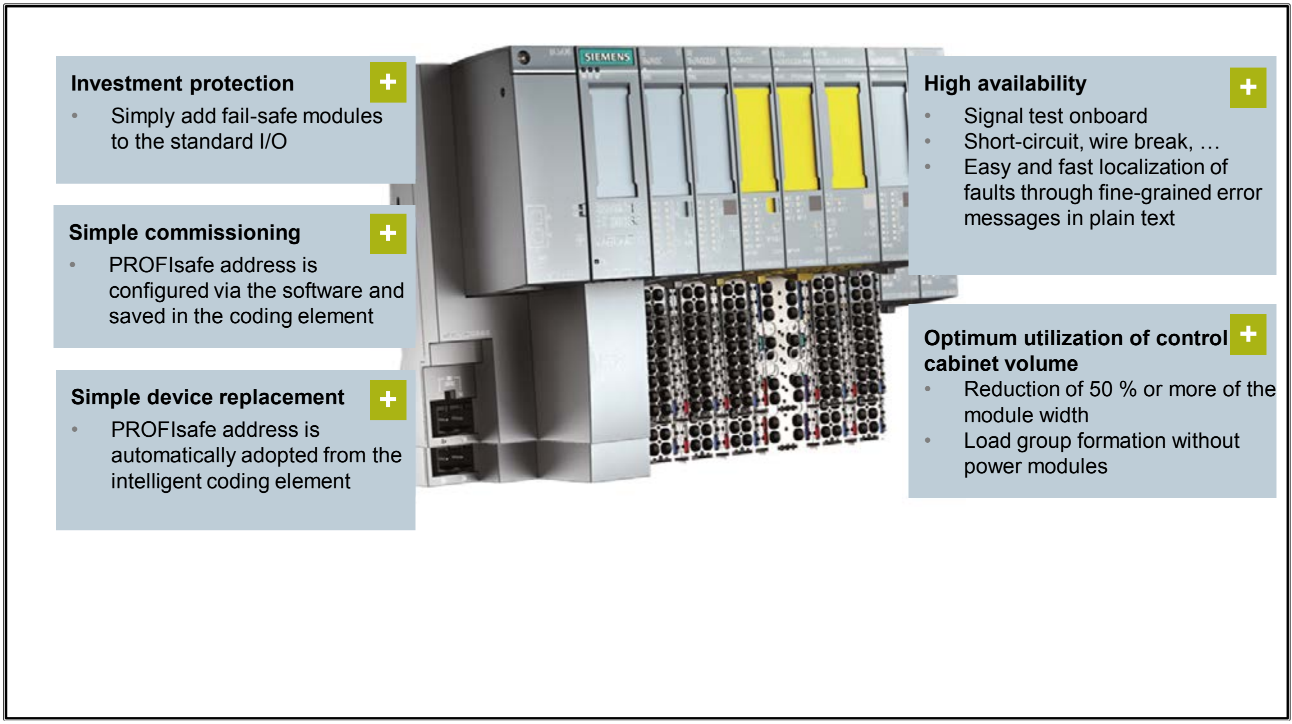
The SINAMICS Safety Integrated Functions:

- STO: Safe Torque Off / Safe Brake Control
- SS1: Safe Stop 1
- SS2: Safe Stop 2
- SOS: Safe Operating Stop
- SLS: Safely Limited Speed
- SSM: Safe Speed Monitor
- SDI: Safe Direction
- SBC: Safe Brake Control
- SP: Safe Position
- SLP: Safe Limited Position
- SBT: Safe Brake Test

Notes

- Encoder-less operation is possible for all asynchronous motors and the synchronous motors 1FU8 (SIEMOSYN).
- If the Basic Functions are to be controlled via TM54F. The Extended Functions, that contain the Basic Functions, must be used.
- Basic Functions are license-free, can also be controlled without license via PROFIsafe.
- For the Extended Functions, a license must be purchased for each axis.
- The Extended Functions can be controlled using PROFIsafe or the Terminal Module TM54F.

2.8.5. SIMATIC ET 200SP



SIMATIC ET 200SP Fail-safe I/O Modules

With the SIMATIC ET 200SP, safety-related communication using PROFIsafe is also possible. The safety modules for digital inputs and outputs (DI and DQ) are the same size as the standard modules. Their functional safety is certified according to EN 61508. They are designed for safety-related use up to SIL 3 according to EN 62061 and PL e according to ISO 13849.

A special characteristic of the F-modules of the SIMATIC ET 200SP is the (station) device-wide assignment of F-addresses using the engineering tool instead of the DIP switch setting on each module (F-address).

When a module is replaced, the F-address, stored in the e-coding, remains in the base unit. If a new module is plugged in, it receives the F-address automatically. New assignment of the F-addresses is therefore unnecessary. This innovation simplifies installation and saves time.

The SIMATIC ET 200SP fail-safe power module can be used to switch off safety-related groups of standard or fail-safe DQ modules. Evaluation of the safety function is then carried out either in the F-CPU or in the F-PM-E power module. This fast and direct group switch-off can be carried out up to SIL 2 / PL d or SIL 3 / Pl e.

2.8.5.1. Overview of ET 200SP and ET 200S - I/O Modules

	ET 200S	ET 200SP F
Digital inputs	4/8 F-DI 24VDC	8 F-DI 24VDC HF • 15 mm module width • Power supply per channel
Digital outputs	4 F-DO 24VDC/2A	4 F-DQ PM 24VDC/2A HF • 15 mm module width
Relay module	1 F-RO 24VDC/230VAC/5A	1 F-RQ 24VDC/24..230VAC/6A • 20 mm module width
Power module	PM-E F pm 24VDC PM-E F pp 24VDC	F PM-E ppm 24VDC/10A • 20 mm module width • 2 F-DI DC24V • 1 F-DQ PPM 2A • PP/PM-switching, parameterizable • Direct switching from F-DI to F-DO up to SIL3 • Fast group shutdown of F-DQ up to SIL3

2.8.5.2. ET 200SP / F-DI and F-DO

Digital input module F-DI 8x24VDC HF

- Up to 8 inputs according to SIL 2/PL d or
- Up to 4 inputs according to SIL 3/PL e
- Channel-specific or module-wide passivation
- Onboard diagnostics: short-circuit and discrepancy time monitoring
- "Provide last valid value"
  - The last valid value before the discrepancy error occurred is provided until the discrepancy has disappeared or the discrepancy time has expired and a discrepancy error is detected.

Digital output module F-DQ 4x24VDC/2A PM HF

- 4 outputs, PM-switching according to SIL 3/PL e
- Channel-specific or module-wide passivation
- Onboard diagnostics: wire break

2.8.5.3. ET 200SP / F-PM, F-RO and F-CM AS-i

Digital power module F-PM-E PPM 24VDC/8A

- Certified up to SIL 3 (IEC 61508), PL e (ISO 13849-1)
- Safety-related shutdown of output modules within the potential group of the F-PM-E

Communication module F-CM AS-i Safety ST

- Certified up to SIL 3 (IEC 61508), PL e (ISO 13849-1)
- Fail-safe communication module for AS-Interface

Digital relay module F-RQ 1x24VDC/24..230VAC/5A ST

- Certified up to SIL 3 (IEC 61508), PL e (ISO 13849-1)
- Electronic module with one relay output

2.8.6. Available Licenses

Available licenses (Industry Mall)

Product Name	Article No.
STEP 7 Safety Advanced V15 *Software Download*	6ES7833-1FA15-0YA5 *6ES7833-1FA14-0YH5*
STEP 7 Safety Advanced V1x -> V15 Upgrade *Software Download*	6ES7833-1FA15-0YE5 *6ES7833-1FA14-0YK5*
Upgrade S7 Distributed Safety V5.4 SP5 -> V15 *Software Download*	6ES7833-1FA15-0YF5 *6ES7833-1FA14-0YY5*
SUS STEP 7 Safety Advanced *Software Download*	6ES7833-1FC00-0YX2 *6ES7833-1FC00-0YY0*
SUS STEP 7 Safety Advanced compact **	6ES7833-1FC00-0YM2

**SUS compact means that regardless of the number of ordered packages, only one data carrier, a USB stick will be delivered.

Contents

3

3. Operating Principle of Safety Integrated

At the end of the chapter the participant will ...

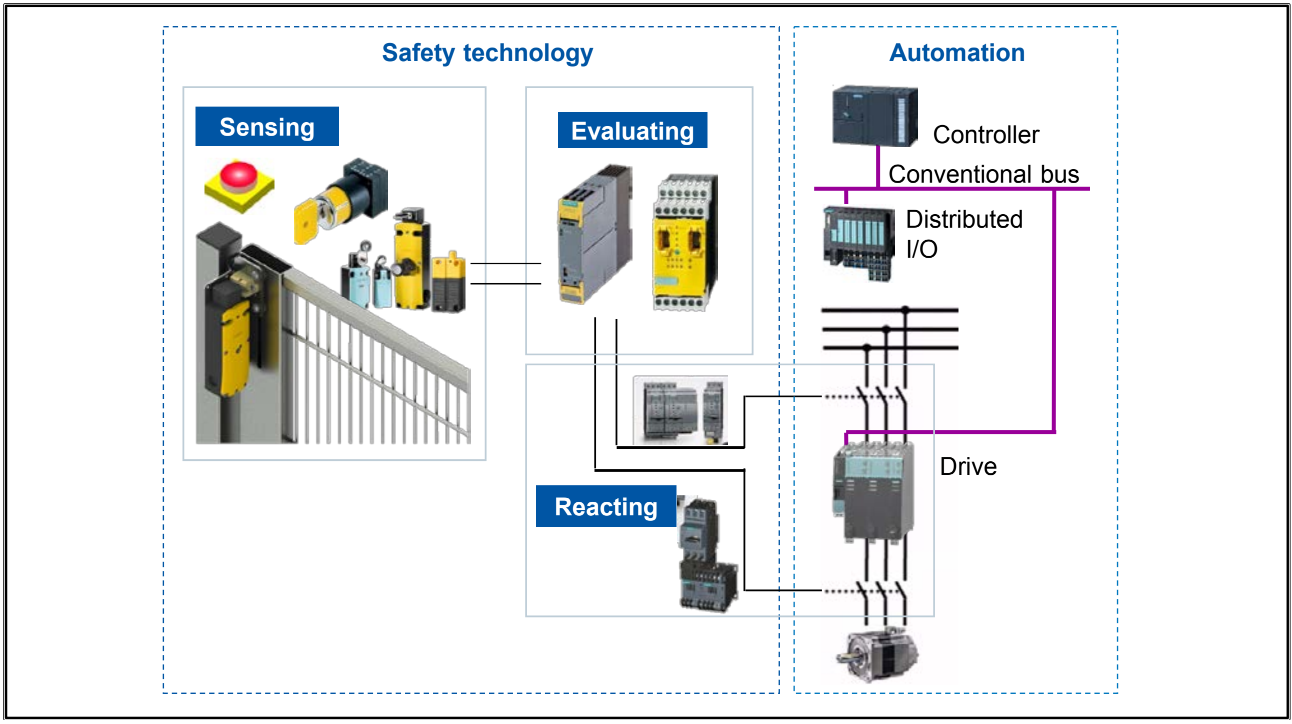
… be able to explain the operating principle of Safety Integrated

… be familiar with the required hardware and software expansions

... be able to explain the principle of PROFIsafe communication

... be able to explain the principle of "Diversified Logic"

3.1. Conventional Safety Technology



Conventional Safety Technology

Standard and safety functions are implemented with separate controllers and bus systems. Safety functions can be implemented with safety relays or with a fail-safe controller.

Functional Controlling

The dangerous machine function is switched via the two positively driven contactors (K1 and K2), which are controlled by a safety relay. The safety relay receives the necessary control signals for functional On/Off switching via wiring from a digital standard output of the standard PLC, which also evaluates the corresponding signals from the plant (including signals of the HMI device) in the standard program.

Protection Functions

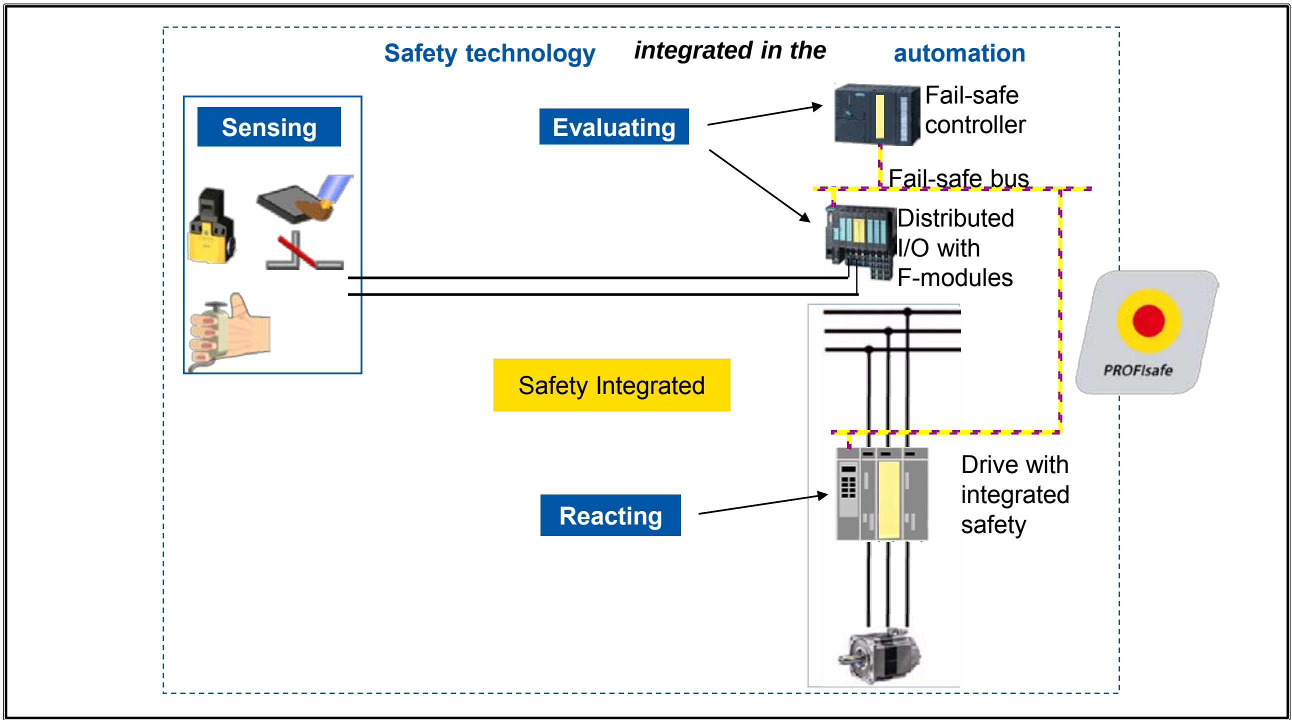
For the protection of the operator, the dangerous machine function is equipped with an Emergency Stop pushbutton and an isolating protection device in the form of a safety door. As soon as a wiring error is detected, the Emergency Stop is pressed or the safety door is opened, the safety relay switches off the motor via contactors K1 and K2 according to Stop Category 0 of EN 60204-1 – independent of the control signals of the standard PLC.

Each time the contactors are energized, the safety relay first checks to determine whether the contacts of the Emergency Stop and the safety door are closed and whether the contactors are released and their feedback contacts are closed.

Wiring

The wiring and architecture of the protection functions are implemented according to EN 61508 in SIL 3 or according to EN 954 in Cat.4: The Emergency Stop pushbutton and the position switches of the safety door are wired via two channels to the safety relay. For control of the dangerous machine function, two contactors connected in series are used. Their feedback and mirror contacts return a feedback signal to the safety relay.

3.2. Integrated Safety Technology



Safety Integrated

A PLC with a fail-safe CPU (F-CPU) and distributed I/O stations (ET 200S via PROFIBUS DP) controls both the standard functions and the safety functions.

Functional Controlling

The dangerous machine function is switched via the two positively driven contactors (K1 and K2), which are now controlled by the safety program of the F-CPU in conjunction with safety-related input and output modules instead of by the safety relay. The conditions for functional On/Off switching are still evaluated by the standard program, which uses tags (e.g. DB) to communicate to the safety program when the contactors are switched on and off.

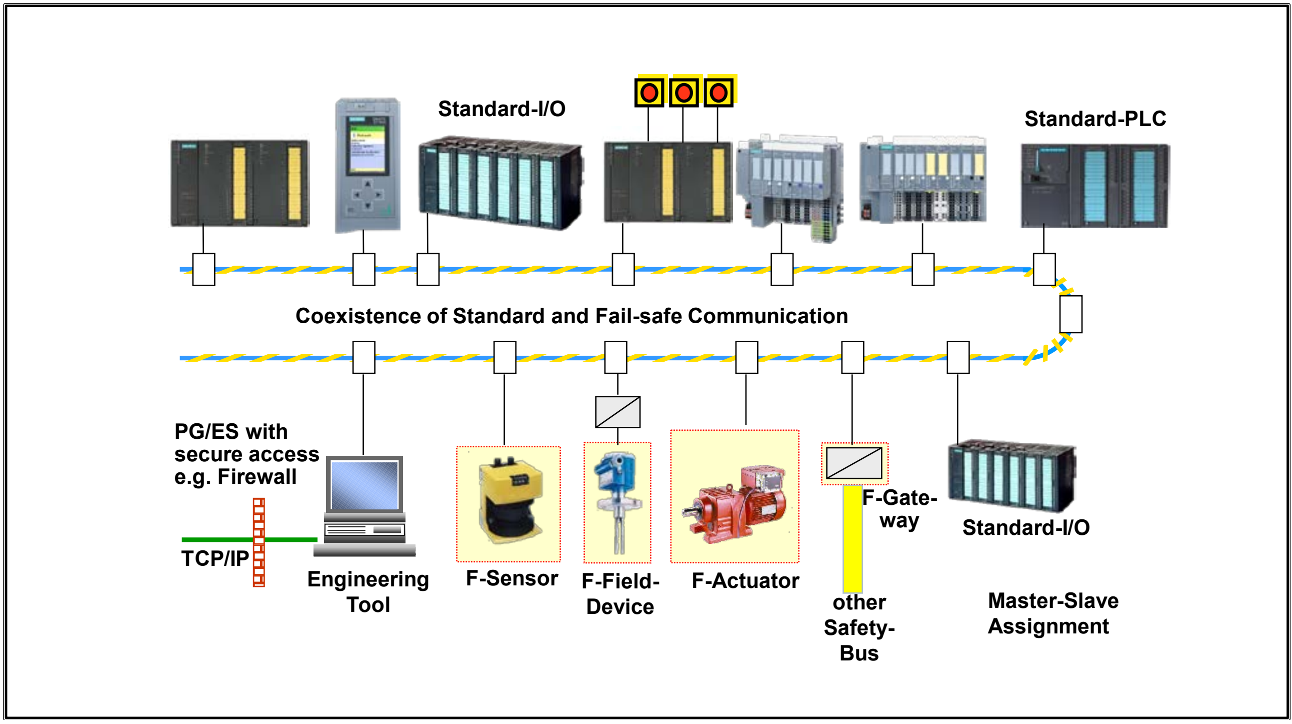
Protection Functions

The protection functions previously described are now no longer controlled by the safety relay, but rather by the safety program of the F-CPU and the safety-related input and output modules (F-DI/DO): As soon as a wiring error is detected, the Emergency Stop pushbutton is pressed or the safety door is opened, the safety program must switch off the motor or contactors K1 and K2 according to Stop Category 0 of EN 60204-1 – independent of the control signals of the standard program. The monitoring of the wiring of the safety-related actuators and sensors is now performed by the F-DI / DO modules.

Wiring

The wiring and architecture of the protection functions according to SIL 3 (EN 62061) Cat.4 (EN 954) is in principle the same: The Emergency Stop command device and the position switches of the safety door are still wired via two channels, however, no longer to a safety relay but to an F-DI module of the safety-related ET 200S station. Two contactors connected in series are still used to switch the dangerous machine function. They are now controlled by an F-DO module and their feedback and mirror contacts are now evaluated by the safety program.

3.3. Safety Integrated Concept



Safety Integrated

Safety Integrated is the completely integrated safety concept for automation and drives by Siemens. Proven technologies and systems from automation engineering are used for the safety technology. Safety Integrated covers the entire chain of safety from sensors and actuators to the controller, including safety-related communication over standard fieldbuses. In addition to their functional tasks, drives and controllers also take on safety tasks. A particular feature of Safety Integrated is that it ensures not only reliable safety, but also a high level of flexibility and productivity.

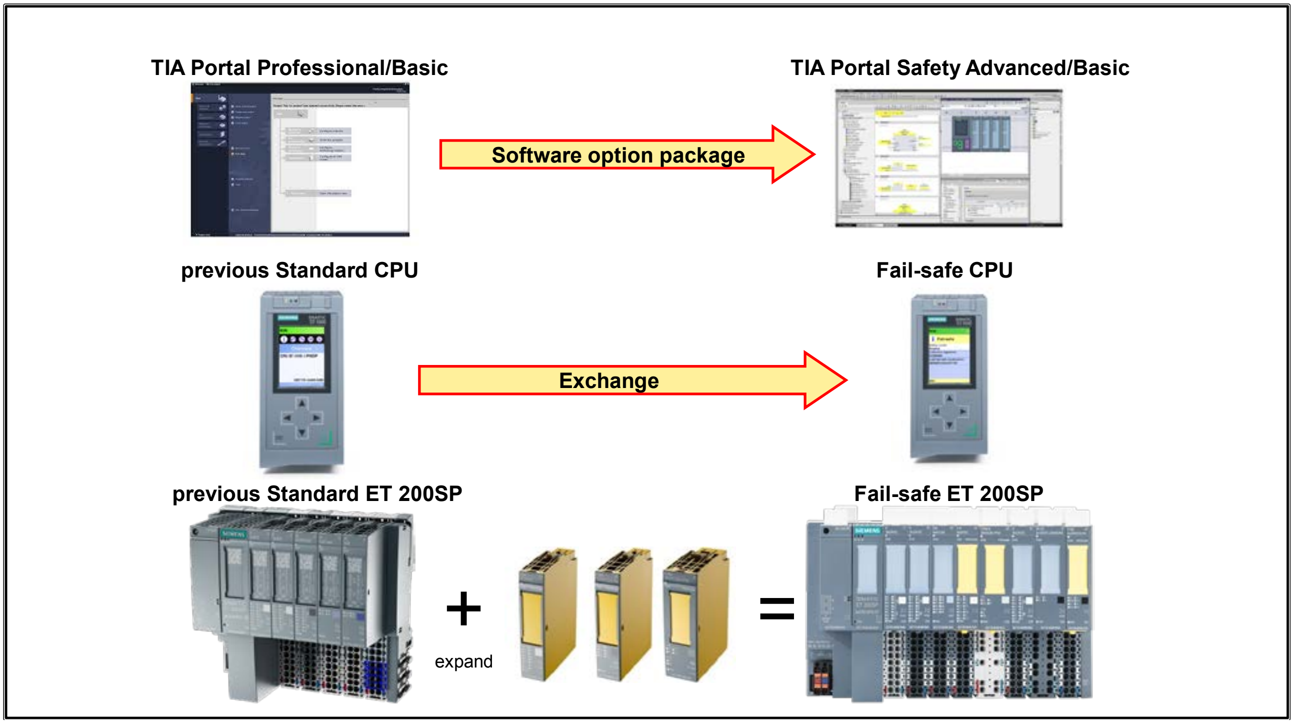
Standard and safety-related devices are connected by a common bus system. The bus can be PROFIBUS, PROFINET or a combination of both, because fail-safe communication is also possible beyond bus boundaries.

Advantages

Integration of safety technology into standard automation systems has the following important advantages:

- Greater flexibility than electromechanical solutions
- Reduction of the wiring effort
- Only one CPU is required due to the coexistence of the standard program and safety program
- Simple communication between the standard program and safety program
- Less engineering effort because configuration and programming is carried out with standard engineering tools

3.4. Required Expansions



F-CPU

In general, it is adequate if the F-CPU used meets at least the same requirements as the previously used standard CPU in terms of performance data and configuration limits (including communication options). The most important parameters are the CPU processing speed, which yields the cycle time and thus the response time of the automation system, and the amount of work memory, which must accommodate the execution-relevant sections of the standard program and safety program.

F-DI/DO

Standard and safety-related input and output modules (F-DI/DO) can also be used in mixed operation. The F-DI/DO modules required instead of the safety relay could also be integrated in an existing ET 200SP device. All I/O modules already in use including their wiring can continue to be used unchanged.

The first BaseUnit must be a light-colored BaseUnit. Light-colored BaseUnit: Establishes a new potential group, electrical isolation from the adjacent module on the left. The first BaseUnit of the ET 200SP is always a light-colored BaseUnit for infeed of the supply voltage L+. During commissioning, ensure that you only use digital signal modules and the power module with the BaseUnit Type A0.

PROFIsafe Communication

The safety-related communication between the F-CPU and the F-DI/DO modules using PROFIsafe is integrated in the fail-safe modules. This is handled automatically and does not need to be programmed regardless of whether F-DI/DO modules are used centrally or as distributed modules via PROFIBUS or PROFINET. Standard communication that has already been configured remains unaffected by the safety-related communication via PROFIsafe.

3.5. What goes with which Software?

TIA Professional + Safety Advanced

+ All fail-safe SIMATIC Controller classes (released in the TIA Portal)
+ Edit/load F-Hardware
+ Edit/load standard program
+ Edit/load safety program
+ Prepare safety printout

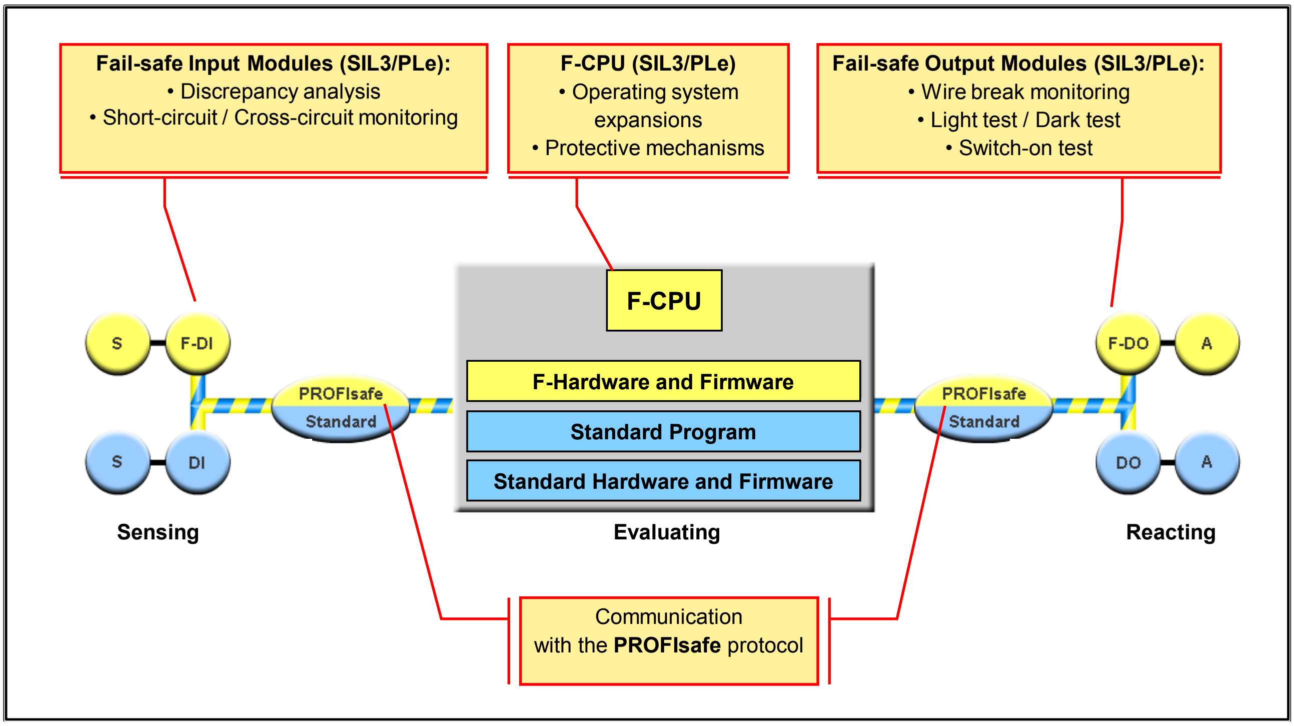
Professional/Basic + Safety Basic

-- Only fail-safe S7-1200
+ Edit/load F-Hardware (S7-1200)
+ Edit/load standard program
+ Edit/load safety program (S7-1200)
+ Prepare safety printout (S7-1200)

TIA Professional/Basic (without Safety)

-- Fail-safe CPU can only be used in standard operation
-- F-Hardware cannot be edited/loaded
+ Edit/load standard program
-- Safety program only has a read-only access
-- Safety printout cannot be prepared

3.6. Hardware and Firmware Expansions



Standard Program

When safety-related functions are integrated in a SIMATIC controller, the standard control functions and their implementation can continue to be used practically unchanged:

- Standard I/O modules and their wiring
- Standard program

F-I/O

The major difference between fail-safe modules and standard modules is that fail-safe modules are designed with two channels internally. Both integrated processors monitor each other and automatically test the input and output circuits. In the event of a fault, they put the F-module into a safe state.

Fail-safe digital input modules acquire (sensing) the signal states of safety-related sensors (e.g. Emergency Stop pushbutton), run short-circuit and cross-circuit tests as well as discrepancy analyses and send corresponding safety message frames to the F-CPU.

Fail-safe digital output modules are suitable for switch-off operations with short-circuit monitoring up to the actuator.

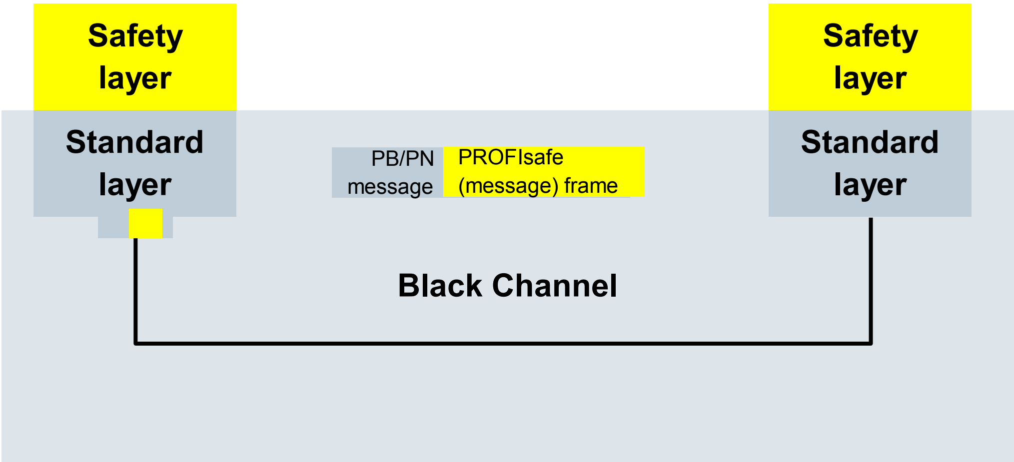
The F-I/O modules communicate with the fail-safe CPU using the PROFIsafe profile.

F-CPU

The standard CPU is simply replaced with a safety-related F-CPU. It combines the functionality of a standard CPU with that of a safety CPU. With a single operating system expanded to include protective mechanisms, standard and safety-related user programs can be executed on one CPU.

3.7. PROFIsafe

3.7.1. Black Channel



- **PROFIsafe is an additional safety layer**
- **PROFIsafe data is transmitted in the user data of the standard communication**
- **Everything underneath the safety layer is considered a "Black Channel"**

PROFIsafe Layer

PROFIsafe is the first open standard (IEC 61784) for safety-related communication that allows standard and safety-related communication via one and the same connection (cable or wireless via WLAN).

With PROFIsafe, the existing network infrastructure for standard communication can also be used at the same time for safety-related communication.

Safety-related data and standard data are transmitted over the same bus with PROFIsafe. The existing standard bus protocols (so-called "Black Channel") are used in which the safety-related data is transported as additional data (PROFIsafe Layer). This means that safety-related communication is independent of the bus system and the lower-level network components.

3.7.2. PROFIsafe Layer

PROFIsafe Layer

Input data / Output data (user data)			Status / Control byte	CRC (cyclic redundancy check)		
1..12 byte(s)	or	13..123 bytes	1 byte	3 bytes	or	4 bytes

- Communication from Controller to Device: Control Byte
- Communication from Device to Controller: Status Byte
- Input data and output data can be expanded to 123 bytes
- 3 or 4 bytes CRC (depending on the amount of data to be transmitted)

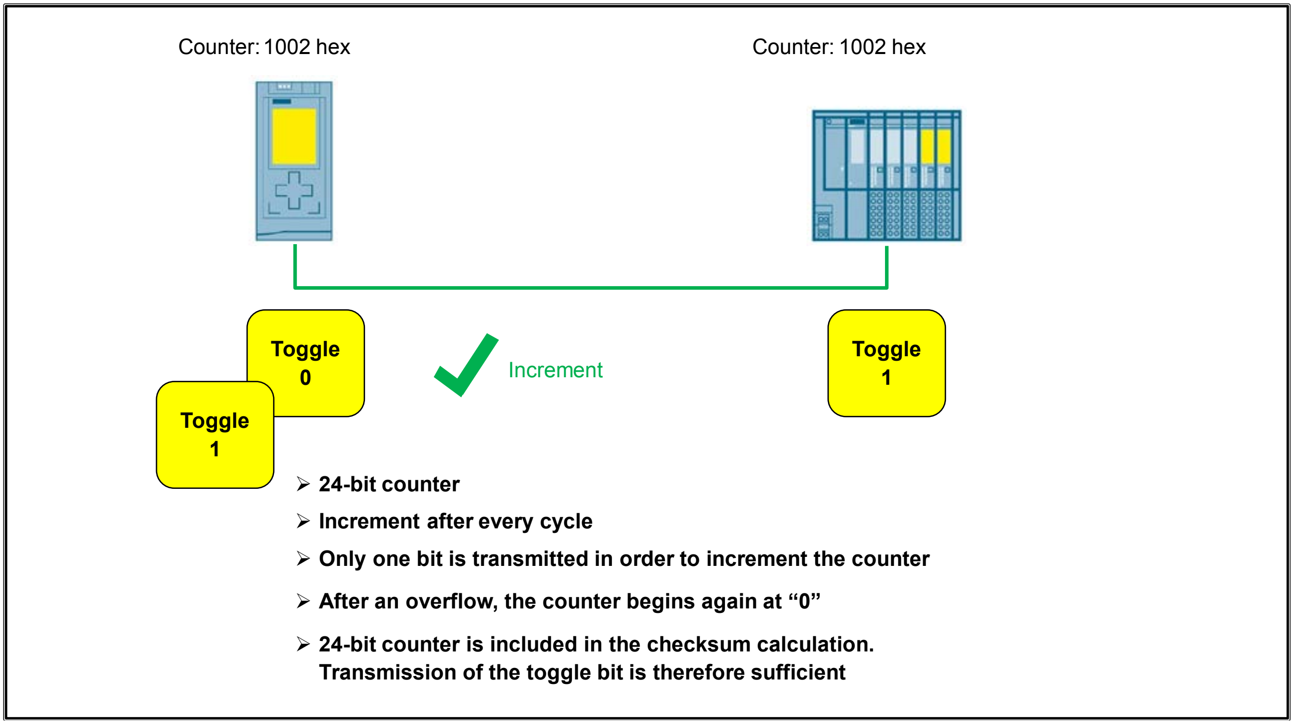
A PROFIsafe message (F-message) that is exchanged between F-Host and its F-Device is carried within the payload of a standard PROFIBUS or PROFINET message. In case of a modular F-Device with several F-Modules, the payload consists of several PROFIsafe messages.

It begins with the F-input / output data taking into account the mentioned data type subset. The data structure of a particular F-Device is defined in the associated GSD file (General Station Description). Production automation and process automation pose different requirements on an F-System. The first works with short signals ("bits") which have to be processed very quickly. The second works with longer process values ("floating point") which may be somewhat slower.

PROFIsafe therefore offers two different lengths for data structures. One is limited to 12 bytes with a CRC signature of 3 bytes. The other is limited to 123 bytes with a 4 byte CRC signature.

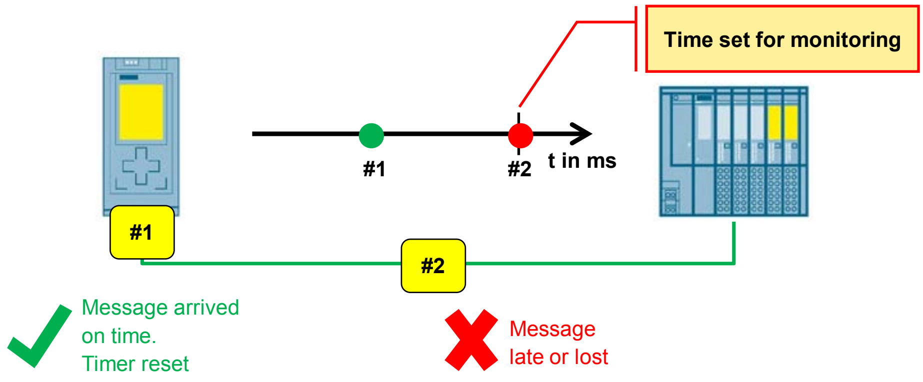
For a PROFIsafe message (F-message) from an F-Host, a control byte follows the F-input / output data, otherwise a status byte. Both serve the synchronization of the PROFIsafe protocol machines. A PROFIsafe message (F-message) ends with a CRC signature which depends on the length of the F-input / output data. The consecutive number is not transmitted with the F-message. Sender and Receiver each have their own counters which are synchronized with the help of the control byte and the status byte. The correct synchronization is monitored through inclusion of the counter value in the CRC signature calculation. The "F-address", as well, is safeguarded through inclusion in the CRC signature calculation.

3.7.3. Consecutive Numbering (Counter)



Using the Consecutive Number, a Receiver can see whether or not it received the messages completely and within the correct sequence. With the acknowledgement, the consecutive number gets back to the Sender for verification. A simple "Toggle Bit" would have been sufficient here. However, due to the storage buffers in some bus components, such as, switches, a 24-bit counter was selected for PROFIsafe.

3.7.4. Monitoring Time (Watchdog Timer)

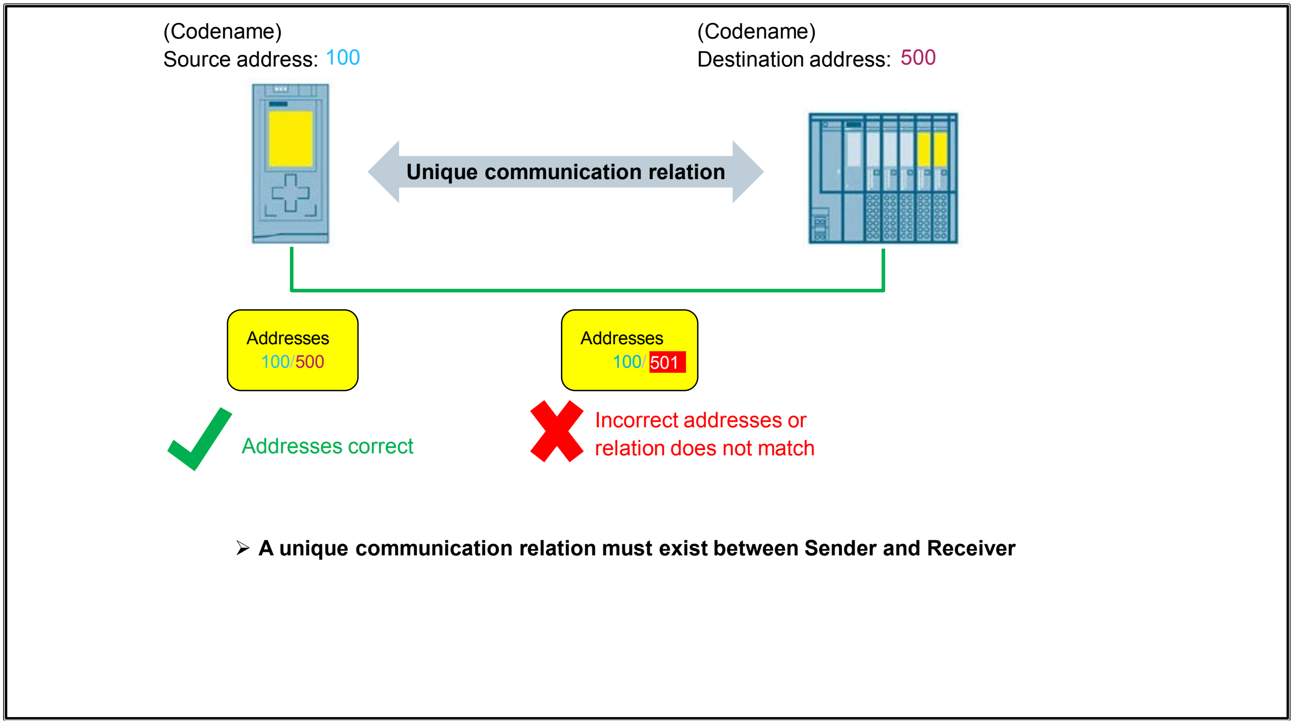


- **The Watchdog is a monitoring function (timer) which trips the safety functions when a data packet does not arrive on time or is lost.**

In F-technology, it is not just a matter of transmitting correct process signals and process values, but also of their update within a process error tolerance time.

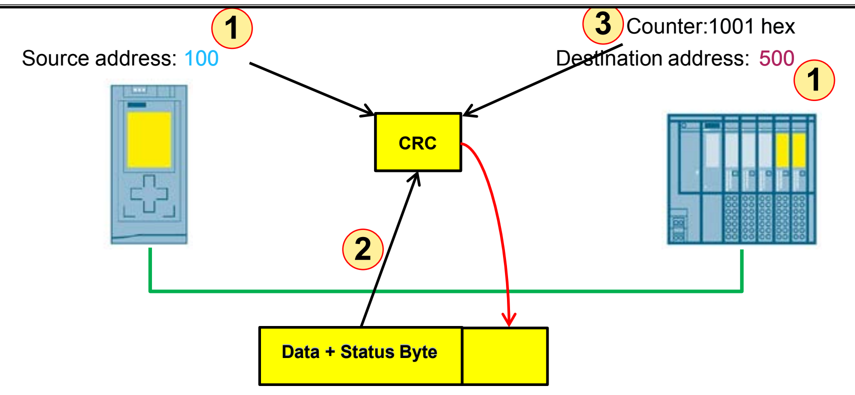
This means that an F-Device can independently trigger the predefined safety measures when the time is exceeded, for example, stopping a movement. For this, the F-Device uses a Watchdog Timer that is restarted when an F-message with a new consecutive number arrives.

3.7.5. Relationship F-Source Address/F-Destination Address



The 1:1 communication relationship between controller and field device simplifies the detection of misdirected F-messages. Sender and Receiver must have identification (codename) that is unique in the network, and can be used for verifying the authenticity of a PROFIsafe message. PROFIsafe uses an "F-Address" as the Sender/Receiver codename.

3.7.6. Formation of the CRC (Cyclic Redundancy Check)

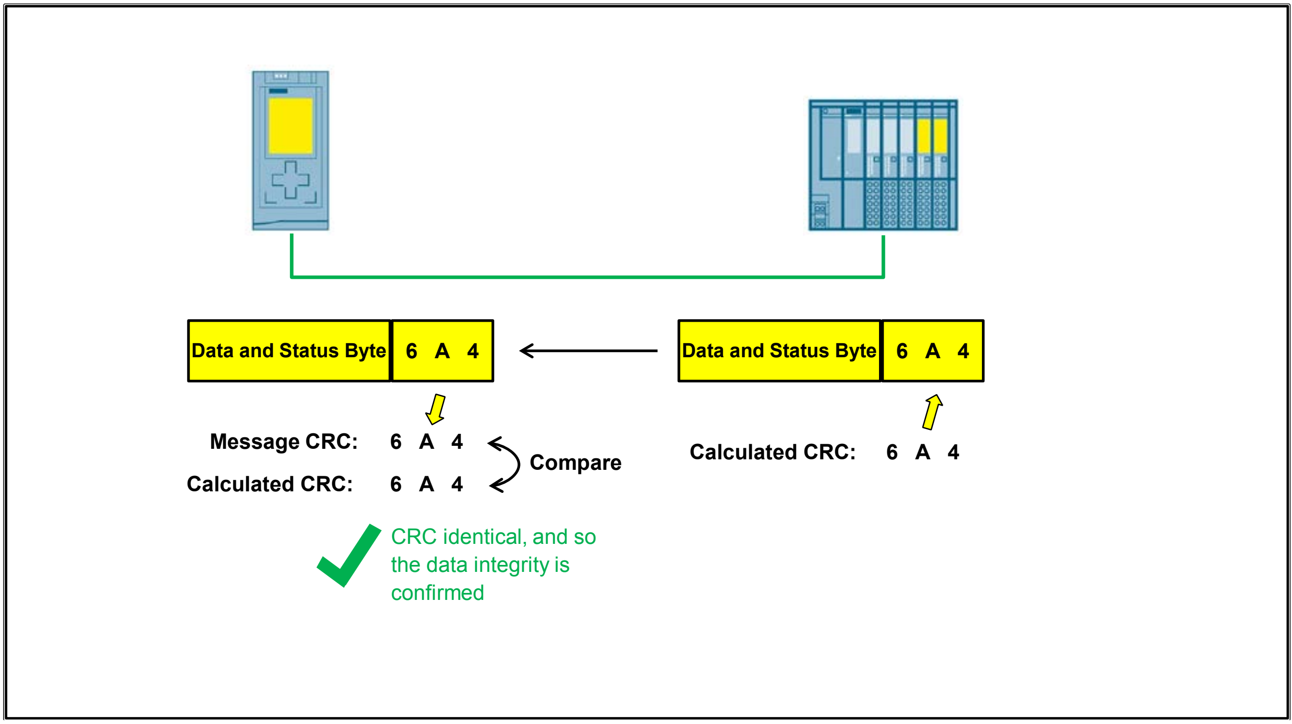


In order to ensure the data integrity, a checksum (CRC) is used. For this, the following information must be read-in :

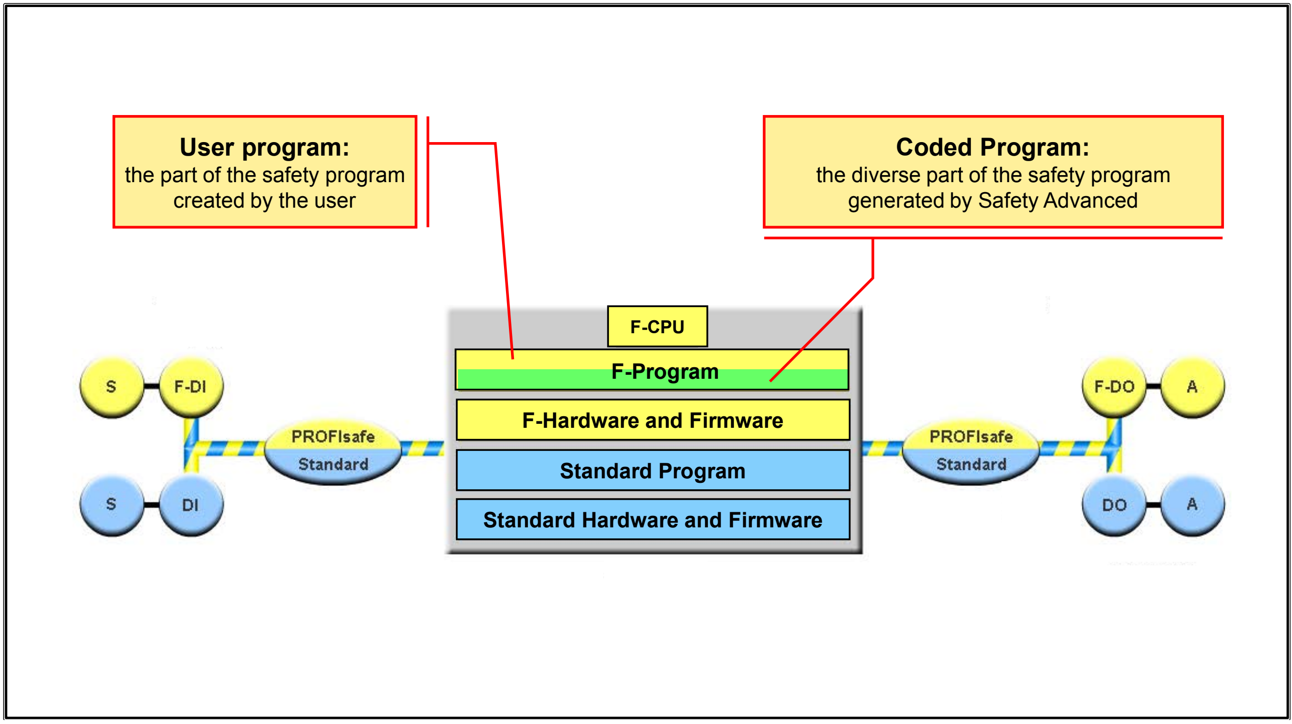
- **Source and destination address (Codename)** 1
- **The data to be transmitted and the status byte** 2
- **Counter** 3

The CRC is calculated from this information and attached to the data packet to be transmitted

3.7.7. Checking the CRC



3.8. Safety program



F-Program

The safety program (F-program) for controlling the safety-related functions of the system is made up of a section created in FBD or LAD by the user and a section generated by Safety Advanced that contains, among other things, the diversified logic for the user section.

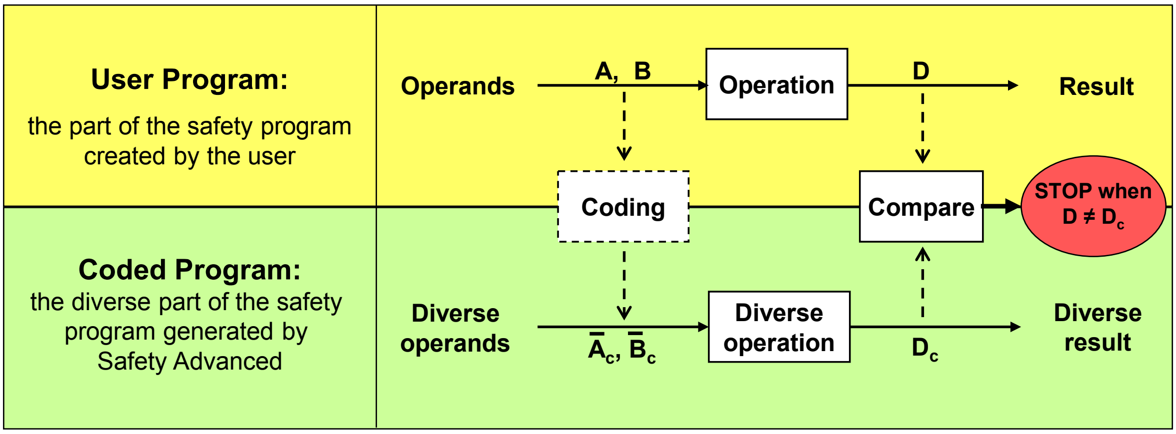
The standard program and safety program are created in the same programming environment. TÜV-certified function blocks for all common safety functions further simplify programming

Co-existence of Standard Program and F-Program

The standard program and safety program are executed independently of each other by the CPU. Due to the integration of the two programs on one CPU, the communication between the two programs can be implemented using global tags.

Changes to the standard program have no effect on the safety program so that its integrity remains intact.

3.8.1. Diversity



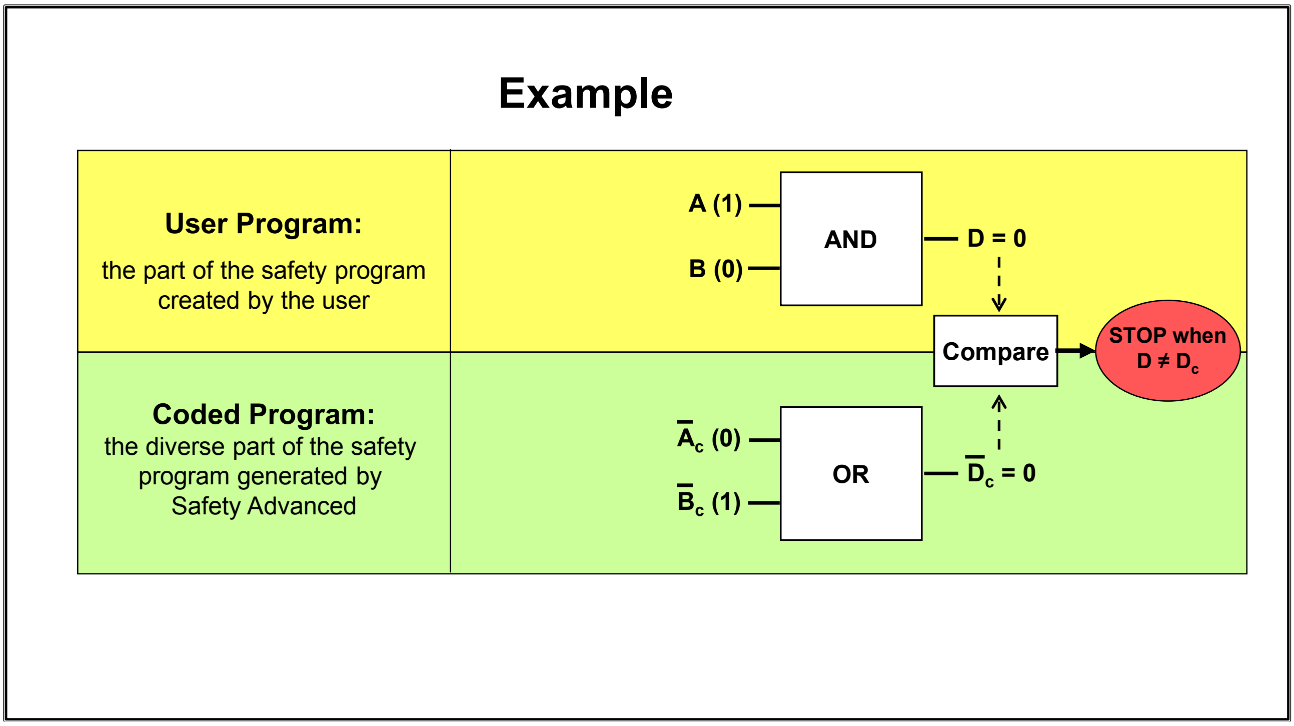
Diversification and Time-based Redundancy

The safety-related SIMATIC S7 CPUs operate according to the principles of time-based redundancy and diversification, which enable implementation of F-systems with only one CPU and one processor. For the user-programmable safety program, the "Safety Advanced" programming tool generates additional F-blocks (F-FC/-FB). These are based on "diversified" logic relative to the user program that uses "diversified" operands and operations.

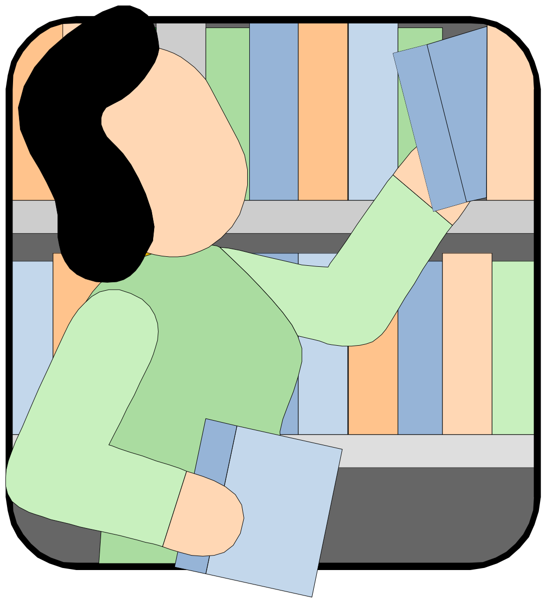
The two parts of the safety program are executed in succession with time-based redundancy, and the results are compared. If an error occurs, the F-CPU reacts and puts the system into safe state.

Safety Advanced also generates F-system blocks that can be used, for example, to handle safety-related PROFIsafe communication with the F-I/O.

3.8.2. Diversity Example



3.9. Additional Information



3.9.1. Error Types

Error Type	Description
Repetition	A packet arrives twice
Deletion	A packet does not arrive at all
Insertion	A wrong packet arrives
Wrong Sequence	The packets arrive in a wrong order
Data Corruption	The data of a packet is corrupted
Delay	A packet arrives outside the allowed timeframe
Masquerade	A standard packet mimics a safety packet
Addressing (error)	No definite communication relation
Revolving memory failures within Switches	First in first out error

Repetition

Old messages that have not been updated are sent again at the wrong point in time.

Deletion

A message is not received or not recognized.

Insertion

A message is inserted that refers to an unexpected or unknown source.

Wrong Sequence

The defined sequence (e.g. consecutive number, time references) of the messages of a particular source is faulty.

Data Corruption

Messages can be corrupted due to faults in a bus node (device), faults in the transmission medium or due to mutual interference of messages.

Delay

Messages can be delayed beyond the permissible window for arrival, e.g. as a result of faults in the transmission medium, overloaded connection cables, mutual interference or bus nodes (devices) that send messages in a manner such that services are delayed or not recognized (e.g. FIFOs in switches, bridges and routers).

Masquerade

A message that comes from an apparently valid source is additionally inserted. Thus a non-safety-related message can be received by a safety-related device, which then classifies it as safety-relevant.

Addressing (Error)

The relationship between Sender and Receiver is not unique.

Revolving Memory Failures within Switches

FIFO - First-In-First-Out - error; the correct data sequence is not adhered to.

3.9.2. Remedies

Remedy / Error Type	(Virtual) Consec. Numbering	Watchdog	CRC (Data)	Codename (Source/Target Address)
Repetition	✓			
Deletion	✓	✓		
Insertion	✓	✓		✓
Wrong Sequence	✓			
Data Corruption			✓	
Delay		✓		
Masquerade		✓	✓	✓
Addressing (error)				✓
Revolving Memory Failures in Switches	✓			

Contents 4

4. Training Device and HW Configuration

At the end of the chapter the participant will ...

... be able to configure fail-safe S7-1500 and ET 200SP Stations

... be able to set the general F-parameters of an F-CPU and an F-module

… be able to assign the F-destination address

4.1. Simulator Setup with S7-1500F and ET 200SP

Case Version 1

Case Version 2

Simulator with S7-1500F

The simulator contains the following components:

- S7-1500 automation system with an S7-1500F CPU
- Digital input module DI 16x24 VDC HF

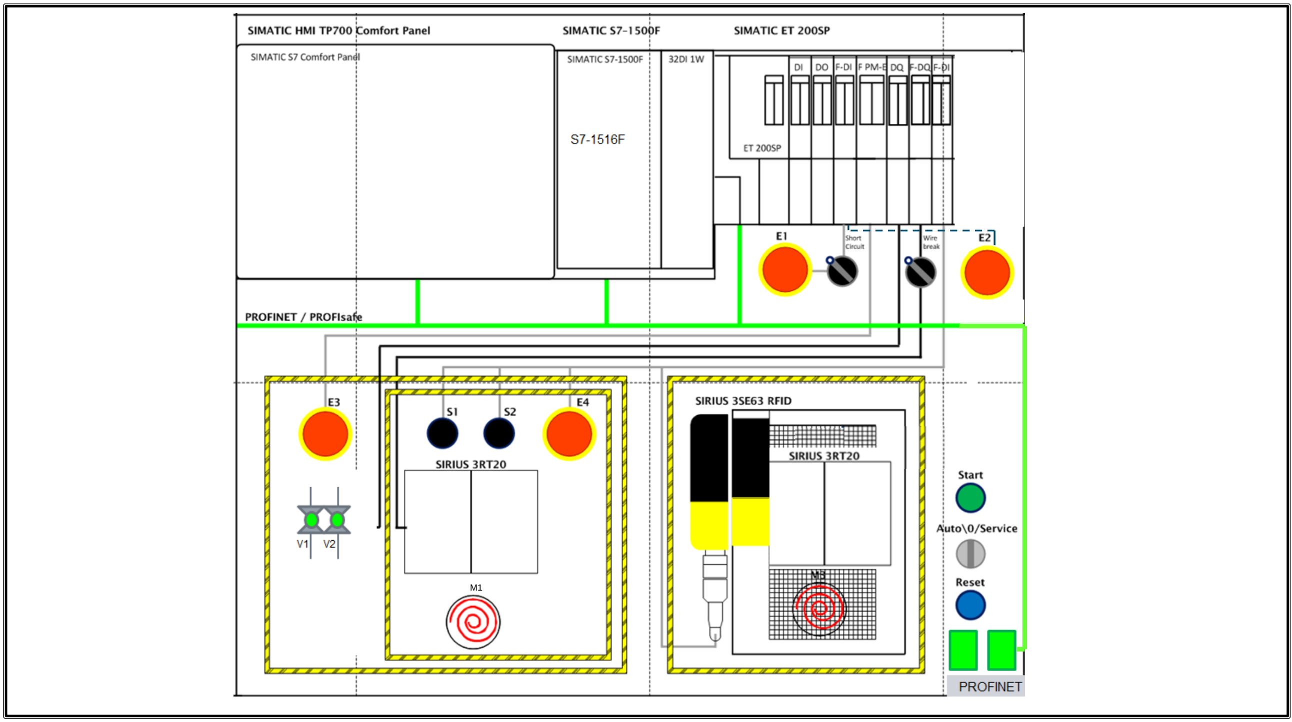
or

- S7-1500 automation system with an S7-1500F CPU
- Digital input module DI 32x24VDC HF
- Digital output module DQ 32x24VDC/0.5A ST
- Analog input module AI 8xUI/RTD/TC ST

ET 200SP

- ET 200SP distributed I/O system with PROFINET interface
- Digital input module F-DI 8x24VDC, 8 inputs according to SIL 2/PL d or 4 inputs according to SIL 3/PL e
- Fail-safe power module F PM-E ppm DC24V/8A
- Digital output module F-DQ 4x24VDC/2A PM HF, 4 outputs, PM-switching according to SIL 3/PL e
- Digital input module F-DI 8x24VDC, 8 inputs according to SIL 2/PL d or 4 inputs according to SIL 3/PL e

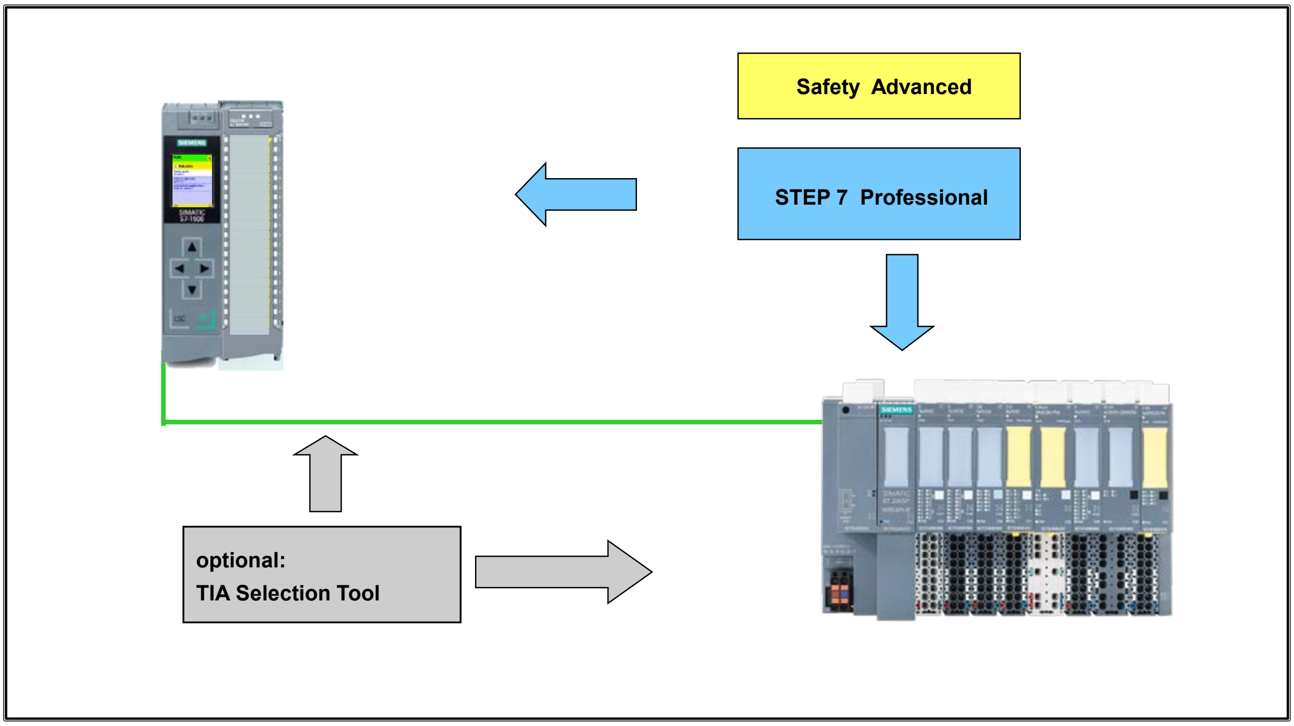
4.1.1. System View of the Training Area



Configuring an S7-1500F

You configure a SIMATIC Safety F-system just as you would a standard S7-1500 automation system. You configure and parameterize the hardware in the Hardware and Network editor as a central and/or as a distributed design (ET 200SP). The fail-safe components are selected, just as in the standard, in the "Hardware catalog" Task Card and you place them in the working area of the Network view or Device view. F-components are represented in yellow.

4.2. Device Configuration of the Simulator's Safety Controller



Hardware Configuration

The F-modules are configured and parameterized with the "STEP 7 Professional" Standard Tool; the safety program is created with the "Safety Advanced" option package.

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation. You can start it directly in the Siemens Industry Mall or you can download it as a file. The TIA Selection Tool provides you with Wizards for selecting the desired devices and networks. Also, there are configurators for selecting modules and accessories as well as for checking the correct functionality.

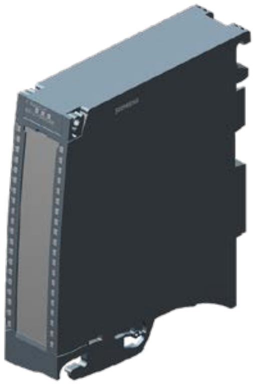
From your product selection or product configuration, the TIA Selection Tool generates a complete order list. You can export this directly to the shopping cart of the Industry Mall or the CA 01.

With the TIA Selection Tool, you can select and configure the SIMATIC S7, SIMATIC ET 200, SIMATIC HMI Panels, SIMATIC IPC, SIMATIC HMI Software and Industrial Communication components. Beyond that, you can create PROFIBUS and PROFINET networks, configure their topology as well as select their associated cables and connectors.

4.3. Configuring an S7-1500F

F-CPU
CPU 1513F-1PN

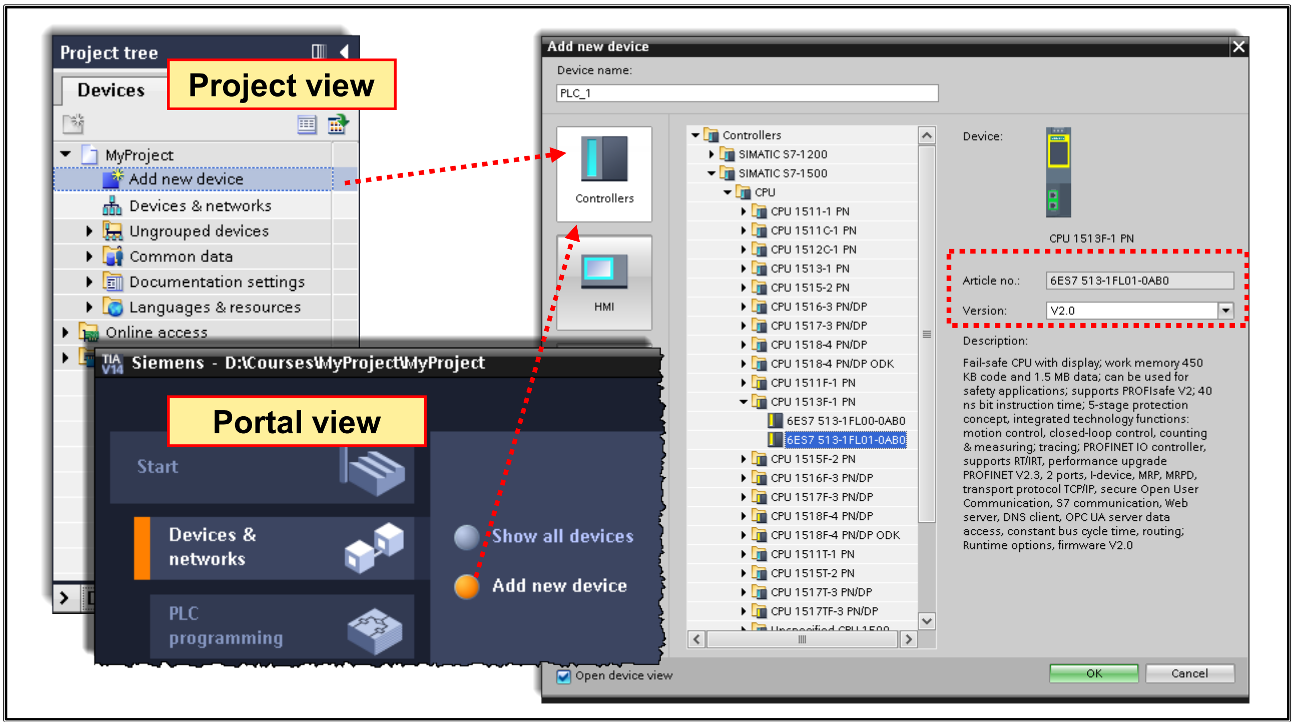
Standard DI
DI 16xDC24V



Configuring an S7-1500F

You configure a SIMATIC Safety F-system just as you would a standard S7-1500 automation system. You configure and parameterize the hardware in the Hardware and Network editor as a central and/or as a distributed design (ET 200SP). The fail-safe components are selected, just as in the standard, in the "Hardware catalog" Task Card and you place them in the working area of the Network view or Device view. F-components are represented in yellow.

4.3.1. F-CPU in TIA Portal



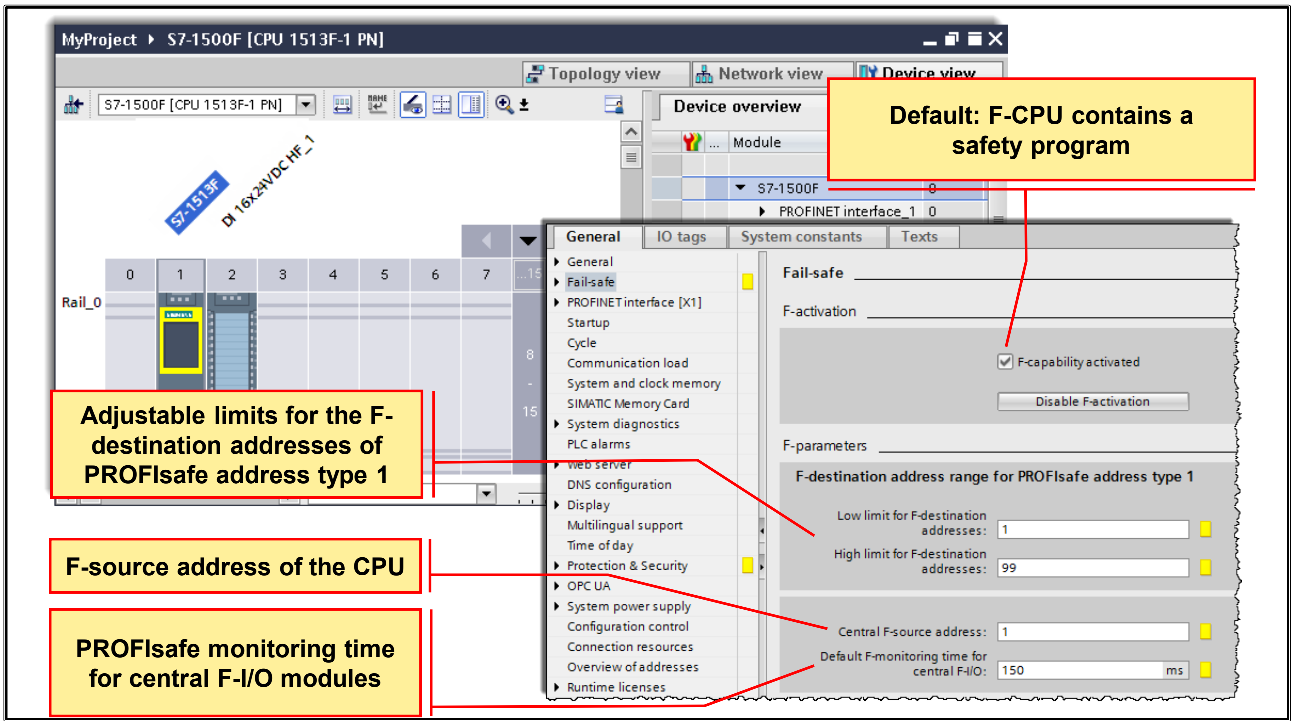
Add New Device

It is possible to create a new device in the project using the Hardware and Network editor with the help of the “Hardware catalog” task card or through the Project tree “Add new device”.

When a new device is created, a suitable rack is also created automatically. The selected device is inserted into the first permitted slot in the rack.

Regardless of the method selected, the added device is visible in the Device view and in the Network view of the Hardware and Network editor.

4.3.2. Fail-safe Capability and PROFIsafe Monitoring Time



F-activation

The F-capability of the CPU must be activated, to download a safety program cannot later to the CPU! This option is thus required for operation of the CPU in safety mode. The activation of F-capability of the CPU is a default setting. If the F-capability activation is deactivated, only a standard program and not a safety program can be downloaded to the CPU.

Default F-Monitoring Time for Central I/O

The default F-monitoring time for the central F-I/O acts on F-I/O adjacent to the F-CPU. You set this parameter in the properties of the F-CPU (select F-CPU, then "Properties > Fail-safe > F-parameters").

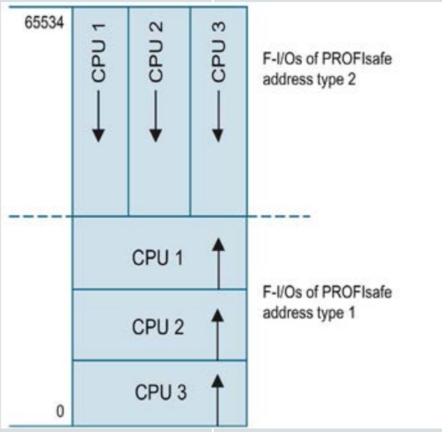
The F-monitoring time is the PROFIsafe monitoring time (Watchdog) for the safety-related communication between the F-CPU and the F-signal modules in the central rack. If the F-I/O does not receive a valid safety message frame from the F-CPU within the assignable monitoring time, the F-signal module passivates itself with a "communication error".

The F-monitoring time can be assigned manually or on a module-specific basis or it can be assigned centrally for all F-I/O modules in the F-parameters of the CPU.

4.3.3. PROFIsafe Address Types

PROFIsafe Address type 1	PROFIsafe Address type 2
For ET 200S, ET 200eco, ET 200pro, ET 200iSP F-modules and S7-300 F-SMs the following applies:	For ET 200SP, ET 200MP F-modules and S7-1500 F-SMs the following applies:

- You have to set the F-destination address on the F-I/O using the DIP switch before you mount the F-I/O. You can assign a maximum of 1022 different F-destination addresses.
- The F-destination addresses of all F-I/Os must be unique within the entire configuration (i.e. CPU wide and network wide) (if necessary, taking into account the destination addresses of the F-I/Os with PROFIsafe address type 2).
- The F-source address has no influence on the uniqueness of the PROFIsafe address.



- Uniqueness of the PROFIsafe address is ensured through the combination of F-source address and F-destination address.
- The F-destination addresses of all F-I/Os only have to be unique CPU-wide.
- The F-source addresses of the F-CPUs only have to be unique network-wide (within the entire network structure)

Defining the F-Destination Address Range for F-I/O of PROFIsafe Address Type 1

With the parameters "Low limit for F-destination addresses" and "High limit for F-destination addresses" you define a range for this F-CPU in which the F-destination address of newly inserted F-I/O of PROFIsafe address type 1 is automatically assigned. An F-destination address, that does not already lie in the F-destination address range, is also newly assigned when you assign a DP-Slave/IO-Device to the F-CPU or when you switch on the F-activation of the F-CPU. The F-destination address is assigned from the "Low limit for F-destination addresses" in ascending order. When no free F-destination address is available in the F- destination address range, the next free F-destination address outside the F- destination address range is assigned and a warning is sent during compilation. The maximum possible F-destination address for ET 200S, ET 200eco, ET 200pro, ET 200iSP F-modules and S7-300 F-SMs is 1022. The F-destination addresses for F-I/O of PROFIsafe address type 1 must be unique network-wide and CPU-wide. Through the selection of different F- destination address ranges for different F-CPUs, you can define different ranges for the automatic assignment of the F-destination address. This makes sense when several F-CPUs are operated on one network. Later, manual address changes are possible.

Example:

You have parameterized the range of the F-destination addresses as follows:

- Low limit for F-destination addresses = 100
- High limit for F-destination addresses = 199

When the first F-I/O of PROFIsafe address type 1 is inserted, the F-destination address 100 is assigned. When a further F-I/O of PROFIsafe address type 1 is inserted, the F-destination address 101 is assigned.

Defining the F-Destination Address Range for F-I/O of PROFIsafe Address Type 2

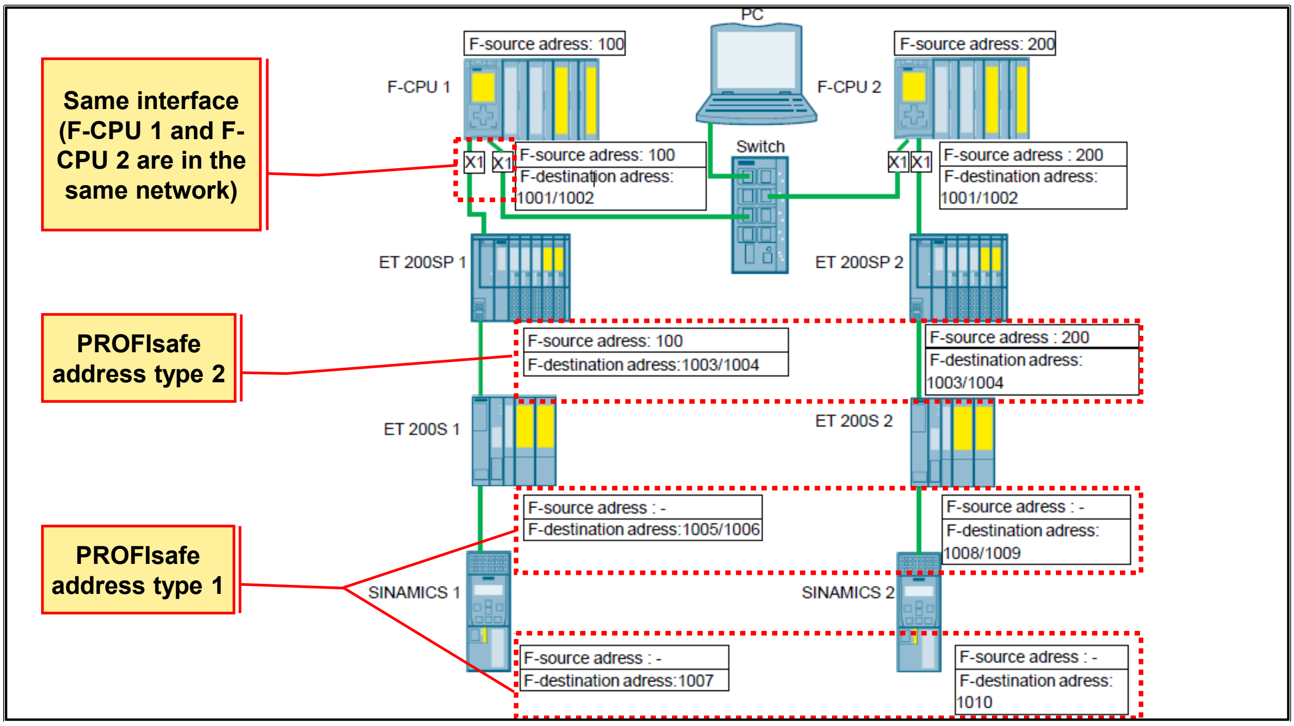
The F-destination address for F-I/O of PROFIsafe address type 2 is automatically assigned from 65534 in descending order for each F-CPU. The low limit represents the Value + 1 parameterized with the parameter "High limit for F-destination addresses" (for F-I/O of PROFIsafe address type 1).

When the value parameterized with the parameter "High limit for F-destination addresses" is reached, a warning is output during compilation.

Defining the F-Source Address for F-I/O of PROFIsafe Address Type 2

With the parameter "Central F-source address" you define the F-source address for F-I/O of PROFIsafe address type 2 which is assigned to this F-CPU. The F-source address must be unique network-wide.

4.3.3.1. System Configuration Example 1



The two system sections are connected via the PN-interface X1 on the respective F-CPU. The two F-CPUs are configured as IO-Controller and have, via the second port of X1, lower-level F-I/O.

Description of the Network Configuration

The configuration consists of one network, that is, each F-CPU could exchange data with every PROFIsafe device via X1. The central F-I/O can only be addressed via the respective F-CPU, and this must be taken into consideration in the CPU-wide uniqueness of the PROFIsafe address.

PROFIsafe Address Type 2

The F-I/O of the ET 200SP belong to the group of address type 2. There, the uniqueness of PROFIsafe addresses is applied as follows:

- The F-source addresses of the F-CPUs must be unique network-wide and
- The F-destination addresses of the F-I/O must be unique CPU-wide.

Since F-CPU 1 and F-CPU 2 are located in the same network, and their source addresses must be unique network-wide. Because the F-destination address of the ET 200SP only has to be unique CPU-wide, the F-destination addresses of the F-I/O in both system sections can be the same. The CPU-wide uniqueness refers to the F-CPU which has the same F-source address as the respective, associated ET 200SP.

PROFIsafe Address Type 1

The F-I/O of the ET 200S and the SINAMICS drive belong to the group of address type 1. The F-source address makes no contribution to the uniqueness of the PROFIsafe address. This means that the F-destination addresses of the F-I/O have to be unique CPU-wide and network-wide.

PROFIsafe Addresses of the Central F-I/O

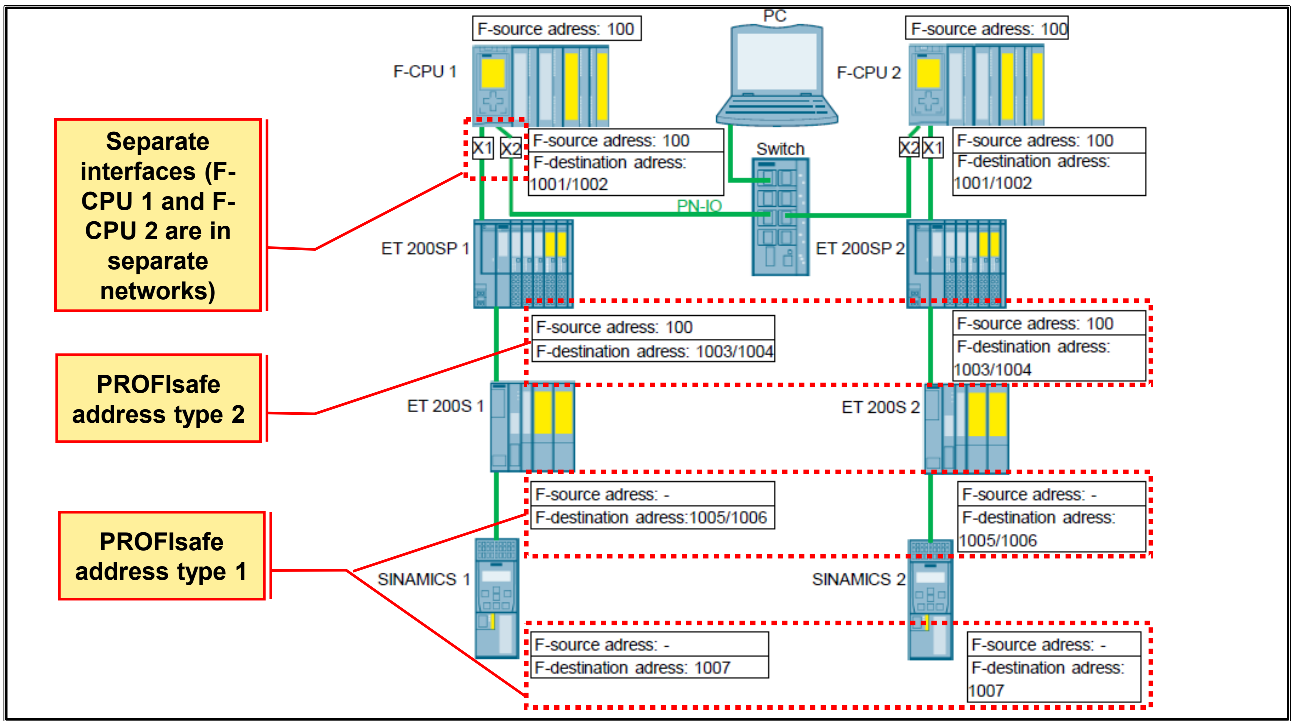
The centrally inserted F-I/O must each have unique F-destination addresses within their own F-CPU. CPU-wide uniqueness includes the central F-I/O and the accessible distributed F-I/O.

For the configuration considered here it means:

The F-destination addresses 1001 and 1002 in the rack with F-CPU 1 are unique CPU-wide and differ from the PROFIsafe addresses of the network formed via X1. There is no overlap with the addresses of the central F-I/O of F-CPU 2 since the F-CPU 2 has not implemented a routing between X1 and the backplane bus.

The same statements generally apply for the F-destination addresses 1001 and 1002 in the rack with F-CPU 2.

4.3.3.2. System Configuration Example 2



The two F-CPUs are configured as IO-Controllers and have, via X1, lower-level F-I/O. The two CPUs are connected by means of the I-Device communication via the PN-interface X2 (as of Firmware 2.0).

Description of the Network Configuration

The configuration consists of three networks:

- lower-level F-I/O to X1 of F-CPU 1
- lower-level F-I/O to X1 of F-CPU 2

PN-IO-connection between F-CPU 1 and F-CPU 2 via X2

The central F-I/O can only be addressed via the respective F-CPU, and this must be taken into consideration in the CPU-wide uniqueness of the PROFIsafe address.

PROFIsafe Address Type 2

The F-I/O of the ET 200SP belong to the group of address type 2. The uniqueness of PROFIsafe addresses is applied as follows:

- The F-source address of the F-CPU must be unique network-wide and
- The F-destination address of the F-I/O must be unique CPU-wide.

Because a routing of the F-CPU between X1 and X2 has not been implemented, both F-CPUs can have the same F-source addresses. The recommendation, however, is still to use different F-source addresses. This is mandatory when F-I/O are connected via X2 which must be assigned to an F-CPU.

Since the F-destination address of the ET 200SP only has to be unique CPU-wide, the F-destination addresses of the F-I/O in both system sections can be the same.

PROFIsafe Address Type 1

The F-I/O of the ET 200S and the SINAMICS belong to the group of address type 1. The F-source address makes no contribution to the uniqueness of the PROFIsafe address. For that reason, the F-destination addresses of the F-I/O must be unique CPU-wide and network-wide.

Because no routing has been implemented between X1 and X2, the F-destination addresses can be the same in both system sections.

PROFIsafe Addresses of the Central F-I/O

The centrally inserted F-I/O must each have unique F-destination addresses within their own F-CPU. CPU-wide uniqueness includes the central F-I/O and the accessible distributed F-I/O.

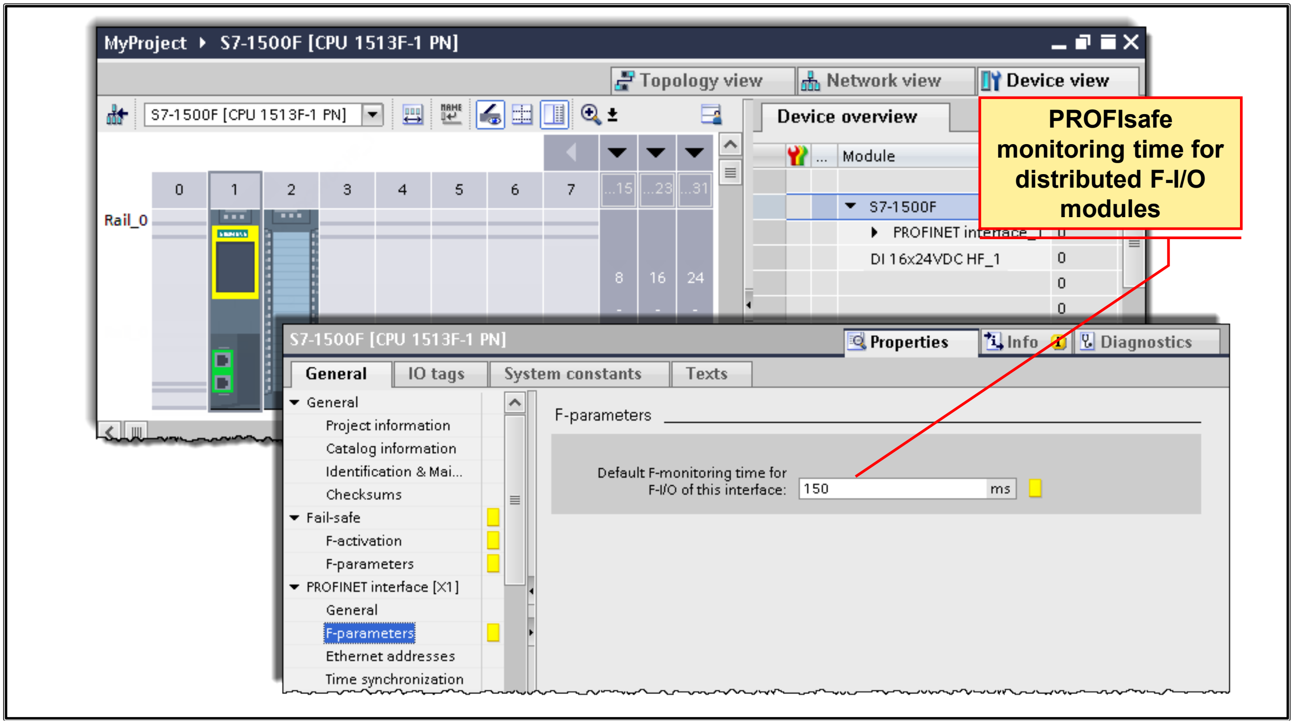
For the configuration considered here it means:

The F-destination addresses 1001 and 1002 in the rack with F-CPU 1 are unique CPU-wide and differ from the PROFIsafe addresses of the network formed via X1. Since a routing between X1 and X2 to F-CPU 2 has not been implemented, F-CPU 1 cannot access the lower-level F-I/O of F-CPU 2.

There is no overlap of the addresses of the F-I/O of F-CPU 1 with the central F-I/O of F-CPU 2 since the F-CPU 2 has not implemented a routing between the backplane bus and the local interface X2.

The same statements generally apply for the F-destination addresses 1001 and 1002 in the rack with F-CPU 2.

4.3.4. PROFIsafe Monitoring Time (Distributed)



Default F-Monitoring Time for Distributed I/O

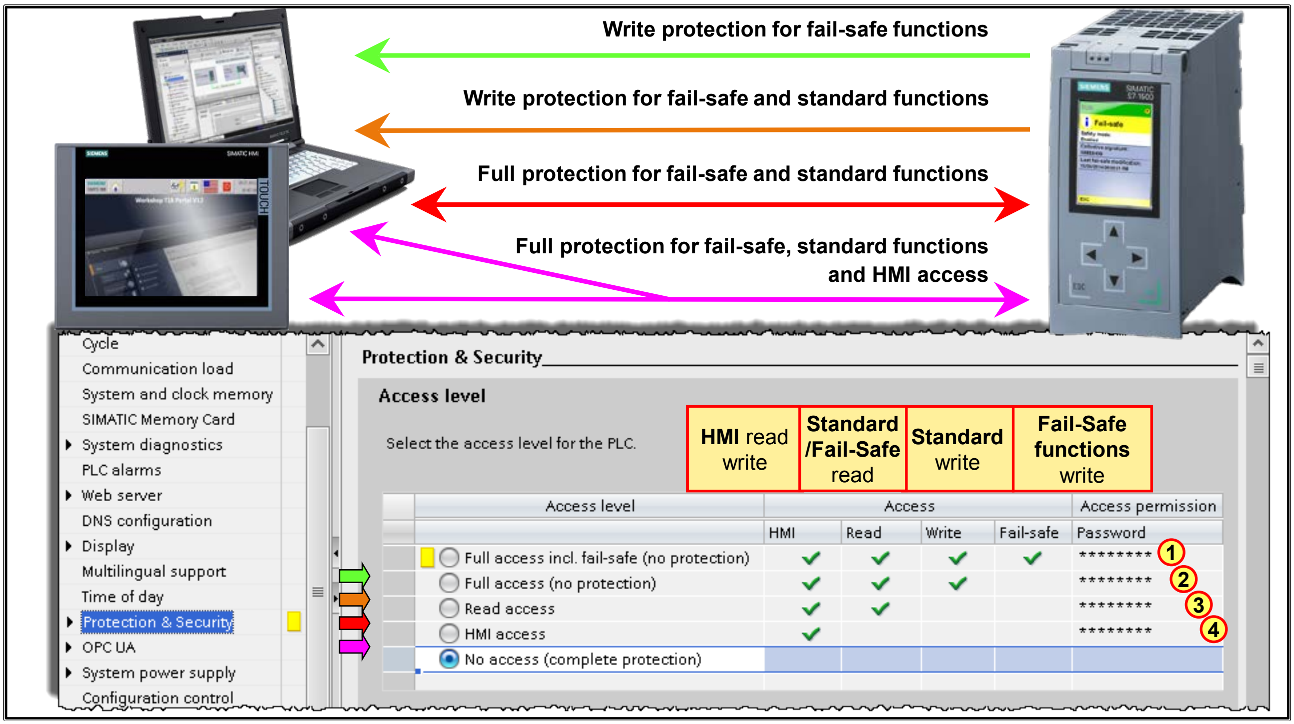
The default F-monitoring time for the F-I/O of this interface acts on the F-I/O assigned to this F-CPU interface (PROFIBUS or PROFINET). You change this parameter in the properties of the relevant interface (select the interface in the "Device overview" tab, then "F-parameters").

Using the different possible settings, you can adapt the F-monitoring time to the conditions of your F-system, for example, to accommodate different bus cycles.

The F-monitoring time is the PROFIsafe monitoring time (Watchdog) for the safety-related communication between the F-CPU and distributed F-I/O. If the F-I/O does not receive a valid safety message frame from the F-CPU within the assignable monitoring time, the F-module passivates itself with a "communication error".

The F-monitoring time can be assigned manually or on a module-specific basis, or it can be assigned centrally for all F-I/O modules in the F-parameters of the CPU.

4.3.5. CPU Password Protection



Protection Levels

With the following protection levels, the access rights (read / write) of the programming device to the CPU are specified:

- Full access incl. fail-safe (no protection): → Default setting for F-CPU
  Read and write access is always permitted.
- Full access (no protection): → Default setting for Standard CPU
  Read access and write access is always permitted.
- Read access: → Write protection
  Read-only access possible. No data can be changed in the CPU, and no blocks or modified hardware configuration or parameter assignment can be downloaded to the CPU without specifying a password.
- HMI access: → Write and read protection for STEP 7
  No write or read access is possible from the engineering. Only the CPU type and identification data can be displayed in the Project tree under "Accessible devices". It is not possible to display online information or blocks under "Accessible devices" without entering a password.
- No access (complete protection): → General write and read protection for STEP 7 and HMI.
  Access for HMI devices without a configured password in the connection is also not possible.

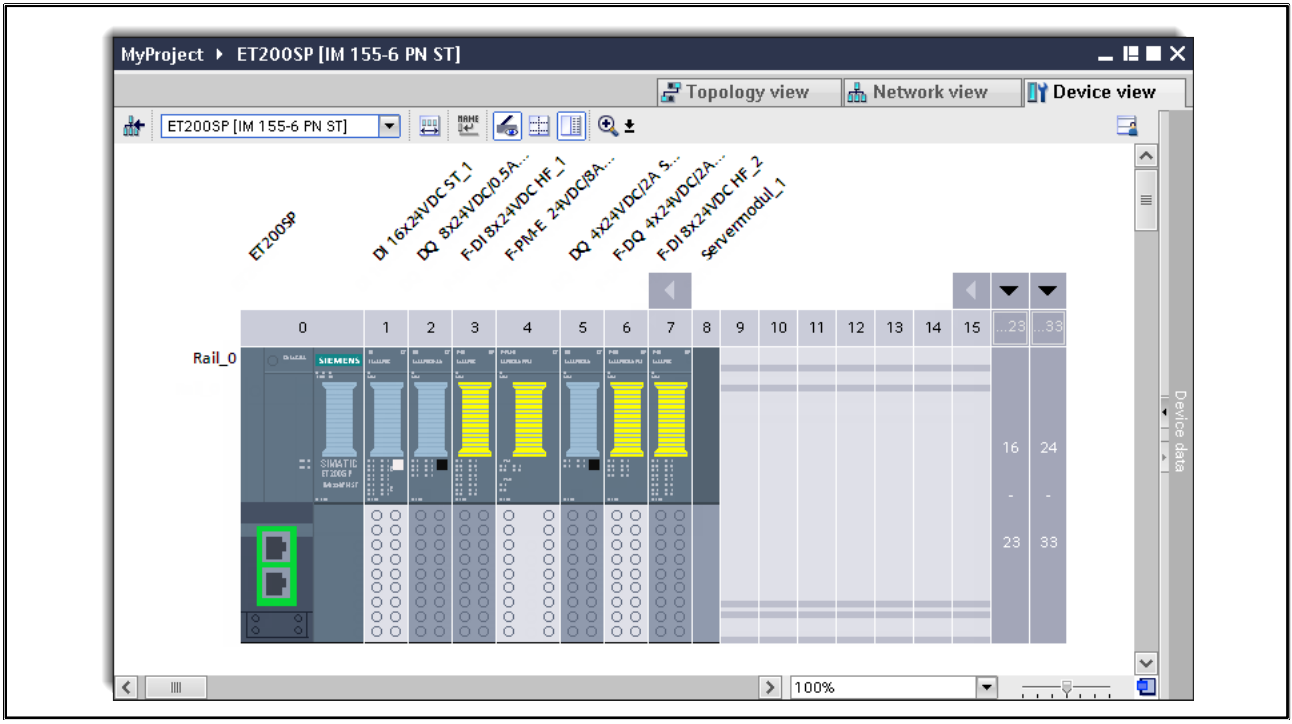
Access Permitted through Passwords

In the example shown, "No access (complete protection)" is selected. This means that without a password, STEP 7 and HMI devices can neither read-access nor write-access the CPU. The above explained protection levels can, however, be lifted again with passwords:

- By specifying a password (4) an HMI device can once again read-access and write-access the CPU. For STEP 7, however, neither read-accesses nor write-accesses are possible.
- By specifying a password (3) an HMI device can once again read-access and write-access the CPU and for STEP 7, only read-accesses are permitted, not write-accesses.
- By specifying a password (2) read-accesses and write-accesses of the standard program of the CPU are possible for both an HMI device as well as for STEP 7.

- By specifying a password (1) read-accesses and write-accesses of the standard section of the CPU are possible for both an HMI device as well as for STEP 7.

4.4. Configuring an ET 200SP

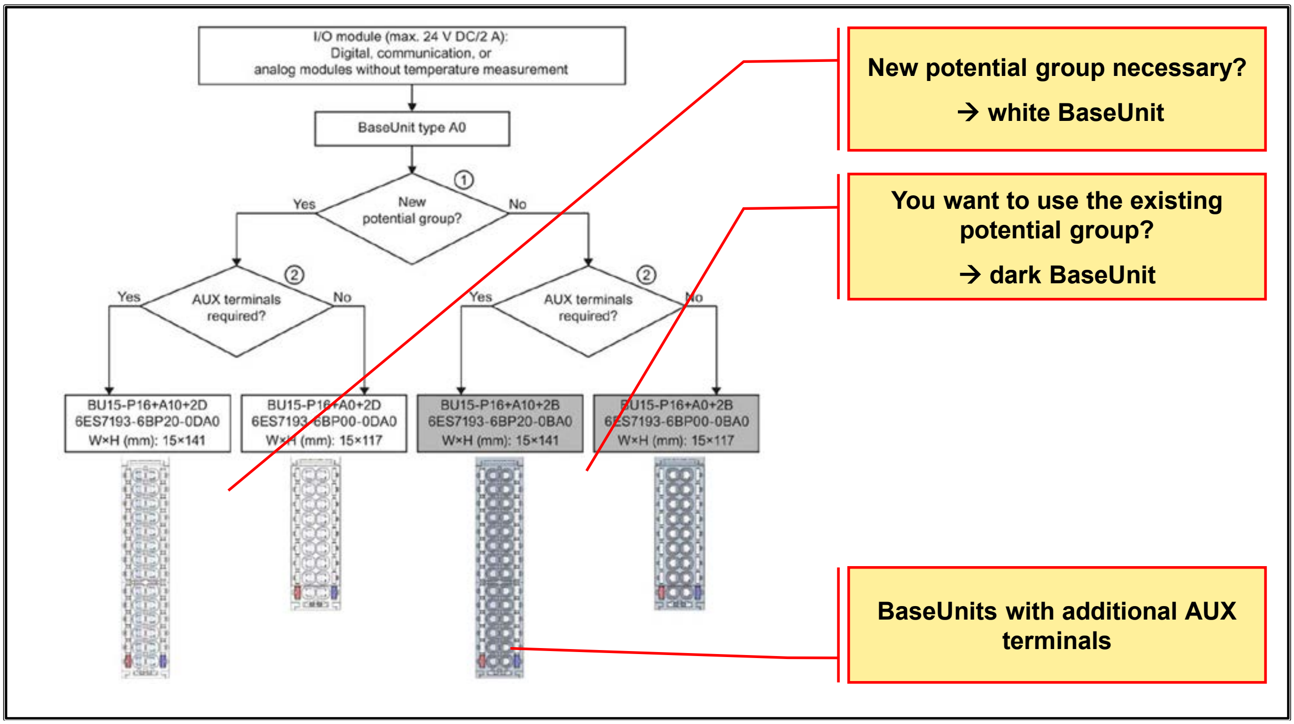


Configuring the F-I/O

You configure the ET 200SP, ET 200S, ET 200eco, ET 200pro, ET 200iSP F-modules and the S7-300 F-SMs as usual in STEP 7.

After you have inserted the F-I/O in the work area of the Device view or Network view, you access the configuration dialogs by selecting the particular F-I/O and the "Properties" tab.

4.4.1. Selecting the Correct Base



Selecting the Correct BaseUnit

There are various BaseUnits available for the ET 200SP distributed I/O system. The BaseUnit determines, among other things, the process connection, the pluggable I/O module and the supply voltage infeed.

Maximum Configuration of a Potential Group

The number of I/O modules that can be used per potential group depends on the following factors:

1. the sum of the current demand of all I/O modules operated in this potential group
2. the sum of the current demand of all loads externally connected to this potential group

The sum of the total current calculated in 1 and 2 (above) must not exceed 10 A.

AUX Terminals

BaseUnits with additional AUX terminals (for example, BU15-P16+A10+2D) facilitate the additional connection of a potential (up to the maximum supply voltage of the module) which you connect via the AUX bus.

Selecting a Suitable BaseUnit

The BaseUnits (BU) are classified according to various types. Each BaseUnit type distinguishes itself through properties which match certain I/O modules. You recognize the BU type by the last two digits of the article number of an I/O module, for example, 4 FDO / 6ES7136-6DB00-0CA0 / BaseUnit Type A0.

4.4.2. BaseUnit for F-PM and F-RQ

Power module
F-PM-E PPM 24VDC/8A

Opens new potential group for group switch-off

BaseUnit: BU20-P6+A2+4D

Article no: 6ES7193-6BP20-0DC0

Relay module
F-RQ 1x24VDC/24..230VAC/5A

Special BaseUnits for F-RQ

BaseUnit: BU20-P8+A4+0B

Article no: 6ES7193-6BP20-0BF0

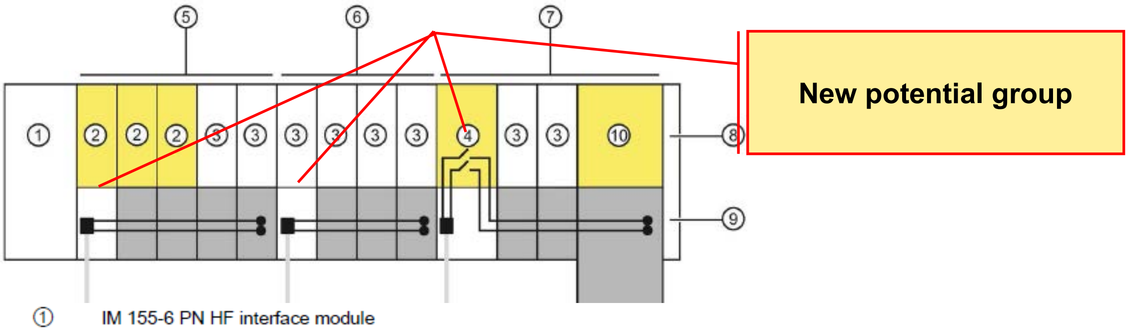
Selecting the Correct BaseUnit

During commissioning, make sure that you only use the power module with the BaseUnit Type C0.

Note

If the last 2 digits of the module's order (article) number/MLFB are also found in the BaseUnit's order (article) number/MLFB, then you will have selected the correct BaseUnit.

4.4.3. ET 200SP with Fail-safe and Non-fail-safe Modules

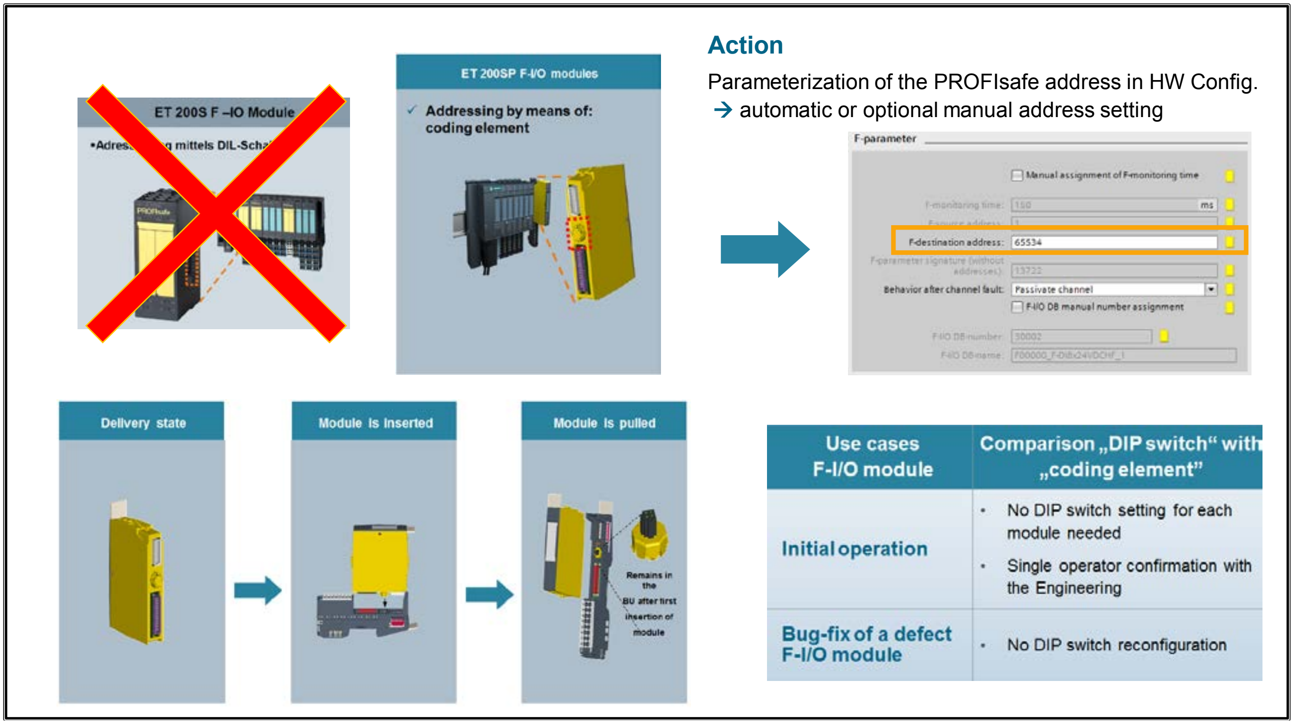


① IM 155-6 PN HF interface module
② F-module
③ Non-fail-safe module
④ Power module F-PM-E 24VDC/8A PPM ST
⑤ Mixed fail-safe and non-fail-safe potential group with BaseUnits BU15..D and BU15..B.
You achieve SIL3/Cat. 4/PLe for the fail-safe modules. No safety category can be achieved with the non-fail-safe motor starter.
⑥ Non-fail-safe potential group with BaseUnits BU15..D and BU15..B
⑦ Fail-safe potential group with BaseUnits BU20..D, BU15..B and BU30-MSx.
Through disconnection of the self-assembling voltage bus, and thus of the non-fail-safe modules, up to SIL2/Cat. 3/PLe is possible.
⑧ Server module
⑨ Self-assembling voltage buses P1/P2
⑩ Fail-safe motor starter F-DS HF

ET 200SP with Fail-safe and Non-fail-safe Modules

You can configure the ET 200SP with fail-safe and non-fail-safe modules. It is not necessary to operate fail-safe and non-fail-safe modules in separate potential groups.

4.4.4. Assembly and Addressing of an ET 200SP/MP F-I/O Module



F-Destination Address for Fail-safe Modules

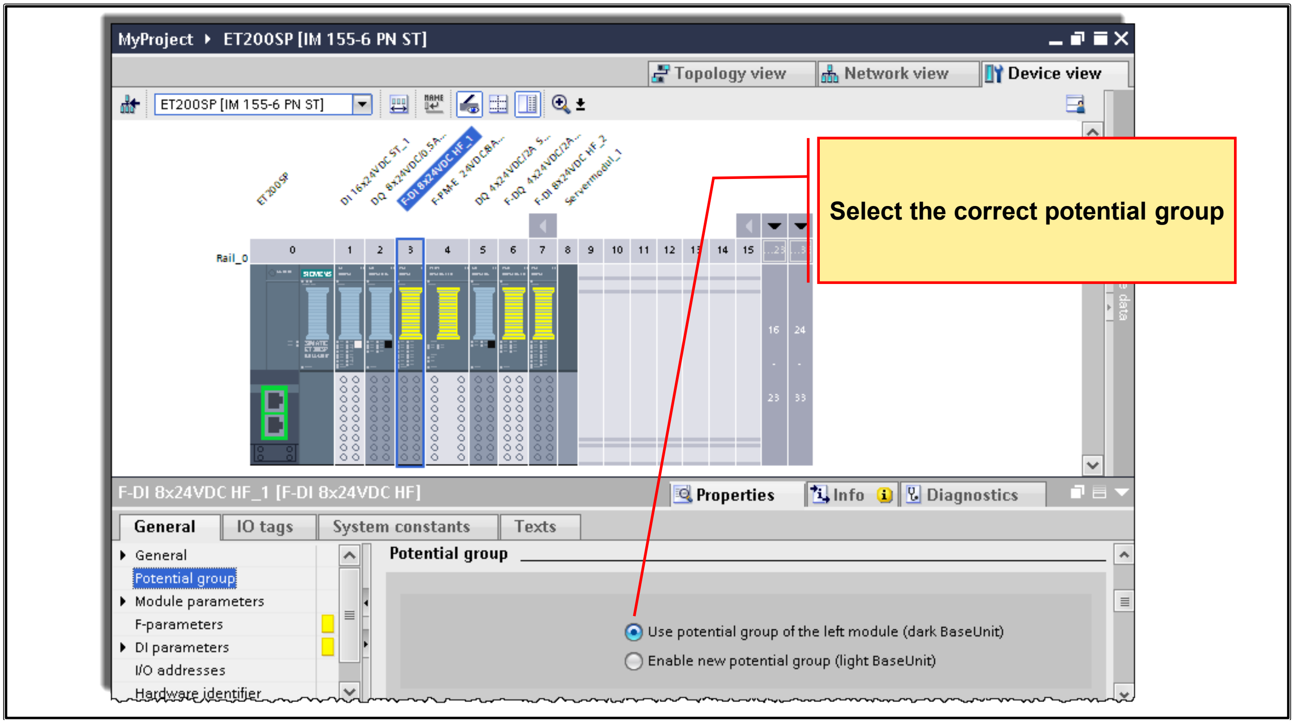
The F-destination address is stored permanently on the coding element of the ET 200SP fail-safe modules. During the F-destination address assignment, the F-module must be supplied with supply voltage L+.

To be Considered when using the Configuration Control:

Before you can use the configuration control together with F-modules, you must assign the F-destination address to the F-modules at the intended slots. For this, each F-module must be inserted in the slot configured for it. Subsequently, the physical configuration can differ from the configured one.

4.4.6. F-I/O Parameters

4.4.6.1. Potential Group



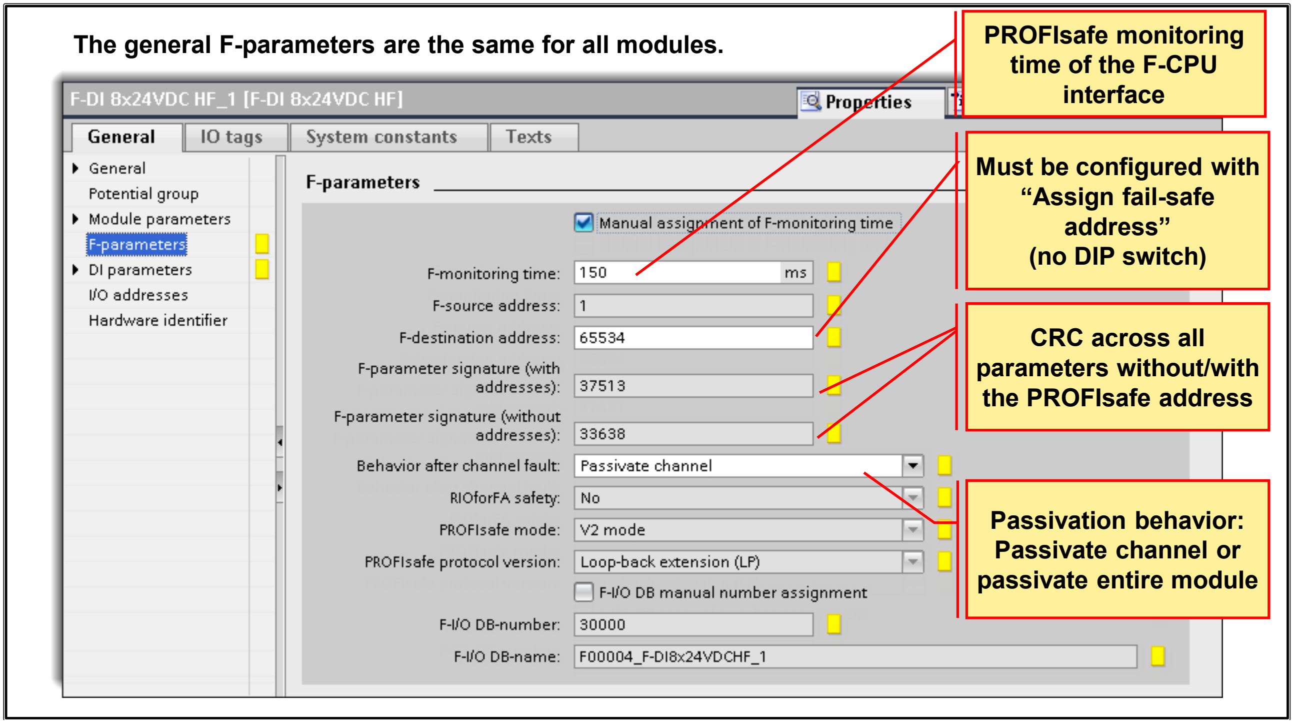
Potential Group

For the ET 200SP distributed I/O system, potential groups are created by a systematic arrangement of the BaseUnits.

To form potential groups, a distinction is made for ET 200SP between 2 BaseUnits:

- BaseUnits BU...D (can be recognized by the light-colored terminal box and the light-colored mounting rail release):
  - open a new potential group (power bus and AUX bus is interrupted to the left)
  - feed in the supply voltage L+ up to an infeed current of 10 A
- BaseUnits BU...B (can be recognized by the dark-colored terminal box and the dark-colored mounting rail release):
  - continue the potential group (power bus and AUX bus fed through)
  - tap the supply voltage L+ for external components or
  - loop through with a maximum total current of 10 A

4.4.6.2. F-Parameter



F-Parameters

In the "F-parameters" tab, settings are made that affect fail-safe communication of the module with the F-CPU.

F-Destination Address

These are the PROFIsafe addresses and serve to uniquely identify the source (F-CPU) and destination (F-module). The PROFIsafe addresses must be unique station-wide and network-wide. In order to prevent incorrect parameter assignment, the F-destination address is automatically assigned. When the F-destination address is manually changed, its station-wide uniqueness is automatically checked but not, however, the network-wide uniqueness! It is then up to the user to ensure this!

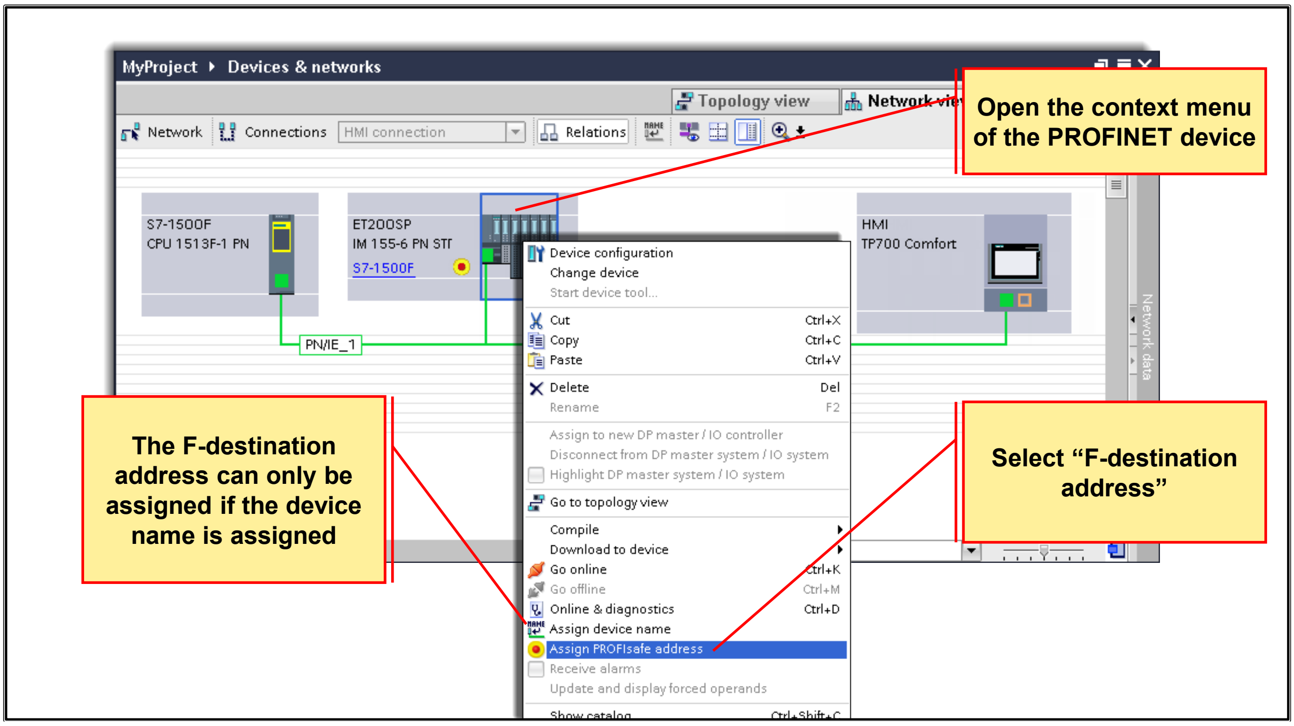
F-Monitoring Time [ms]

This is the PROFIsafe monitoring time (Watchdog) for safety-related communication between the F-CPU and F-I/O. If the F-I/O does not receive a valid safety message frame from the F-CPU within the assignable monitoring time, the F-module passivates itself with a "communication error". The F-monitoring time can be assigned manually or on a module-specific basis or it can be assigned centrally for all F-I/O modules in the F-parameters of the CPU.

Behavior after Channel Faults

As of S7 Distributed Safety V 5.4, the behavior of F-I/O modules after channel faults (e.g. short-circuit, overload, discrepancy error, wire break) can be configured. If the F-I/O supports this parameter (e.g. for ET 200SP, ET 200S F-modules), you can set whether the entire module is passivated after a channel fault occurs or only the faulty channel(s).

4.5. ET 200SP Assigning a Fail-safe Address



ET 200SP - Assigning a Fail-safe Address

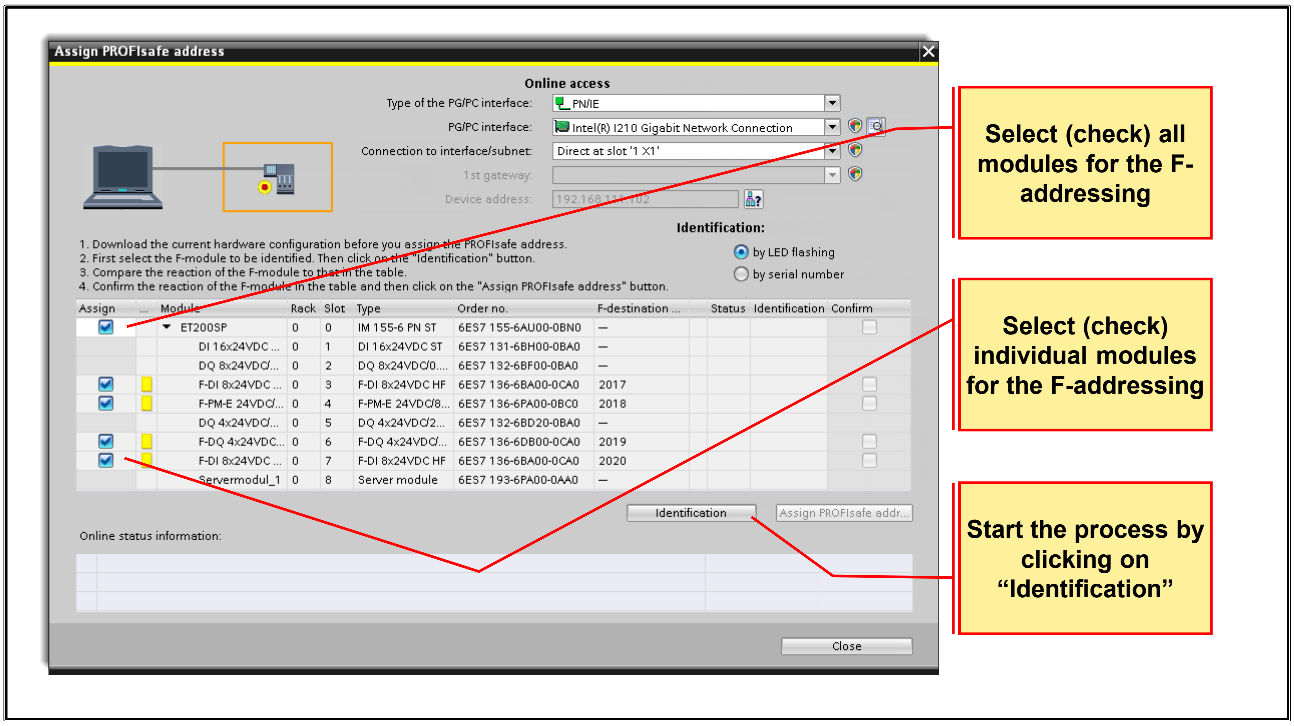
ET 200SP fail-safe modules do not have a DIP switch for assigning the unique F-destination address for each module. Instead you assign the PROFIsafe address directly in STEP 7. You assign the F-destination address parameter in the hardware configuration for the F-module. For supported configurations, the F-source address corresponds to the "Basis for PROFIsafe addresses" of the associated F-CPU. Beyond that, an assignment is required in the following cases:

- Subsequent insertion of an F-module during first commissioning
- Repair of the ET 200SP
- Replacement of the BaseUnit
- Commissioning of a serial machine
- Change to the F-destination address
- Change to the "Basis for PROFIsafe addresses" parameter of the associated F-CPU (changes the F-source address).

A reassignment is not necessary in the following cases:

- Power OFF/ON
- Replacement of an F-module (repair case) without PG/PC
- Change to the configuration if a new BaseUnit is inserted before an F-module
- Repair/replacement of the interface module

4.5.1. Identifying F-Modules



Identifying F-Modules

By pressing the "Identification" button, you confirm the correctness of the addresses for the F-I/O. Therefore, proceed cautiously when confirming (identifying) the F-I/O “by LED flashing” or “by serial number” of the interface module. The following requirements must be fulfilled:

- The ET 200SP is configured.
- The configuration was loaded into the ET 200SP.
- The ET 200SP is accessible online.

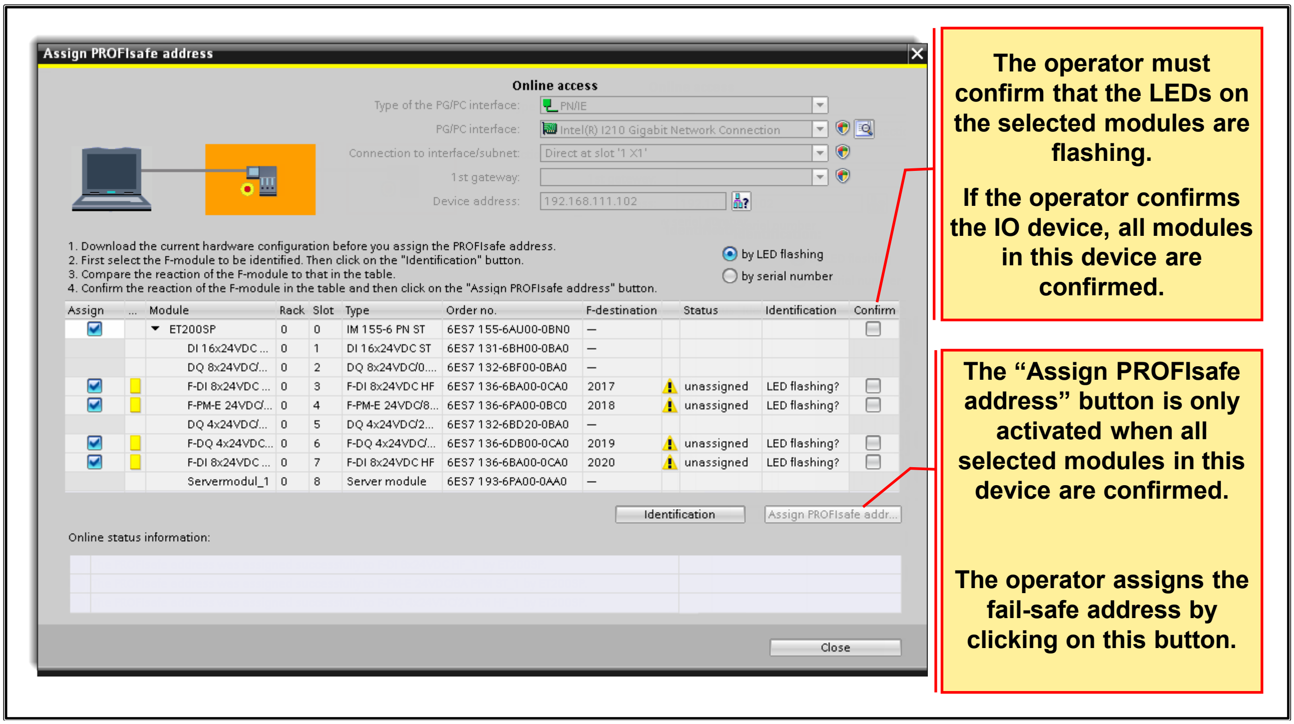
Identification "by LED flashing"

This is the default setting. During the identification, the DIAG and STATUS LEDs of the F-modules to be identified flash.

Identification "by serial number"

If you cannot see the F-modules, you can still identify them using the serial number of the interface module.

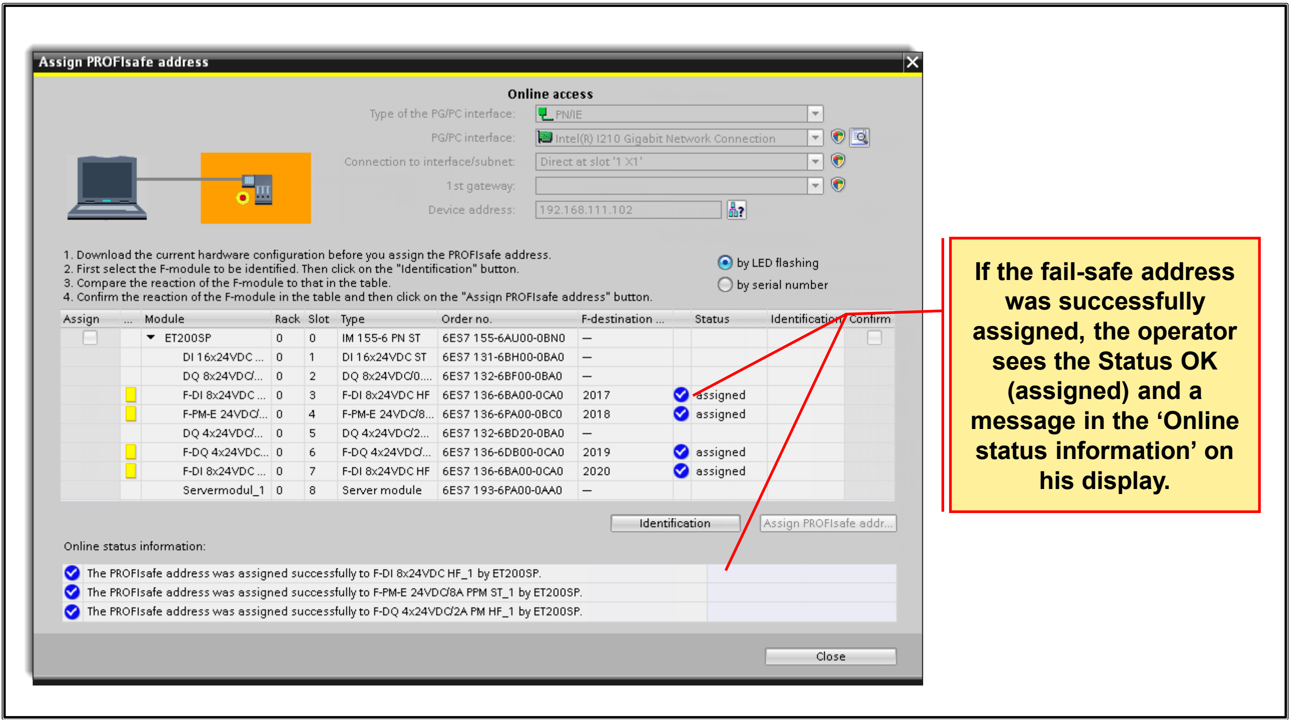
4.5.2. Assigning an F-Destination Address



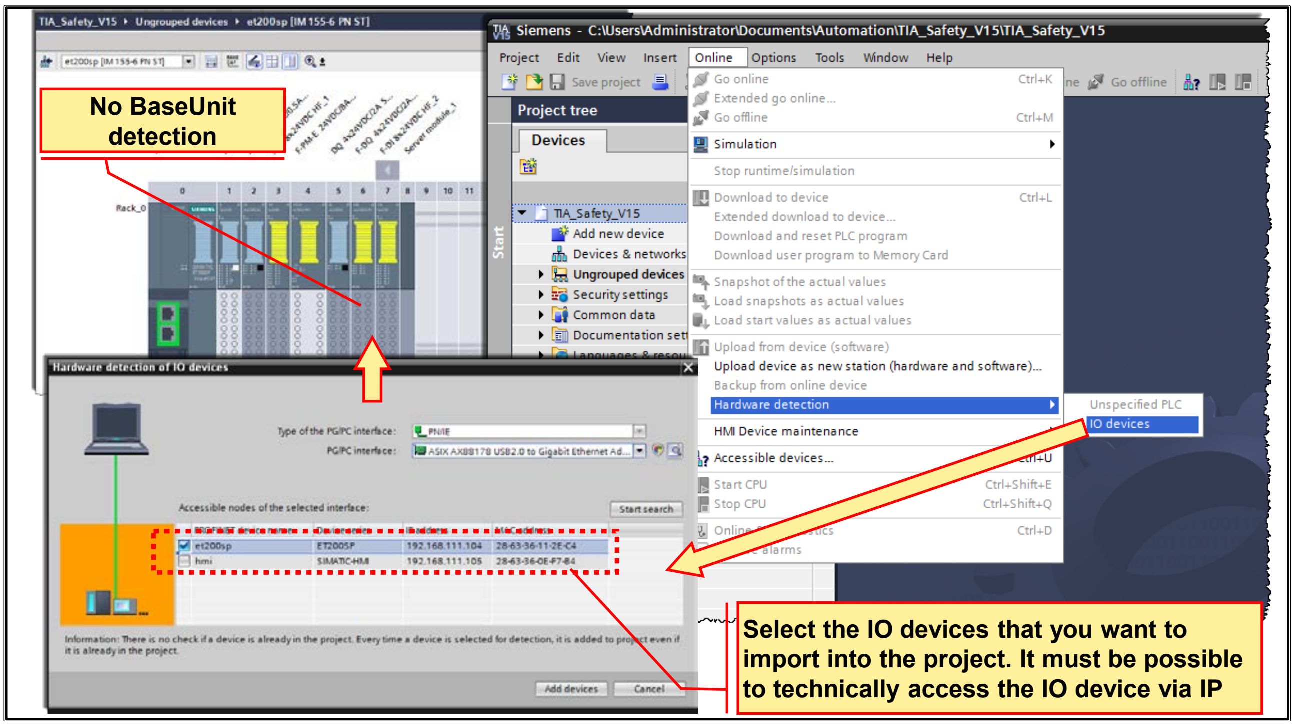
Assigning an F-Destination Address

In order to assign the F-destination address, you must confirm the "Confirm… assignment" dialog within 60 seconds.

4.5.3. F-Destination Address Status



4.6. Configuring an IO device through hardware detection



You have the possibility to detect a real existing IO device and to import it into your project. You find the IO device in STEP 7 through the "Hardware detection" function. A detected device can be imported into your project. STEP 7 inserts the IO device with all the modules and submodules.

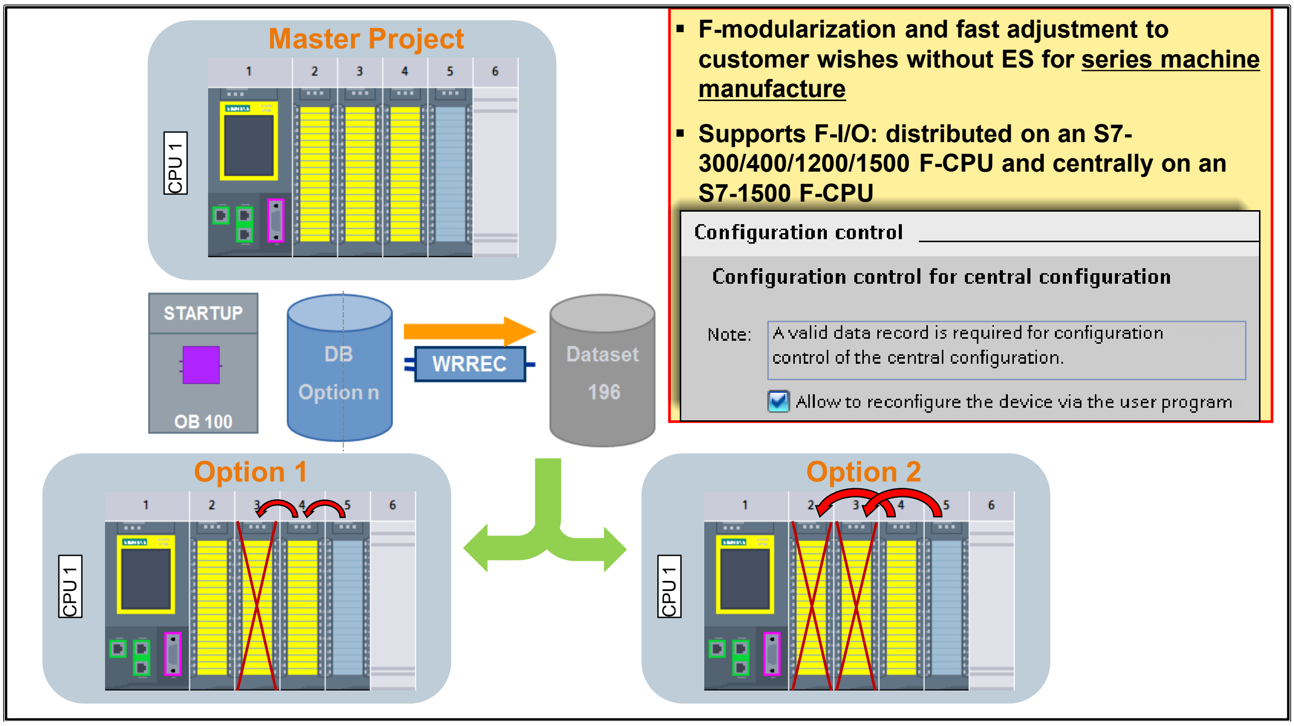
Prerequisites

- STEP 7 (TIA Portal) as of V15
- It must be possible to technically access the IO device via IP

Result of the hardware detection

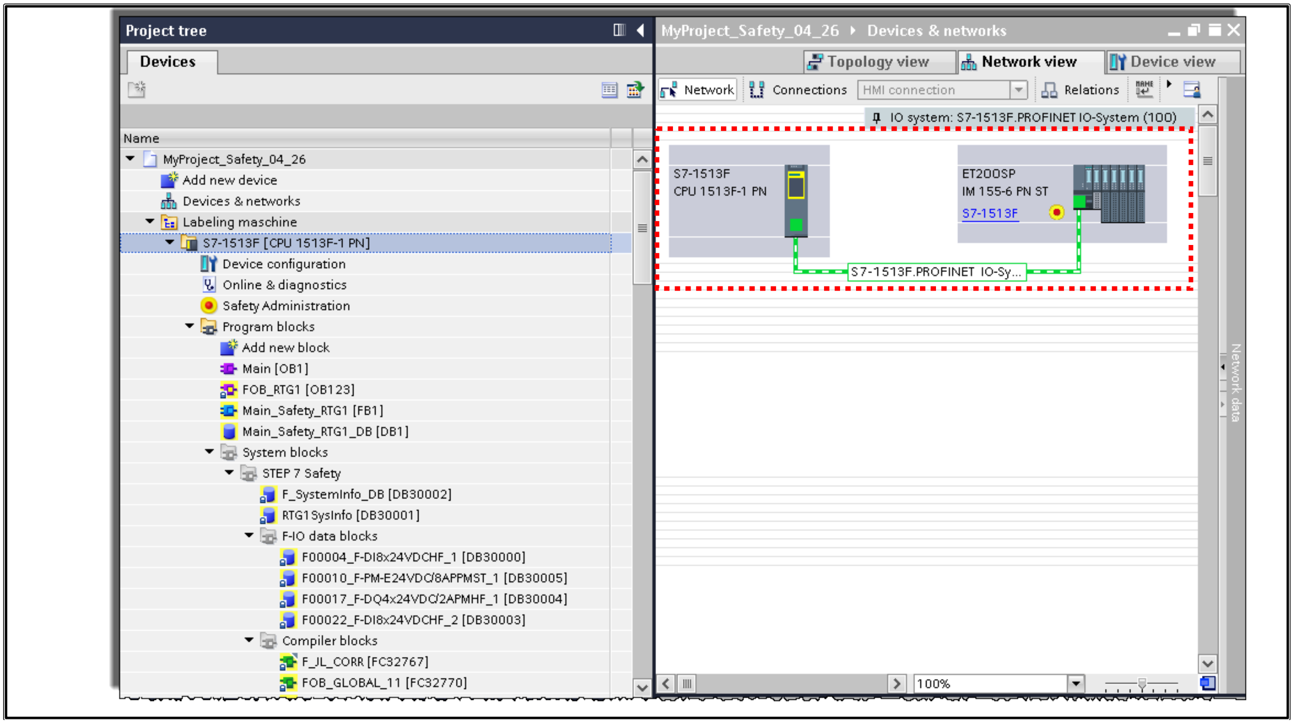
- If the hardware detection is successful, STEP 7 inserts the IO device with all the modules and submodules into the project.
- An IO device configured via hardware detection responds as follows:
  - Modules configured through the "Hardware detection" are configured as if they have been inserted from the catalog.
  - STEP 7 imports the MAC address of the detected IO device into the project.
  - STEP 7 imports the IP address into the project.
  - STEP 7 imports the PROFINET device name into the project.
- IO devices configured through "Hardware detection" have neither an IP subnet nor an IO controller assigned.

4.7. Configuration Control (Option Handling) for F-I/O



For configuration control (option handling) with F-I/Os proceed as with the standard I/O devices. Detailed information can be obtained by searching for "Configuration control (option handling)" in the help of STEP 7. You also find a detailed application example in safety advanced manual (Entry ID: 54110126).

4.8. Task Description: Creating a Project and Hardware Station



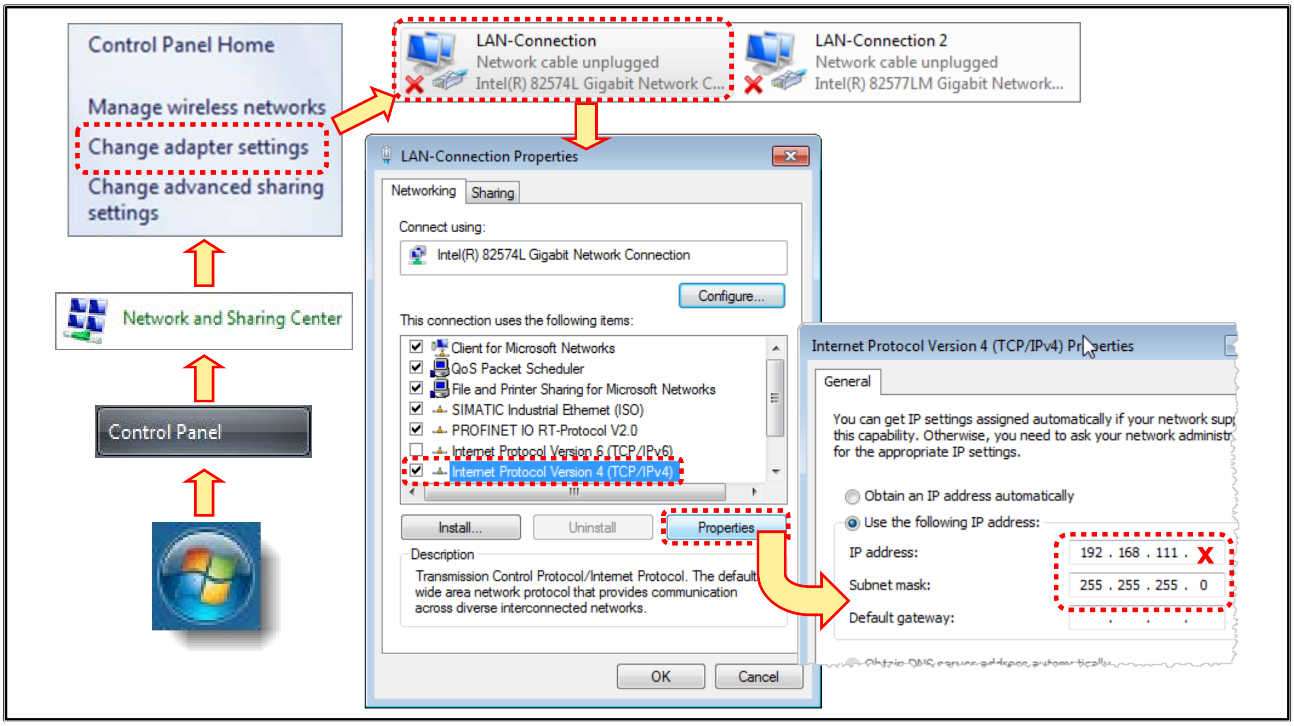
Task Description

You are to create the hardware configuration of the CPU and the ET 200SP in a new project.

What to Do

What you have to do will be explained on the following pages.

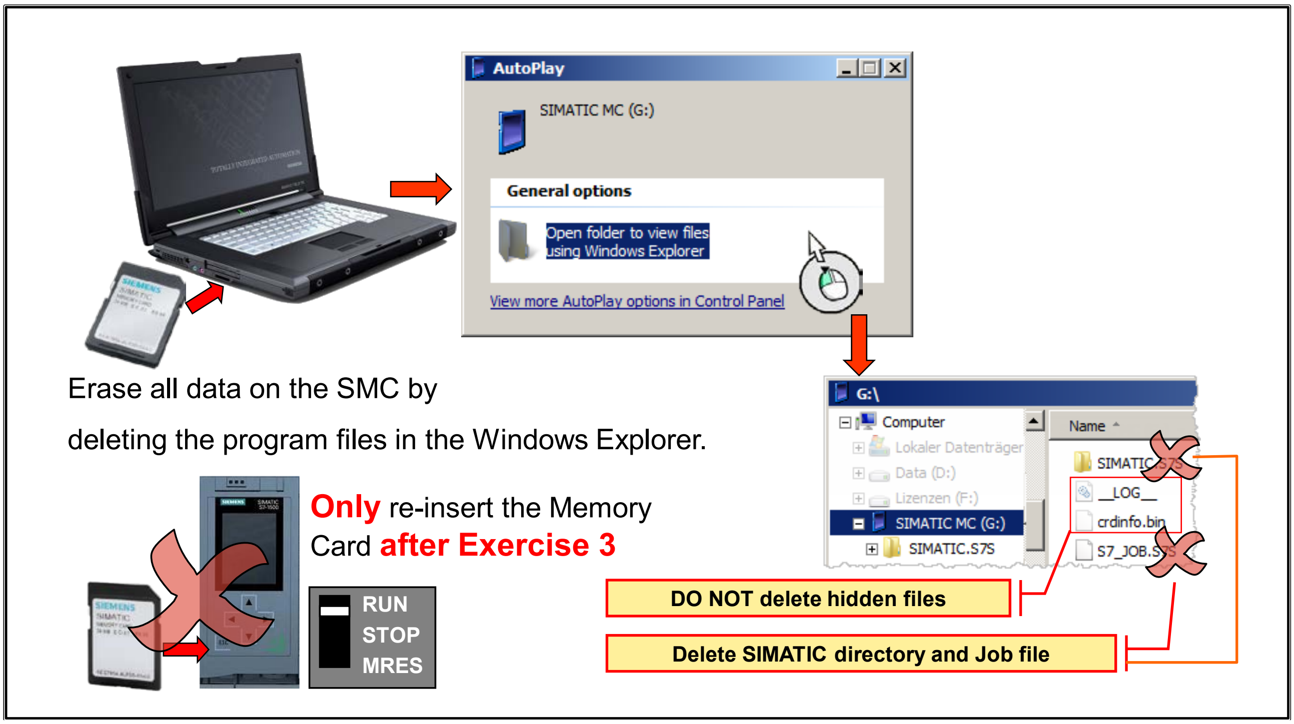
4.8.1. Exercise 1: Setting the IP Address of the PG



Task and What to Do:

1. Connect the Ethernet interface "Intel(R) 82574L" of the PG to the "P1" or "P2" connection on the training device using an Ethernet cable.
2. Assign the IP address 192.168.111.X and the subnet mask 255.255.255.0 to this PG interface. Proceed as shown in the picture.

4.8.2. Exercise 2: Erasing the SIMATIC Memory Card (SMC)



Task

In order to completely erase the CPU, the SIMATIC Memory Card of the CPU must also be erased.

What to Do:

1. Insert the SIMATIC Memory Card in the PG's card reader.
   With the contact surfaces facing up, insert the Memory Card in the PG's card reader. If it is a SIMATIC Field PG of the type M4, it has two card readers. The left reader is used for SIMATIC Memory Cards.

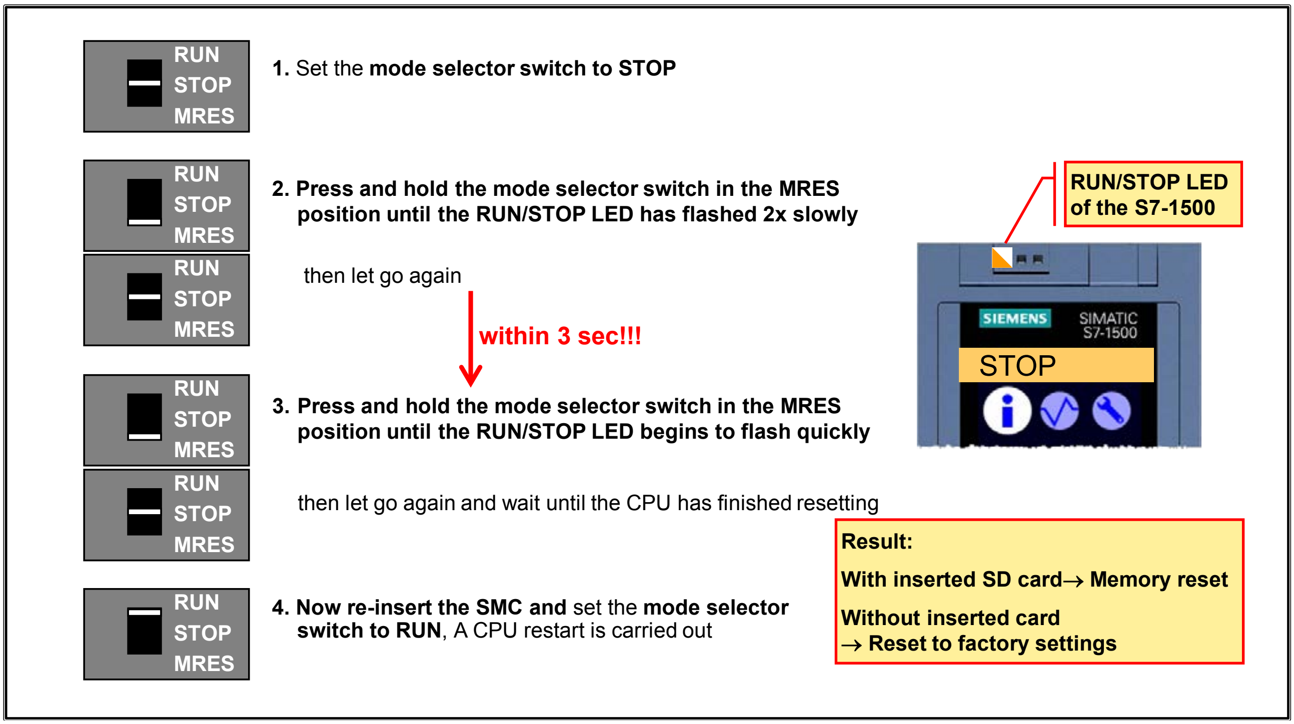
2. Erase the SIMATIC Memory Card.
   A Windows dialog appears to open Windows Explorer. Open the folder. Depending on the Windows Explorer settings, concealed files are either displayed or hidden.

Caution!

If they are visible, they must not be deleted under any circumstances! Delete the SIMATIC directory and the Job file.

3. Do **NOT** insert the SIMATIC Memory Card in the CPU. Close the window with the Windows Explorer and remove the memory card from the PG. Remember to first activate the Windows function "Remove hardware safely"!

4.8.3. Exercise 3: Resetting and Restarting the CPU



Task

In the last exercise you erased the SMC of the CPU. Now, you are to reset the CPU to its factory settings. For this, an MRES **without** SMC must be carried out.

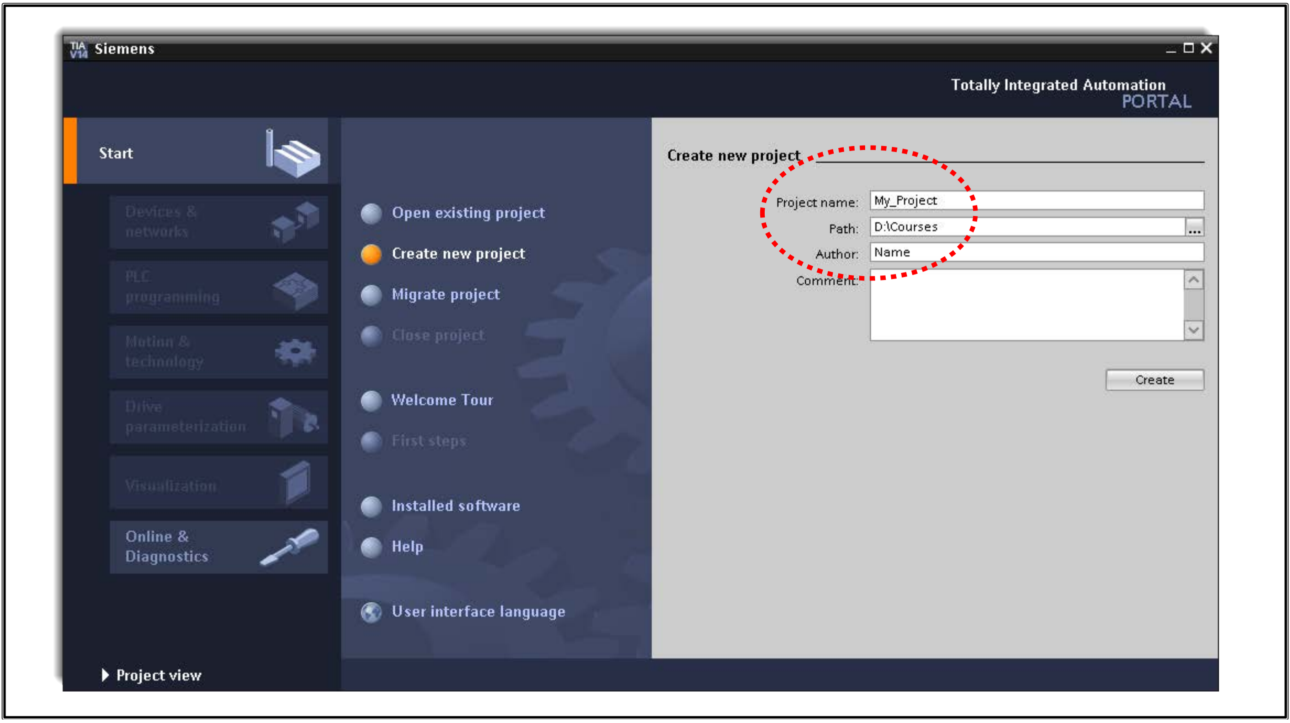
What to Do

1. Perform the MRES without SMC directly on the CPU following the steps shown in the picture.
2. Re-insert the SMC into the CPU.
3. Restart the CPU by switching the mode selector switch from STOP to RUN.

Result:

- The CPU remains in STOP because no user program is loaded.
- The I/O modules show with green flashing lights that they are not parameterized.

4.8.4. Exercise 4: Creating a New Project



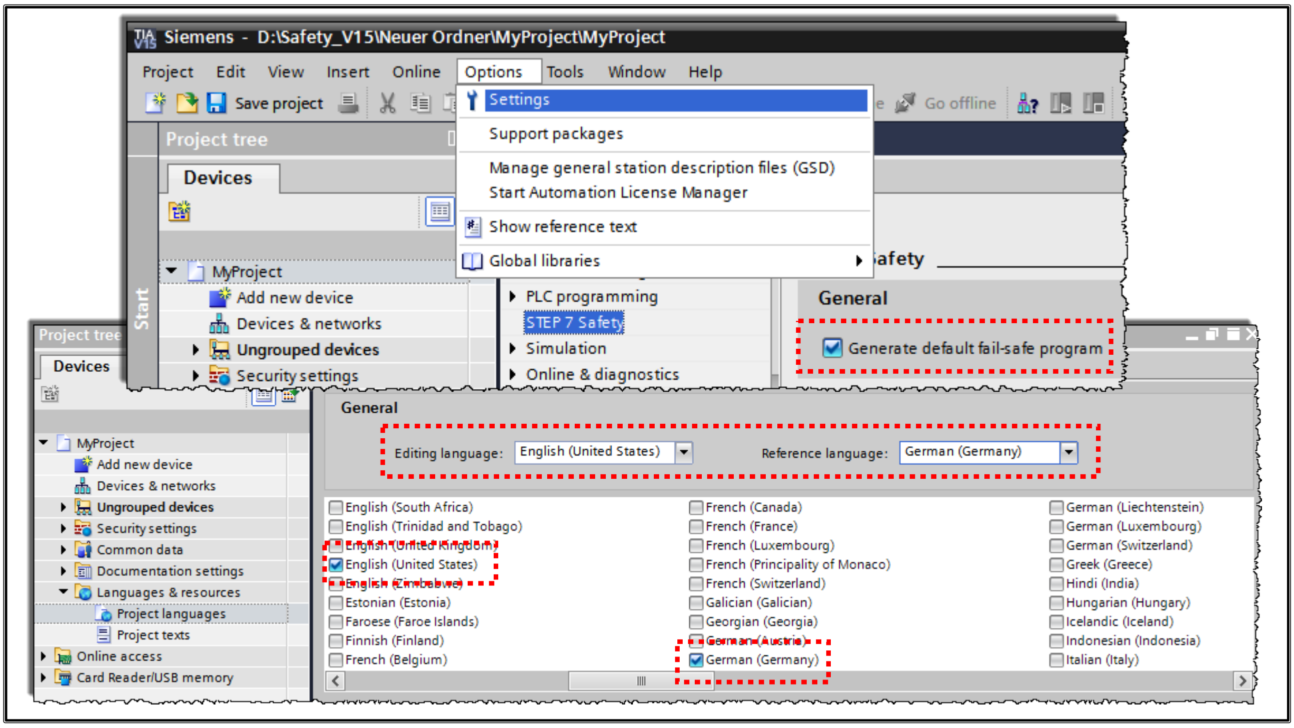
Task:

You are to create a new TIA Portal V15 project:

What to Do:

1. Open the TIA Portal V15.
2. Create a new project with the name “MyProject” in the folder D:\Courses.
   Portal view > Start > Create new project or Project view > Project > New or via the “New” button in the toolbar of the Project view.

4.8.5. Exercise 5: Checking the Project Settings



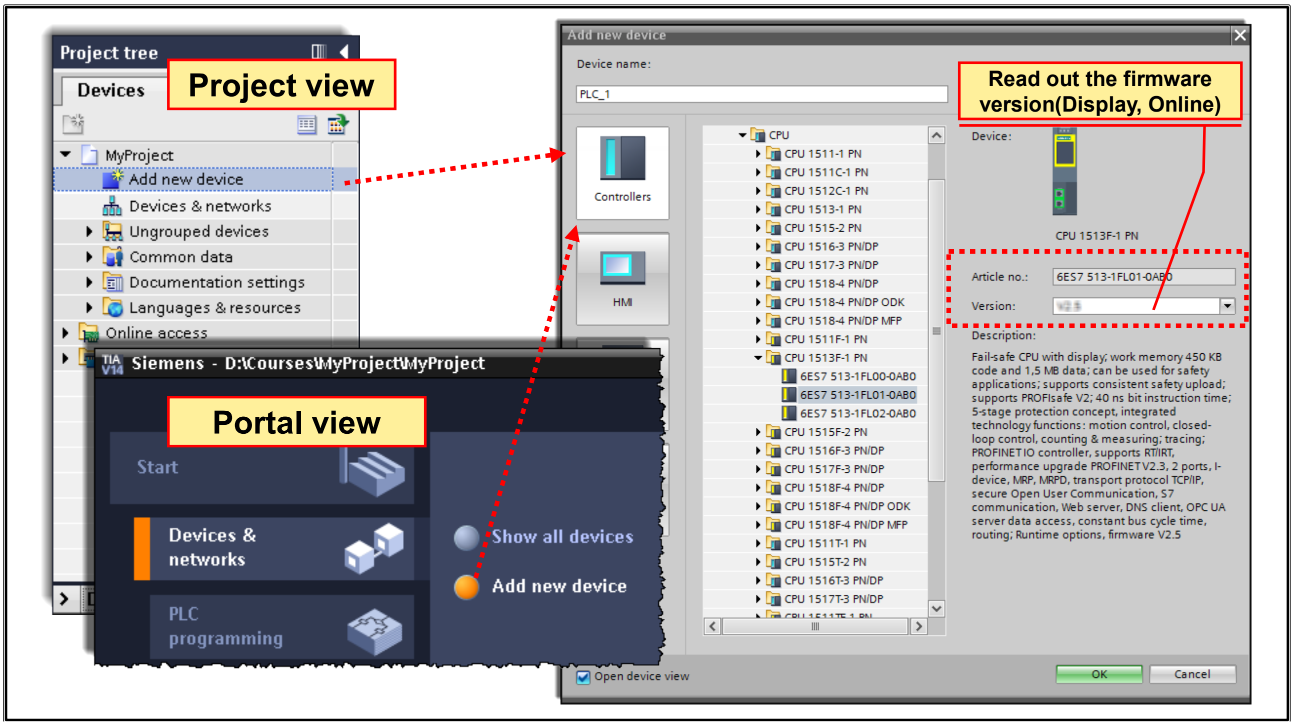
Task

You are to check the project settings for STEP 7 Safety.

What to Do

1. Switch to the Safety-relevant project properties.
   “Options” -> “Settings” -> “STEP 7 Safety”.
2. Activate the point “Generate default fail-safe program”.
3. Open the settings of the project languages.
   "Project tree"->"Languages & resources"->"Project languages"
4. Activate the languages English (United States) and German (Germany).
5. Select English as Editing language and German as Reference language.

4.8.6. Exercise 6: Creating an S7-1500F Station



Task

As a "new device", you are to create an S7-1500F-CPU whose firmware version corresponds to that of your training controller.

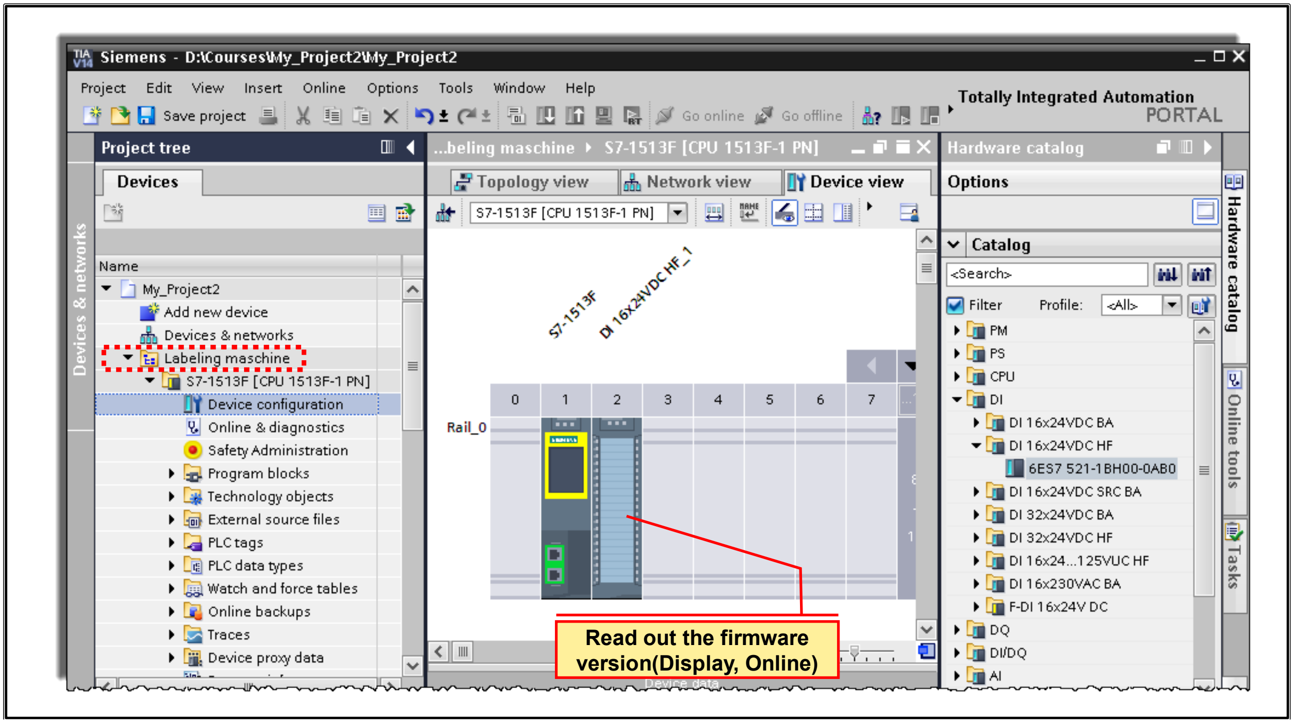
What to Do

1. Read out the firmware version of your CPU. You can do this directly via the CPU-Display or via the online function of the TIA Portal.

   Note: If you want to read out the firmware via online function of the TIA Portal the CPU need an IP address!

2. Activate the menu option: "Add new device".
3. Select the relevant CPU of your training device with the correct firmware as device.

4.8.7. Exercise 7: Creating a Device Group and Configuring the S7-1500F



Task

You are to configure the S7-1500 station which matches your actual training device. In addition, you are to create a new device group “Labeling machine”.

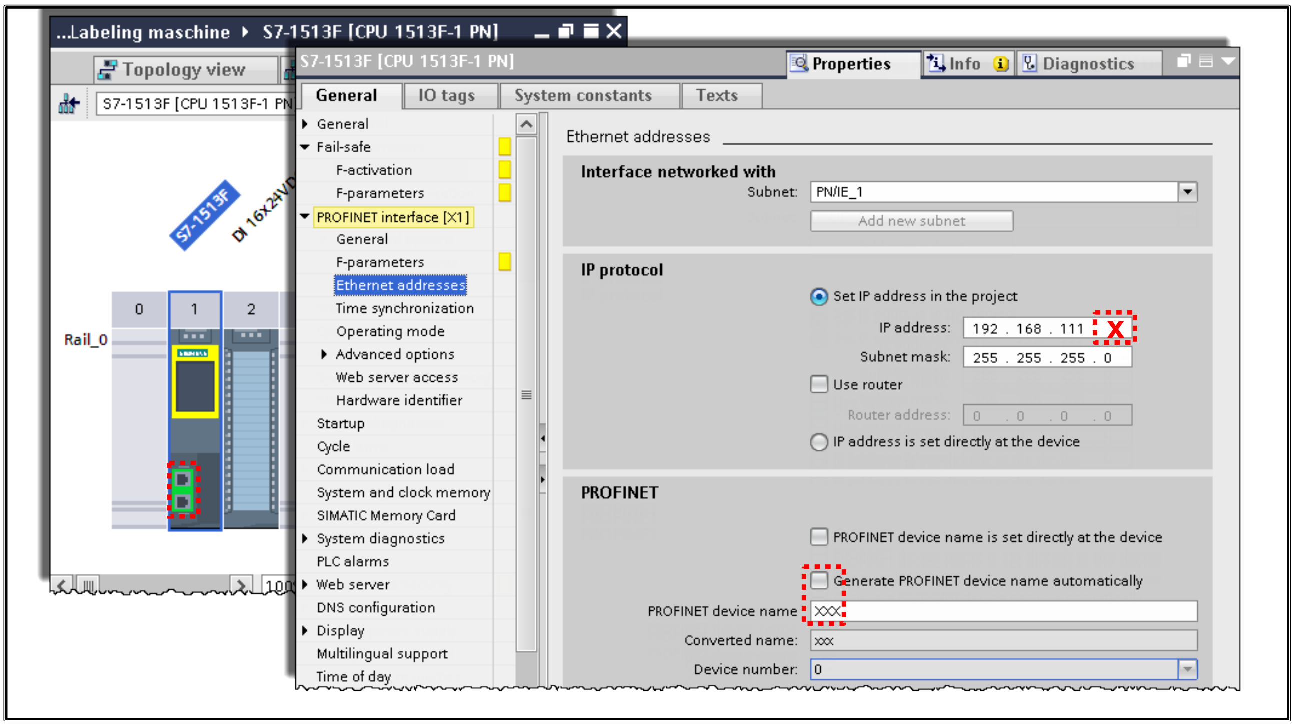
What to Do

1. Switch to the ‘Device view’ and open the ‘Hardware catalog’.
2. Using drag & drop configure the signal module of the S7-1500 station that corresponds exactly to your training device. Pay exact attention to the firmware version of the module. You can read out the firmware via the CPU-Display or via the online function of the TIA Portal.

   Note: If you want to read out the firmware via online function of the TIA Portal the CPU need an IP address!

3. Generate a device group “Labeling machine” (right-click on the project).
4. Assign the CPU to the generated device group.

4.8.8. Exercise 8: CPU Properties: IP Address and PROFINET Name



Task

You are to assign a PROFINET name and an IP address to the CPU.

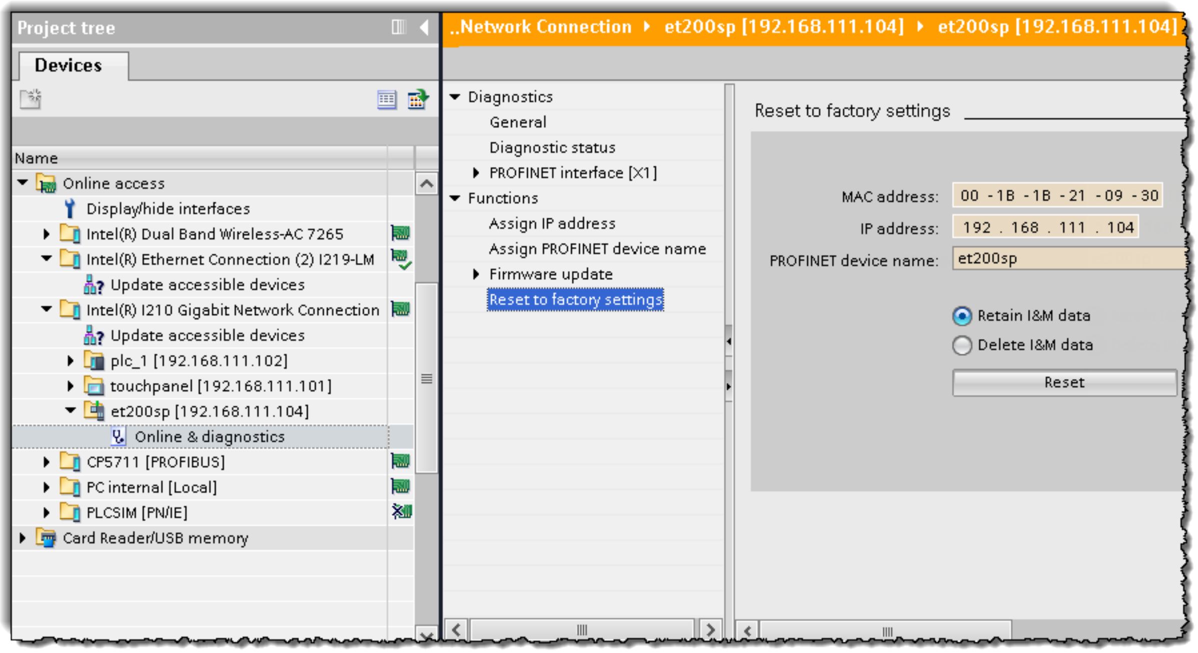
What to Do

1. Switch to the Project view.
2. Double-click on the "device configuration" of the CPU.
3. In the "Device view", select the CPU.
4. Open the “PROFINET interface” tab and enter the IP address, subnet mask and the device name.

Note for the device name:

Optionally, the device name can also be generated automatically. The PROFINET device name is then adopted from the CPU name in the “General” tab.

4.8.9. Exercise 9: ET 200SP: Resetting to Factory Settings



Task

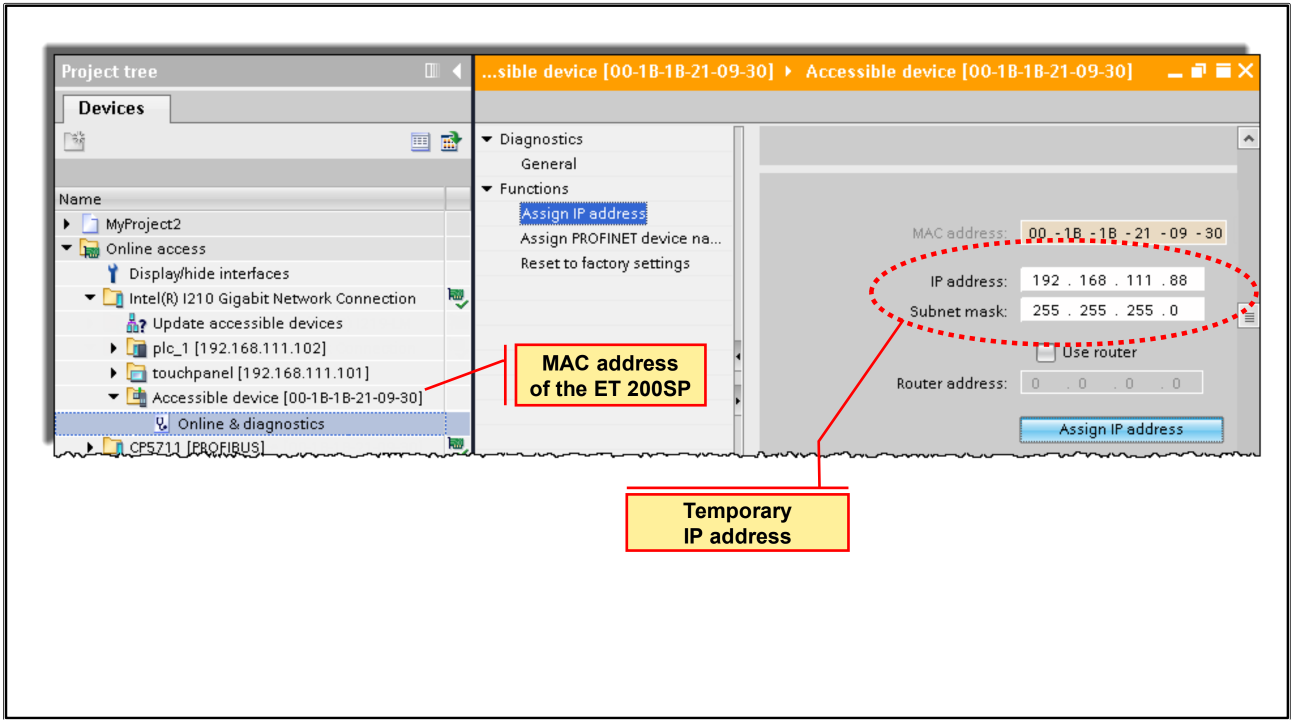
All settings so far (IP address, subnet mask and PROFINET name) of the Interface module of the ET 200SP station are to be deleted through a "Reset to factory settings". In the following exercises, you will then transfer your own settings onto the ET 200SP station,

What to Do:

1. Open the Online access and there select the interface you are connected to your training device.
2. There, activate "Update accessible devices" by double-clicking on it and wait until the list is completed.
3. Open the ET 200SP and there activate the function "Online & diagnostics" by double-clicking on it.
4. In the "Online & diagnostics" window, open the "Functions" tab.
5. There, activate "Reset to factory settings" and confirm the dialog.
6. Close the "Online & diagnostics" window.
7. Check the success of the reset to factory settings in the Inspector window under “INFO > General”. In addition, you will find the ET 200SP without an IP address and without a device name under “Accessible devices”.

Leave all windows open for the next exercise.

4.8.10. Exercise 10: Assign a temporary IP address



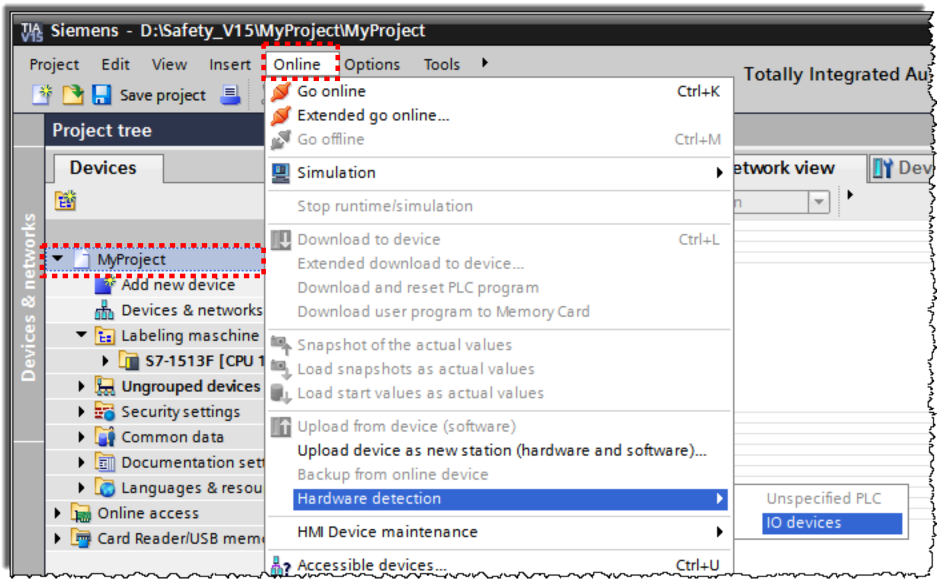
Task

In the following exercises, the entire ET 200SP station will be read-in via the hardware detection functionality of TIA Portal. For this function, the ET 200SP requires an IP address. In the previous exercise, the IP address was deleted by the reset to factory settings (0.0.0.0). You are now to assign a temporary IP address.

What to Do

1. Update the accessible devices of the interface.
   "Update accessible devices".
   -> The ET 200SP is now only accessible via MAC address (see picture).
2. To assign a temporary IP address, switch to the
   "Functions -> Assign IP address" tab. There, enter the temporary IP address shown in the picture as well as the subnet mask and confirm via "Assign IP address" (see above).

4.8.11. Exercise 11: Detect the ET 200SP



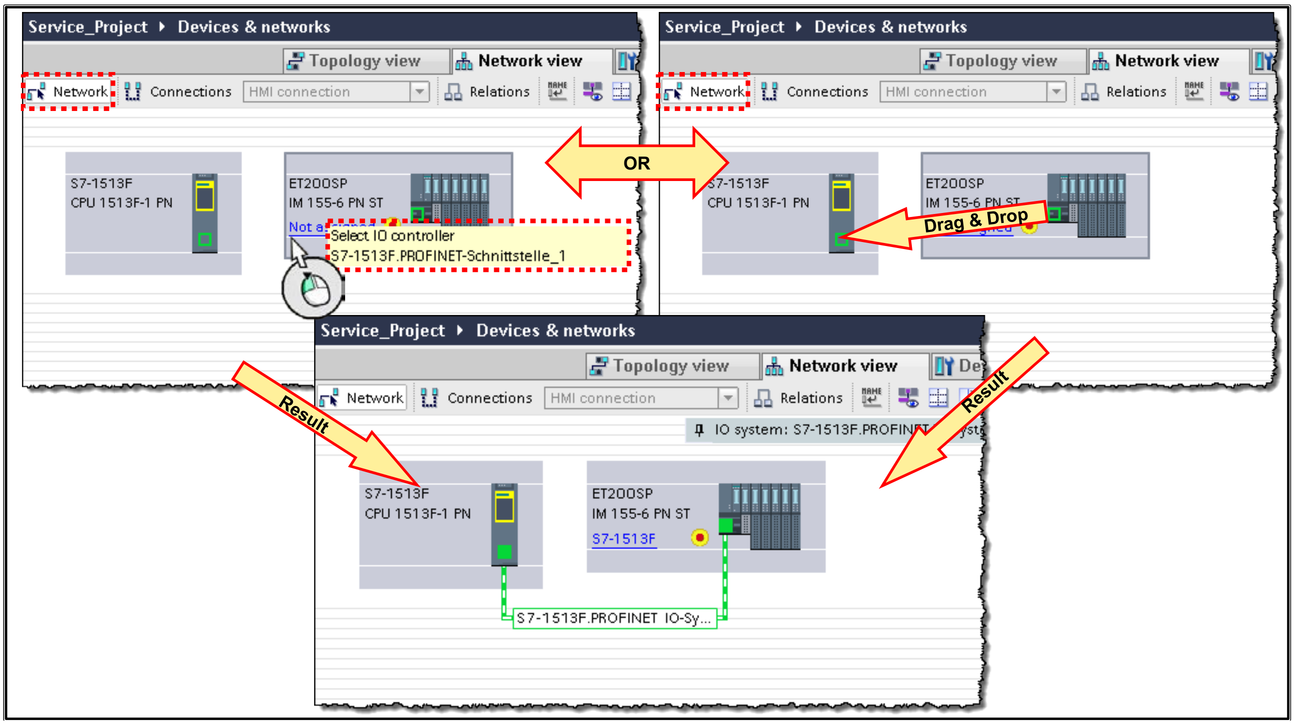
Task

You are to read-in the entire ET 200SP station into the project.

What to Do

1. Select (highlight) your project "MyProject" in the Project tree.
2. Start the Hardware detection for IO devices.
   "Online" -> "Hardware detection" -> "IO devices"
3. In the dialog that appears, search the network for the ET 200SP station. To do so, select the PG/PC interface used and press "Start search".
4. Select the ET 200SP station via the option box (left) and add the device.

4.8.12. Exercise 12: Networking the ET 200SP with the CPU



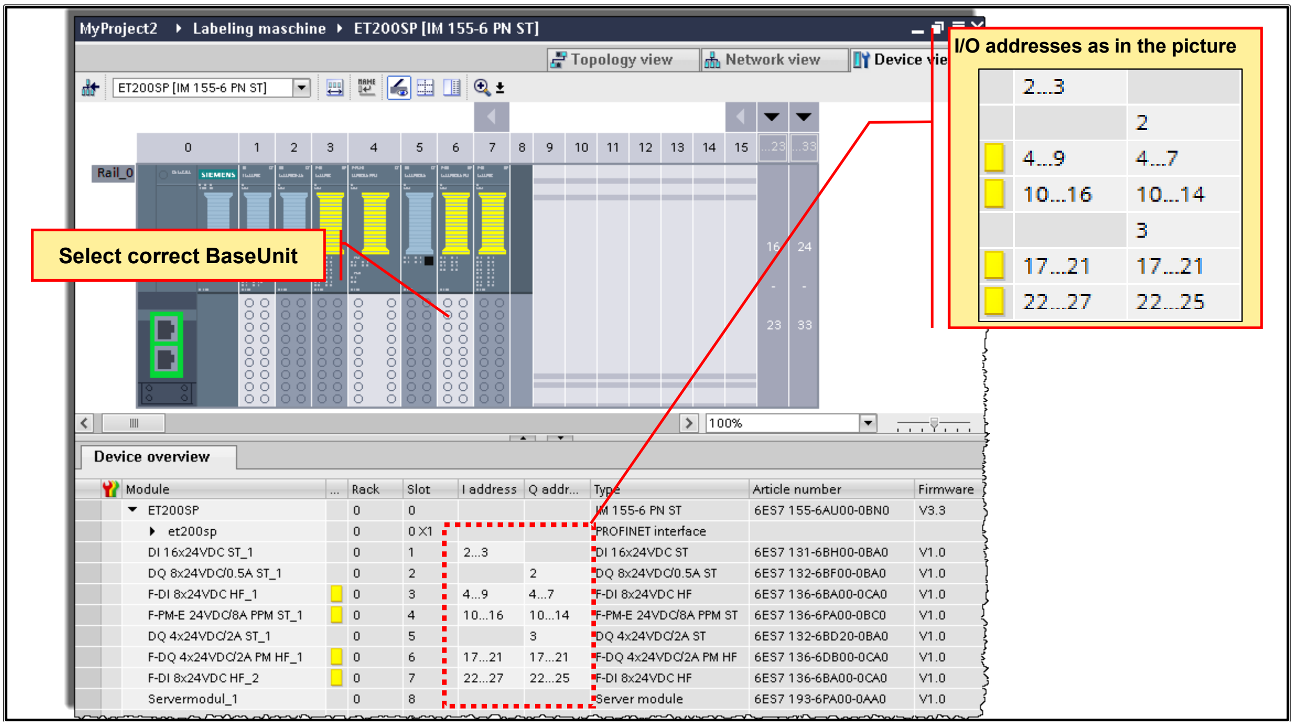
Task

After the ET 200SP IO-Device is added, it must now be assigned to an IO-Controller or networked with a CPU. In case there are several CPUs in the network, a co-ordination or monitoring of the I/O addresses by the IO-Controller and IO-Device can only be done through this unique assignment.

What to Do

1. In the Hardware and Network editor, select the Network view and there choose the "Network" tab.
2. Network the ET 200SP with the CPU by connecting the Ethernet interface of the ET 200SP with the Ethernet interface of the CPU using drag & drop (right picture) or by directly assigning the ET 200SP station to the CPU (left picture).

4.8.13. Exercise 13: Customize configuration of the ET 200SP



Task

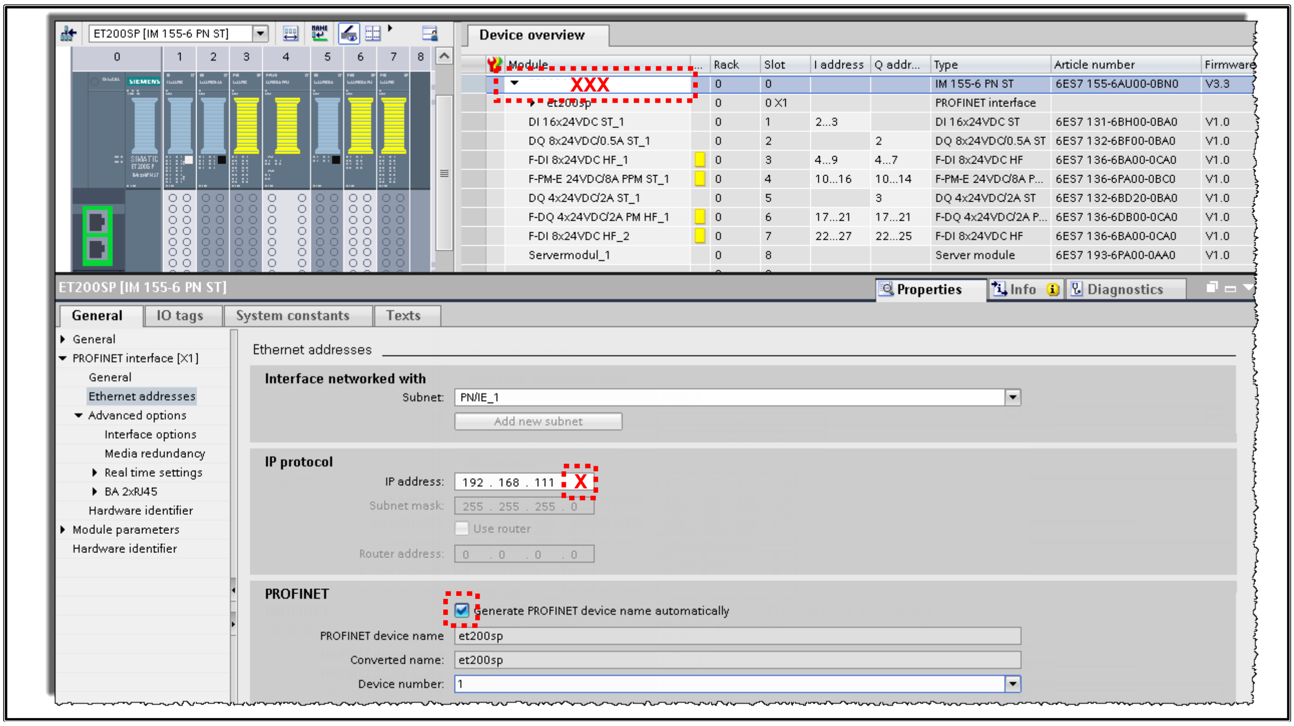
The ET 200SP has digital input and output modules. The I/O addresses used in the STEP 7 program must match the addresses of the DI/DO modules parameterized here. The potential groups (BaseUnit) must also be checked since these cannot be read-in via a hardware detection.

The current address assignment can be found in the lower/right section of the working area in the Hardware and network editor in the "Device view" tab of the module. The addresses can be changed in the table.

What to Do

1. In the Hardware and network editor, select the "Device view" tab of the ET 200SP.
2. Compare all potential groups (BaseUnit) in the project with the ones that exist physically. If necessary, exchange unlike potential groups.
3. Open the "Device overview" tab and, in the table, enter the I/O addresses shown in the picture.
4. Save your project.

4.8.14. Exercise 14: Assigning the ET 200SP Device Name and IP Address



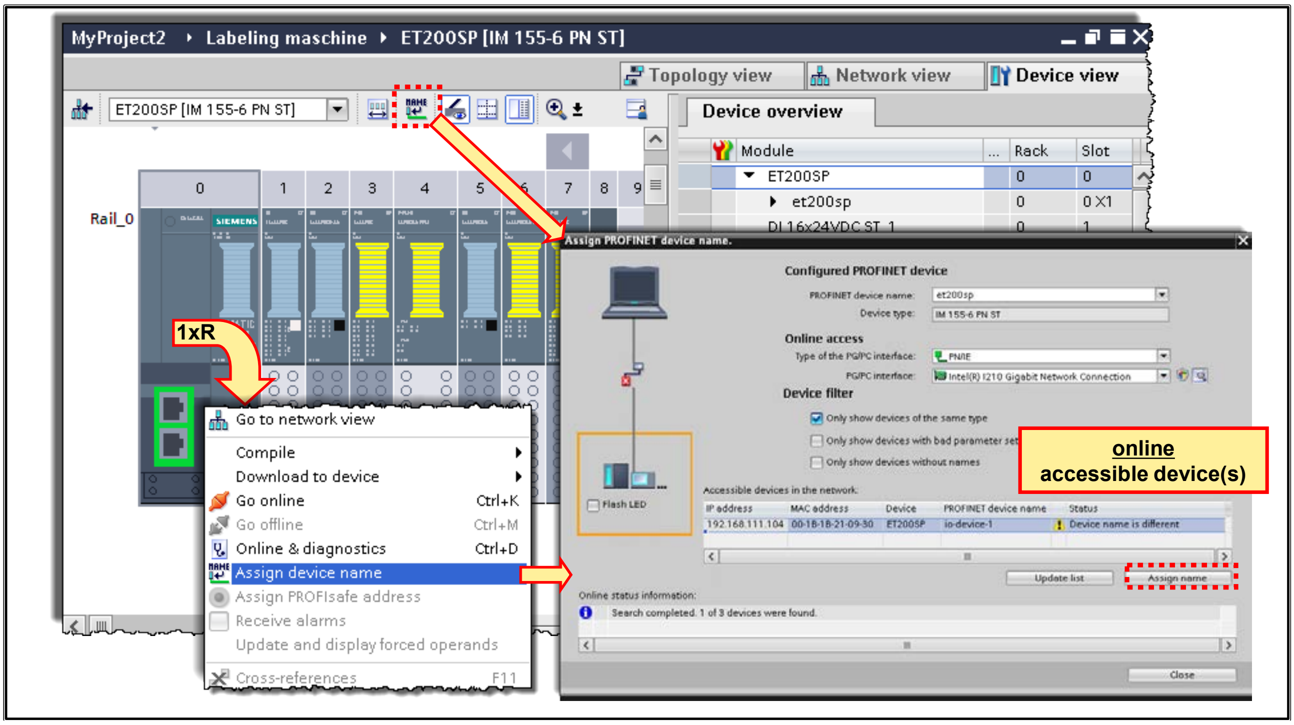
Task

You are to set the IP address, the subnet mask and the PROFINET device name of the ET 200SP.

What to Do

1. In the Hardware and Network editor, select the "Device view" of the ET 200SP.
2. Open the "Device overview" and enter the device name.
3. Select the IM module on Slot 0 and open the "Properties" tab in the Inspector window.
4. Then select the "Ethernet addresses" tab and under "IP protocol" enter a suitable IP address and subnet mask. In the same tab you will also find the PROFINET device name that you previously edited in the "Device overview" tab.
5. Also assign the ET 200SP station to the device group “Labeling machine”.
6. Save your project.

4.8.15. Exercise 15: Assigning the ET 200SP Device Name ONLINE



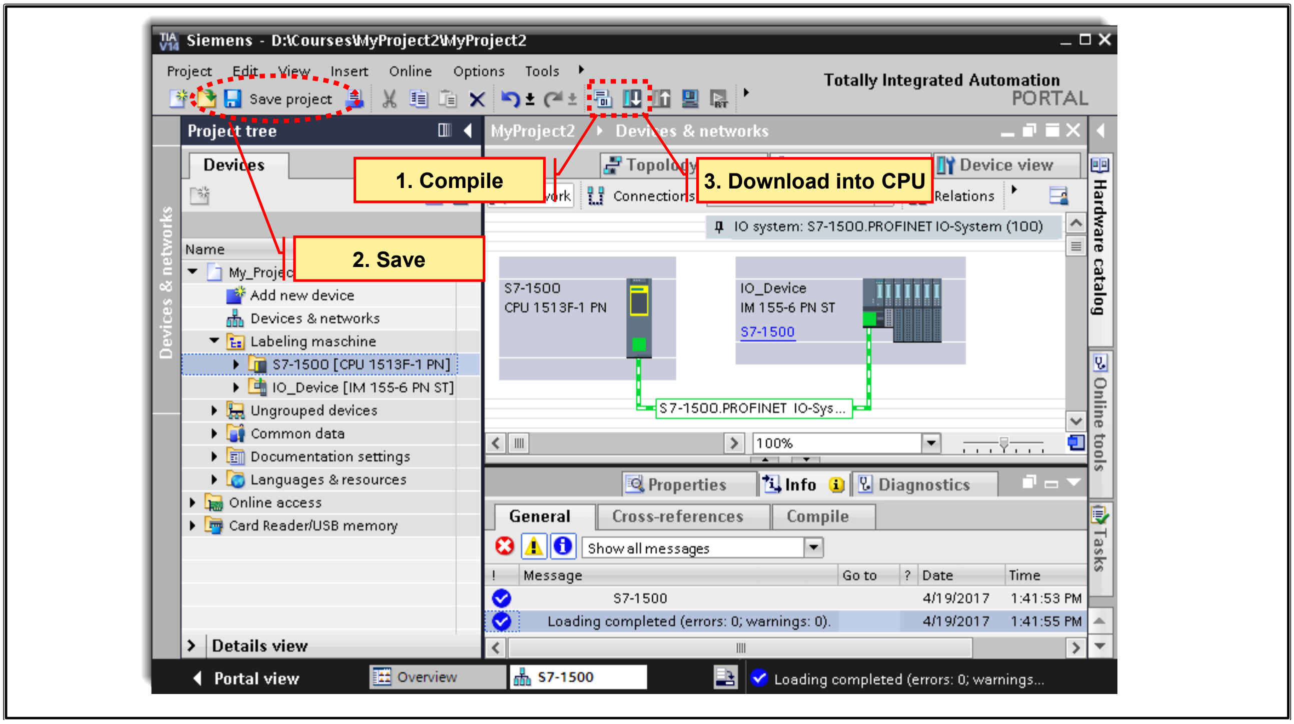
Task

The PROFINET device name previously assigned offline must now be assigned to the ET 200SP online, so that the IO-Controller or the CPU can assign the offline-configured IP address during system startup of the ET 200SP.

What to Do

1. In the Hardware and Network editor, select the "Device view" of the ET 200SP.
2. Right-click on the Interface module or the module on Slot 0 and in the menu that appears, activate the item "Assign device name".
3. In the dialog that appears, check the (offline) PROFINET device name.
4. Under "Type of the PG/PC interface", select the interface through which you are connected to the PROFINET (see picture). Click on "Update list" in order to display all accessible devices.
5. In the lower part of the dialog, under the (online) "Accessible devices in the network", select the ET 200SP or the Interface module IM156-6 and activate "Assign name".

4.8.16. Exercise 16: Compiling the HW Configuration and Downloading it into the CPU



Task

Now that the PROFINET I/O system is completely configured and parameterized, the project must be compiled, saved and downloaded into the CPU.

What to Do

1. Compile the station by selecting the S7-1500 station in the Project tree and then clicking on the Compile button (see picture). In the Inspector window under "Info", check whether the compilation was successful. Should errors have occurred, correct them.
2. Save your project.
3. Download the station into the CPU by clicking on the Download button (see picture). In the Inspector window under "Info", check whether the loading was successful.

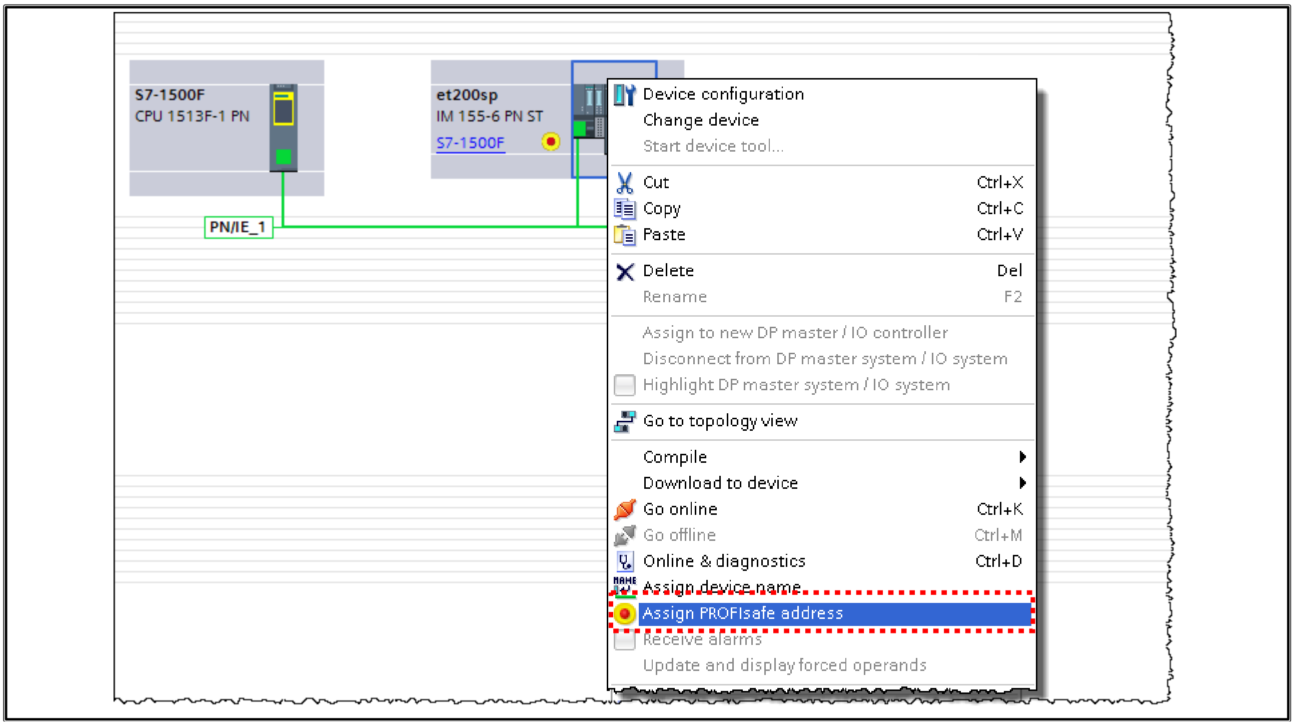
Note:

The buttons “Download” and “Compile” only carry out a download of changes or a compilation of changes. Detailed information on the topic of Downloading and Compiling follows in Chapter 6 “Programming”.

Result:

The ET 200SP should now be accessible but errors could still be pending in some F-modules.

4.8.17. Exercise 17: ET 200SP: Assigning a Fail-safe Address



Task

ET 200SP fail-safe modules do not have a DIP switch for assigning the unique F-destination address for each module. Instead you assign the PROFIsafe address directly in STEP 7.

The fail-safe addresses must be assigned to the ET 200SP online. The assignment occurs via the identification “by LED flashing”.

Note:

It may be that the currently assigned destination address by chance matches your configured destination address. If this is the case, Step 6 cannot be carried out.

What to Do

1. In the "Hardware and network" editor, select the "Device view" of the ET 200SP.
2. Right-click on the ET 200SP station.
3. In the menu that appears, activate the item "Assign PROFIsafe address".
4. In the dialog that appears, on the left-hand side click on the first checkbox of “Assign”.
5. Then click on the button “Identification” to identify the F-destination addresses.
6. In the dialog, on the right-hand side click on the first checkbox of “Confirm” and then on the button “Assign PROFIsafe address”.
7. After the F-destination addresses (PROFIsafe addresses) have been assigned, you can close the dialog.

Result:

If there are still errors pending on modules, this is because the parameterization of channel parameters of individual modules has not yet been adjusted.

The correct parameterization will be done in the next chapter “Sensor-Actuator Connection”.

Contents 5

5. Sensor / Actuator Connection

At the end of the chapter the participant will ...

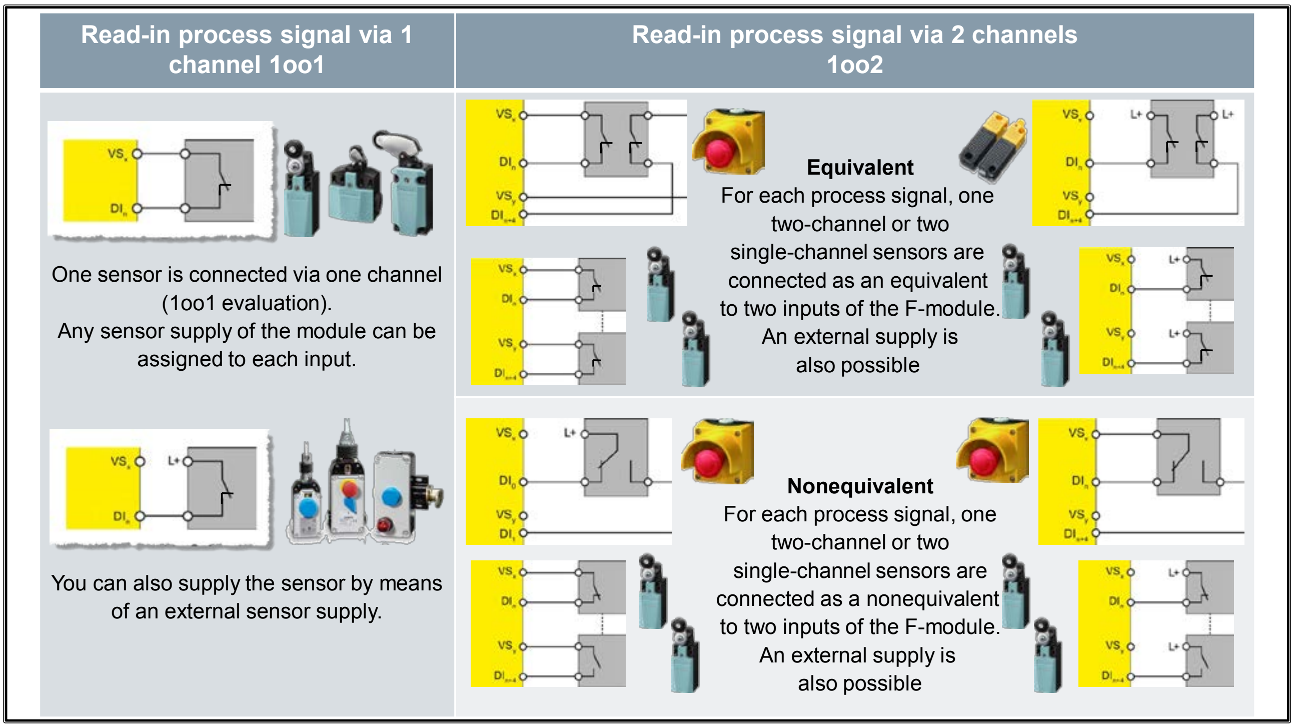
… be able to explain how a sensor is correctly connected and how the module must be parameterized

… be able to explain how an actuator is correctly connected and how the module must be parameterized

… understand and be able to explain the different fault/error detection measures of fail-safe modules

… be able to parameterize the fail-safe input and output modules of the training controller according to the wiring of the training devices

5.1. Overview: Sensor Connection to F-DI Modules



1oo1 Evaluation

For the 1oo1 evaluation, the sensor is present once.

Sensor Supply

The sensor supply can be powered internally or externally.

Connecting a Sensor via 1 Channel

For each process signal, one sensor is connected via one channel (1oo1 evaluation). Any sensor supply of the module can be assigned to each input. If the short-circuit test is not activated or the sensor supply for digital inputs is set to "External sensor supply", you must route the cables in a short circuit-proof manner.

1oo2 Evaluation, Equivalent/Nonequivalent

For equivalent/nonequivalent 1oo2 evaluation, two input channels are occupied by:

- One two-channel sensor
- Two single-channel sensors
- One nonequivalent sensor

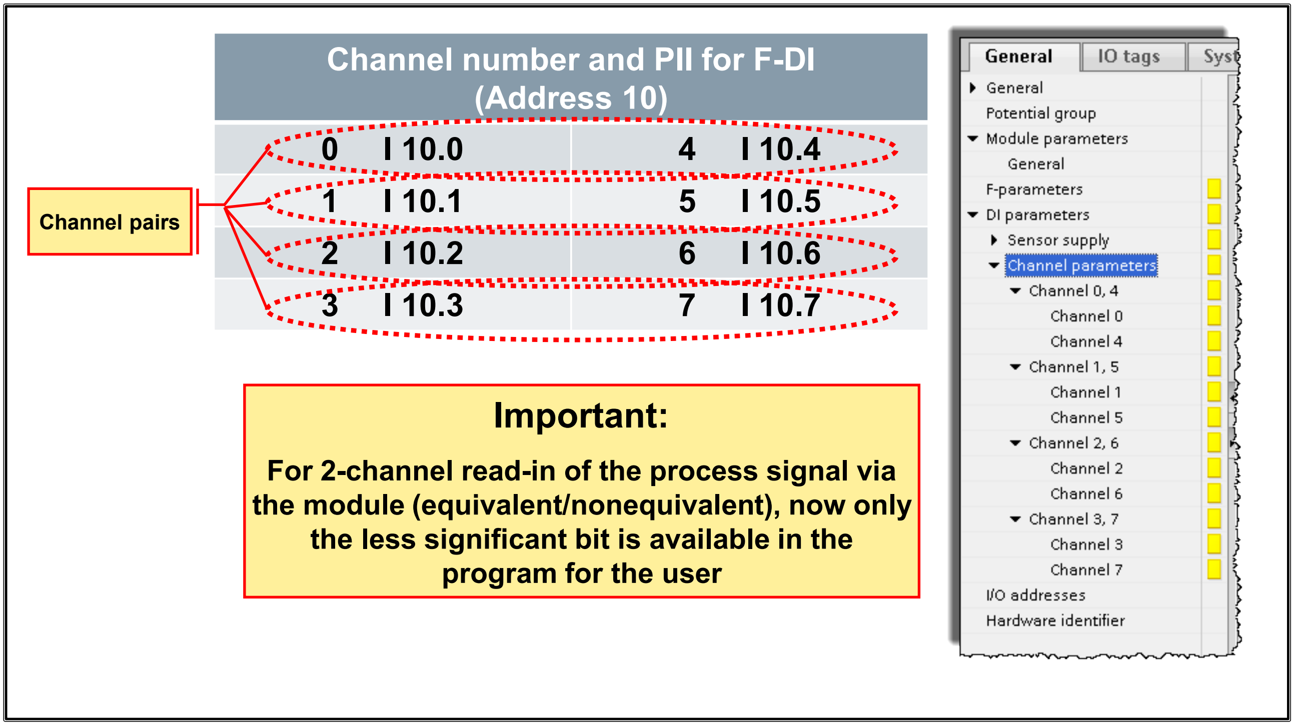
The input signals are compared internally for equivalence or nonequivalence.

Note that for 1oo2 evaluation, two channels are combined into a channel pair. The number of available process signals of the F-module is reduced accordingly.

Wiring Scheme

For each process signal, a two-channel sensor is connected as an equivalent sensor to two inputs of the F-module; or, for each process signal, two single-channel sensors that acquire the same process value are connected to two inputs of the F-module.

5.2. F-DI Module Channel Structure



Channel Pairs and Addresses

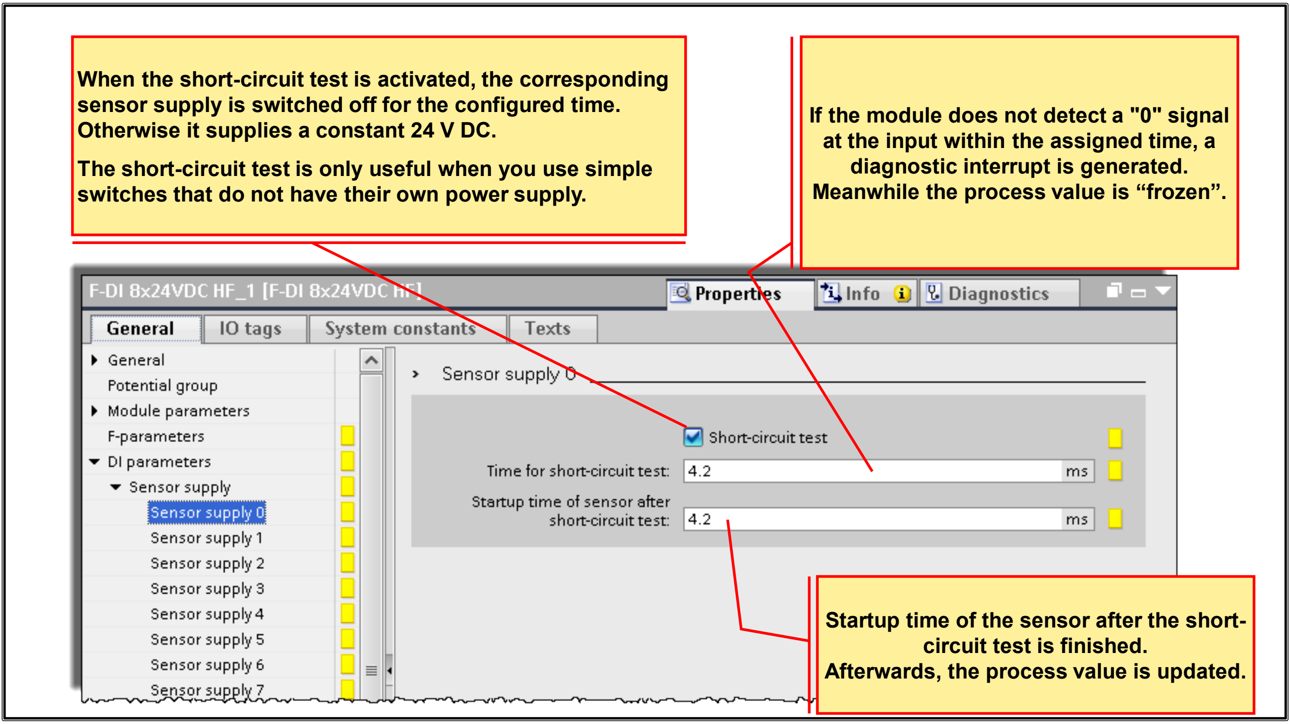
The association of a channel to a channel pair has no relevance for 1-channel sensors and 1oo1 evaluation. Each channel of the channel pair is evaluated independent of the other and has its own separate address (if the module address 16 is set, this would be inputs I 16.0 and I 16.4).

For a 1oo2 evaluation, the sensor signals must be wired to the module channels which can be evaluated by the module as a channel pair or with which it can run a discrepancy analysis (in the picture channel pairs (1;5), as well as (2;6) and (3;7)).

For a 1oo2 evaluation, a channel pair always occupies only the lower input address and only this is available in the program.

5.3. F-DI Parameters

5.3.1. Sensor Supply (1)



Short-circuit Test

Here, you activate the short-circuit detection for the channels of the F-module for which "Internal sensor supply" is set. The short-circuit test is only useful when you use simple switches that do not have their own power supply. For switches with a power supply, for example 3-/4-wire proximity switches, a short-circuit test is not possible.

The short-circuit detection temporarily switches off the sensor supply. The length of the switch-off duration corresponds to the configured "Time for short-circuit test". If a short circuit is detected, the F-module triggers a diagnostic interrupt, and the input is passivated.

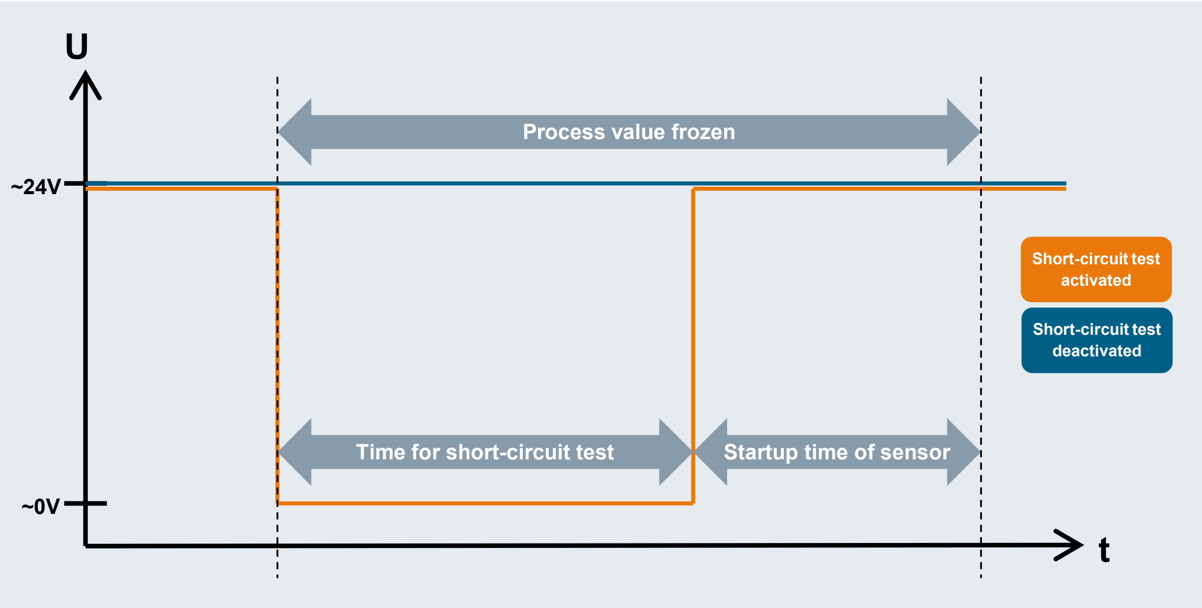
The following short circuits are detected:

- Short-circuit of input to L+
- Short-circuit of the input of another channel if this has a "1" signal
- Short-circuit of the input with sensor supply of another channel
- Short-circuit of the sensor supply with sensor supply of another channel

If the short-circuit test is deactivated, you must route your cables in a short-circuit-proof and cross-circuit-proof manner or select an interconnection type (discrepancy, nonequivalent) that detects cross-circuits also based on discrepancy.

During the execution time of the short-circuit test (time for short-circuit test + startup time of sensor after short-circuit test), the last valid value of the input before the start of the short-circuit test is forwarded to the F-CPU. Activation of the short-circuit test thus affects the response time of the respective channel or channel pair.

5.3.2. Short-circuit Test



Time for Short-circuit Test

When the short-circuit test is activated, the corresponding sensor supply is switched off for the parameterized (assigned) time. If the module does not detect a "0" signal at the input within the assigned time, a diagnostic message is generated.

Observe the following during parameter assignment:

- If the channel is passivated, this can also be caused by too-high capacitance between the sensor supply and input. This is made up of the capacitance per unit length of the cable and the capacitance of the utilized sensor. If the connected capacitance is not discharged within the assigned time, you must adjust the "Time for short-circuit test" parameter.
- The available values for the input delay depend on the "Startup time of sensor after short-circuit test" and the "Time for short-circuit test" of the parameterized sensor supply.

Startup Time of Sensor after Short-circuit Test

In addition to the switch-off time ("Time for short-circuit test"), a startup time must also be specified for implementation of the short-circuit test. By means of this parameter you communicate to the module the amount of time the utilized sensor needs for startup after switching on the sensor supply. In this way, you prevent an undefined input state due to settling processes in the sensor.

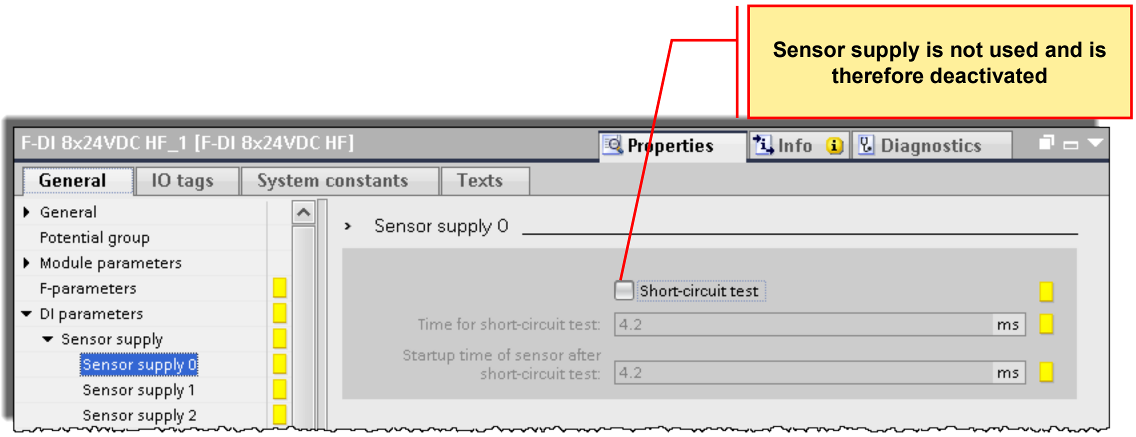
Observe the following during parameter assignment:

- This parameter must be greater than the settling time of the utilized sensor.
- Because the assigned time affects the response time of the module, we recommend that the time be set as small as possible, but large enough that your sensor is reliably settled.
- The available values for the input delay depend on the "Startup time of sensor after short-circuit test" and the "Time for short-circuit test" of the parameterized sensor supply.

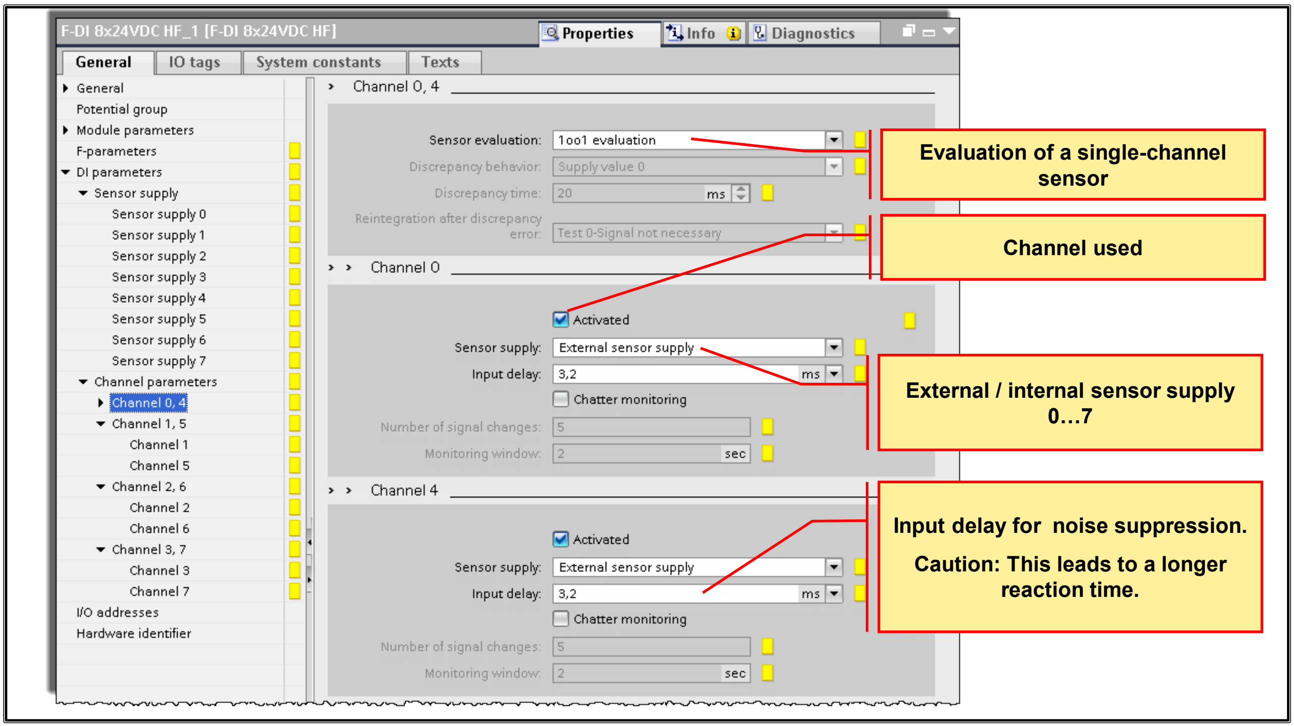
5.3.3. Sensor Supply (2)

Sensor supplies

- Every supply can be used for every input
- If you don't use a supply, it is deactivated



5.3.4. Channel Parameters for Single-channel Evaluation (1)



Activated

Inputs that are not used should be deactivated to lessen the load on the CPU and to allow faster updating of the process image for inputs (PII).

Sensor Evaluation and Interconnection

1oo1 evaluation

For 1oo1 evaluation, there is one sensor and it is connected to the F-DI module via one channel.

If the quality of the sensor is lower than the quality stipulated in the required safety class, redundant sensors connected via two channels must be used.

Sensor Supply

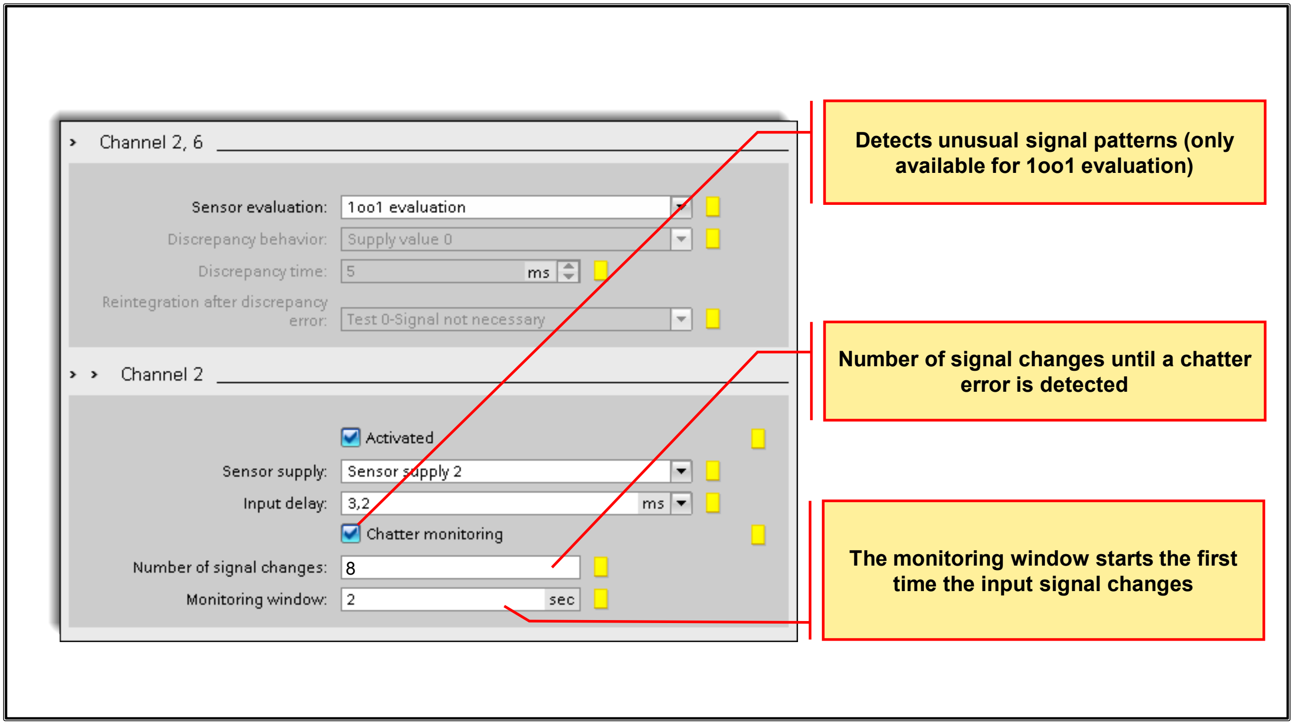
Here, you select between one of the internal sensor supplies VS_0 to VS_n or an external sensor supply. An internal sensor supply must be selected to make use of the short-circuit test.

Input Delay

An input delay is the minimum time that a changed input signal must be present at the module to be detected and encoded as a new signal. The input delay serves to suppress ("debounce") short interference pulses. To suppress coupled-in noise, you can set an input delay time for a channel or a channel pair.

Interference pulses whose pulse time is less than the set input delay time (in ms) are suppressed. Suppressed interference pulses are not visible in the PII. A high input delay suppresses longer interference pulses but also has a longer reaction time as a result. The available values for the input delay depend on the "Startup time of sensor after short-circuit test" and the "Time for short-circuit test" of the parameterized sensor supply.

5.3.5. Channel Parameters for Single-channel Evaluation (2)



Chatter Monitoring

Chatter monitoring is a process control function for digital input signals. During 1oo1 evaluation, it detects and signals unusual process-related signal characteristics, such as too frequent fluctuation of the input signal between "0" and "1". If signal characteristics like these occur, it is a sign that the sensors are faulty or there are process-related instabilities. Each input channel has a parameterized (assigned) monitoring window. The monitoring window is started the first time the input signal changes. If the input signal changes within the monitoring window at least as often as the assigned "Number of signal changes", a chatter error is detected. If no chatter error is detected within the monitoring window, the next signal change restarts the monitoring window. If a chatter error is detected, a diagnostic is signaled. If the chatter error does not occur for a period equal to three times the assigned monitoring window time, the diagnostic is reset.

Number of Signal Changes

This specifies the number of signal changes after which a chatter error is to be signaled.

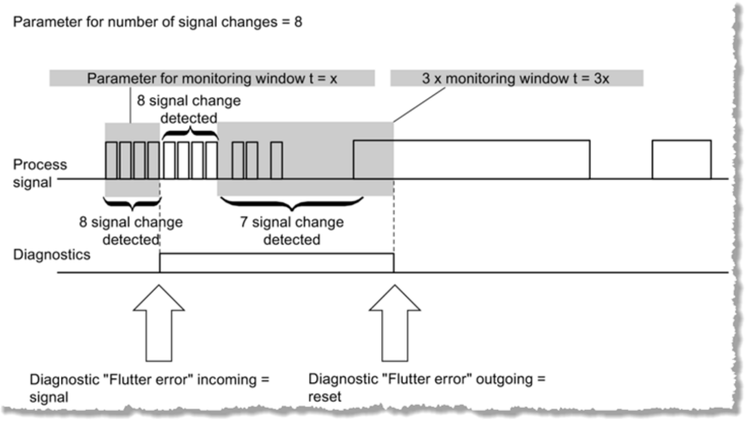
Monitoring Window

This specifies the time for the chatter monitoring window. You can set the monitoring window time from 1 to 100 sec in 1 sec increments. If you set 0 sec, you can parameterize a monitoring window of 0.5 sec.

5.3.6. Chatter Monitoring

Chatter monitoring

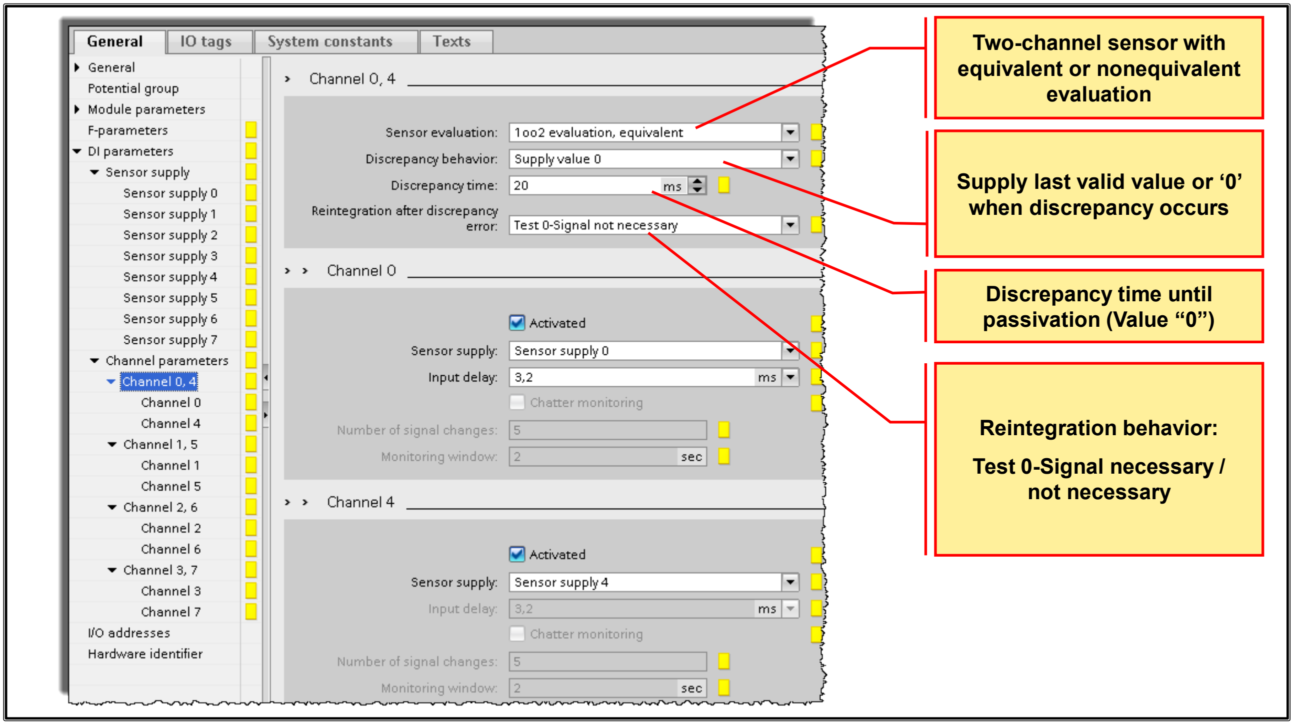
An assigned monitoring window is available for each input channel. The monitoring window starts with the first signal change of the input signal. If the input signal changes within the monitoring window at least as often as the assigned "Number of signal changes", a chatter error is detected. If no chatter error is detected within the monitoring window, the next signal change restarts the monitoring window.



Diagnosis chatter error

If a chatter error is detected, a diagnostic is signaled. If the chatter error does not occur for the monitoring window for three times the configured period, the diagnostic is reset.

5.3.7. Channel Parameters for Two-channel Evaluation



1oo2 Evaluation, Equivalent / Nonequivalent

For equivalent/nonequivalent 1oo2 evaluation, two input channels are occupied by:

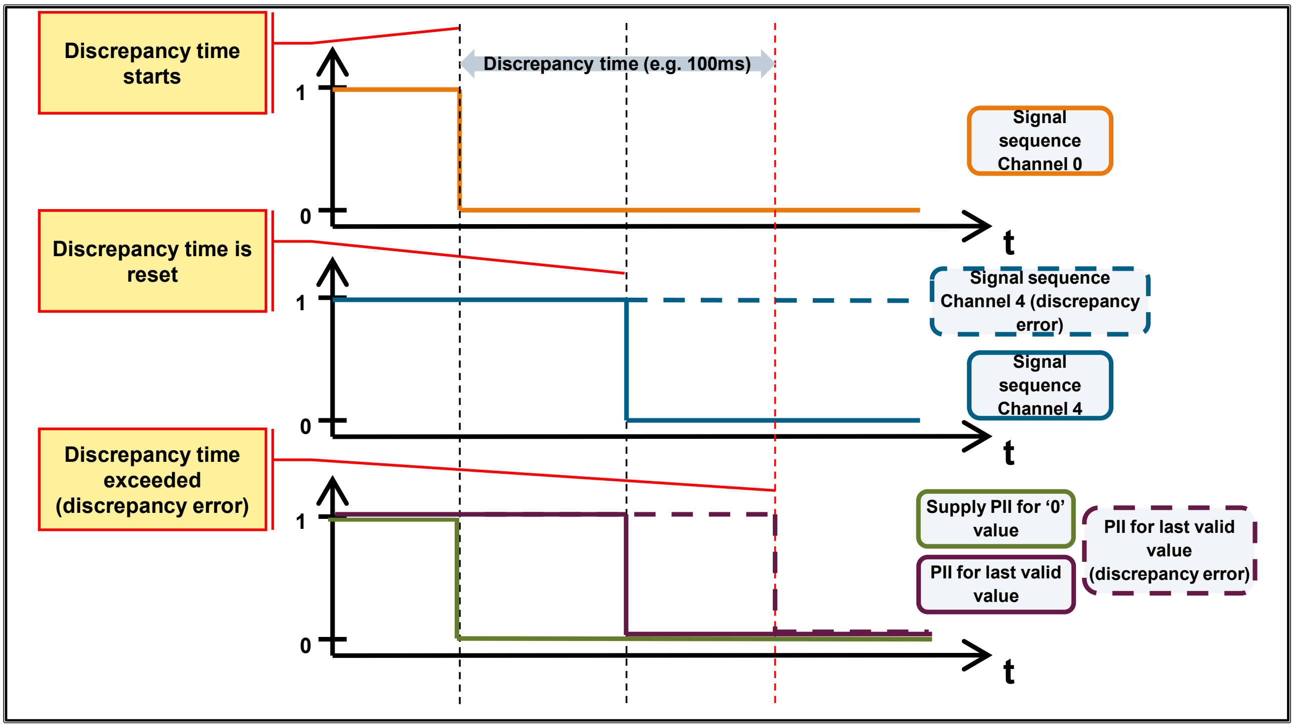
- One two-channel sensor
- Two single-channel sensors
- One nonequivalent sensor

The input signals are compared internally for equivalence or nonequivalence. Note that for 1oo2 evaluation, two channels are combined into a channel pair. The number of available process signals of the F-module is reduced accordingly.

Discrepancy Analysis

When you use a two-channel sensor or two single-channel sensors that acquire (measure) the same physical process variable, the sensors will, for example, respond slightly delayed with respect to each other due to the limited precision of their arrangement. The discrepancy analysis for equivalence/nonequivalence is used in the case of fail-safe inputs in order to infer the presence of faults from the time characteristic of two signals with the same functionality. The discrepancy analysis is initiated if a different level (for nonequivalence check, the same level) is detected for two associated input signals. A test is conducted to determine whether the difference (for nonequivalence check, the agreement) has disappeared after expiration of an assigned time – the so-called discrepancy time. If not, a discrepancy error exists.

5.3.8. Discrepancy Behavior



Discrepancy Behavior

For "Discrepancy behavior" you parameterize (assign) the value that is to be made available to the safety program in the F-CPU during the time that a discrepancy exists between the two input channels involved, which means, when the discrepancy time is running. You assign the discrepancy behavior parameter as follows:

- "Supply last valid value"
- "Supply value 0"

Two settings are possible for the behavior of the module channel while the discrepancy time is running:

"Supply last valid value"

The last valid value (old value) from before the discrepancy occurred is made available to the safety program in the F-CPU as soon as a discrepancy is detected between the signals of the two input channels involved. This value is provided until the discrepancy has disappeared, or until the discrepancy time has expired and a discrepancy error is detected. After expiration of the discrepancy time, the value '0' is always signaled to the safety program of the CPU if a discrepancy error is detected!

Caution:

Because a discrepancy error is only detected after the discrepancy time has elapsed, the reaction time of the controller is prolonged. If very fast PLC reactions to fault conditions are required for safety reasons, the discrepancy time should be set no longer than is actually necessary.

"Supply value 0"

Because, with this setting, the "safe" value "0" is already signaled to the safety program of the F-CPU while the discrepancy time is running, the reaction time of the PLC is not increased. This is because the value "0" is the value that is signaled to the CPU anyway under a fault condition (after the discrepancy time has elapsed).

Discrepancy Time

The discrepancy behavior is only relevant while the discrepancy time is running! If the discrepancy is still present even after expiration of the discrepancy time, the module detects this as an error and signals the value "0" to the F-CPU for the channel involved (same as always under a fault condition).

In most cases, the discrepancy time is started, but does not fully expire because the signal differences disappear again after a short time.

For equivalence check: Select a discrepancy time of sufficient length so that, under fault-free conditions, the difference between the two signals always disappears before the discrepancy time has expired.
For nonequivalence check: Select a discrepancy time of sufficient length so that, under fault-free conditions, the agreement of the two signals always disappears before the discrepancy time has expired.

Behavior while Discrepancy Time is Running

While the assigned discrepancy time is running internally on the module, either the ‘last valid value’ or "0" is provided to the safety program in the F-CPU by the input channels involved, depending on how the discrepancy behavior is parameterized.

Behavior after Expiration of Discrepancy Time

For equivalence check: If, after expiration of the assigned discrepancy time, the input signals do not agree, for example, due to wire break on a sensor line, a discrepancy error is detected and the "Discrepancy error" diagnostic message is generated with information on the faulty channels.
For nonequivalence check: If, after expiration of the assigned discrepancy time, the input signals do not differ, for example, due to wire break on a sensor line, a discrepancy error is detected and the "Discrepancy error" diagnostic message is generated with information on the faulty channels.

Reintegration after Discrepancy Error

With this parameter you define when a discrepancy error is regarded as eliminated, thus enabling reintegration of the input channels involved. You have the following parameter assignment options:

- "Test 0-Signal necessary"
- "Test 0-Signal not necessary"

Requirements

You have assigned parameters as follows:

"Sensor evaluation"**:** "1oo2 evaluation, equivalent" OR "1oo2 evaluation, nonequivalent"

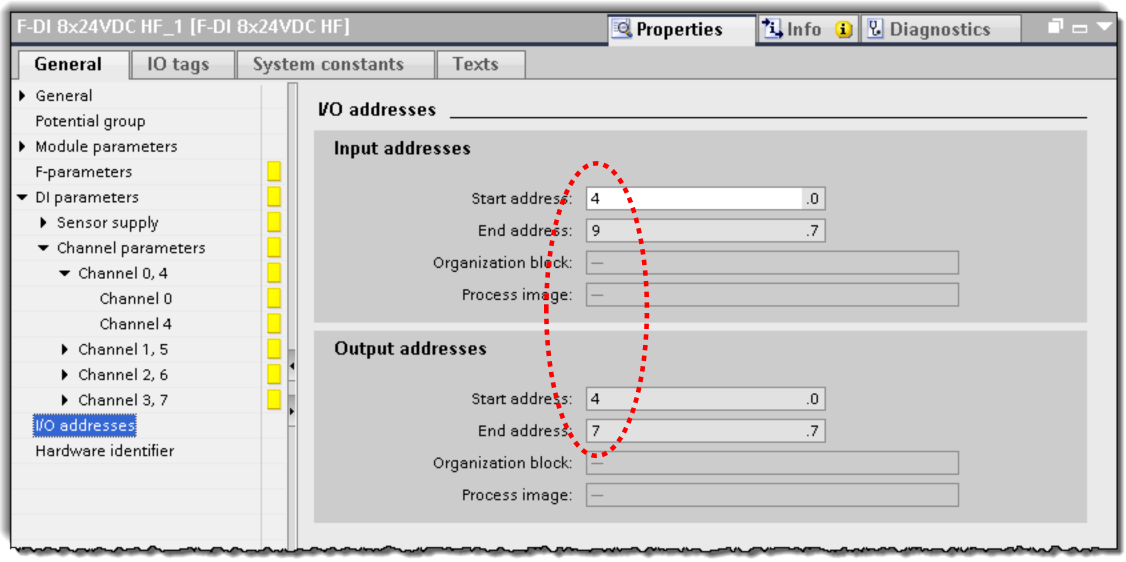
"Test 0-Signal Necessary"

If you have assigned "Test 0-Signal necessary", a discrepancy error is only regarded as eliminated when a 0 signal is once again present at both input channels involved. If you are using nonequivalent sensors, that is, you have set the "Sensor evaluation" to "1oo2 evaluation, nonequivalent", a 0 signal must once again be present at the lower-order channel of the channel pair.

"Test 0-Signal Not Necessary"

If you have assigned "Test 0-Signal not necessary", a discrepancy error is regarded as eliminated when a discrepancy no longer exists at both input channels involved.

5.3.9. I/O Addresses



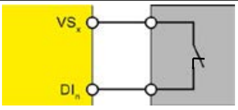
Addresses of Inputs and Outputs

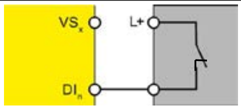
Just as for standard modules, the addresses of fail-safe input and output modules can be freely set by the user. In addition to the standard input and output user data, the fail-safe input or output modules occupy additional bytes in the process image for inputs and process image for outputs for processing safety-related PROFIsafe communication. An F-DI module therefore also occupies bytes in the process image for outputs, and an F-DQ module also occupies bytes in the process image for inputs. You may only access the addresses occupied by user data and value status. The other address ranges occupied by the F-modules are assigned, among other things, for safety-related communication between the F-modules and F-CPU in accordance with PROFIsafe. For 1oo2 evaluation of the sensors, the two channels are combined. For 1oo2 evaluation of the sensors, you may only access the low-order channel in the safety program.

Process Image

In addition to the process images PII and PIQ that are updated automatically by the operating system, up to 15 process image partitions (PIP) can be parameterized (CPU-specific, PIP 1 to max. PIP 15). Thus it is possible, independent of the cyclically updated OB1 process image (OB1-PI), to update process image partitions (PIP) depending on the execution of interrupt OBs. Each I/O address range or each input module and output module can be assigned to only one process image partition. If a module is assigned to one of the process image partitions (PIP), then the module can no longer be part of the cyclic process image (OB1-PI).

5.3.10. Example: Reading-in a Process Signal via 1 Channel 1oo1 up to SIL3/Cat.3/PLd





Error detection / Error	Internal Vs and short-circuit test activated	Internal Vs and short-circuit test deactivated	External sensor supply
Short-circuit of input with other channels or sensor supplies	YES*	NO	NO
Short-circuit with L+ at DI	YES	NO	NO
Short-circuit with M at DI	YES*	YES*	NO
Short-circuit with L+ at VS	YES	NO	-
Short-circuit with M at VS or defect	YES	YES	-
Discrepancy error	-	-	-

*)The error detection only occurs with a signal distortion. That is, the signal read differs from the sensor signal.
If there is no signal distortion vis-à-vis the sensor signal, no error detection is possible and is also not necessary from a safety point of view.

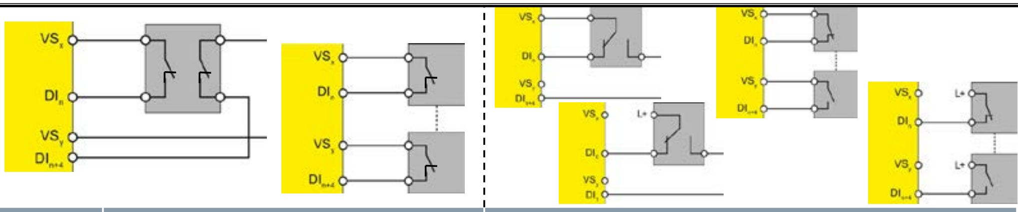
Warning: If the short-circuit test is not activated or the sensor supply for digital inputs is set to "External sensor supply“, you must route your cables in a short-circuit-proof manner.

Warning: In order to achieve SIL3/Cat.3/PLd with this wiring, a suitably qualified sensor is necessary.

Sensor Use

When fail-safe input modules are used, the substitute value '0' is forwarded to the CPU after faults are detected, which causes the safety program to execute a safe reaction. Therefore, be aware that the sensors must also be implemented in such a way that they supply a 0 signal if the safety program is to execute the safe reaction.

5.3.11. Example: Reading-in a Process Signal via 2 Channels 1oo2 up to SIL3/Cat.4/PLe



Error detection / Error	Equivalent evaluation	Nonequivalent evaluation
Short-circuit of channel pair, with other channels or other sensor supplies	YES*	YES
Short-circuit with L+ at DI	YES* / YES(if short-circuit test active)	YES* / YES (if short-circuit test active)
Short-circuit with M at DI	YES*	YES*
Short-circuit with L+ at VS	YES	YES (if used)
Short-circuit with M at VS or defect	YES	YES (if used)
Discrepancy error	YES	YES

*) The error detection only occurs with a signal distortion. That is, the signal read differs from the sensor signal (discrepancy error).

If there is no signal distortion vis-à-vis the sensor signal, no error detection is possible and is also not necessary from a safety point of view.

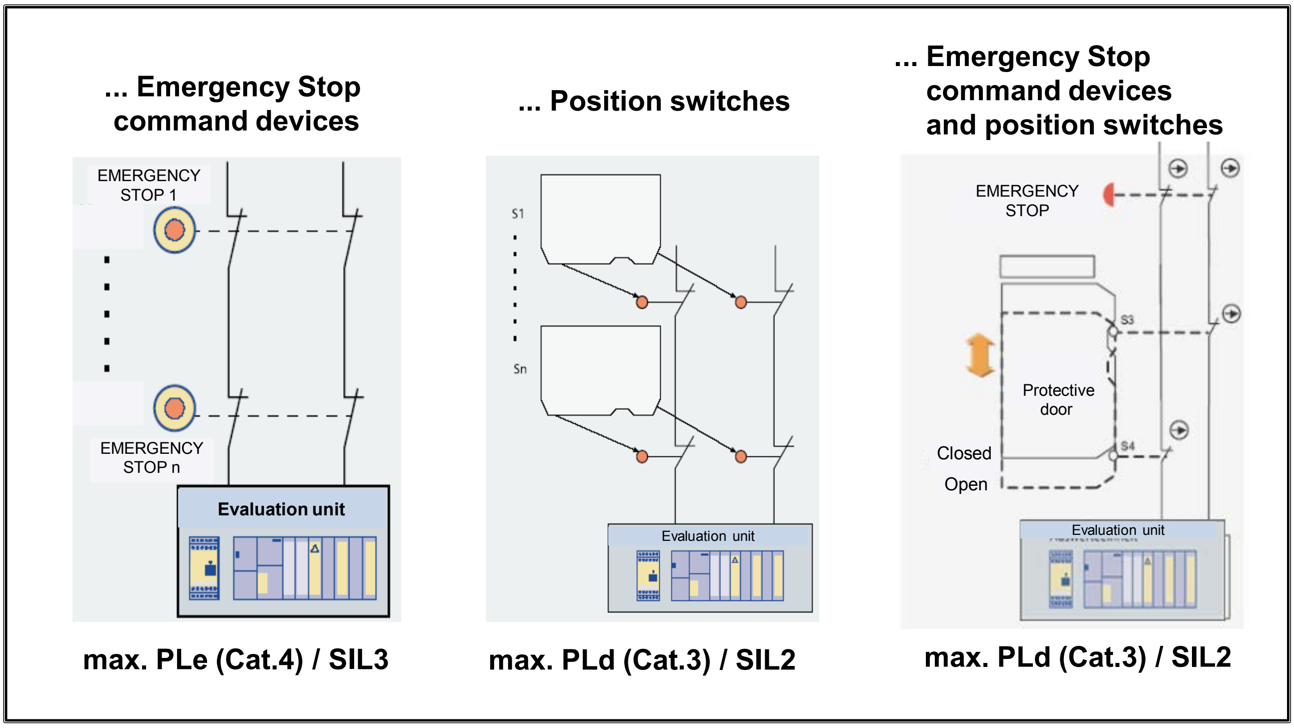
Warning: In order to achieve SIL3/Cat.4/PLe with this wiring, a suitably qualified sensor is necessary.

Nonequivalent Sensor

If a nonequivalent sensor is used for the shutdown, its normally closed contact must be wired to the lower channel address of the input module so that the 0 signal can be evaluated in the safety program when the button is actuated.

If the nonequivalent sensor is used as an enabling button, its normally open contact must be wired to the lower channel address of the input module so that the 1 signal can be evaluated in the safety program when the button is actuated.

5.3.12. Series Connection of Sensors



Series connection

In general, sensors can be connected in series in all categories.

Cat.4 / PLe / SIL3 requires, however, that

– every fault is detected

and

– an accumulation of faults does not lead to loss of the safety function.

... of Emergency Stop command devices:

Emergency Stop command devices may be connected in series **up to Cat.4 / PLe / SIL3**: The failure and/or simultaneous pressing of the command devices can be ruled out.

... of position switches:

Up to Cat.3/PLd/SIL2, position switches (e.g. safety door monitoring) may be connected in series unless several safety doors are simultaneously opened on a regular basis (as otherwise fault detection is not possible).

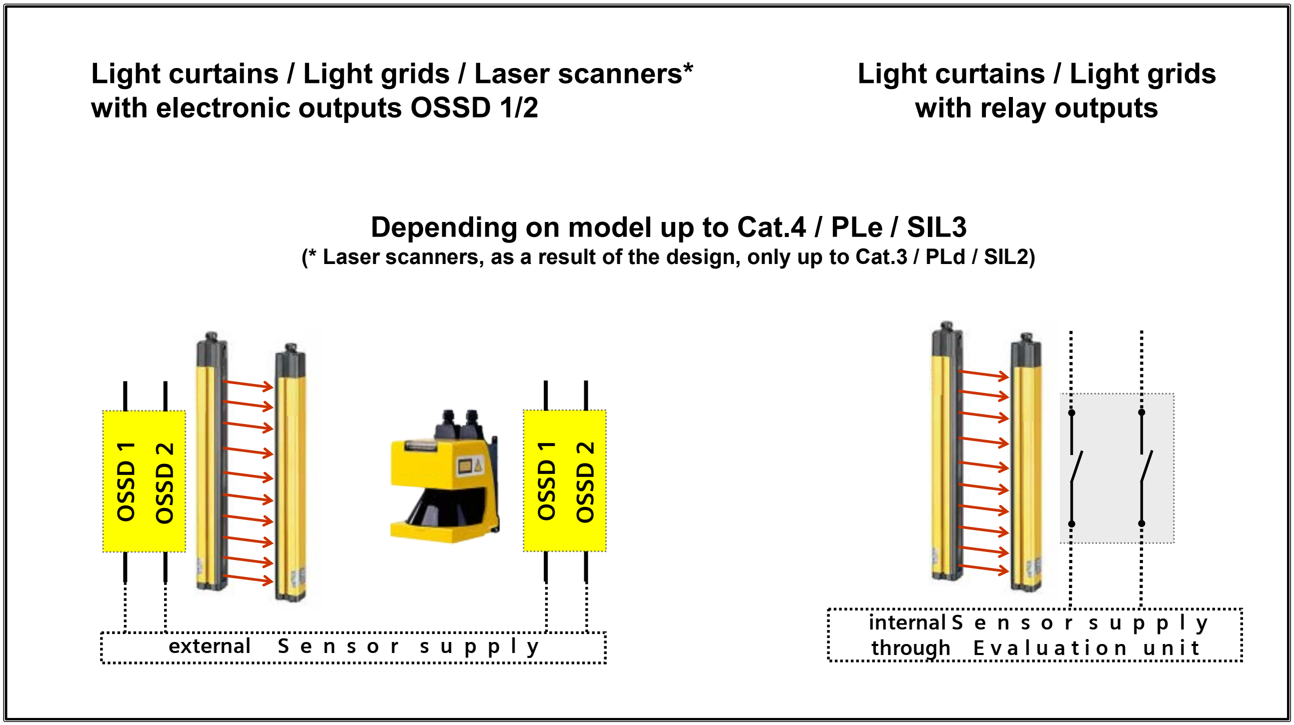
In Cat.4/PLe/SIL3, position switches must never be connected in series because, in this case, every hazardous fault must be detected (independent of operating personnel).

... of Emergency Stop command devices and position switches:

Up to Cat.3/PLd/SIL2, position switches (e.g. safety door monitoring) and Emergency Stop command devices may be connected in series unless several safety doors or Emergency Stop command devices are simultaneously actuated on a regular basis (as otherwise fault detection is not possible).

In Cat.4/PLe/SIL3, position switches and Emergency Stop command devices must never be connected in series because, in this case, every hazardous fault must be detected (independent of operating personnel).

5.3.13. Examples for Connection of Electro-sensitive Protective Equipment: Light Curtains / Grids / Laser Scanners



Electro-sensitive Protective Equipment

- **...with electronic outputs**

Sensors with OSSD outputs (Output Signal Switching Device – outputs) have an integrated cross-circuit / short-circuit detection. On the part of the evaluation unit, this must therefore be deactivated (for F-DI modules in the HW Config).

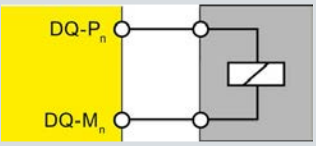
- **...with relay outputs**

Sensors with relay outputs cannot achieve cross-circuit / short-circuit detection due to their isolated contacts.

For Cat.4 / PLe / SIL3 applications, the cross-circuit / short-circuit detection must therefore be activated on the part of the evaluation unit (for F-DI modules in the device configuration).

5.4. Overview: Actuator Connection to F-DO Modules

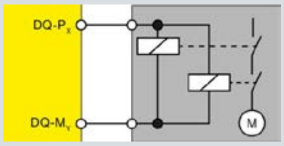
Connection of one load per output

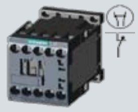


Each of the 4 fail-safe digital outputs consists of one P-switch (DQ-P) and one M-switch (DQ-M). You connect the load between the P-switch and the M-switch. So that voltage is applied to the load, both switches are always energized.

Connection of two loads per output

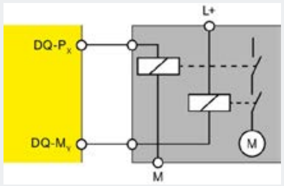
Recommended





Parallel to P and M

In order to manage cross-circuits between the P and M-switch of a fail-safe digital output, both relays are connected in parallel to P and M.

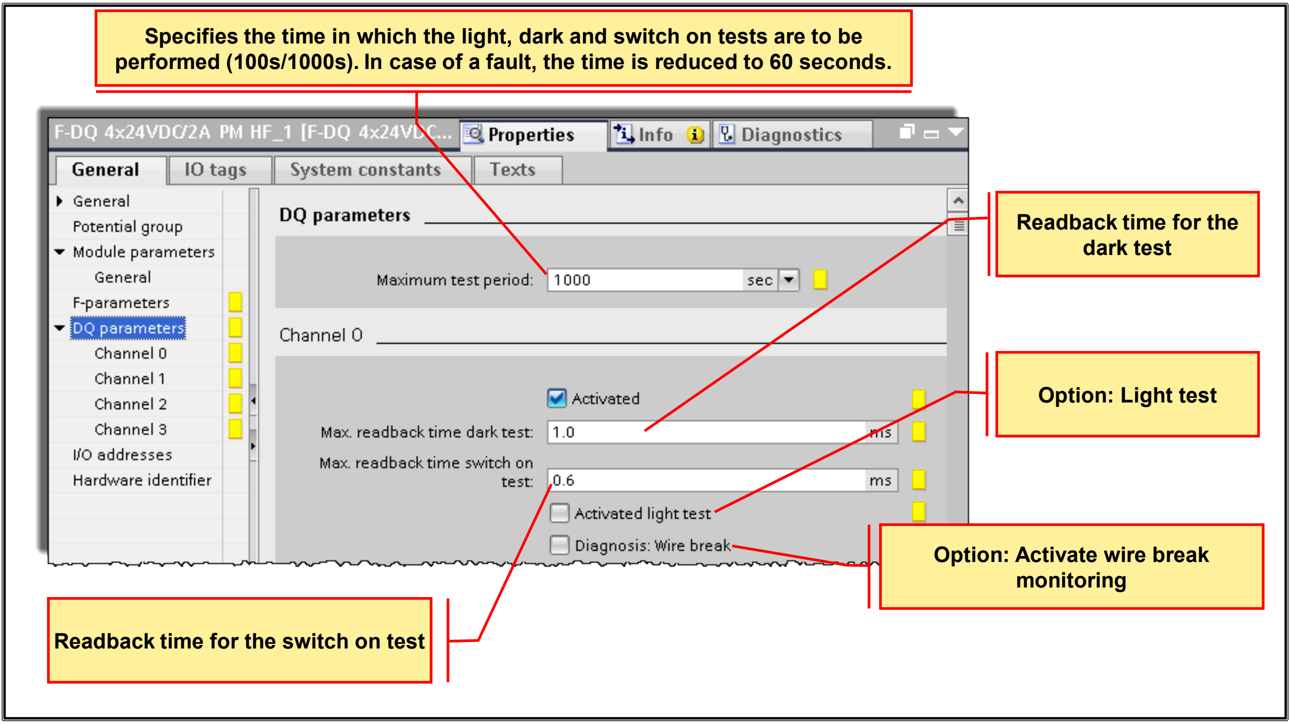


to L+ and M

You can switch two relays with one fail-safe digital output. Make sure that the same reference potential is used and that the NO contacts of both relays are switched in series.

5.5. F-DQ Parameters

5.5.1. Channel Parameters (1)



Maximum Test Period

With this parameter, you specify the time within which the light, dark and switch-on tests (complete bit pattern test) occur module-wide. The tests are repeated after expiration of this time. Under fault conditions, the test period is shortened to 60 seconds.

- Use "1000 s", for example, to reduce wear and tear on your actuators.
- Use "100 s" to detect errors faster.

Activated

If you select this check box, you activate the corresponding channel for signal processing in the safety program. You can deactivate an unused channel with this parameter.

Readback Time

The readback time is the maximum time after switching off the output that a feedback signal can still be detected before the "short-circuit" error triggers passivation of the output channel. The readback time must be set long enough, especially when capacitive loads are being switched, to allow the discharge of the switched capacitance within the readback time.

The readback time is also the dark period for shutdown tests. For checking the actuator wiring, 0 signals are switched to the output while the output is active. A sufficiently slow actuator does not respond to the temporary switch-off of the output and remains switched on.

Activated Light Test

Overload and wire break are detected by a 0 signal at the output. During the light test, a test signal is switched to the output channel while the output channel is inactive (output signal "0"). The output channel is then switched on briefly (= "light period") and read back. A sufficiently slow actuator does not respond to this and remains switched off.

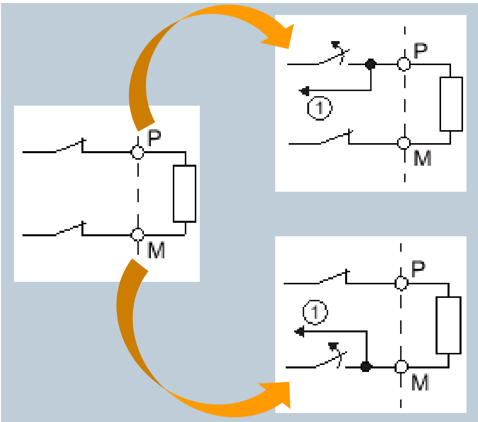
Diagnosis: Wire Break

You use a wire-break check for monitoring the connection from the output channel to the actuator. When you select the check box, you activate the wire break monitoring for the corresponding channel. In order to detect a wire break when the output signal is "0", you must activate the light test.

5.5.2. Dark Test

Dark test

- The dark test is part of the bit pattern test.
- A test signal is switched to the output channel while the output channel is active ("1").
- The output channel is then briefly deactivated (= "dark period") and read back.
- A sufficiently slow actuator does not respond to this and remains switched on.



"Max. readback time dark test" must be set as low as possible but high enough so that the output channel is not passivated.

The dark test detects the following faults:

- ✓ Short-circuit P to L+
- ✓ Short-circuit M to ground
- ✓ Cross-circuit

① Readback

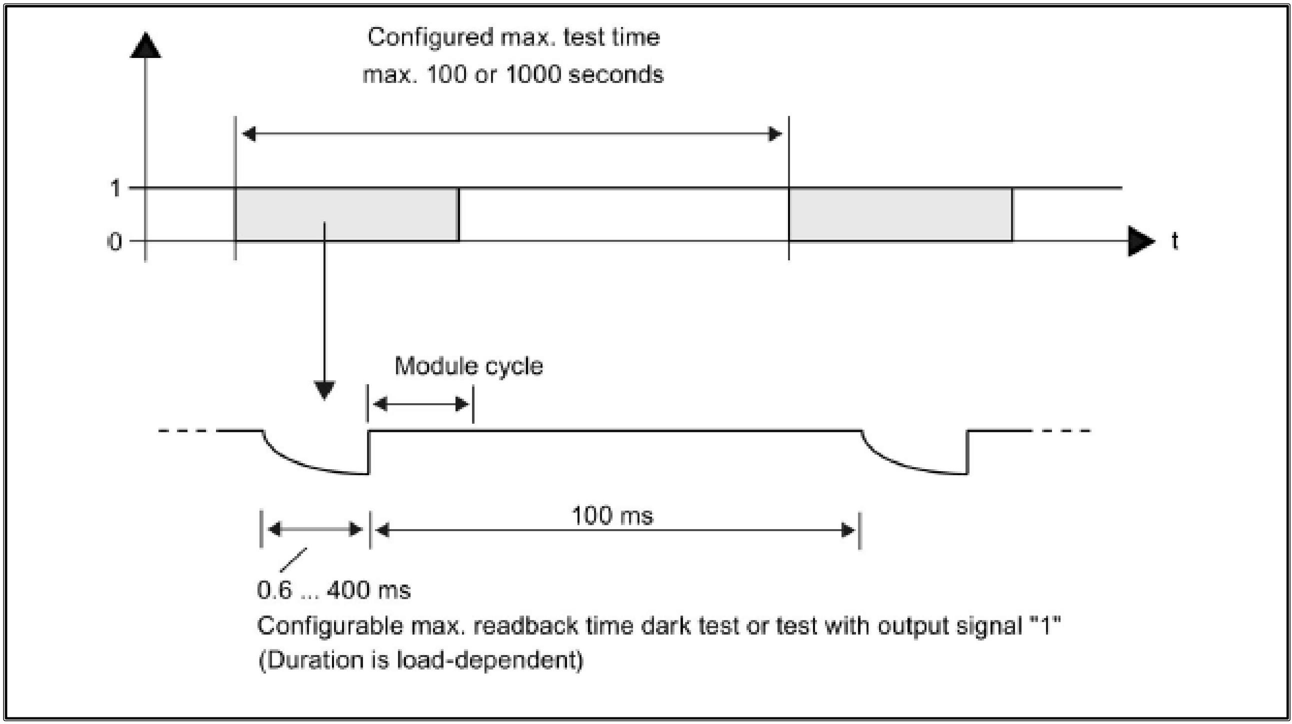
Max. Readback Time Dark Test

Dark tests are switch-off tests during the bit pattern test. During the dark test, a test signal is switched to the output channel while the output channel is active (output signal "1"). The output channel is then switched off briefly (= "dark period") and read back. A sufficiently slow actuator does not respond to this and remains switched on. If, after expiration of the readback time of the dark test, the expected signals (P-readback and M-readback) could not be correctly read back, the output channel is passivated. While a bit pattern is active (switch test is being performed), no new process values are switched to the output channels. Consequently, a higher "Max. readback time dark test" setting increases the reaction time of the F-module. The parameter also affects the detection of a short-circuit (cross-circuit) with "1" signal at the change of the output signal from "1" to "0" by the safety program.

Setting the Readback Time Dark Test

Because the fault reaction time is extended by the amount of the readback (dark test) period, we recommend that you use trial and error to set the readback time dark test as low as possible but high enough that the output channel is not passivated. Determine the readback time required for your actuator from the diagram in section "Switching of capacitive loads". If the capacitance of the actuator is not known, you may have to carefully find the value for the readback time light test through trial and error. This may also be necessary due to component variation in the actuator or external influences.

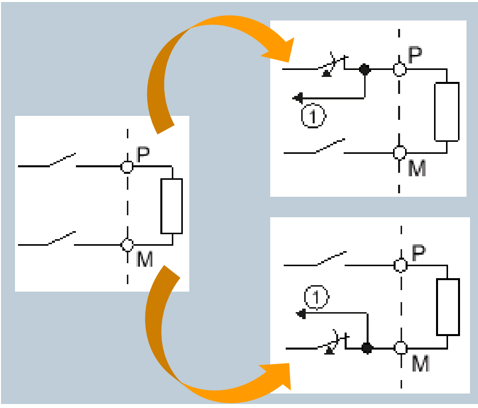
5.5.3. Dark Test Signal Sequence



5.5.4. Switch-on Test

Switch on test

- The switch on test is part of the bit pattern test.
- During the switch on test, the **P-switch and the M-switch** of the output channel **are alternately closed** and read back when the output channel is inactive ("0").
- Unlike the light test, no current flows through the connected load during the test.



① Readback

"Max. readback time switch on test" must be set as low as possible but high enough so that the output channel is not passivated.

The switch on test detects the following faults:

- ✓ Short-circuit P to L+
- ✓ Short-circuit M to ground
- ✓ Cross-circuit

Max. Readback Time Switch On Test

The switch-on test is part of the bit pattern test. During the switch-on test, the P-switch (current-sourcing switches) and M-switch (current-sinking switch) of the output channel are closed and read back alternately when the output channel is inactive (output signal "0"). Unlike the light test, no current flows through the connected load during the switch-on test. If the signal could not be correctly read back after expiration of this time, the output channel is passivated.

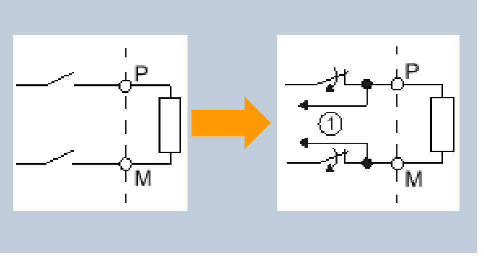
The switch-on test detects the following faults:

- Short-circuit to L+ when output signal is "0"
- Short-circuit to M when output signal is "0"

5.5.5. Light Test

Light test

- A test signal is switched to the output channel while the output channel is inactive ("0").
- The output channel is switched on briefly during the light test and read back. A sufficiently slow actuator does not respond to this and remains switched off.
- Unlike the switch on test, **the P-switch and the M-switch switch simultaneously** during the light test and **current flows through the connected load**.



The light test detects the following faults:

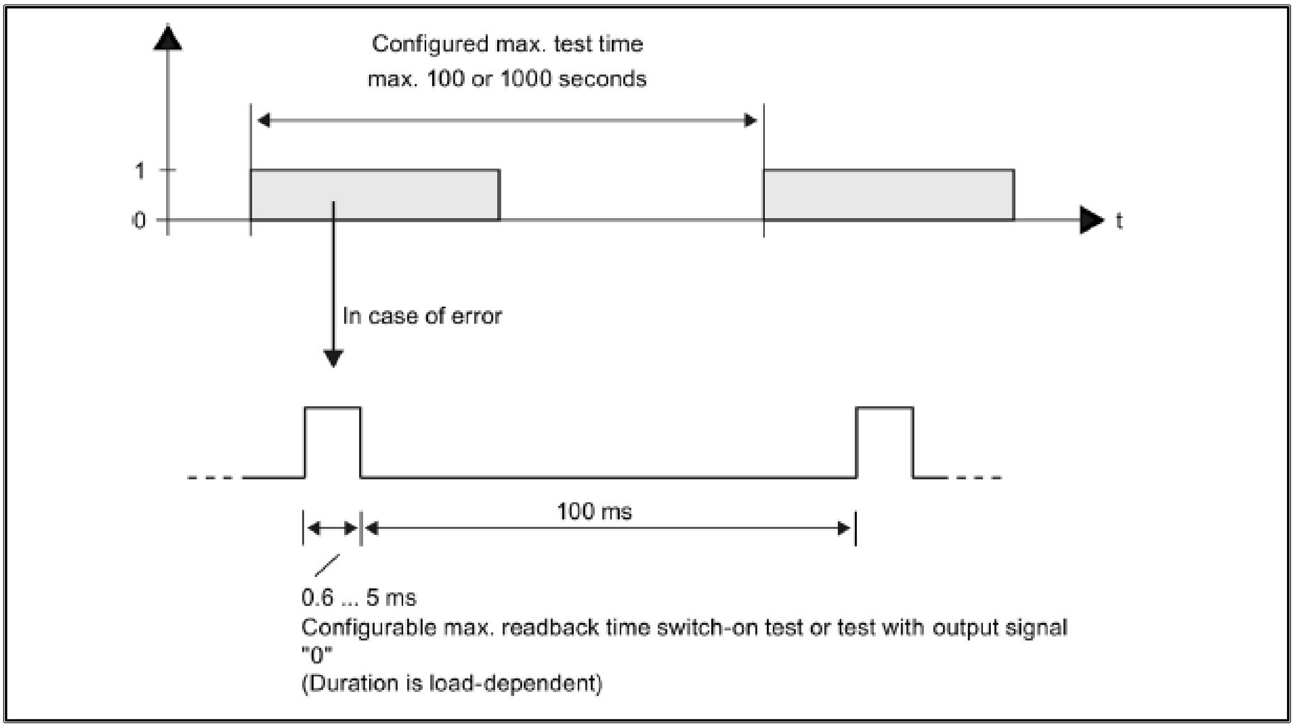
- ✓ Overload with a "0" signal at the output
- ✓ Wire break with a "0" signal at the output

① Readback

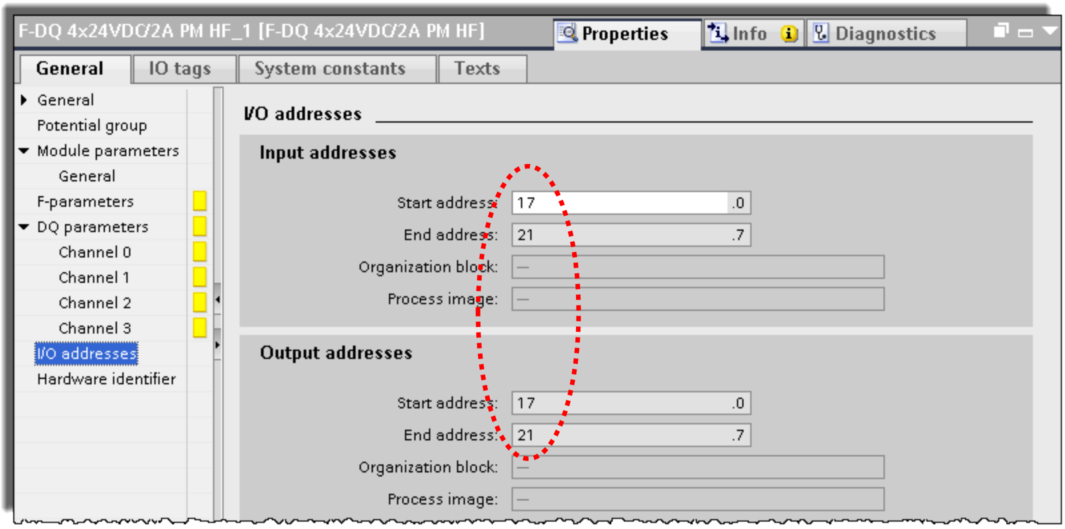
Activated Light Test

During the light test, a test signal is switched to the output channel while the output channel is inactive (output signal "0"). The output channel is then switched on briefly (= "light period") and read back. A sufficiently slow actuator does not respond to this and remains switched off. Unlike the switch-on test, P-switch (current-sourcing switches) and M-switch (current-sinking switch) switch simultaneously during the light test and current flows through the connected load. In case of faulty readback signals, the signal is present at the output channel for the assigned readback time before the fault triggers passivation of the output channel. While a bit pattern is active (switch test is being performed), no new process values are switched to the output channels. Consequently, a higher "Max. readback time switch-on test" setting increases the reaction time of the F-module. For each output channel, a light pulse with assigned duration occurs within the assigned maximum test time. When a light pulse detects a fault, the same light pulse (i.e. the same bit pattern) is repeated once after 100 ms. If the fault persists, the maximum test time is automatically shortened to 60 seconds and a diagnostic message is generated. If the error no longer exists, the output channel is reintegrated after the next fault-free test cycle.

5.5.6. Light Test Signal Sequence



5.5.7. I/O Addresses



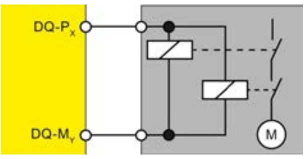
Addresses of Inputs and Outputs

Just as for standard modules, the addresses of fail-safe input and output modules can be freely set by the user. In addition to the pure input and output user data, the fail-safe input or output modules occupy additional bytes in the process image for inputs and process image for outputs for processing safety-related PROFIsafe communication. An F-DI module therefore also occupies bytes in the process image for outputs, and an F-DQ module also occupies bytes in the process image for inputs. You may only access the addresses occupied by user data and value status. The other address ranges occupied by the F-modules are assigned, among other things, for safety-related communication between the F-modules and F-CPU in accordance with PROFIsafe.

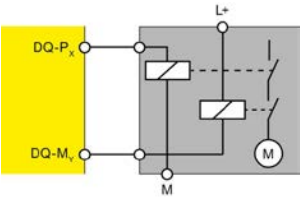
For 1oo2 evaluation of the sensors, the two channels are combined.

For 1oo2 evaluation of the sensors, you may only access the low-order channel in the safety program.

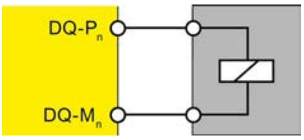
5.5.8. Example: Actuator Connection up to SIL3/Cat.4/PLe



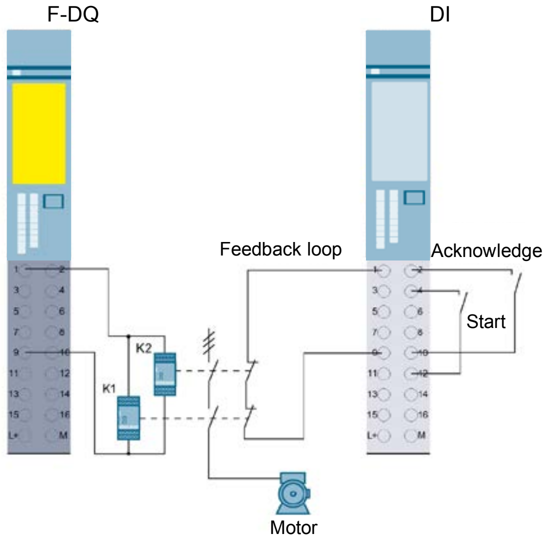
A "wire break" fault is only detected if the wire break disconnects both relays from P or M.



With a cross-circuit between the P-switch and the M-switch of the output, the module detects the fault and disables the output. However, because of the external fault, the actuator continues to be supplied with current. ->route the cables in a cross-circuit-proof manner



In order to achieve SIL3/Cat.4/PLe with this wiring, a suitably qualified actuator, for example in accordance with IEC 60947, is required.



Caution!

You must always install a feedback loop / feedback which monitors for a possible actuator failure!

Connection of Two Loads in Parallel for each Digital Output

In order to manage cross-circuits between the P-switch (current-sourcing switches) and M-switch (current-sinking switch) of a fail-safe digital output, we recommend the lower wiring version in the picture. With this circuit, you achieve SIL3/Cat.4/PLe.

Connection of Loads for each Digital Output to L+ and M

You can switch 2 relays with one fail-safe digital output. Pay attention to the following conditions:

- Same reference potential
- The NO contacts of both relays must be switched in series.

With this circuit, you achieve SIL3/Cat.4/PLe (process status readback required). When two relays are connected to one digital output (as in the picture above), the "wire break“ and "overload" faults are only detected at the P-switch of the output (not at the M-switch).

With a cross-circuit between the P-switch and the M-switch of the output, the module detects the fault and disables the output. However, because of the external fault, the actuator continues to be supplied with current. To prevent short-circuits between the P-switch and the M-switch of a fail-safe digital output, you must route the cables used to connect the relays to the P-switch and M-switch in a cross-circuit-proof manner.

Connection of One Load for each Digital Output

Each of the 4 fail-safe digital outputs consists of one P-switch (DQ-Pn) and one M-switch (DQ-Mn). You connect the load between the P-switch and the M-switch. So that voltage is applied to the load, both switches are always energized. With this circuit, you achieve SIL3/Cat.4/PLe.

Evaluating the Feedback Signals

In order to detect contact welding of contactors, their feedback or readback signals must be evaluated in the safety program. The block library of Safety Advanced provides a certified block for this purpose.

If a readback error is detected for one group, this group is shutdown. The other group can continue to be switched-on functionally and shutdown safely.

5.6. F-Power Module: F-PM-E 24VDC/8A PPM

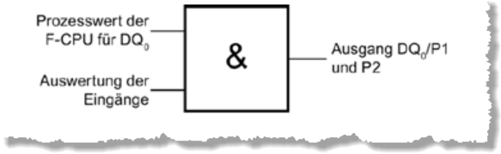
F-PM-E 24VDC/8A PPM

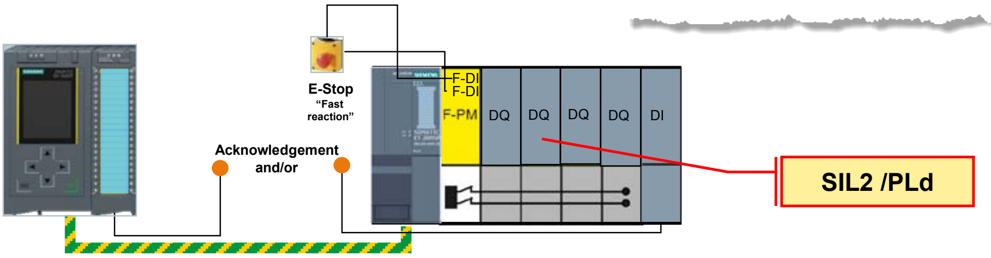
- 2 inputs (SIL 3/PL e)
- 1 output PM or PP switching, output current 8 A (SIL 3/PL e)

Safety-related shutdown of standard DQ modules

The evaluation of the safety function takes place

- Only in the F-CPU or
- F-CPU and Onboard F-DI





Safety-related Shutdown of Standard DQ Modules by the F-PM-E

With this cost-effective solution, when a fault is detected in the process or on the F-PM-E 24VDC/8A PPM ST power module, there is a full and simultaneous shutdown of all affected outputs of the standard DQ modules. With the safety-related shutdown of standard DQ modules, you achieve SIL2/Cat.3/PLd. You can use the F-PM-E 24VDC/8A PPM ST power module with all standard DQ modules within a potential group.

Digital Output of F-PM

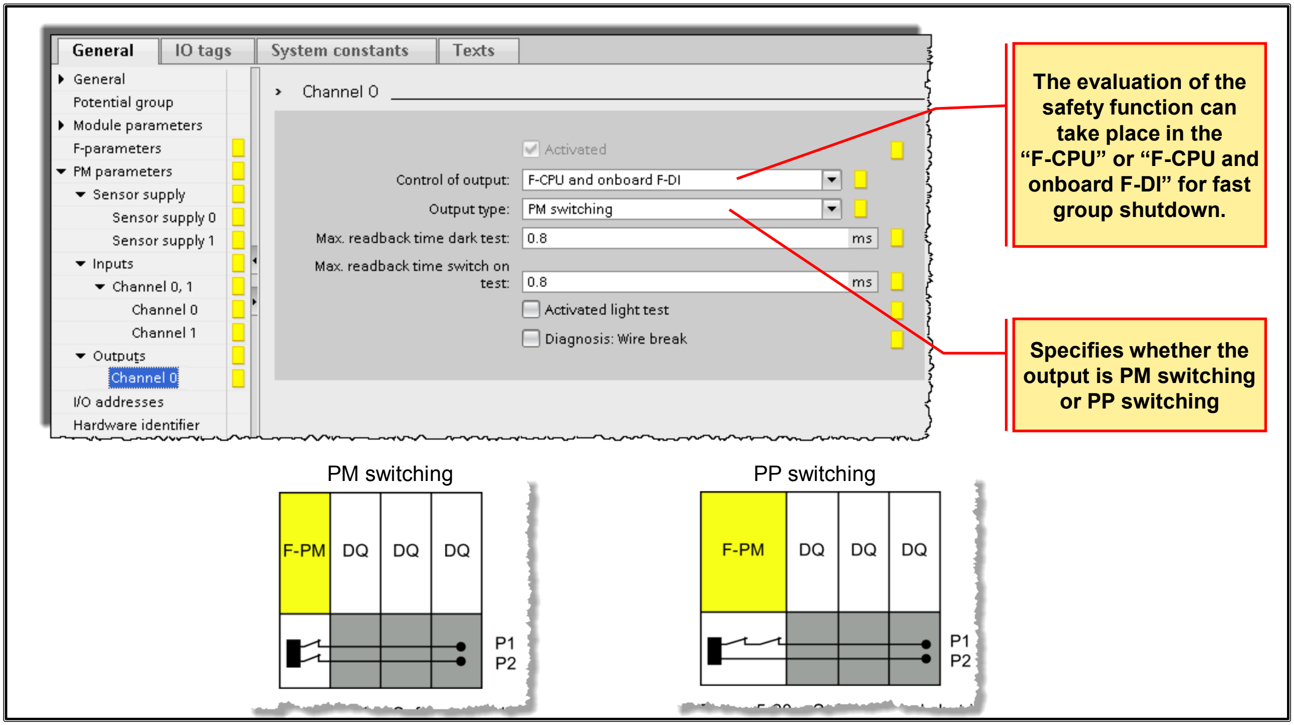
The digital output switches the voltage L+ and M using two electronic switches. The switched voltage and ground are fed to the internal voltage buses P1 and P2. In addition, the switched voltage and ground are available at the BaseUnit at DQ-P0 and DQ-M0.

This results in two possible connections, which you can also use simultaneously:

- A load can be connected directly to the BaseUnit.
- You can use the internal voltage buses P1 and P2 for supplying standard modules and for safety-related shutdown. You can, in turn, connect loads to the standard modules.

In the event of a cross-circuit between L+ and DQ, the activated (energized) actuator is no longer shut down. To prevent cross-circuits between L+ and DQ, you must route the cables used to connect the actuators in a cross-circuit-proof manner, for example, as separate, sheathed cables or in separate cable ducts. For the F-PM-E, the ground wire for the BaseUnit must be installed redundantly for safety reasons. Otherwise, if a single ground wire is interrupted, it might no longer be possible to shut down voltage bus P2 in a safety-related manner.

5.7. F-PM Channel Parameters



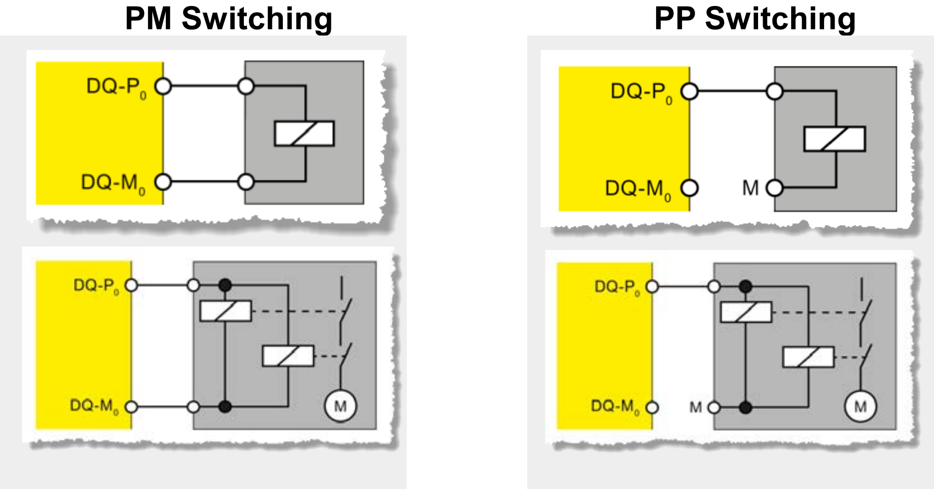
Safety-related Shutdown of Standard Output Modules, PM Switching

The F-PM-E 24VDC/8A PPM ST power module together with the appropriate BaseUnit opens a new potential group. Standard DQ modules which you use in this potential group can be shut down in a safety-related manner through the F-PM-E 24VDC/8A PPM ST power module. For this, the F-PM-E 24VDC/8A PPM ST power module shuts down the voltage buses P1 and P2 in a safety-related manner.

Safety-related Shutdown of Standard Output Modules, PP Switching

The F-PM-E 24VDC/8A PPM ST power module together with the appropriate BaseUnit opens a new potential group. Standard DQ modules which you use in this potential group can be shut down in a safety-related manner through the F-PM-E 24VDC/8A PPM ST power module. For this, the F-PM-E 24VDC/8A PPM ST power module shuts down the voltage bus P1 in a safe manner.

5.8. F-PM Actuator Connection: PM / PP Switching



Caution!

It is no longer possible to shut down an actuator if a cross circuit has developed between L+ and DQ. To prevent cross circuits between L+ and DQ, you must route the cables used to connect the actuators in a cross-circuit proof manner (for example, as separate, sheathed cables or in separate cable ducts).

Connection of One Load to the Digital Output, PP-switching (see picture, upper right)

The fail-safe digital output consists of two P-switches (current-sourcing switches) for DQ-P0 and one M-switch (current-sinking switch) for DQ-M0. In this application, you connect the load between the P-switch DQ-P0 and ground. So that voltage is applied to the load, the two P-switches are always energized. With a suitably qualified actuator, you also achieve SIL3/Cat.4/PLe with this circuit.

Connection of One Load to the Digital Output, PM-switching (see picture, upper left)

The fail-safe digital output consists of two P-switches for DQ-P0 and one M-switch for DQ-M0. You connect the load between the P-switches DQ-P0 and the M-switch DQ-M0. So that voltage is applied to the load, the two P-switches and the M-switch are always energized. With a suitably qualified actuator, you also achieve SIL3/Cat.4/PLe with this circuit.

Connection of Two Loads in Parallel to the Digital Output, PP-switching

With the wiring version in the picture at the bottom right, you achieve SIL3/Cat.4/PLe. When two relays are connected in parallel, the same rules apply as for PM-switching.

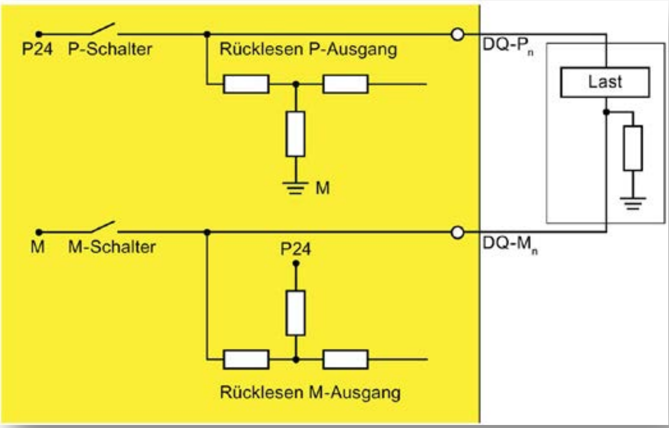
Connection of Two Loads in Parallel to the Digital Output, PM-switching

With the wiring version in the picture at the bottom left, you achieve SIL3/Cat.4/PLe. With a parallel connection of two relays to one digital output, a "wire break" is only detected if both relays are disconnected from P or M due to the wire break. The diagnostics generated in this case is not safety-relevant.

5.9. Switching of loads with ground

If the following two conditions are met a PM Switching module detects a short circuit:

- If loads that have a connection between chassis and ground are switched by the module for example to improve the EMC properties.
- If chassis and ground are connected at the power supply unit.



From the perspective of the F-module, the M-switch is bridged by the chassis-ground connection.

Remedy:

- Reduce the capacitance value between chassis and ground at the load end to less than 2 µF.
- Increase the value of the resistance between chassis and ground at the load end to more than 100 kΩ.

OR:

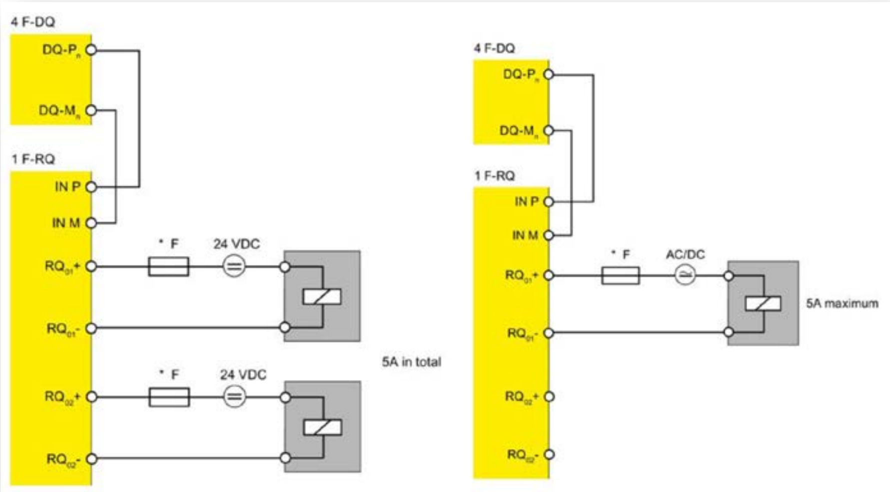
- Use a PP-switching module.

5.10. F-Relay Module: F-RQ 1x24VDC/24..230VAC/5A

Galvanically isolated switching with:

ET 200SP 1 F-RQ

- **1 relay output (2x two-channel NO contacts)**
- SIL 3 / PL e if controlled with an F-DQ



Shutting Down Loads via a Single Pole

With this application, you can use an F-RQ module to switch two loads having a total of 5 A and one or two power supplies in conformity with SELV/PELV via a single pole.

Shutting Down a Load with 1 F-RQ Module via Two Poles

With this application, you can use one F-RQ module to switch a load with a maximum of 2.5 A and one power supply in conformity with SELV/PELV via two poles.

Shutting Down a Load with 2 F-RQ Modules via Two Poles

With this application, you can use two F-RQ modules to switch a load with a maximum of 5 A via two poles.

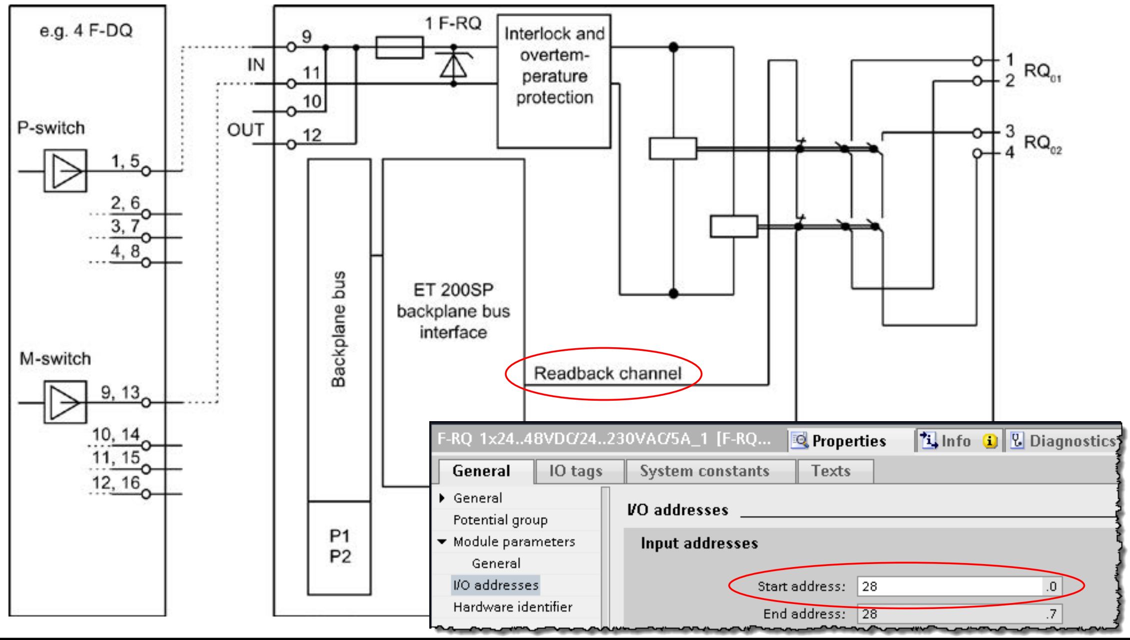
Shutting Down Loads with 2 F-RQ Modules via a Single Pole

With this application, you can use two F-RQ modules to switch two loads each having 5A via a single pole. A single power supply is not in conformity with SELV/PELV.

5.11. Switching an F-Relay Module with F-DQ

Internal structure

- Module-internal feedback signal through process image for inputs:



Connection of the 24 V DC Supply

You apply the 24 V DC control voltage to IN P (terminal 9) and IN M (terminal 11). The 24 V DC is ordinarily supplied by a PM-switching fail-safe output (for example, digital output module F-DQ 4x24VDC/2A PM HF). In this case, you connect the P-output of the F-DQ to IN P of the F-RQ module and the M-output to IN M of the F-RQ module.

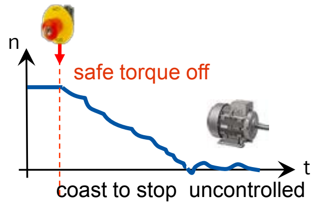
Alternatively, connection to a PP-switching fail-safe output is possible. Note, however, that external line-to-line faults at the P-input cannot be controlled. In this case IN M would be connected directly to the chassis ground of the control voltage. Mixing up the control voltage at inputs IN P and IN M causes destruction to the F-RQ module.

5.12. Stop Categories in Accordance with EN 60204-1

The shut-down of a drive can occur in various ways in accordance with EN 60204-1:

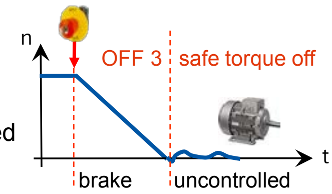
Stop Category 0

- Energy supply is immediately switched off
- Switch-off electromechanical or electronic
- Galvanic isolation is not required



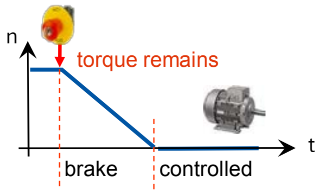
Stop Category 1

- Drive is electrically braked into shut-down (standstill)
- The energy supply is switched off when shut-down is completed
- Switch-off electromechanical or electronic
- Galvanic isolation is not required



Stop Category 2

- Drive is electrically braked into shut-down (standstill)
- The energy supply maintained when shut-down is completed



EN 60204-1

Safety of machinery – Electrical equipment of machines – Part 1: General requirements

Stop Cat. 0

Shut-down by immediately switching off the energy supply to the machines / drive machinery. This does not have to occur electromechanically because; electrical isolation is not necessary.

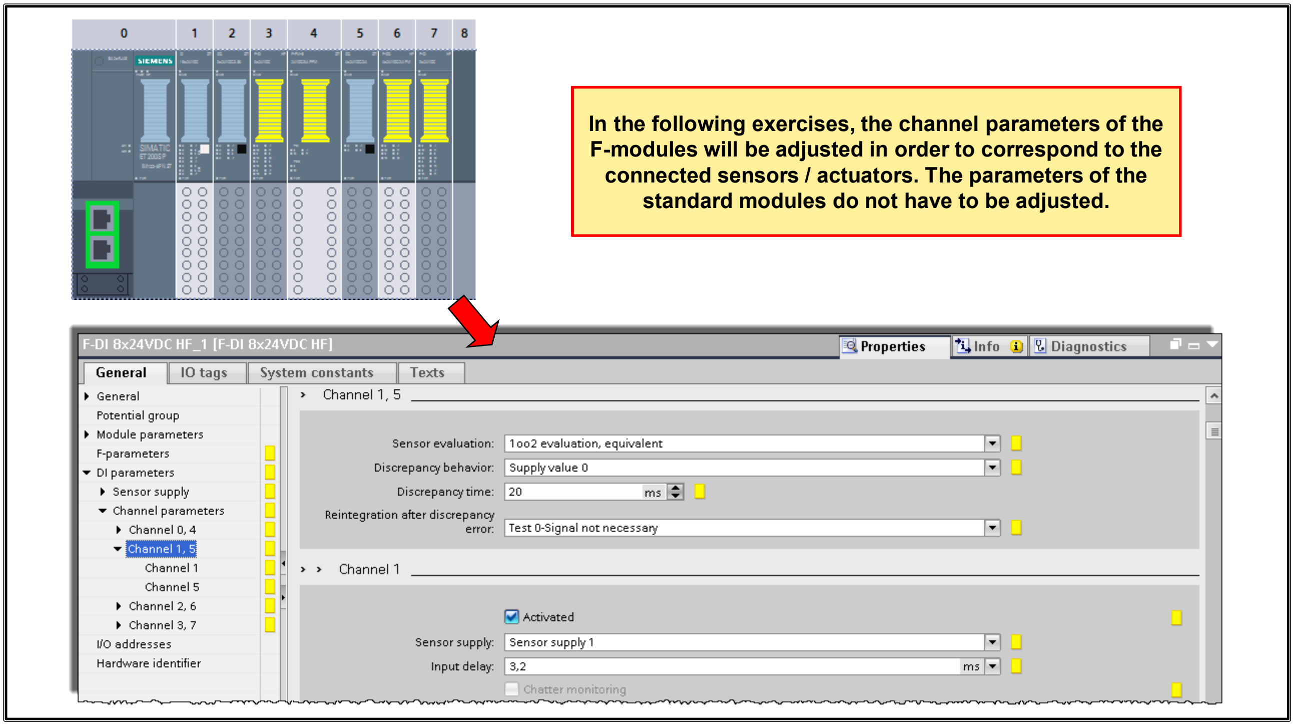
Stop Cat. 1

Controlled shut-down, whereby the energy supply to the machines / drive machinery is maintained to achieve shut-down; the energy supply is only interrupted when the shut-down has been completed (standstill);
Controlled shut-down: shut-down of a machine movement with electric energy to the machines / drive machinery which is maintained during the shut-down process.

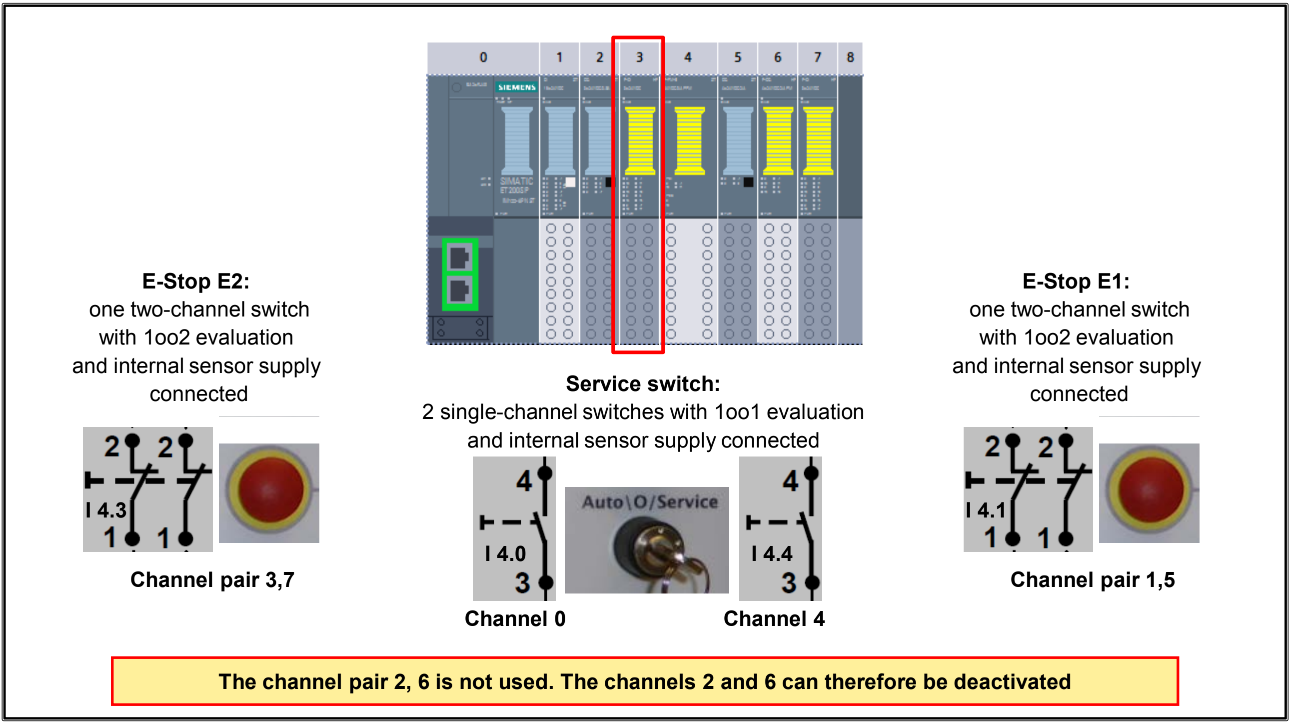
Stop Cat. 2

Controlled shut-down in which the energy supply to the machines / drive machinery is maintained.

5.13. Task Description: Adjusting the F-Module Parameters



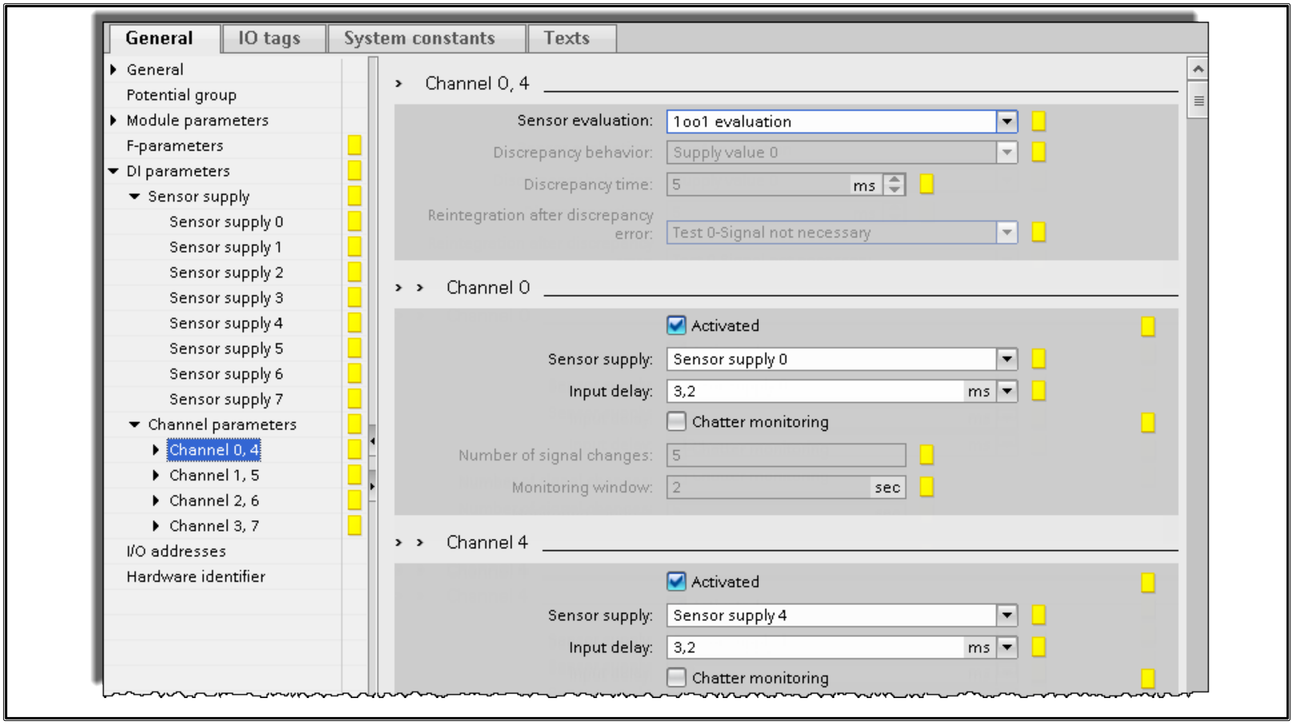
5.13.1. Exercise 1: Parameterizing F-DI Slot 3



Task and What to Do

1. Open the channel parameters of the F-DI module on Slot 3

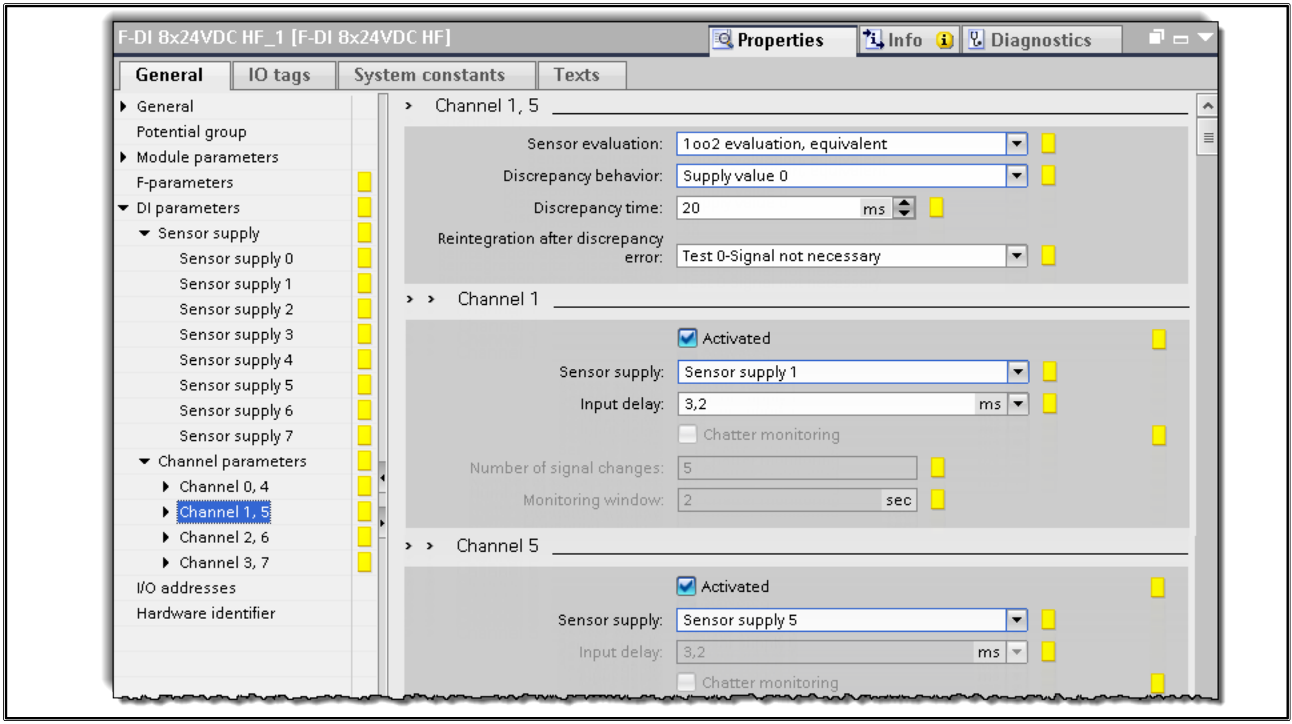
5.13.1.1. Re: Exercise 1: Service Switch Channel 0, 4



Task and What to Do

1. You are to parameterize the channel pair 0, 4 as shown in the picture.

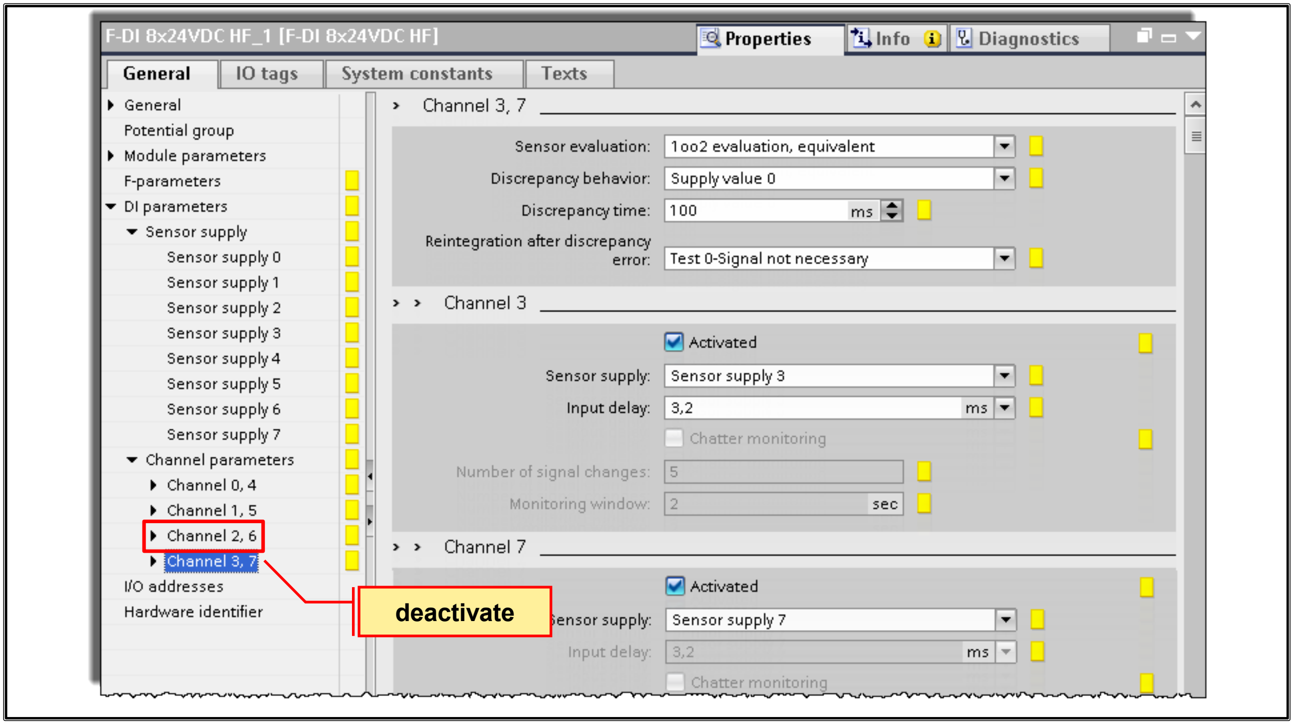
5.13.1.2. Re: Exercise 1: E-Stop E1 Channel 1, 5



Task and What to Do

1. You are to parameterize the channel pair 1, 5 as shown in the picture.

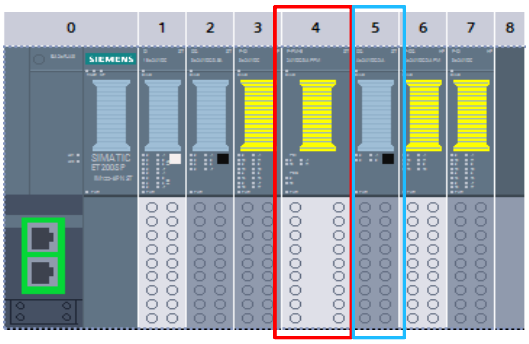
5.13.1.3. Re: Exercise 1: E-Stop E2 Channel 3, 7



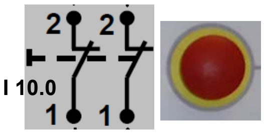
Task and What to Do

1. You are to parameterize the channel pair 3, 7 as shown in the picture.
2. You are to deactivate the channel pair 2, 6

5.13.2. Exercise 2: Parameterizing F-PM Slot 4

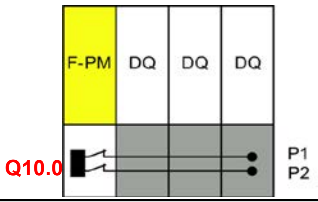


E-Stop E3:
one two-channel switch
with 1oo2 evaluation
and internal sensor supply
connected



Channel pair 0,1

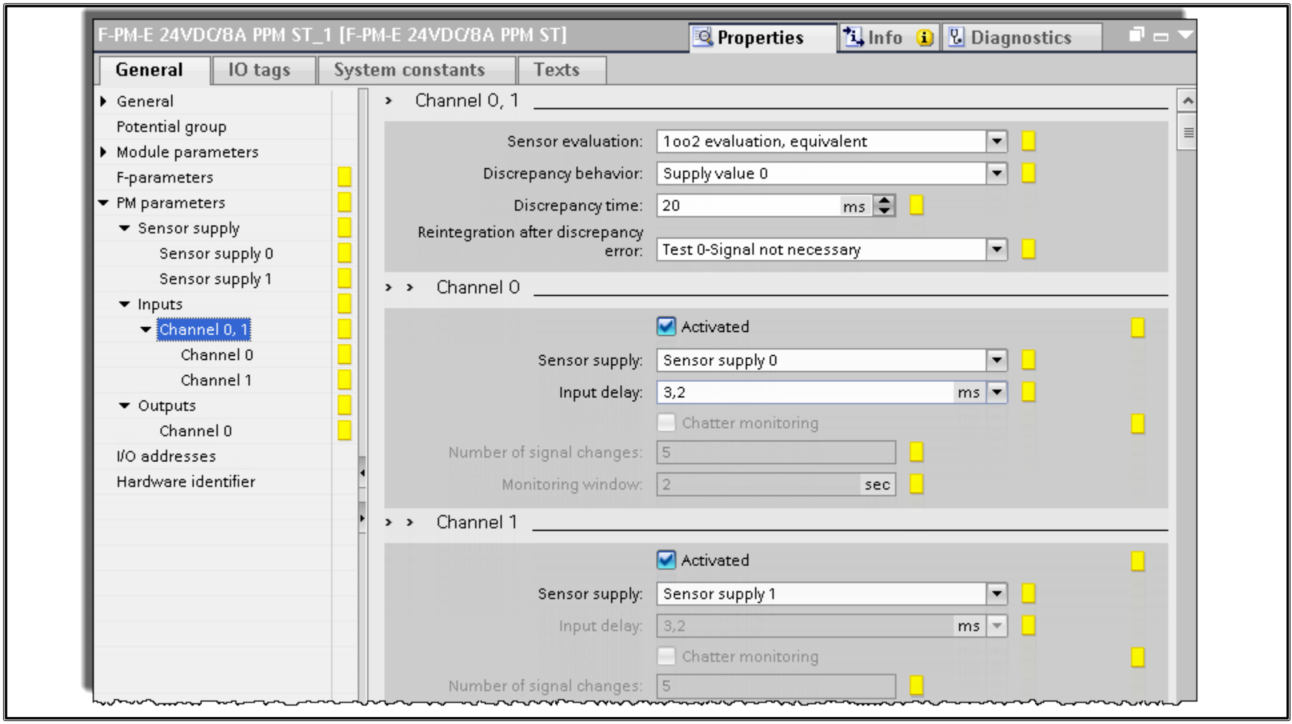
Switch-off Standard DQ module Slot 5:
The fail-safe output (Q10.0) switches the supply
to the standard DQ module on with “1” and off with “0”.
In that way, the shut-off valves V1 and V2 connected to it
can be switched-off in a safety-related manner.



Task and What to Do

1. Open the channel parameters of the F-PM module on Slot 4.

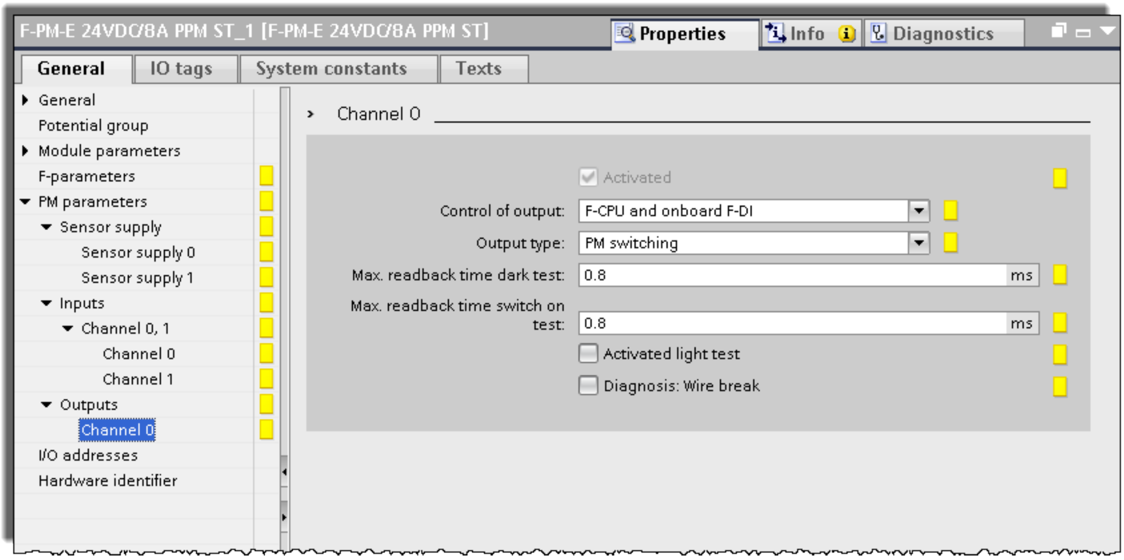
5.13.2.1. Re: Exercise 2: E-Stop E3 Channel 0, 1



Task and What to Do

1. You are to parameterize the input channel pair 0, 1 as shown in the picture.

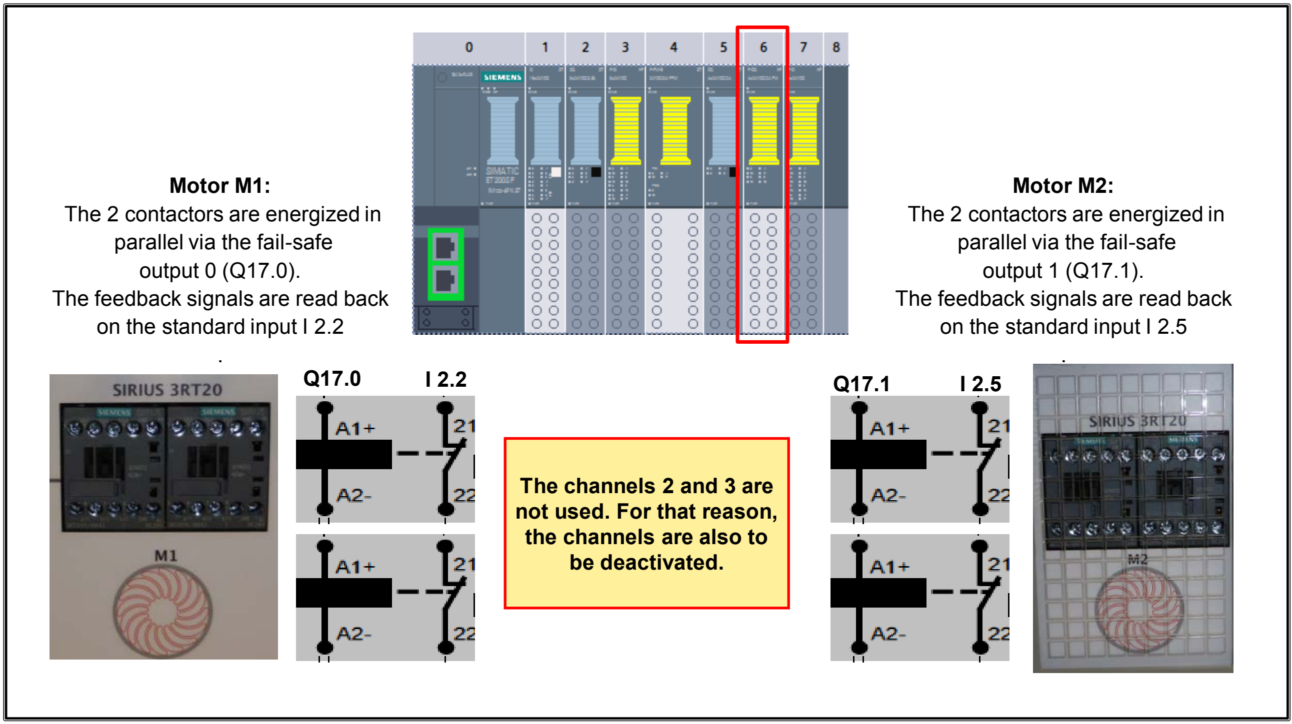
5.13.2.2. Re: Exercise 2: Switching-off the Standard DQ, Channel 0



Task and What to Do

1. You are to parameterize the output channel 0 as shown in the picture.

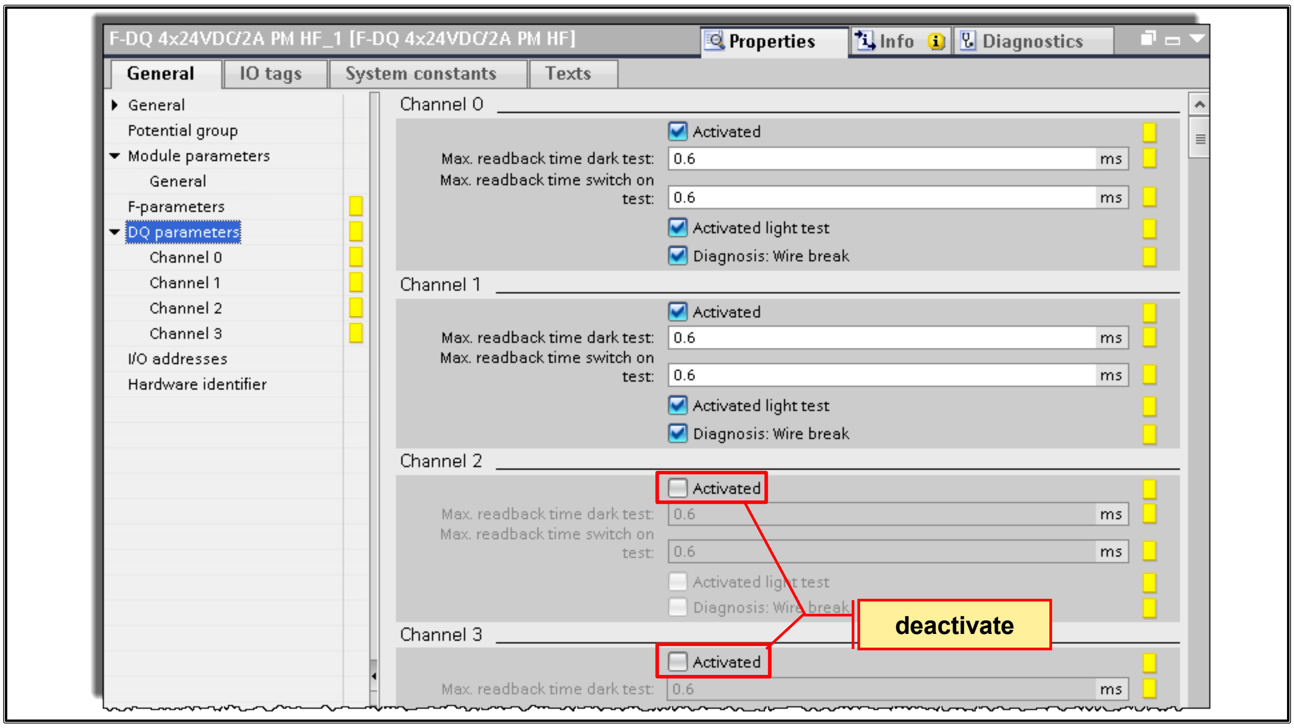
5.13.3. Exercise 3: Parameterizing F-DQ Slot 6



Task and What to Do

Open the channel parameters of the F-DQ module on Slot 6

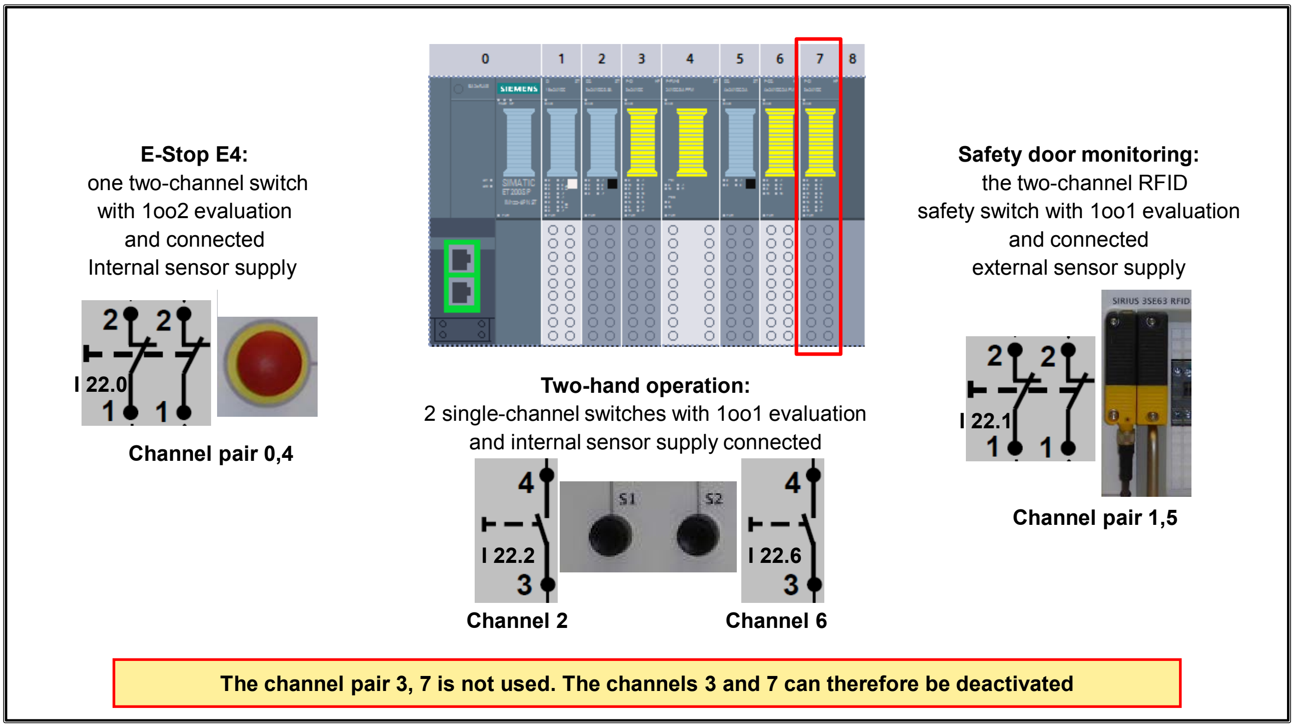
5.13.3.1. Re: Exercise 3: Controlling Motor 1 and Motor 2, Channel 0, 1



Task and What to Do

1. You are to parameterize the output channels 0 and 1 as shown in the picture.
2. You are to deactivate channels 2 and 3

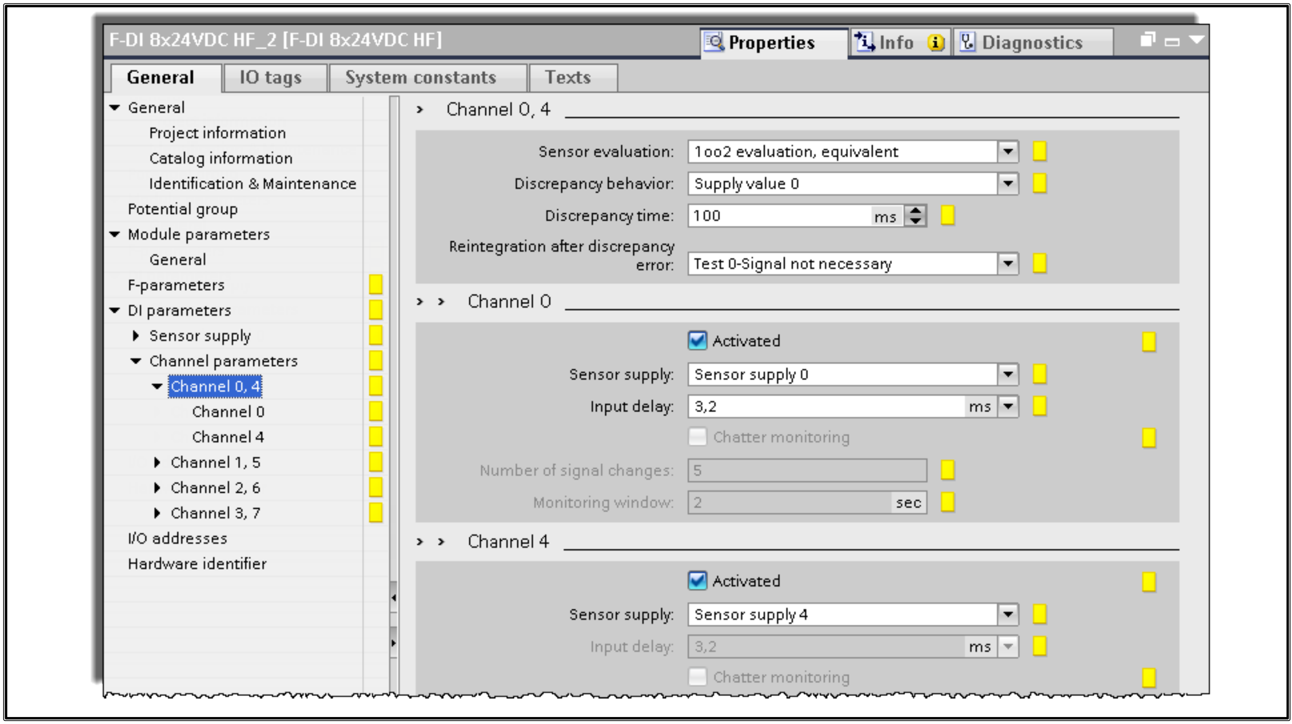
5.13.4. Exercise 4: Parameterizing F-DI Slot 7



Task and What to Do

Open the channel parameters of the F-DI module on Slot 7

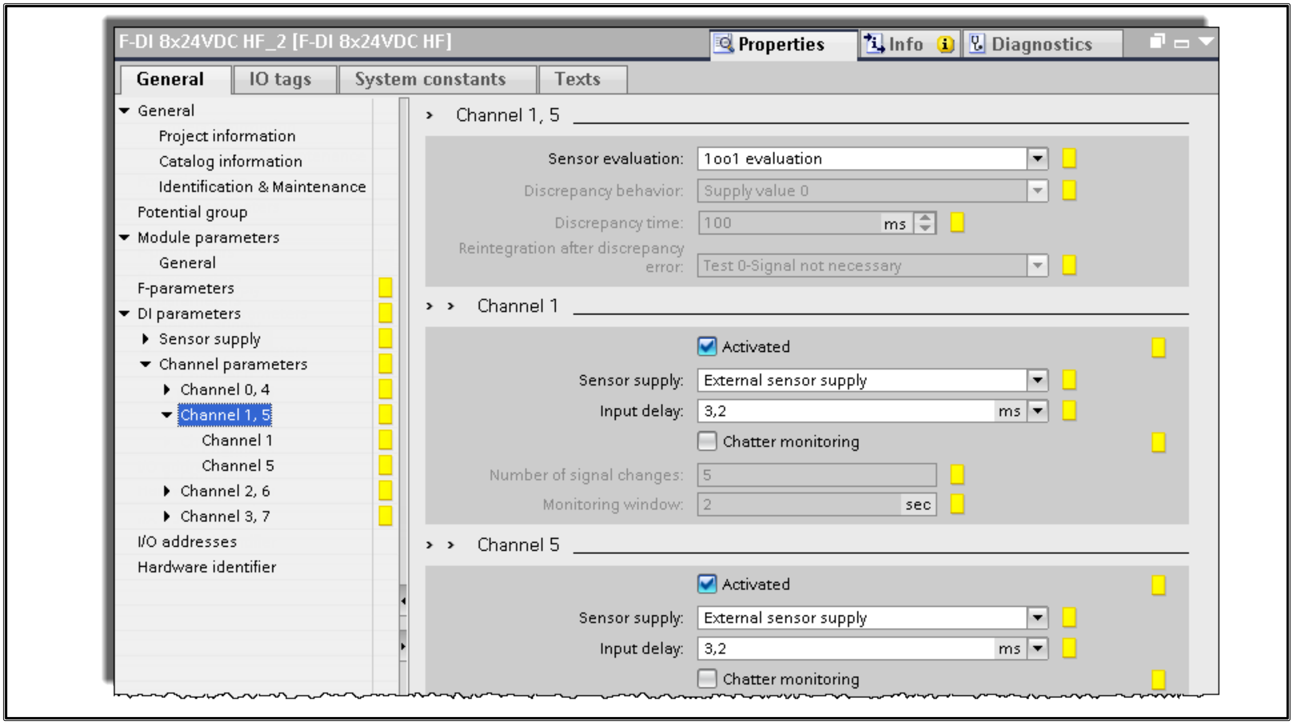
5.13.4.1. Re: Exercise 4: E-Stop E4, Channel 0, 4



Task and What to Do

1. You are to parameterize the input channel pair 0, 4 as shown in the picture.

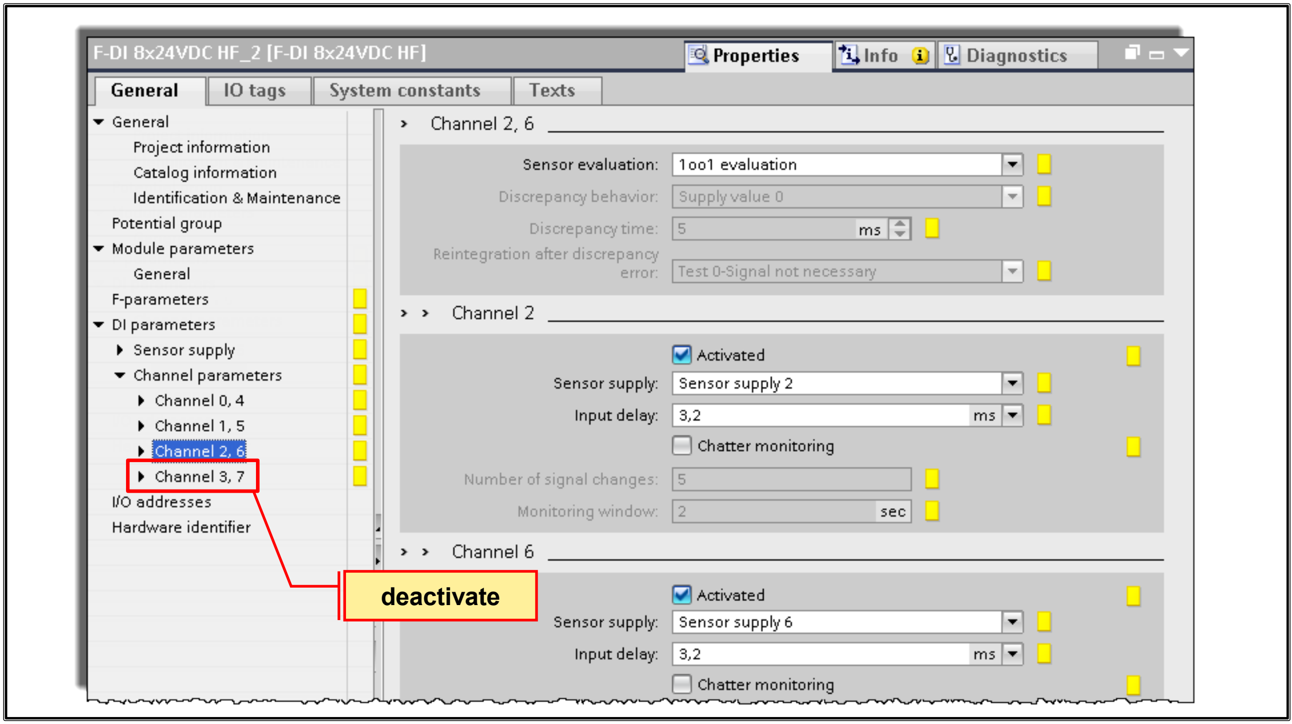
5.13.4.2. Re: Exercise 4: RFID Safety Switch, Channel 1, 5



Task and What to Do

1. You are to parameterize the input channel pair 1, 5 as shown in the picture.

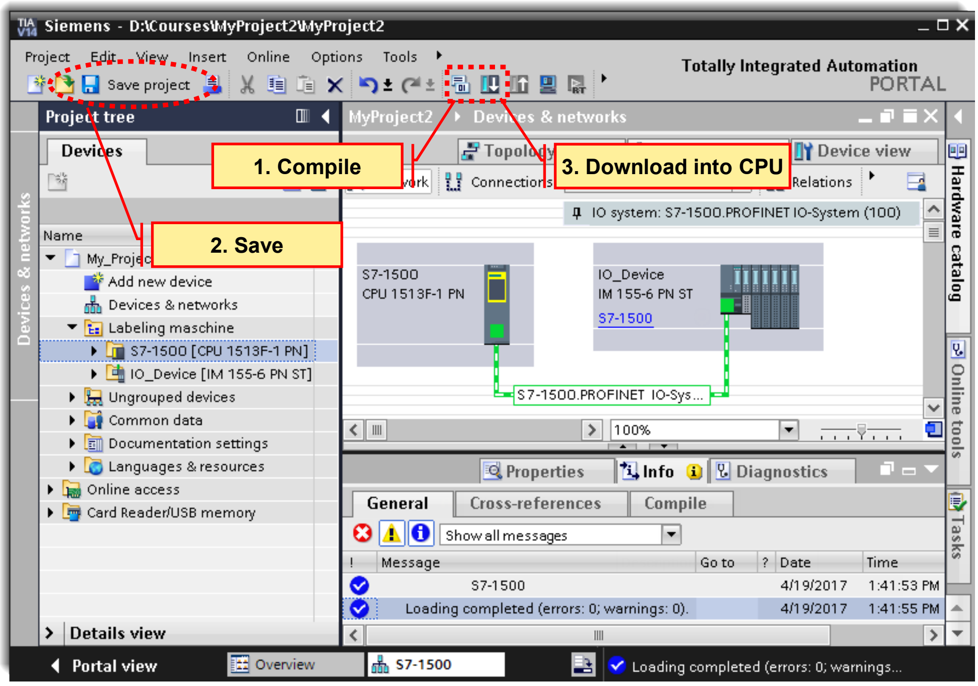
5.13.4.3. Re: Exercise 4: Two-hand Monitoring, Channel 2, 6



Task and What to Do

1. You are to parameterize the input channel pair 2, 6 as shown in the picture.
2. You are to deactivate the channel pair 3, 7

5.13.5. Exercise 5: Compiling the HW Configuration and Downloading it into the CPU



Task

Now that the PROFINET I/O system is completely configured and parameterized, the project must be completely compiled, saved and downloaded into the CPU.

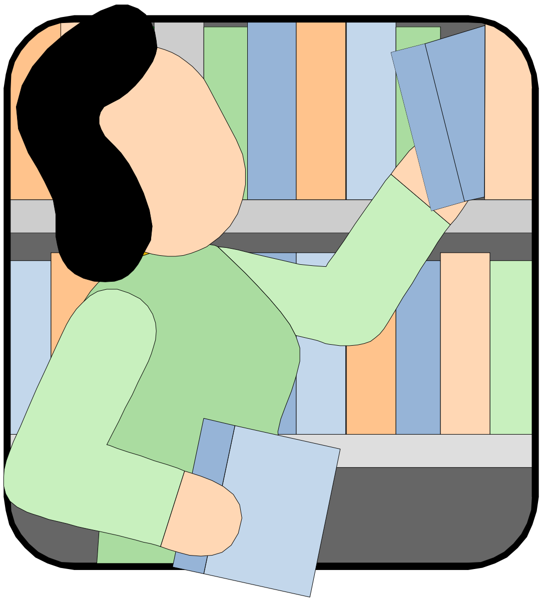
What to Do

1. Compile the hardware configuration by selecting the S7-1500 station in the Project tree and then clicking on the Compile button (see picture). In the Inspector window under "Info", check whether the compilation was successful. Should errors have occurred, correct them.
2. Save your project.
3. Download the entire station into the CPU by clicking on the Download button (see picture). In the Inspector window under "Info", check whether the loading was successful.
4. Save your project.

Result:

All modules should now be error-free and errors should no longer be pending on the CPU.

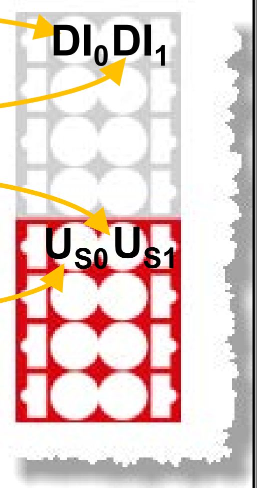
5.14. Additional Information



5.14.1. Terminal Assignment ET 200SP / F-DI

Terminal assignment

Terminal	Assignment	Terminal	Assignment
1	DI_0	2	DI_1
3	DI_2	4	DI_3
5	DI_4	6	DI_5
7	DI_6	8	DI_7
9	U_{S0}	10	U_{S1}
11	U_{S2}	12	U_{S3}
13	U_{S4}	14	U_{S5}
15	U_{S6}	16	U_{S7}
L+	24V DC	M	M



- **DI_n:** Fail-safe digital input, Channel n
- **U_{Sn}:** Internal sensor supply, Channel n

Terminal assignment

The F-DI 8×24VDC HF digital input module has 8 fail-safe inputs DI0 to DI7 (SIL3). You can combine two of these inputs each into one input.

You can combine the following inputs:

- DI0 and DI4
- DI1 and DI5
- DI2 and DI6
- DI3 and DI7

Channels DI0, DI1, DI2 and DI3 supply the process signals.

Connecting two single-channel sensors via two channels (SIL3/Cat.3/PIe)

For each process signal, two single-channel sensors that acquire the same process value are connected to two inputs of the F-module (1oo2 evaluation).

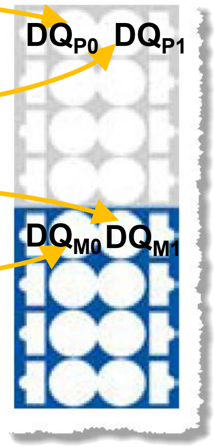
Connecting a two-channel sensor via two channels (SIL3/Cat.4/PIe)

For each process signal, a two-channel sensor is connected to two inputs of the F-module (1oo2 evaluation). You supply the sensors from two different sensor supplies.

5.14.2. Terminal Assignment ET 200SP / F-DQ

Terminal assignment

Terminal	Assignment	Terminal	Assignment
1	DQ-P$_0$	**2**	DQ-P$_1$
3	DQ-P$_2$	**4**	DQ-P$_3$
5	DQ-P$_0$	**6**	DQ-P$_1$
7	DQ-P$_2$	**8**	DQ-P$_3$
9	DQ-M$_0$	**10**	DQ-M$_1$
11	DQ-M$_2$	**12**	DQ-M$_3$
13	DQ-M$_0$	**14**	DQ-M$_1$
15	DQ-M$_2$	**16**	DQ-M$_3$
L+	24V DC	**M**	M



- **DQ-P$_n$:** Fail-safe digital output, Channel n, P-switching
- **DQ-M$_n$:** Ground for fail-safe digital output, Channel n, M-switching

Unwanted Activation of F-I/O with Fail-safe Outputs

If an F-I/O with fail-safe outputs is passivated for longer than the time period specified in the safety-related characteristics (> 100 hours) without the fault being corrected, you must rule out the possibility that a second fault is causing unwanted activation of the F-I/O, putting the F-system into a dangerous state. Although the probability of such hardware faults is very low, an unwanted activation of the F-I/O with fail-safe outputs must be prevented through appropriate circuit design or organizational measures. One possibility would be to switch off the power supply of the passivated F-I/O within a time period of 100 hours, for example. For systems that have product standards, the required measures are standardized.

For all other systems, the system operator must create its own concept for the necessary measures and have them confirmed by the accepting authority.

Characteristic of the Shutdown of F-modules with Fail-safe Outputs

When a fault is detected, a channel-by-channel shutdown takes place. In addition, it is also possible to react to critical process states staggered over time or to disable outputs individually and in a safety-related manner.

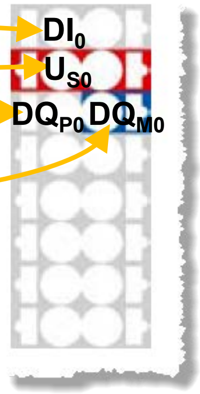
Switching of Loads that are Not Designed to be Ground-free

The F-DQ 4×24VDC/2A PM HF can switch loads that have a connection between the chassis ground and earth ground of at least 100 kΩ. Otherwise, a short circuit is detected. From the point of view of the F-module, the M-switch (current-sinking switch) is bypassed through the chassis ground to earth ground connection.

5.14.3. Terminal Assignment ET 200SP / F-PM

Terminal assignment

Terminal	Assignment	Terminal	Assignment
1	DI_0	**2**	DI_1
3	U_{S0}	**4**	U_{S1}
5	$DQ\text{-}P_0$	**6**	$DQ\text{-}M_0$
7	AUX	**8**	AUX
L+	24V DC	**M**	M
L+	24V DC	**M**	M



- **DI_n:** Fail-safe digital input, Channel n
- **U_{Sn}:** Internal sensor supply, Channel n
- **$DQ\text{-}P_0$:** Fail-safe digital output, Channel 0, P-switching
- **$DQ\text{-}M_0$:** Ground for fail-safe digital output, Channel 0, M-switching
- **AUX:** Terminal for PE or as voltage bus (free for use up to 230 V AC)

Assignment of the Inputs

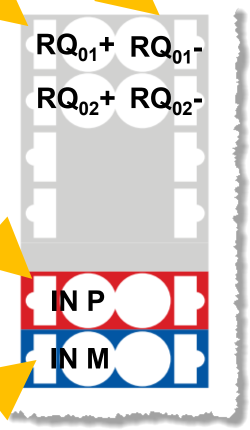
The F-PM-E power module has 2 fail-safe inputs DI0 and DI1 (SIL3). You can combine the two inputs into one input.

Channel DI0 supplies the process signal. The interconnections of the inputs are the same as the F-DI module.

5.14.4. Terminal Assignment ET 200SP / F-RQ

Terminal assignment

Terminal	Assignment	Terminal	Assignment
1	RQ_{01}+	2	RQ_{01}-
3	RQ_{02}+	4	RQ_{02}-
5	-	6	-
7	-	8	-
9	IN P	10	OUT P
11	IN M	12	OUT M
13	AUX	14	AUX
15	AUX	16	AUX

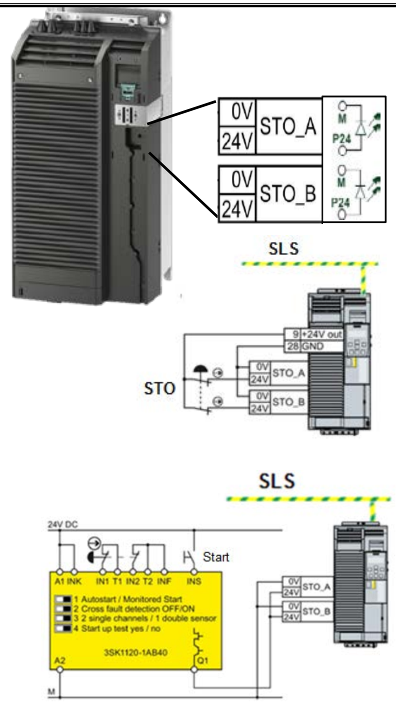


Connection of the Load Voltage and Load

The connections of the relay output are electrically-isolated NO contacts. This means that you must supply the supply voltage externally. Connect the load supply (supply 1) and the load (load 1) in series to the connections RQ01 (terminals 1; 2). This ensures that the NO contacts of the relay interrupt the current flow of the load supply through the load. The two relay contacts connected in series enable shutdown to continue if one of the two relays is defective. The second circuit is electrically independent from the first. They are logically interconnected through the common control. This means that the potential in the circuit composed of RQ02 (terminals 3; 4), supply 2 and load 2 may be different.

5.14.5. SINAMICS G120: STO / SS1 in PL(e) SIL3 E-Stop via Terminals on PM240-2 FSD-FSF

- With the SINAMICS PM240-2 FSD-F Power Module, the STO function is supported via terminals.
- The STO function is integrated in the Basic Functions of the **CU240E-2 as well as the CU250S-2**.
- The STO function via terminals on the PM240-2 FSD-FSF can be used in parallel to the safety functions on the Control Unit.
- The PM240-2 filters signal changes through light and dark tests at the safe inputs (fixed hardware filter suppresses signal changes ≤ 4 ms).
- The function fulfills Performance Level (PL) e according to EN ISO 13849-1: 2006 as well as Safety Integrity Level 3 (SIL 3) according to IEC 61508:2010
- Provided that the inverter is error-free, then in the worst-case, 20 ms for STO and 24 ms for SBC can be used as reaction times.
- Certificate



5.14.6. Help on Using Safety Technology

	Contents	Attainable
Safety Evaluation Tool	Tool for verifying the required safety levels	Online tool www.siemens.com/safety-evaluation-tool
Function examples	Instructions for functions and applications	Internet download http://support.automation.siemens.com/WW/view/de/20208582/136000
Sitrain	Product and standards training courses	Internet contact http://www.siemens.de/sitrain-safetyintegrated
Support	The right support for every project phase	Internet contact http://support.automation.siemens.com

Contents 6

6. Programming

At the end of the chapter the participant will ...

… be able to explain the structure of an F-program

… be able to explain which functions are programmed in the standard program and which in the F-program

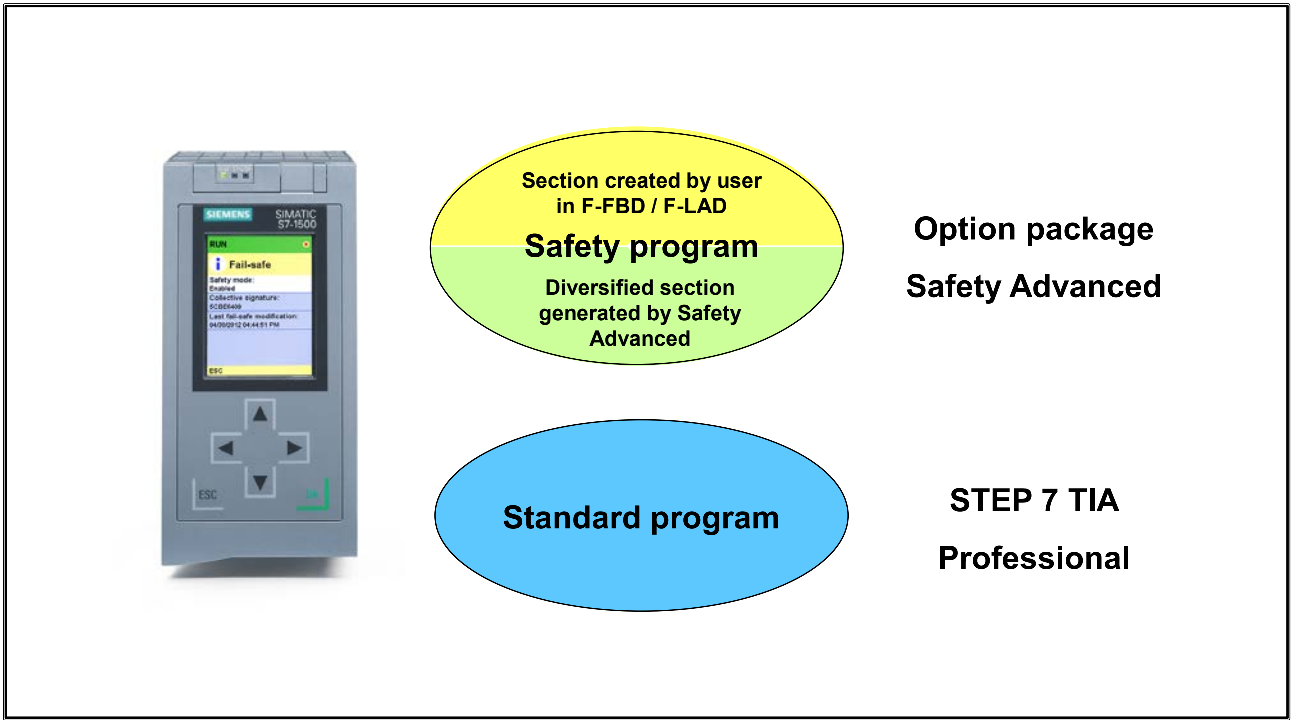
… be able to explain and program a data exchange between the standard program and the F-program

… be familiar with and will be able to use the operations permitted in the F-program

… be familiar with and will be able to use the specified safety functions

… be able to program the depassivation of F-modules

6.1. User Program of an F-CPU



User Program of an F-CPU

The user program of a safety-related CPU (F-CPU) comprises **a standard program for controlling the standard functions** and an additional **safety program for controlling the safety-related functions** of the system.

Users create the standard program with standard STEP 7 and the safety program with the STEP 7 option package "Safety Advanced".

The standard FBD/LAD Editor in STEP 7 is used for programming. Available IEC-certified safety functions can also be incorporated into the program.

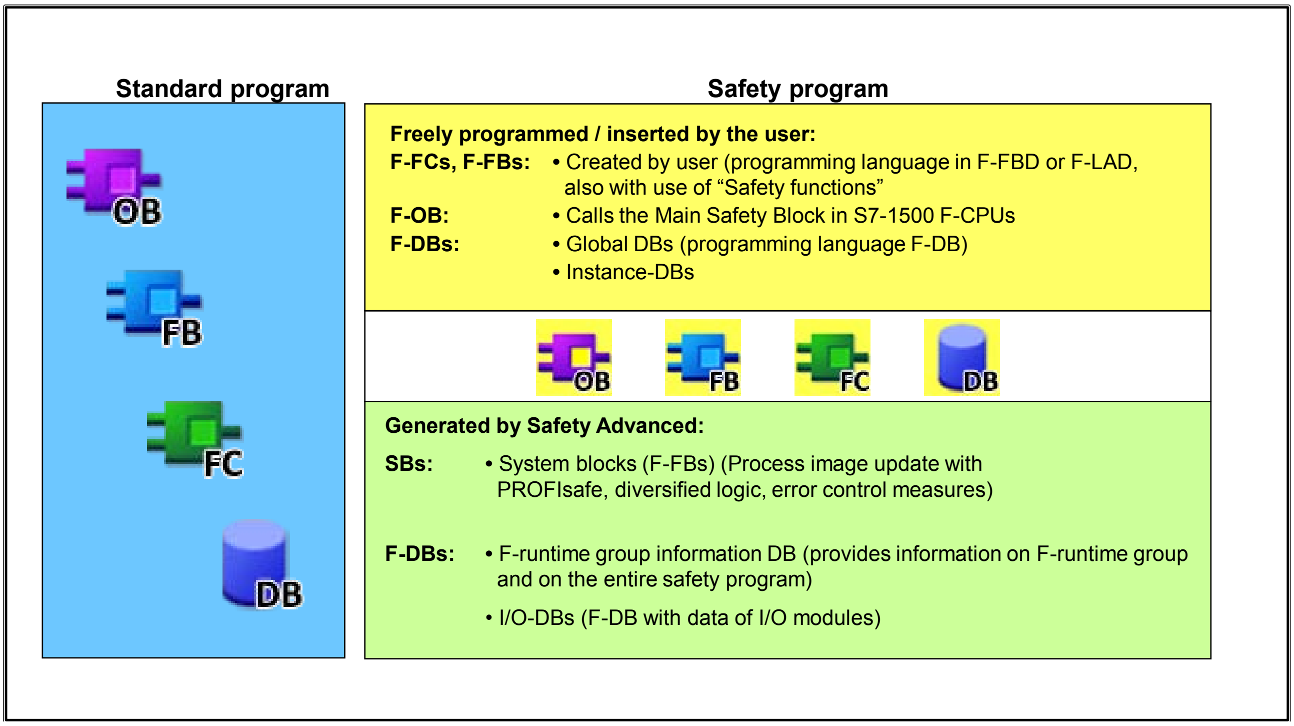
F-Program

The safety program (F-program) is made up of a section created in FBD or LAD by the user and a section generated by Safety Advanced that contains, among other things, the diversified logic for the user section.

Co-existence of Standard Program and F-program

The standard program and safety program are executed independently of each other by the CPU. Due to the coexistence of the two programs on one CPU, the communication program between the two programs can be implemented using global tags. Changes to the standard program have no effect on the safety program so that its integrity remains in place.

6.2. Blocks of the Safety Program



F-FC, F-FB

The user can program the required safety functions in the programming languages "F-FBD" and/or "F-LAD". These programming languages basically correspond to the standard FBD and LAD languages, but are restricted in their set of operations and the data types and operand areas they can use.

F-DBs

Data blocks for storing global data are also available in the safety program. The approach for creating/modifying safety-related data blocks (F-DBs) and using them in programs is the same as for standard DBs. The only restriction involves the data types available for use. Instance data blocks of safety-related FBs (regardless of whether they are created by the user or copied from the safety functions of Safety Advanced) are not edited by the user as in the standard case but are instead generated by STEP 7.

SBs

In order to create an executable safety program from the user-programmed safety program, Safety Advanced generates so-called "F-system blocks" (SBs) in the form of F-FBs when saving and compiling the hardware configuration and when compiling the safety program. These blocks serve to detect faults and ensure the fault reaction so that failures of the F-system result in a safe state. Furthermore, they carry out the communication between the F-CPU (process image) and F-I/O using the PROFIsafe safety protocol.

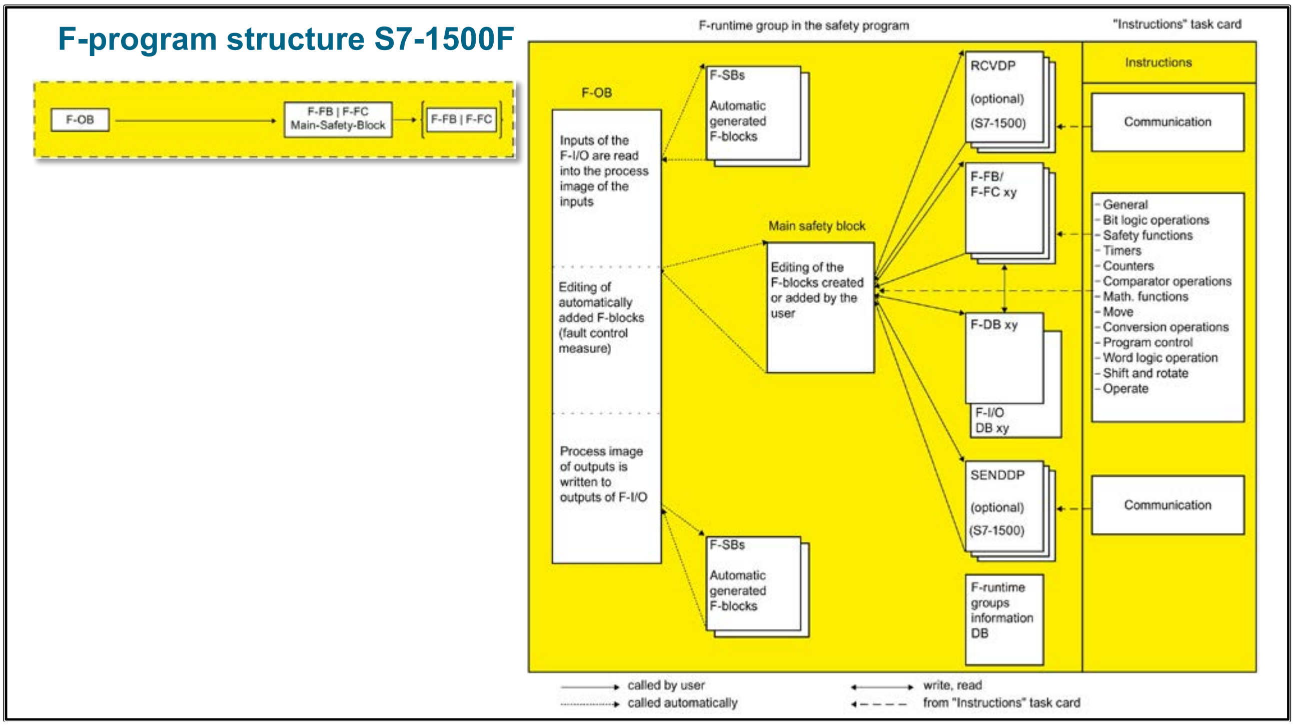
F-runtime Group Information DB

The F-runtime group information DB provides you with information about the F-runtime group and the overall safety program.

F-OB

The F-OB calls the main safety block of an F-runtime group in S7-1500 F-CPUs.

6.3. Structure and Processing of the Safety Program



Structure of the F-program, Runtime Groups

Structured programming of the safety program is possible just like with the standard program. The safety program can consist of one or two independent "runtime groups" that represent self-contained programs. By dividing the safety program into two runtime groups, it is possible to differentiate between time-critical and non-time-critical safety functions within the safety program. The shorter the response time of a safety-related function must be in the process, the shorter the call interval of the runtime group (or the F-OB in which the main safety block is programmed) must be in which this safety-related function is programmed.

By integrating a runtime group or the corresponding "main-safety-block" in an F-OB, it is ensured that the safety program will be executed at defined intervals, which is essential for determining the response times of the safety program and thus the safety functions in the system.

Instructions for the Safety Program

In the "Instructions" Task Card you will find, depending on the F-CPU used, instructions which you can use to program the safety program.

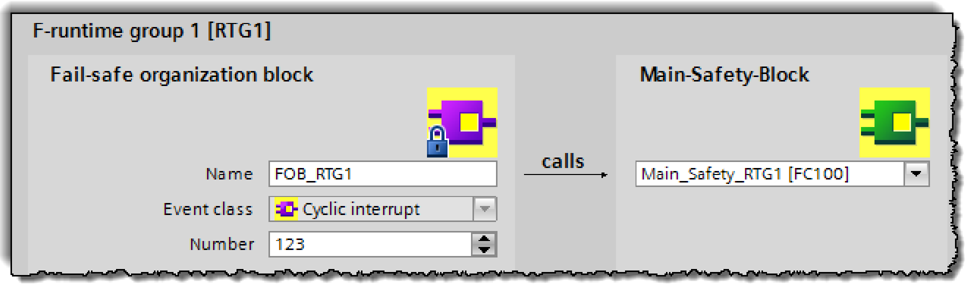
You will find instructions that you are familiar with from the standard user program, such as, bit logic operations, mathematical functions, functions for program control and word logic operations.

In addition there are instructions with safety functions, for example, for two-hand monitoring, discrepancy analysis, muting, E-STOP/E-OFF, safety door monitoring, feedback monitoring and instructions for safety-related communication between F-CPUs.

6.4. Main-Safety-Block S7-1500F

Main-Safety-Block S7-1500F

- First F-block which can be programmed by the user
- Calls all user-created, application-specific F-blocks
- Must be assigned to an F-runtime group (Safety Administration)
- Default setting TIA Portal: An F-runtime group including Main-Safety-Block is automatically generated with the call in the F-OB when an F-CPU is created

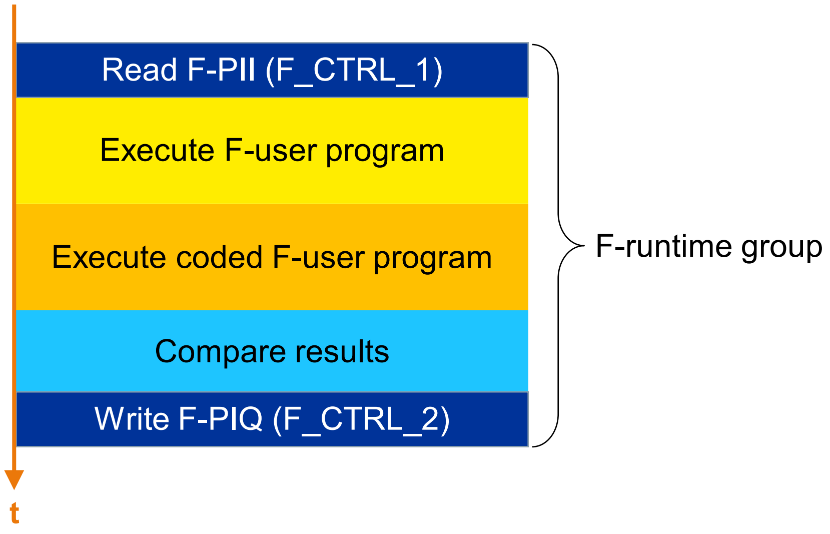


Main-Safety-Block

Each runtime group is represented by a "main-safety-block", an F-FC or F-FB that serves as an entry into the safety program and whose call for that purpose is ordinarily programmed in an F-OB. The user can program the logic of the F-program directly in this block, and/or he can use it to call other safety-related blocks for purposes of F-program structuring. In addition to the user-created program in the main-safety-block, Safety Advanced also generates further calls of automatically generated blocks with which safety functions are implemented, that serve as I/O drivers, or which contain the diversified logic, etc.

6.5. F-Runtime Group

F-runtime group in detail (with execution sequence):



- A maximum of 2 F-runtime groups is possible for each F-CPU!

F-Runtime Groups

To make it easier to handle, a safety program consists of one or two "F-runtime groups". An F-runtime group is a logical construct of several related F-blocks which is formed internally by the F-system.

An F-runtime group consists of:

- An F-OB which calls the Main-Safety-Block
- A Main-Safety-Block (F-FB/F-FC which you assign to the F-OB)
- If necessary, additional F-FBs/F-FCs which you program with FBD/LAD and call from the Main-Safety-Block
- If necessary, one or more F-DBs
- F-I/O DBs
- F-runtime group information DB
- F-blocks from the project library or from global libraries
- F-system blocks (F-SBs)
- Automatically generated F-blocks (Compiler blocks)

Structuring of the Safety Program in Two F-runtime Groups

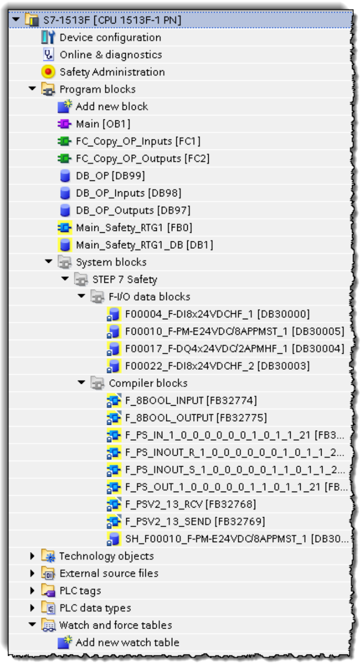
You can divide your safety program into two F-runtime groups. If portions of the safety program (one F-runtime group) run in a faster execution level, you achieve faster safety circuits with shorter response times.

6.6. The Safety Program

The safety program always contains…

- User-created F-blocks
  - Managed in the Program blocks folder
  - Call in the Main-Safety-Block

- System-generated F-blocks (Coded Processing)
  - Are created when the user program is compiled
  - Managed by the system in their own block folders
  - Supplement the user-created program with
    - Fault control measures
    - Safety-relevant tests



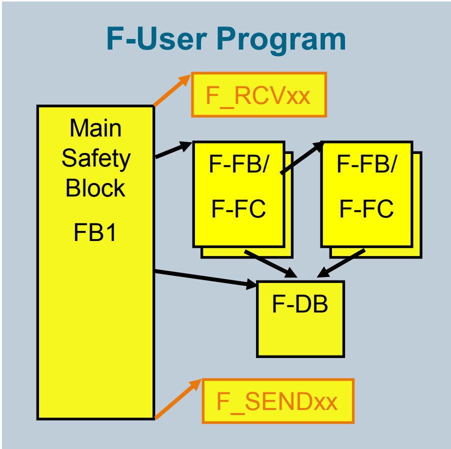
Note

You are not permitted to insert F-system blocks from the "System blocks" folder into a Main-Safety-Block/F-FB/F-FC.

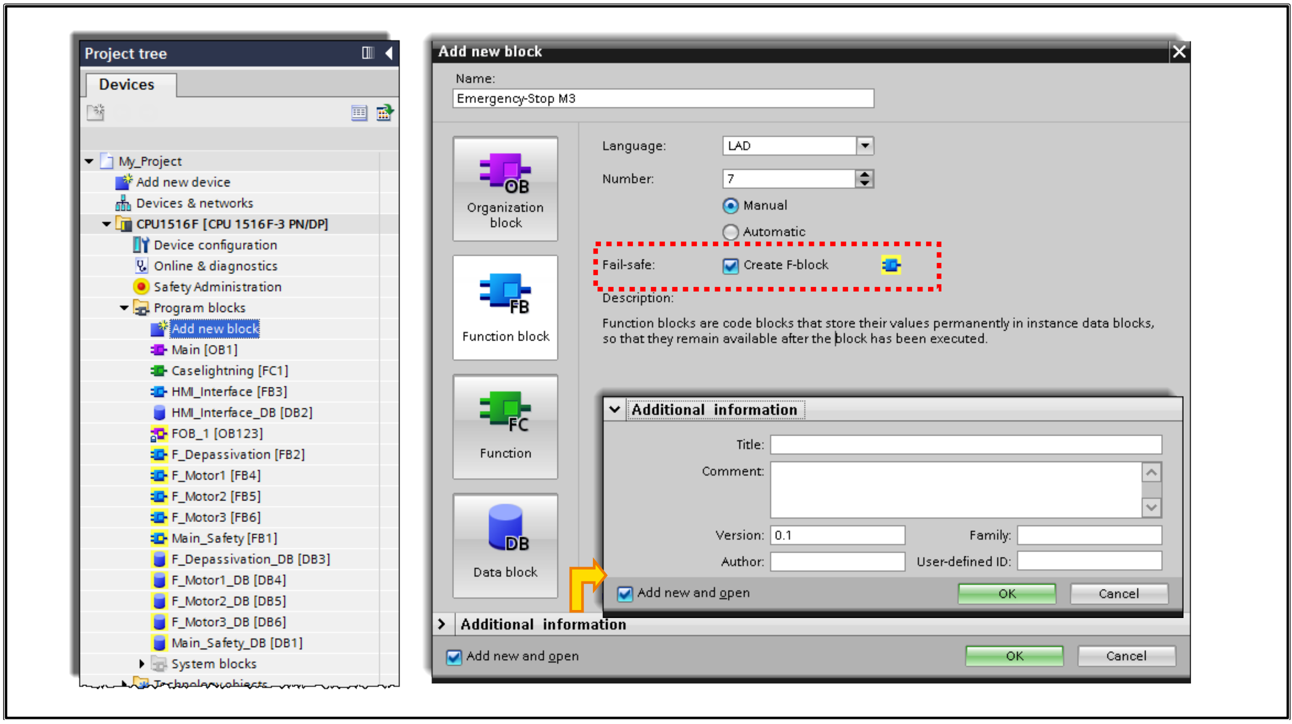
6.7. Structure of the Safety Program

Structure of the safety program

- Always at the beginning, call of:
  - F_RCVDP
- After that, call of:
  - User-created F-blocks
  - F-library blocks
  - Fail-safe instructions (Bit-logic, timers, counters, …)
- Always at the end, call of:
  - F_SENDDP



6.8. Creating an F-FC / F-FB



F-FC / F-FB

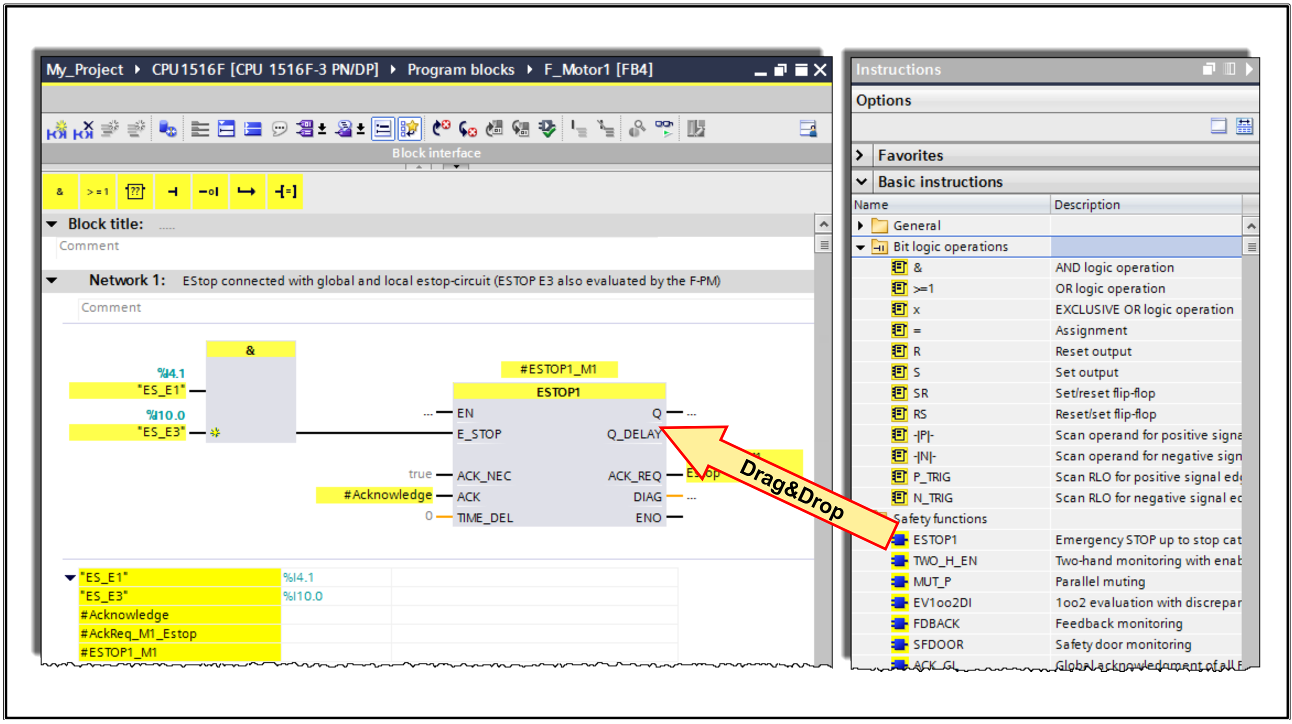
The functions (FCs) and function blocks (FBs) of the safety program are created in exactly the same way as those of the standard program; only the "Fail-safe" or "Create F-block" option has to be activated.

Main-Safety-Block

The Main-Safety-Block of a runtime group is created and programmed just like any other F-block. The user can program the safety-related logic directly in this block, and/or he can use the block to call other safety-related blocks in it for purposes of program structuring.

The property - that an F-FC or F-FB is to be used as a "Main-Safety-Block" - is only assigned to this block when the runtime group is created within the "Safety Administration". When the safety program is compiled, the calls of the blocks generated by Safety Advanced are then integrated in the Main-Safety-Block.

6.9. Programming an F-FC / F-FB in F-FBD / F-LAD



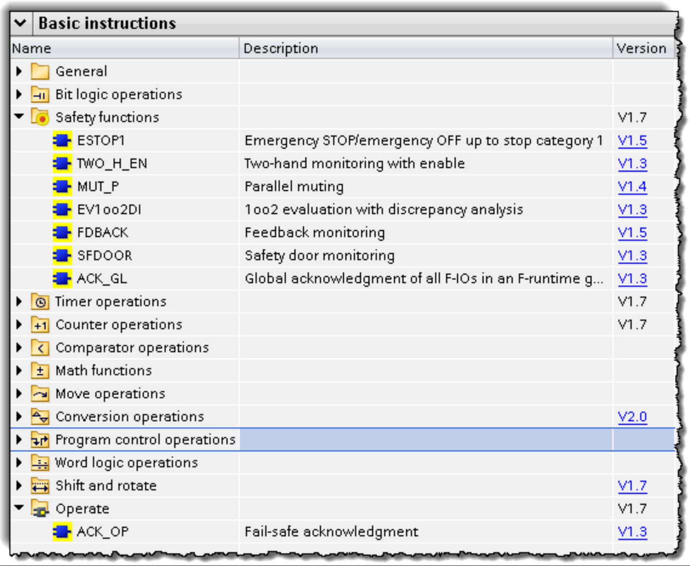
Programming with F-LAD / F-FBD

Fail-safe blocks are edited in the same way as standard blocks. The programming languages F-FBD and F-LAD correspond to the standard FBD and LAD languages, but are restricted in their set of operations and the data types and operand areas that they can use. It is not possible to program using Statement List (STL) in safety-related blocks. The editor marks all safe operands within F-blocks in yellow.

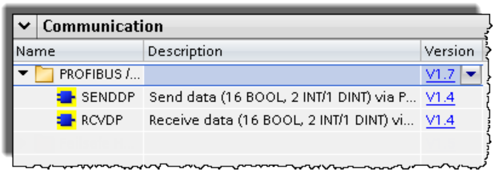
6.9.1. Safety Library

Safety functions from the library

- Contains certified F-blocks for the following safety functions:



Name	Description	Version
General		
Bit logic operations		
Safety functions		V1.7
ESTOP1	Emergency STOP/emergency OFF up to stop category 1	V1.5
TWO_H_EN	Two-hand monitoring with enable	V1.3
MUT_P	Parallel muting	V1.4
EV1oo2DI	1oo2 evaluation with discrepancy analysis	V1.3
FDBACK	Feedback monitoring	V1.5
SFDOOR	Safety door monitoring	V1.3
ACK_GL	Global acknowledgment of all F-IOs in an F-runtime g...	V1.3
Timer operations		V1.7
Counter operations		V1.7
Comparator operations		
Math functions		
Move operations		
Conversion operations		V2.0
Program control operations		
Word logic operations		
Shift and rotate		V1.7
Operate		V1.7
ACK_OP	Fail-safe acknowledgment	V1.3

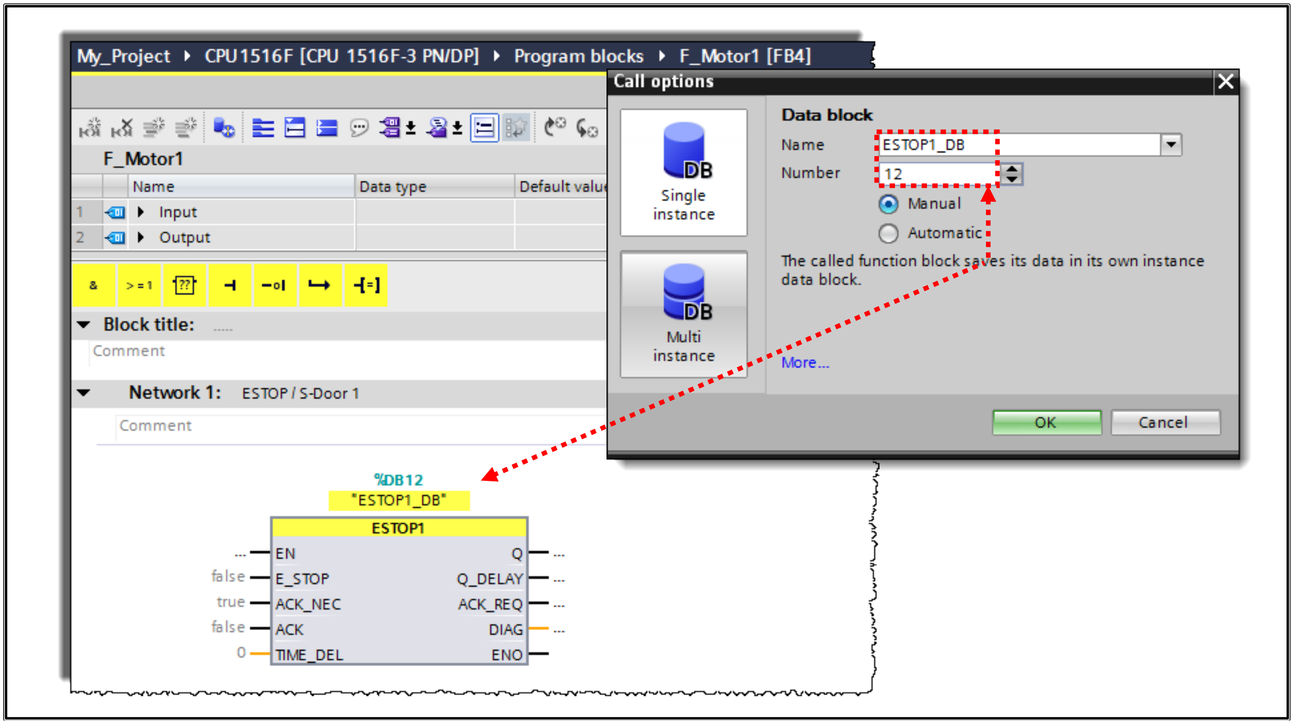


Name	Description	Version
PROFIBUS /...		V1.7
SENDDP	Send data (16 BOOL, 2 INT/1 DINT) via P...	V1.4
RCVDP	Receive data (16 BOOL, 2 INT/1 DINT) vi...	V1.4

Instructions for the Safety Program

In the "Instructions" Task Card you will find, depending on the F-CPU used, instructions which you can use to program the safety program. You will find instructions that you are familiar with from the standard user program, such as, bit logic operations, mathematical functions, functions for program control and word logic operations. In addition there are instructions with safety functions, for example, for two-hand monitoring, discrepancy analysis, muting, E-STOP, safety door monitoring and feedback monitoring.

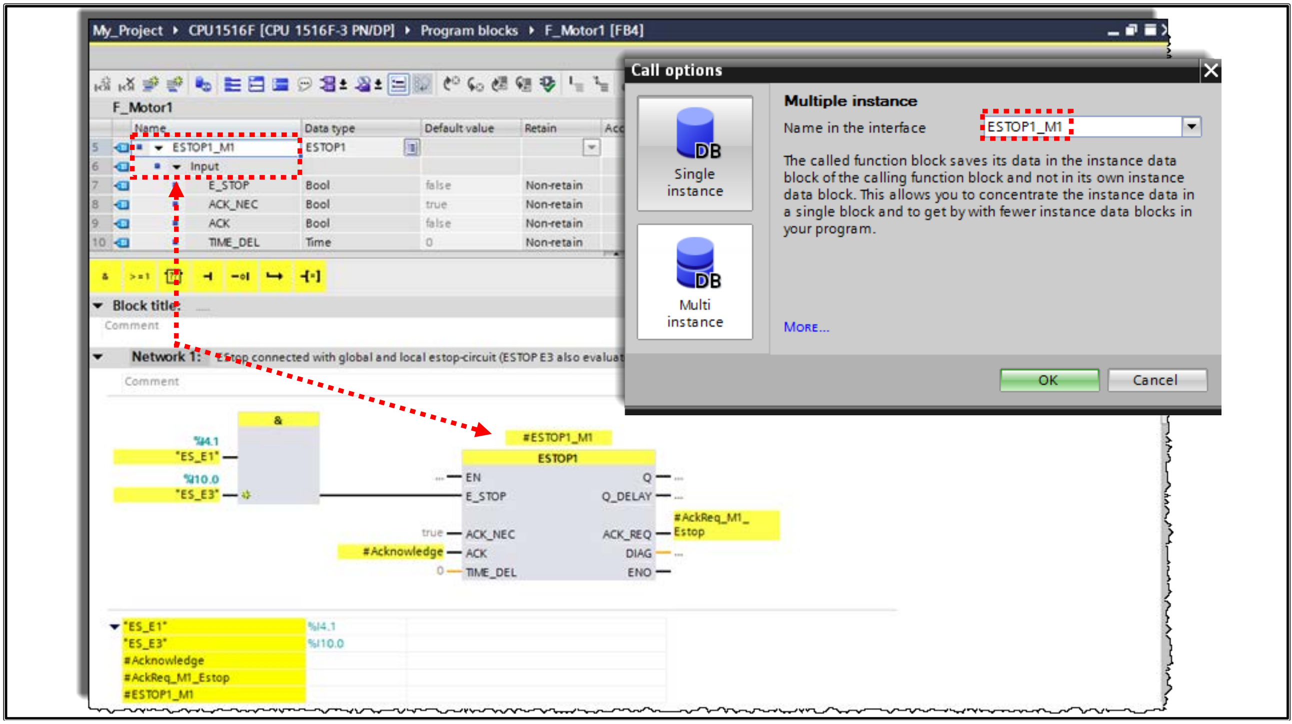
6.9.2. Instances



F-Blocks

Safety-related block calls are programmed in exactly the same way as standard block calls. Only safety-related blocks may be called in the safety program. Accordingly, only safety-related blocks are available for selection in the "FB blocks" and "FC blocks" folders in the "Overview" of the editor. When the call of a safety function is integrated or programmed, the required instance DBs are generated by STEP 7.

6.9.3. Multiple Instances



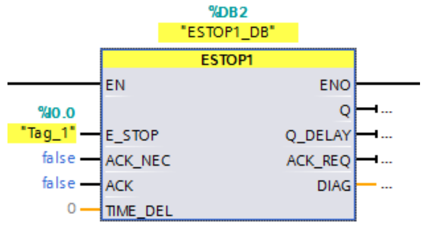
Multiple Instances

STEP 7 also supports the multi-instance concept in safety programs in order to also enable an object-oriented programming style here. This allows multiple instances of user functions as well as safety functions to be declared and called.

6.9.4. Boolean constants FALSE for "0" and TRUE for "1"

Programming with TRUE and FALSE

The Boolean constants "FALSE" for ‘0’ and "TRUE" for ‘1’ are available for S7-1500 F-CPUs.

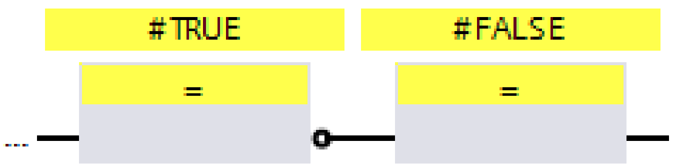


You can also create "1" or "TRUE" in a tag with the help of the Assignment instruction.

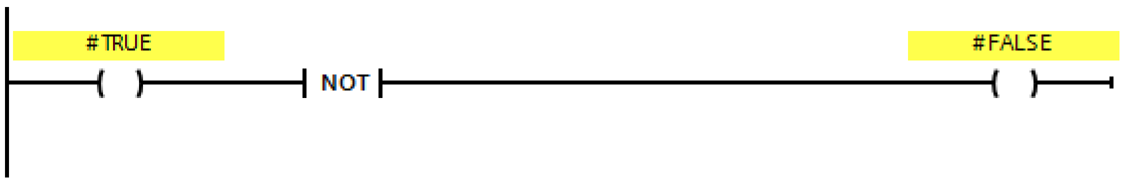
To do so, do not interconnect the box input of the Assignment instruction in FBD. In LAD, you interconnect the input directly with the power rail.

You obtain a tag with "0" or "FALSE" by subsequent inversion with the instruction Invert RLO.

Example FBD:



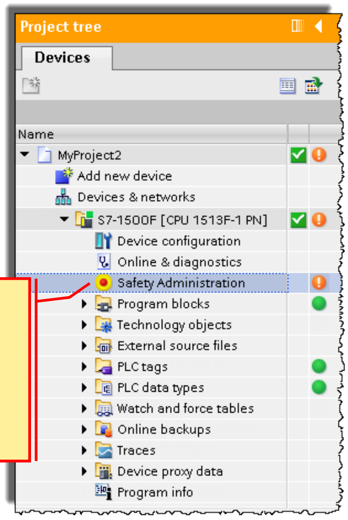
Example LAD:

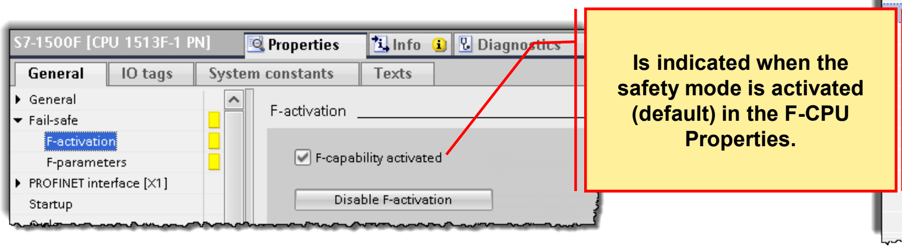


6.10. Safety Administration Editor

The Safety Administration Editor supports you in the following tasks:

- Displaying the status of the F-program (safety program)
- Defining/changing general settings for the F-program
- Displaying information about F-compliant PLC-data types
- Displaying the status of the safety mode
- Creating/organizing F-runtime groups
- Displaying information about the F-blocks
- Defining/changing the access protection
- Displaying the collective F-signature





General

The safety mode status, the safety program status and the collective F-signature is displayed under "General".

F-Runtime Groups

A safety program consists of one or two F-runtime groups. Under "F-runtime group" you define the blocks and properties of an F-runtime group.

F-Blocks

Under "F-blocks" you obtain information about the F-blocks used in your safety program and their properties.

F-Compliant PLC-Data Types

Under "F-compliant PLC data types" you obtain information about the created F-compliant PLC data types (UDT). There, you also obtain information about whether an F-compliant PLC data type (UDT) is used in the safety program.

Access Protection

Under "Access protection" you can set up, change or revoke the password for the safety program. Access protection is mandatory for productive operation.

Web Server F-Admins

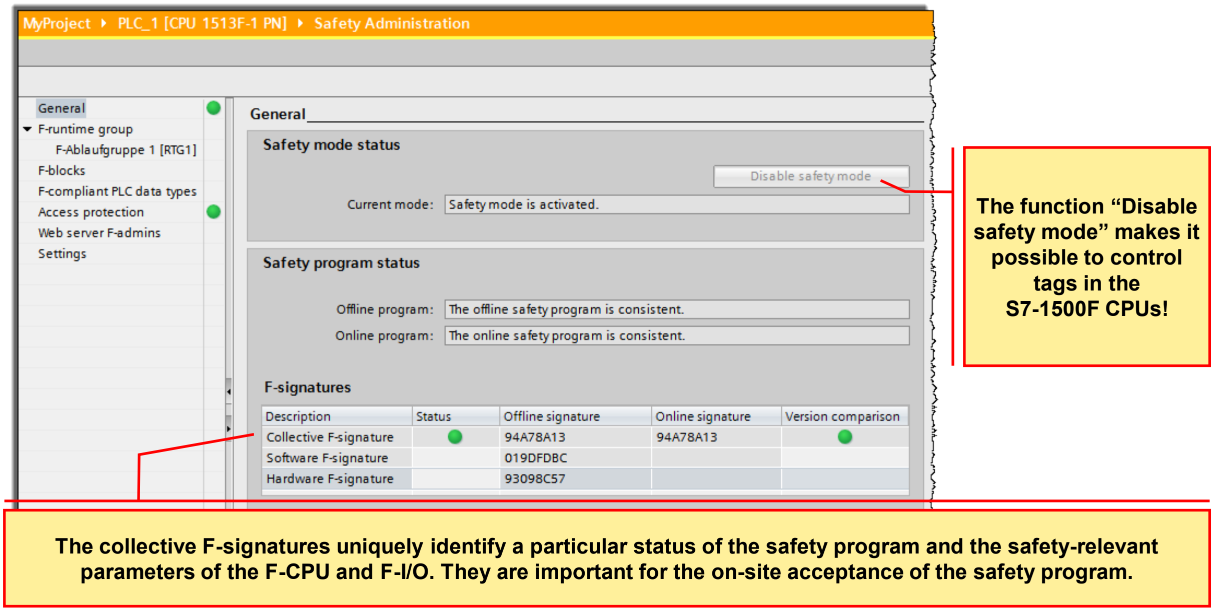
Under "Web server F-admins" you obtain information about users with the "F-Admin" attribute for the Web server of the F-CPU.

Settings

Under "Settings" you set the parameters for the safety program.

6.10.1. General

- The safety mode status, the safety program status and the collective F-signature are displayed in "General".



Safety Mode Status

The "Safety mode status" shows the current status of the safety mode. The prerequisite is an existing online connection to the selected F-CPU.

Disable Safety Mode

For an existing online connection and active safety mode operation, you have the option of using the "Disable safety mode" button to disable the safety mode for the selected F-CPU. The safety mode can be deactivated only for the entire safety program and not for individual F-runtime groups.

Requirement: "Safety mode can be disabled" is selected in the "Settings" area.

Safety Program Status

The "Safety program status" displays the current status of your online and offline program.

The following statuses are possible:

- Consistent (with information if no password has been assigned.)
- Inconsistent
- Modified

Program Signature

"Program signature" displays the collective F-signature offline, for F-CPUs S7-1200/1500 the software F-signature as well as the hardware F-signature offline, and the "Time stamp" displays the time of the last compilation process.

6.10.1.1. When does the Signature change? (1)

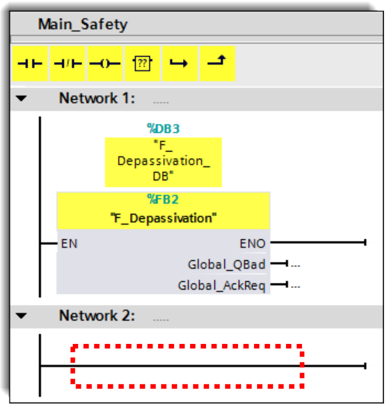
Functional signature of F-blocks

Easy comparison of changes in the F-program through the functional signature.
The functional signature of F-blocks is only changed when the logic in the F-block changes and not because the block number is changed or a new version.

Example of the signatures before a change:

Collective F-signature	
Collective F-signature	1191C305
Current compilation	
Safety program state	The offline safety program is consistent.
Compilation time	4/24/2017 10:15:50 AM (UTC +2:00)
Used Versions	
STEP 7	STEP 7 Professional V14 Update 1
Safety	STEP 7 Safety V14

Block name [Block number]	Function in safety program	Used and compiled in F-RTG	Signature
Main_Safety [FB1]	F-FB	RTG1	E3BA07D8
F_Depassivation [FB2]	F-FB	RTG1	FA5A604B
F_Depassivation_ [DB83]	F-IDB	RTG1	27E959F6



6.10.1.2. When does the Signature change? (2)

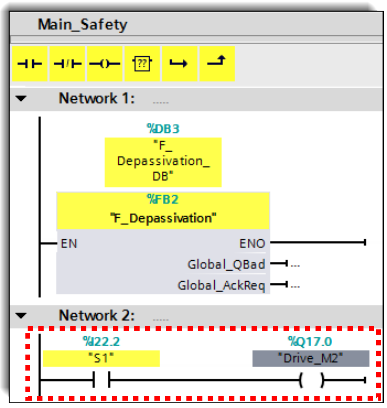
Functional signature of F-blocks

Easy comparison of changes in the F-program through the functional signature.
The functional signature of F-blocks is only changed when the logic in the F-block changes.

Example of the signatures after a change: signature changed

Collective F-signature	
Collective F-signature	49C7C2CC
Current compilation	
Safety program state	The offline safety program is consistent.
Compilation time	4/24/2017 10:41:37 AM (UTC +2:00)
Used Versions	
STEP 7	STEP 7 Professional V14 Update 1
Safety	STEP 7 Safety V14

Block name [Block number]	Function in safety program	Used and compiled in F-RTG	Signature
Main_Safety [FB1]	F-FB	RTG1	B57CC2AA
F_Depassivation [FB2]	F-FB	RTG1	FA5A604B
F_Depassivation_ [DB83]	F-IDB	RTG1	27E959F6

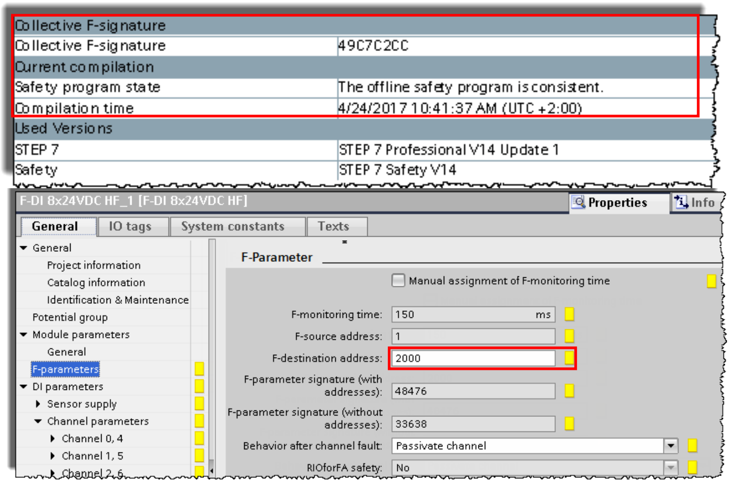


6.10.1.3. When does the Signature change? (3)

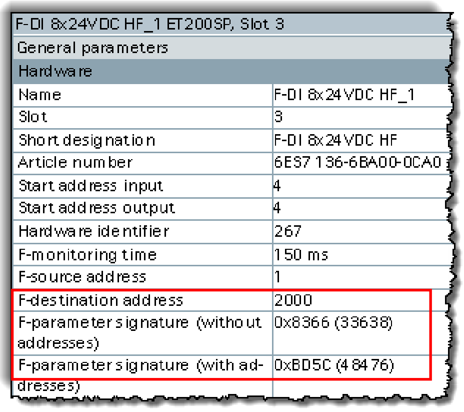
Parameter signature of F-I/O with and without address:

If this is identical, then only the PROFIsafe address has changed. In this case, the other F-parameters of the F-I/O module do not have to be compared individually.

Example of the signatures before a change:



Collective F-signature	
Collective F-signature	49C7C2CC
Current compilation	
Safety program state	The offline safety program is consistent.
Compilation time	4/24/2017 10:41:37 AM (UTC +2:00)
Used Versions	
STEP 7	STEP 7 Professional V14 Update 1
Safety	STEP 7 Safety V14



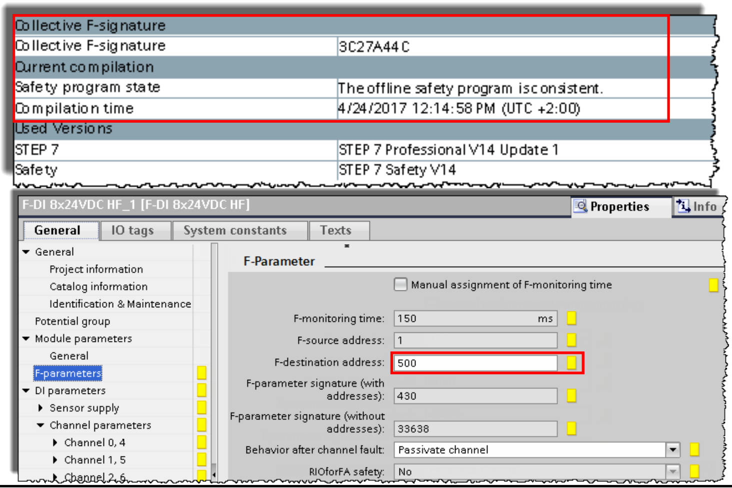
F-DI 8x24VDC HF_1 ET200SP, Slot 3	
General parameters	
Hardware	
Name	F-DI 8x24VDC HF_1
Slot	3
Short designation	F-DI 8x24VDC HF
Article number	6ES7 136-6BA00-0CA0
Start address input	4
Start address output	4
Hardware identifier	267
F-monitoring time	150 ms
F-source address	1
F-destination address	2000
F-parameter signature (without addresses)	0x8366 (33638)
F-parameter signature (with addresses)	0xBD5C (48476)

6.10.1.4. When does the Signature change? (4)

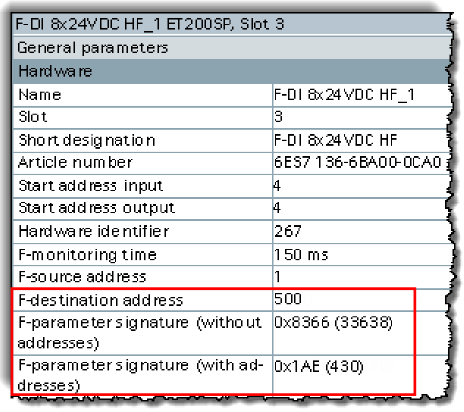
Parameter signature of F-I/O with and without address:

If this is identical, then only the PROFIsafe address has changed. In this case, the other F-parameters of the F-I/O module do not have to be compared individually.

Example of the signatures after a change: signature changed



Collective F-signature	
Collective F-signature	3C27A44C
Current compilation	
Safety program state	The offline safety program is consistent.
Compilation time	4/24/2017 12:14:58 PM (UTC +2:00)
Used Versions	
STEP 7	STEP 7 Professional V14 Update 1
Safety	STEP 7 Safety V14

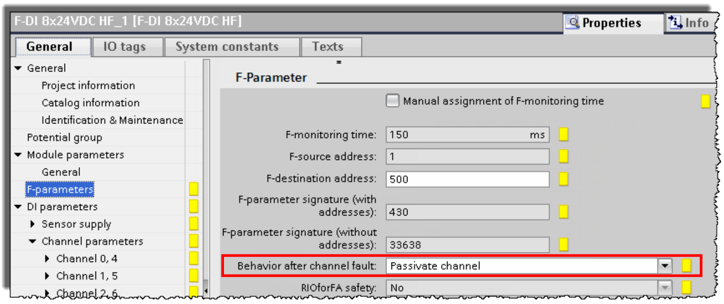


F-DI 8x24VDC HF_1 ET200SP, Slot 3	
General parameters	
Hardware	
Name	F-DI 8x24VDC HF_1
Slot	3
Short designation	F-DI 8x24VDC HF
Article number	6ES7 136-6BA00-0CA0
Start address input	4
Start address output	4
Hardware identifier	267
F-monitoring time	150 ms
F-source address	1
F-destination address	500
F-parameter signature (without addresses)	0x8366 (33638)
F-parameter signature (with addresses)	0x1AE (430)

6.10.1.5. When does the Signature change? (5)

Changing a different F-parameter of the F-I/O module
Example of the signatures before a change:

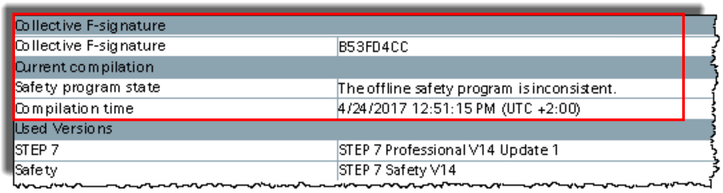
Collective F-signature	
Collective F-signature	3C27A44C
Current compilation	
Safety program state	The offline safety program is consistent.
Compilation time	4/24/2017 12:14:58 PM (UTC +2:00)
Used Versions	
STEP 7	STEP 7 Professional V14 Update 1
Safety	STEP 7 Safety V14



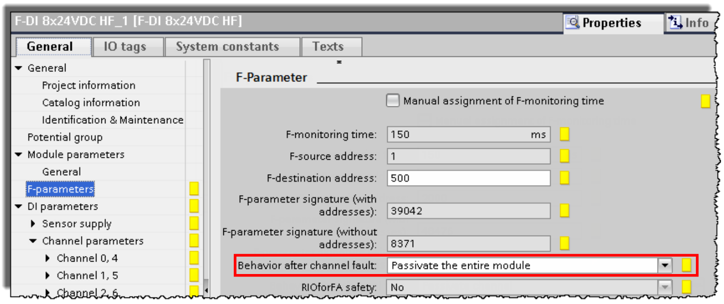
F-DI 8x24VDC HF_1 ET200SP, Slot 3	
General parameters	
Hardware	
Name	F-DI 8x24VDC HF_1
Slot	3
Short designation	F-DI 8x24VDC HF
Article number	6ES7 136-6BA00-0CA0
Start address input	4
Start address output	4
Hardware identifier	267
F-monitoring time	150 ms
F-source address	1
F-destination address	500
F-parameter signature (without addresses)	0x8366 (33638)
F-parameter signature (with addresses)	0x1AE (430)

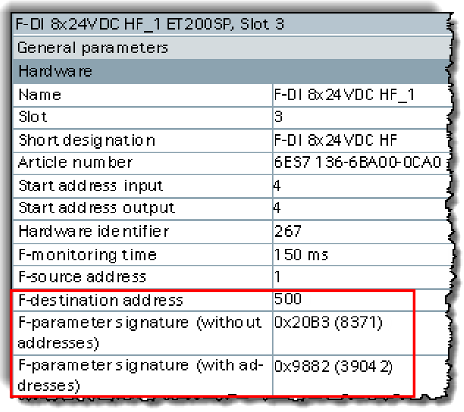
6.10.1.6. When does the Signature change? (6)

Changing a different F-parameter of the F-I/O module
Example of the signatures after a change: signature changed



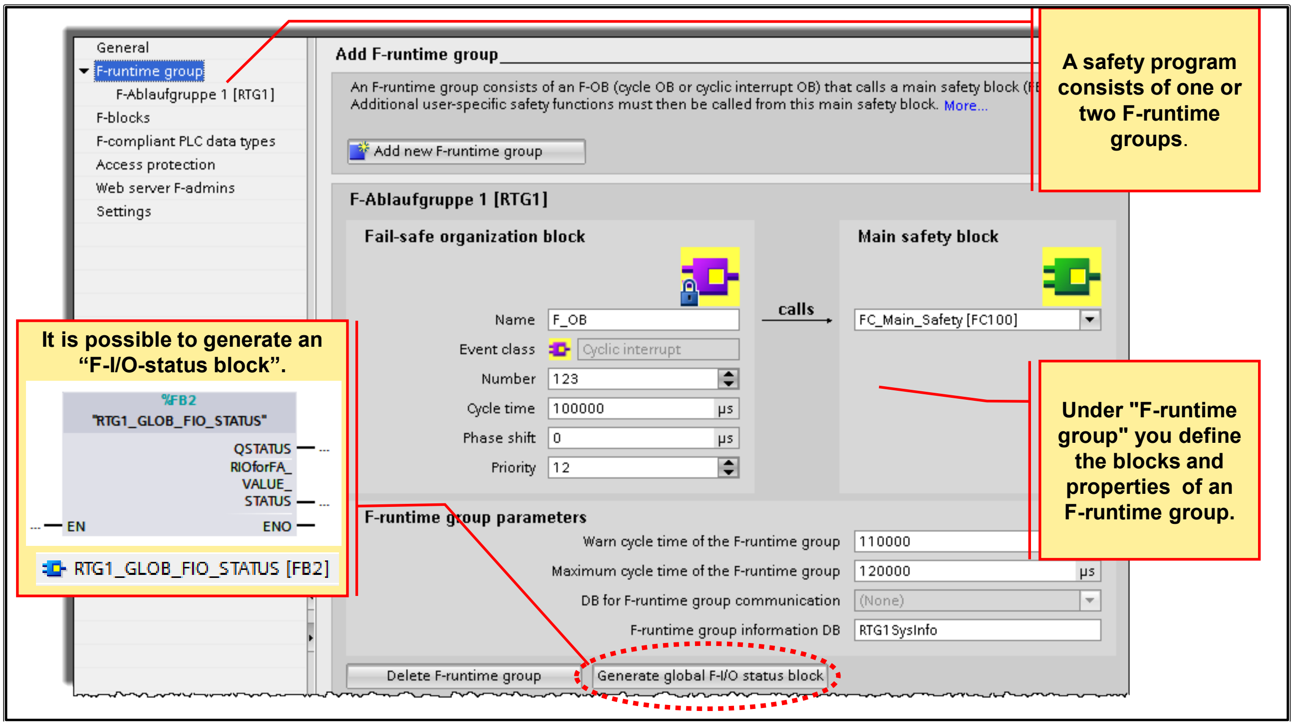
Collective F-signature	
Collective F-signature	B53FD4CC
Current compilation	
Safety program state	The offline safety program is inconsistent.
Compilation time	4/24/2017 12:51:15 PM (UTC +2:00)
Used Versions	
STEP 7	STEP 7 Professional V14 Update 1
Safety	STEP 7 Safety V14





F-DI 8x24VDC HF_1 ET200SP, Slot 3	
General parameters	
Hardware	
Name	F-DI 8x24VDC HF_1
Slot	3
Short designation	F-DI 8x24VDC HF
Article number	6ES7 136-6BA00-0CA0
Start address input	4
Start address output	4
Hardware identifier	267
F-monitoring time	150 ms
F-source address	1
F-destination address	500
F-parameter signature (without addresses)	0x20B3 (8371)
F-parameter signature (with addresses)	0x9882 (39042)

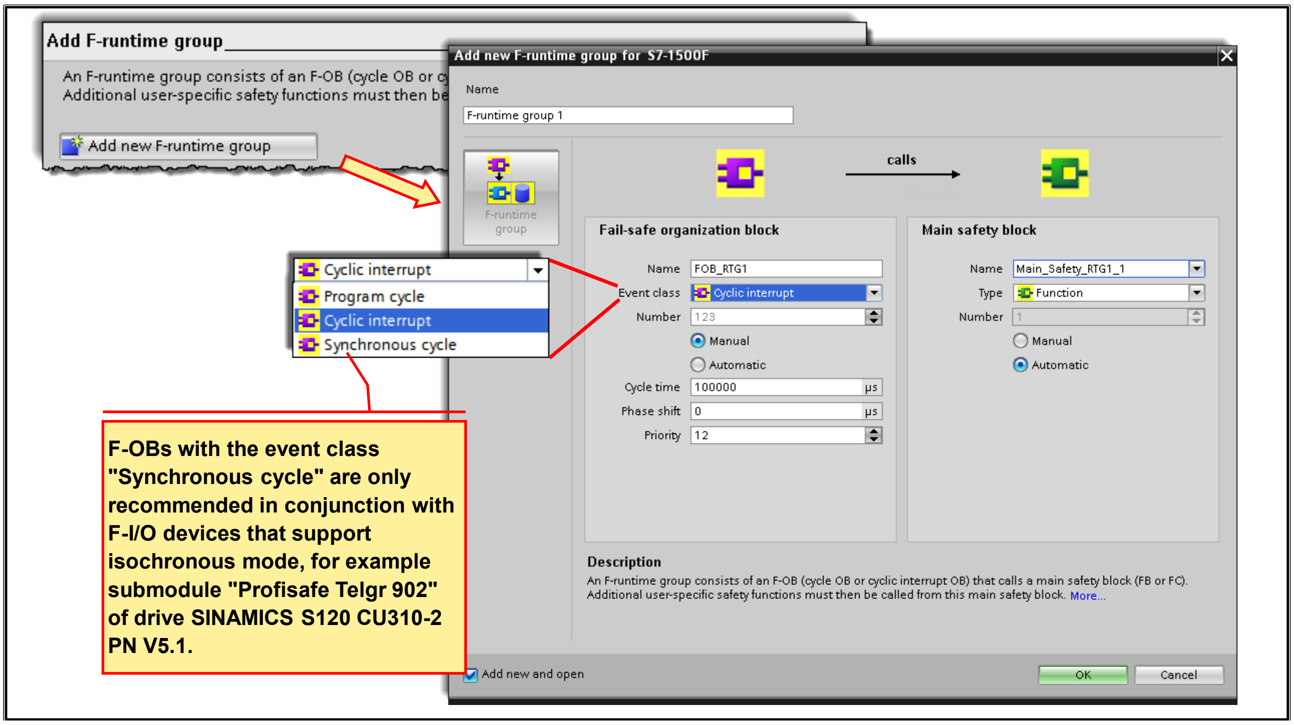
6.10.2. F-Runtime Groups



Rules:

- The channels (channel values and value status) of an F-I/O may only be accessed from one individual F-runtime group.
- Tags of the F-I/O DB of an F-I/O may only be accessed from one F-runtime group and only from the F-runtime group from which access to the channels and value status of this F-I/O occurs (if access exists).
- F-FBs can be used in several F-runtime groups but they must be called with different instance DBs.
- Instance DBs to F-FBs may only be accessed from the F-runtime group in which the associated F-FB is called.
- A tag of a global F-DB may only be accessed from one F-runtime group (however, a global F-DB may be used in several F-runtime groups).
- (S7-1200, S7-1500) You cannot call the Main-Safety-Block. It is automatically called by the assigned F-OB.
- (S7-1200, S7-1500) The F-OB should be created with the highest priority of all OBs.
- The process image for inputs and outputs of standard I/O, memory bits and tags of DBs of the standard user program may be accessed either reading or writing from several F-runtime groups. (also see data exchange between standard user program and safety program)
- F-FCs can generally be called in several F-runtime groups.

6.10.3. Creating an F-Runtime Group



For an F-OB you can select between the event classes "Program cycle", "Cyclic interrupt" or "Synchronous cycle".

In the case of the F-runtime group created by default, the F-OB has the event class "Cyclic interrupt". To change the event class of the F-OB of an already created F-runtime group, you need to delete and F-runtime group and create a new one.

Cyclic interrupt

We recommend creating the F-OB with the event class "Cyclic interrupt" as "cyclic interrupt OB". The safety program will then be called and run at fixed time intervals.

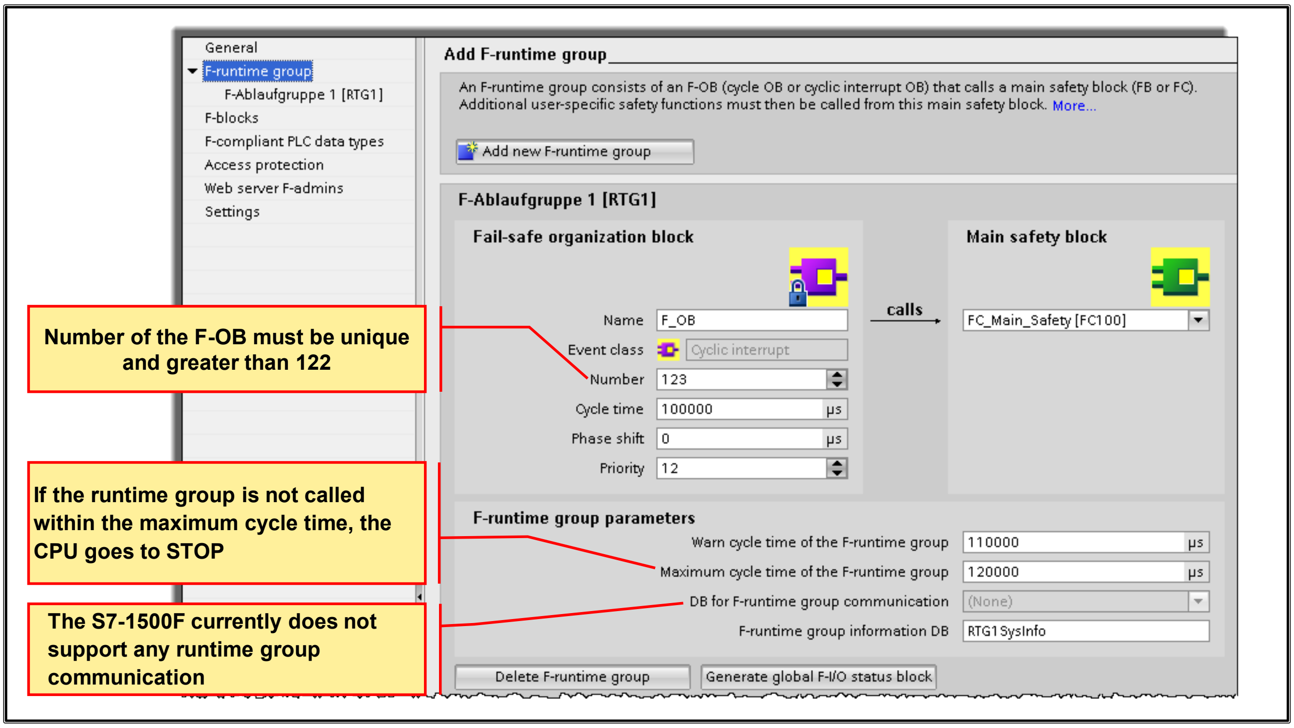
Synchronous cycle

F-OBs with the event class "Synchronous cycle" are only recommended in conjunction with F-I/O devices that support isochronous mode, for example submodule "Profisafe Telgr 902" of drive SINAMICS S120 CU310-2 PN V5.1.

Program cycle

F-OBs with the event class "Program cycle" are not recommended, as these have the lowest priority "1".

6.10.4. F-Runtime Group - Settings



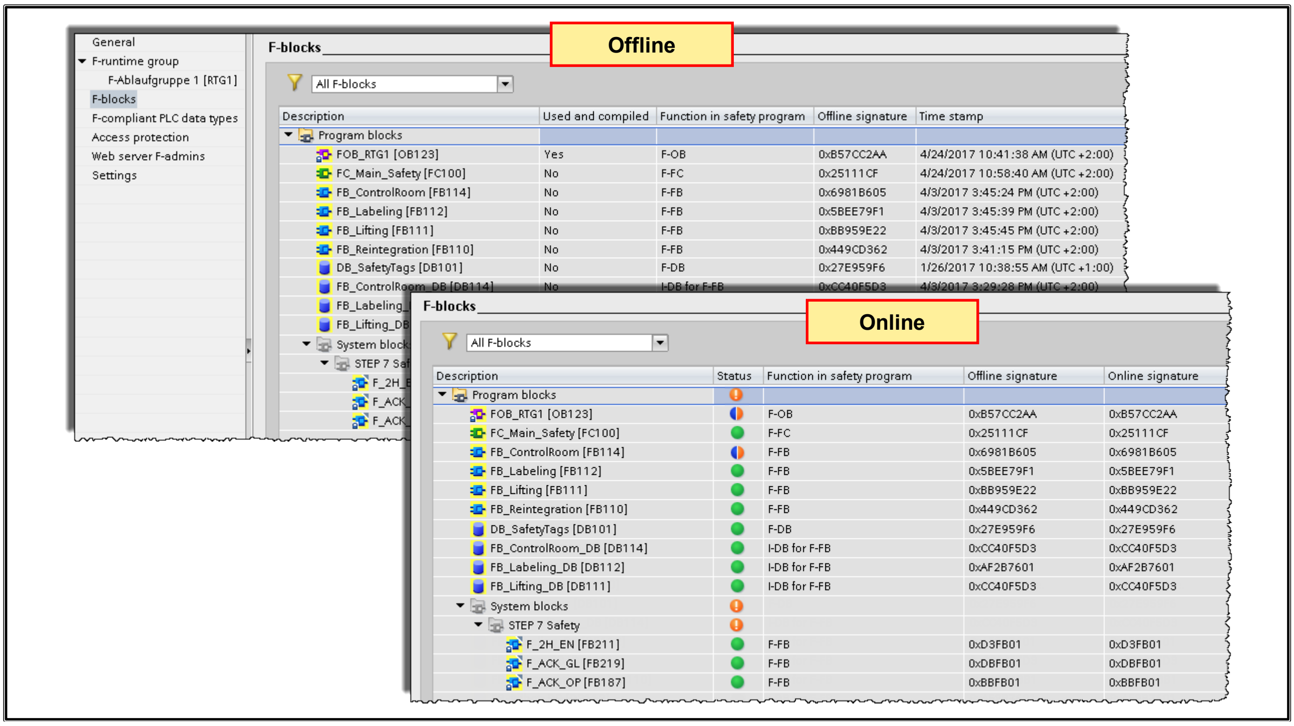
Parameters of the F-Runtime Group

The F-CPU performs monitoring of the F-cycle time in the F-runtime group. Two parameters are available for this:

- If "Warn cycle time of the F-runtime group" is exceeded, an entry is written in the diagnostic buffer of the F-CPU. You can use this parameter to determine, for example, whether the cycle time exceeds a required value without the F-CPU going to STOP.
- If "Maximum cycle time of the F-runtime group" is exceeded, the F-CPU goes to STOP. For "Maximum cycle time of the F-runtime group" select the maximum time that may elapse between two calls of this F-runtime group (maximum of 20000000 µs).

Under "F-runtime group information DB", assign a name for the F-runtime group information DB.

6.10.5. F-Blocks



Displayed Information

The following information is displayed for F-blocks in offline mode:

- Has the F-block been compiled and used?
- Function of F-lock in the safety program
- Offline signature
- Time stamp of the last change

The following information is displayed for F-blocks in online mode:

- Status (whether block has the same time stamp online and offline)
- Function of F-block in the safety program
- Offline signature
- Online signature
- The F-blocks are hierarchically displayed just as in the "Program blocks" folder.

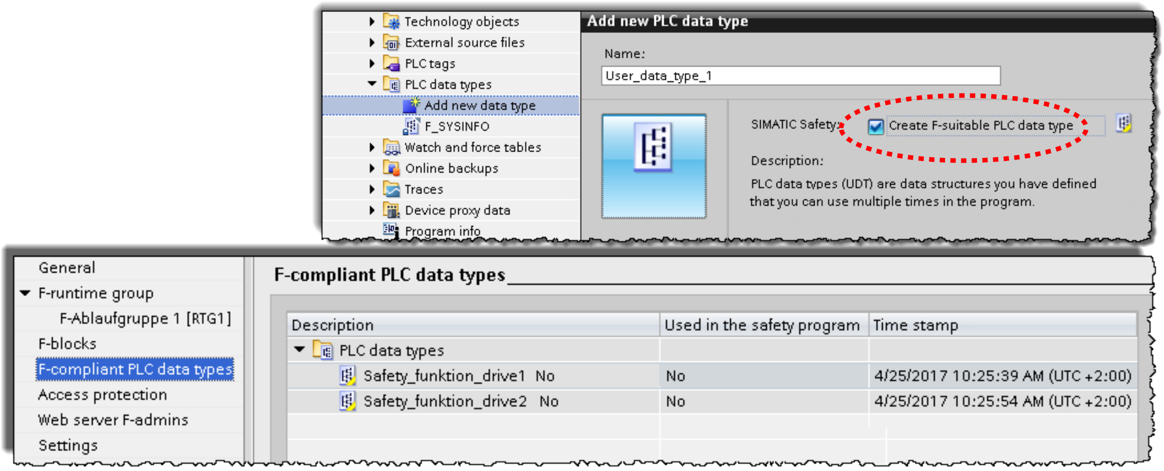
Filter Function

Using the filter function, you can select whether you want to view all F-blocks of a certain F-runtime group or the entire safety program.

- Select "All F-blocks" from the drop-down list to view all F-blocks.
- Select an F-runtime group from the drop-down list to see all F-blocks of this F-runtime group.

6.10.6. F-Compliant PLC-Data Types

- F-UDTs are declared and used just like UDTs.
- In F-UDTs, you can use all data types that are allowed in the F-program.
- The nesting of F-UDTs within other F-UDTs is not supported!
- F-UDTs can be used in the safety program as well as in the standard program.



Displayed Information

The following information is displayed for F-compliant PLC data types (UDT) in offline mode:

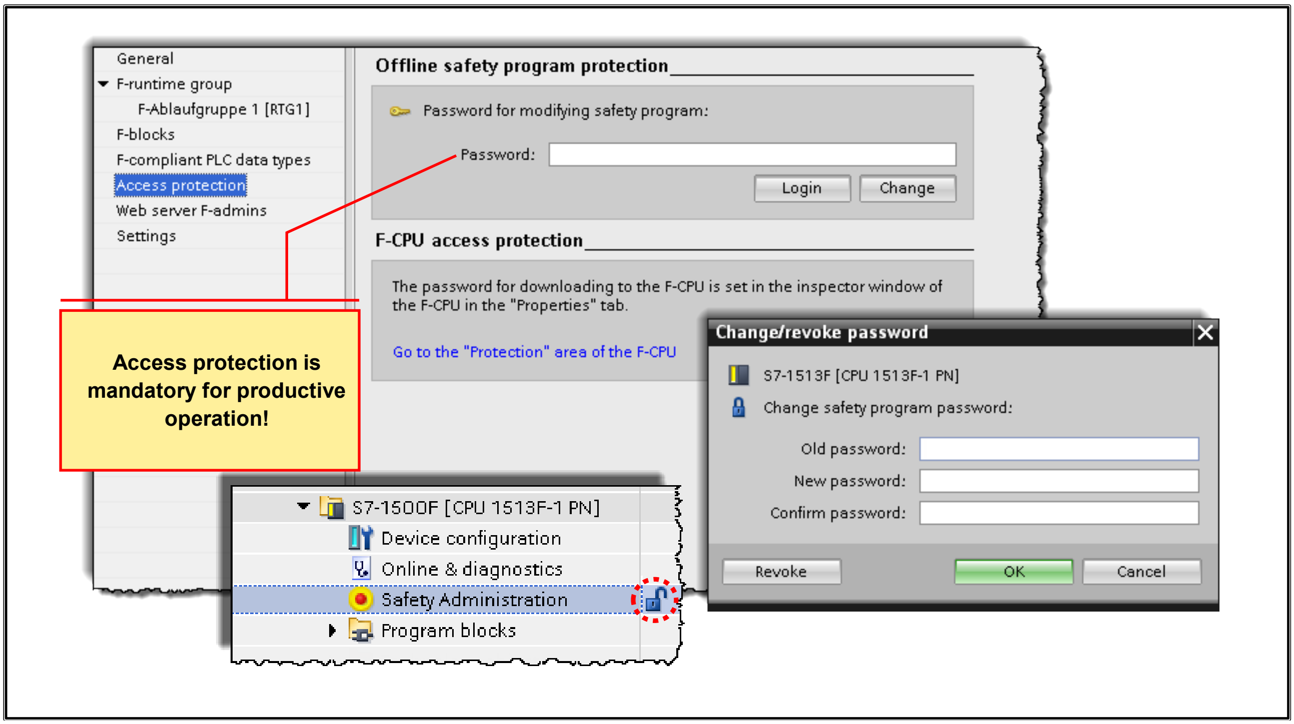
- Is the F-compliant PLC data type used in the safety program?
- Time stamp of the last change.

The following information is displayed for F-compliant PLC data types (UDT) in online mode:

- Status (whether the F-compliant PLC data types (UDT) have the same time stamp online and offline)

The F-compliant PLC data types (UDT) are displayed hierarchically just as in the "PLC data types" folder.

6.10.7. Access Protection



Overview of Access Protection

You can protect access to the SIMATIC Safety F-system by two password prompts: one for the safety program and another for the F-CPU.

The password for the safety program is available in two forms:

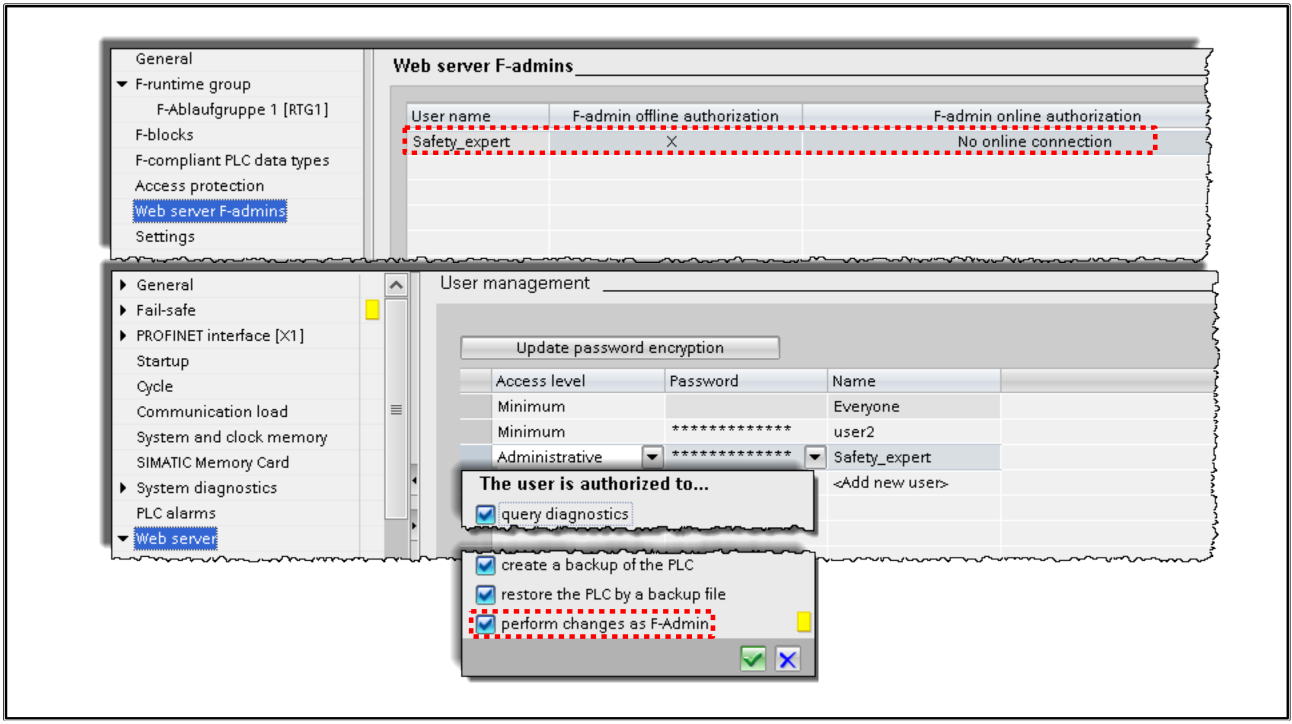
- The offline password is part of the safety program in the offline project on the PG/PC.
- The online password is part of the safety program in the F-CPU.

Note:

Safety program recompilation is required after changes to standard DBs to which the safety program has read or write access. These standard DBs are not governed by the safety program access protection.

Please note that you also need the online password to download the safety-relevant changes to the hardware configuration. This is also true for changes to F-I/O not used in the safety program. You must also recompile and download the safety program for the download to be consistent.

6.10.8. Web Server F-Admins

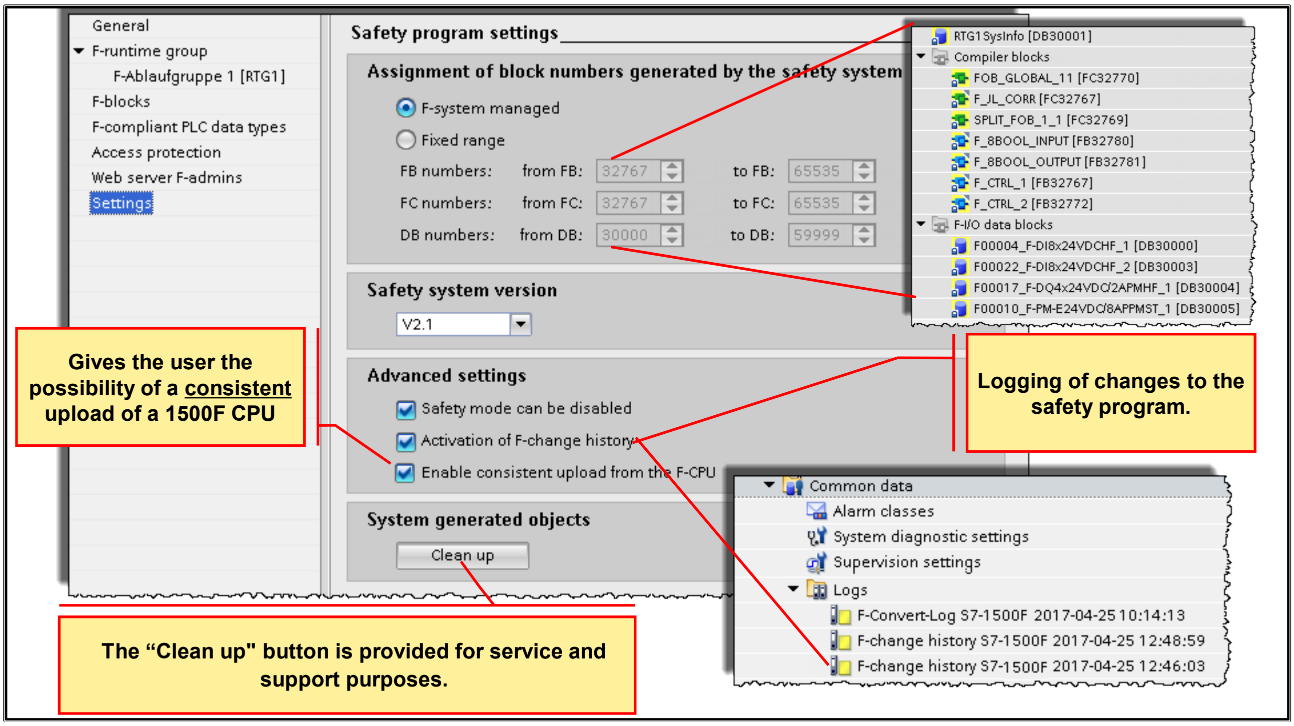


Functionality

You must have the "F-admin" rights in order to carry out restoration of a backup via the Web server of your F-CPU. You assign the "F-Admin" rights in the hardware configuration of the F-CPU under the User management of the Web server.

In this section, you obtain information on which users have the "F-Admin" rights online or offline for F-CPUs that support this right. You can see from this whether a change to the "F-Admin" rights is active on the F-CPU. In order to make a change to the "F-Admin" rights effective, you must load the configuration to the F-CPU.

6.10.9. Settings (1)



Number Ranges of the Generated F-System Blocks

The number ranges parameterized (assigned) here are used by the F-system for new, automatically generated F-blocks.

At this point, you can select whether the number ranges are managed by the F-system or if a fixed range specified by you is used.

- "F-System managed": The number ranges are managed automatically by the F-system, depending on the F-CPU used. The F-system selects an available number range. The start and end ranges of the number ranges are displayed.
- "Fixed range": You can select the start and end ranges of the number ranges from the available range. The available range depends on the F-CPU used.

Safety System Version

This parameter is used to specify the safety system version (including version of the F-system blocks and automatically generated F-blocks). Usually, you do not need to make any settings for this parameter. When a new F-CPU is created with STEP 7 Safety, the latest available version for the F-CPU created is automatically preset.

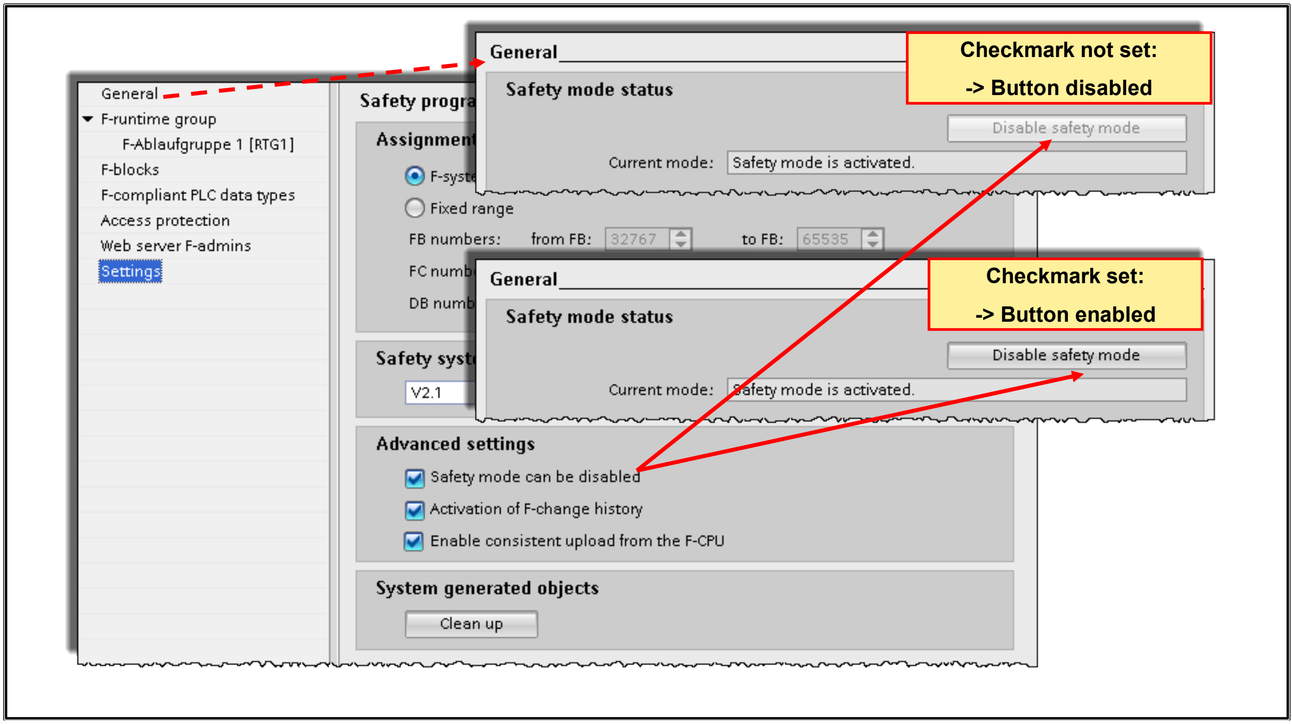
System Generated Objects

The "Clean up" button is provided for service and support purposes.

Enable Consistent Upload from the F-CPU

This option allows you to load the loaded project data (including safety-relevant project data) consistently from the F-CPU. The option can only be activated if the F-CPU and the firmware of the F-CPU support the loading of the project data (including safety-relevant project data). S7-1500 F-CPUs as of firmware V2.1 are supported. S7-1500 F Software Controllers are not supported. With every change to this option you must load the project data to the F-CPU. Note that the activation of this option extends the loading of the safety-relevant project data into the F-CPU.

6.10.10. Settings (2)



Safety Mode can be Disabled

If you deselect the "Safety mode can be disabled" option, you can prevent the disabling of the safety mode for a safety program.

When you change the setting for this option, you must recompile the safety program and download it to the F-CPU for the change to become effective. This changes the collective F-signature of your safety program.

We recommend that you disable this option before you start production and before acceptance of the safety program to prevent an unintentional disabling of the safety mode.

Activation of F-Change History

Enable the logging of changes to the safety program by using the "Activation of F-change history" option in the Safety Administration Editor. The F-change history behaves just like the standard change history.

An F-change history is created for each F-CPU in the Project tree under "Common data/logs".

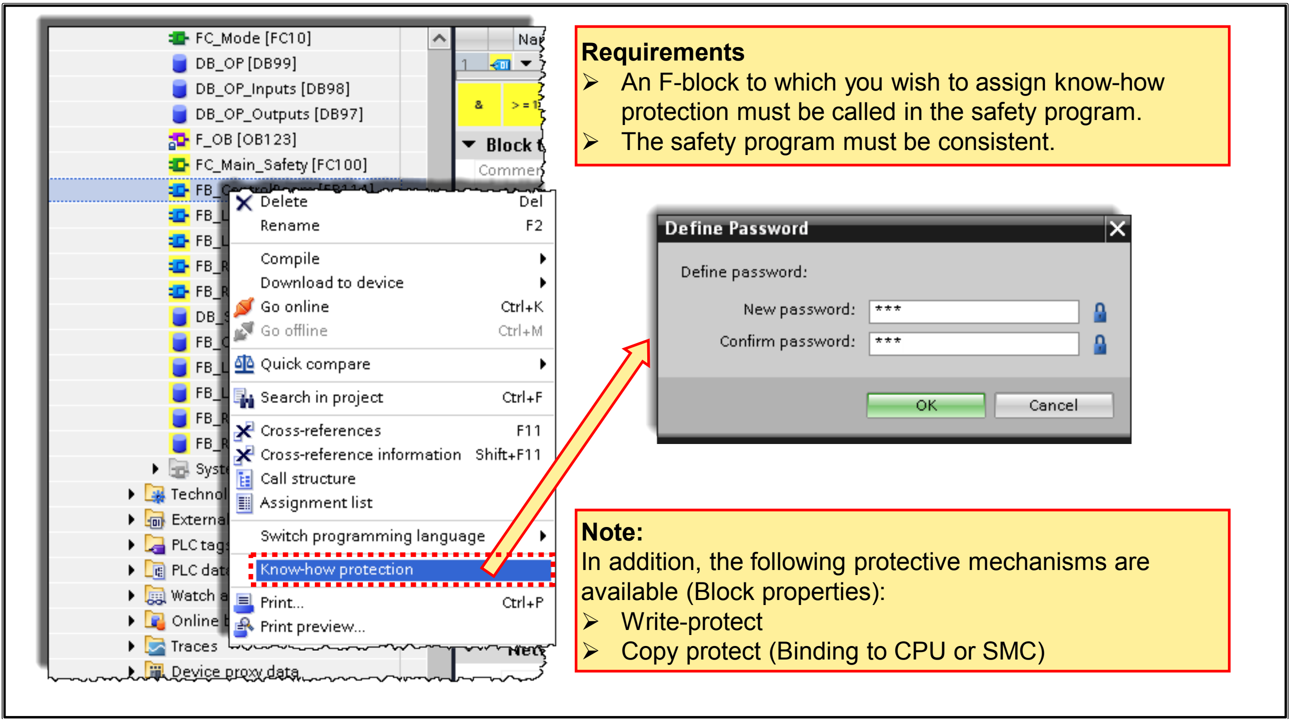
The following is logged in the F-change history:

- Collective F-signature
- User name
- Compile time stamp
- Download of the safety program with time stamp
- Compiled F-blocks with signature and time stamp

The F-change history can contain a maximum of 5000 entries per F-CPU. When the 5000 entries are exceeded, a new F-change history is created using the name pattern "F-change history <CPU name> YYYY-MM-DD hh:mm:ss".

6.11. Know-how Protection

6.11.1. Creating



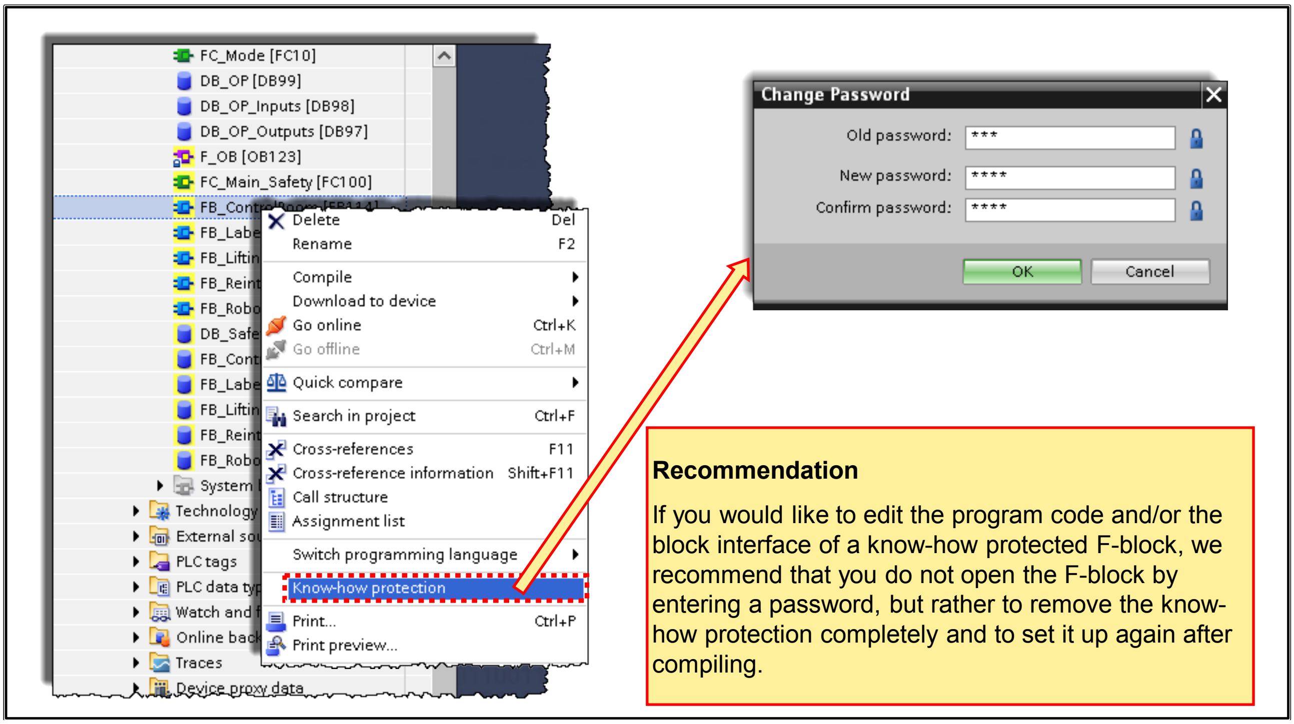
Requirements:

- An F-block to which you wish to assign know-how protection must be called in the safety program.
- Before you can set up the know-how protection for an F-block, the safety program must be consistent. For this purpose, compile the safety program.

Notes:

- No source code is output for know-how protected F-blocks in the safety summary. Therefore, create the safety summary (for example, to carry out a code review or to accept the F-block) before you set up the know-how protection.
- If you would like to edit the program code and/or the block interface of a know-how protected F-block, we recommend that you not open the F-block by entering a password. Instead remove the know-how protection completely and to set it up again after compiling.
- When a know-how protected F-block or F-blocks called by it are renamed, the signature of the know-how protected F-block is not changed until the password is entered when opening or removing the know-how protection.

6.11.2. Removing



Recommendation

If you would like to edit the program code and/or the block interface of a know-how protected F-block, we recommend that you do not open the F-block by entering a password, but rather to remove the know-how protection completely and to set it up again after compiling.

6.12. Compiling

6.12.1. Compiling the Safety Program (1)

Compiling the Safety Program

- Regardless of the option selected, a consistency check is always performed.
  - This consistency check extends across all selected blocks
  - STEP 7 V5.5: "Check block consistency" was only one option
- Search the entire program for syntax errors
- Compile the entire program into CPU-readable code
- Same procedure and buttons as for compiling a standard program
- When compiling a know-how protected block, it must first be opened!
- The content which is compiled depends on the selection in the Project tree

Compiling the Safety Program

To compile a safety program, follow the same procedure as for compiling a standard user program. You can start at various points to accomplish this in STEP 7. Regardless of the option selected, a consistency check is always performed. This consistency check extends across all selected blocks. If no errors are detected by the consistency check, the status of the compiled safety program is consistent.

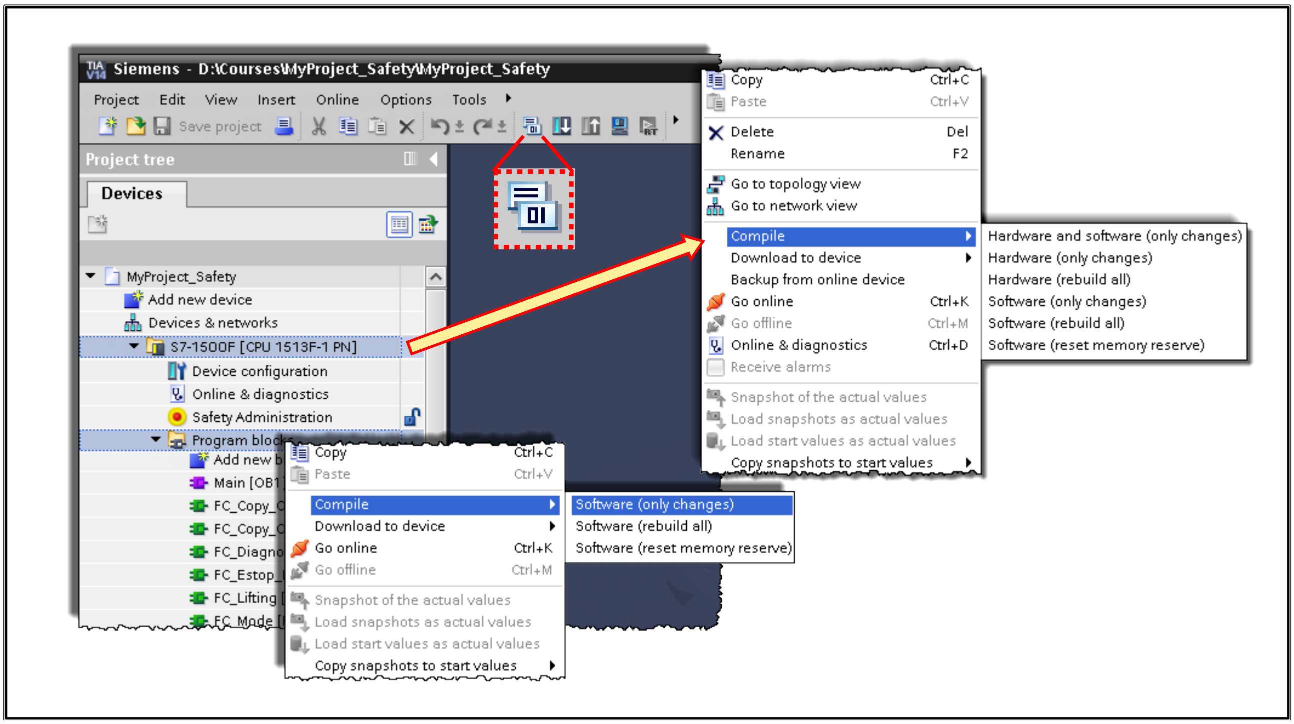
"Safety Program is Consistent"

After the safety program is successfully compiled, a consistent safety program is always located in the "Program blocks" folder. Nevertheless, there can be F-blocks that are not called in an F-runtime group. These F-blocks are shown in the "F-blocks" area of the Safety Administration editor and are identified with "No" in the "Used & compiled" column.

Result "Safety Program is Not Consistent"

When the safety program is compiled with the result "Safety program is not consistent", only the selected F-blocks were compiled. Additionally needed F-blocks and F-system blocks were not generated. The safety program in the "Program blocks" folder is not consistent and is thus not executable.

6.12.2. Compiling the Safety Program (2)



Compiling the Safety Program

The consistency of the offline safety program exists only if the safety program is completely compiled after every safety-relevant change – whether the change is in the hardware configuration or parameter assignment, or, in the safety program itself. Only a consistent safety program is given an offline signature.

Software (Only Changes)

Only the modified blocks of the standard program and safety program are compiled.

Software (Rebuild All)

All blocks of the standard program and safety program are compiled.

Reporting Compiling Errors

You can recognize whether or not the compilation was successful based on the message in the Inspector window under "Info > Compile"; error messages and warnings are output. To learn about how to eliminate compiling errors, refer to the Help on STEP 7, "Eliminating compiling errors".

6.13. Downloading into the CPU

6.13.1. Downloading the Safety Program into the CPU (1)

Downloading the Safety Program

- After the F-program is successfully compiled, it can be downloaded into the F-CPU.
- Same procedure and buttons as for downloading a standard program
- Only consistent download or the downloading of all blocks possible
- In the "Load preview" dialog, enter data (for example, password of the F-CPU) and set the requirements for downloading (for example, that the F-CPU is switched to STOP mode before downloading).
- The content which is downloaded depends on the selection in the Project tree

Downloading the Safety Program

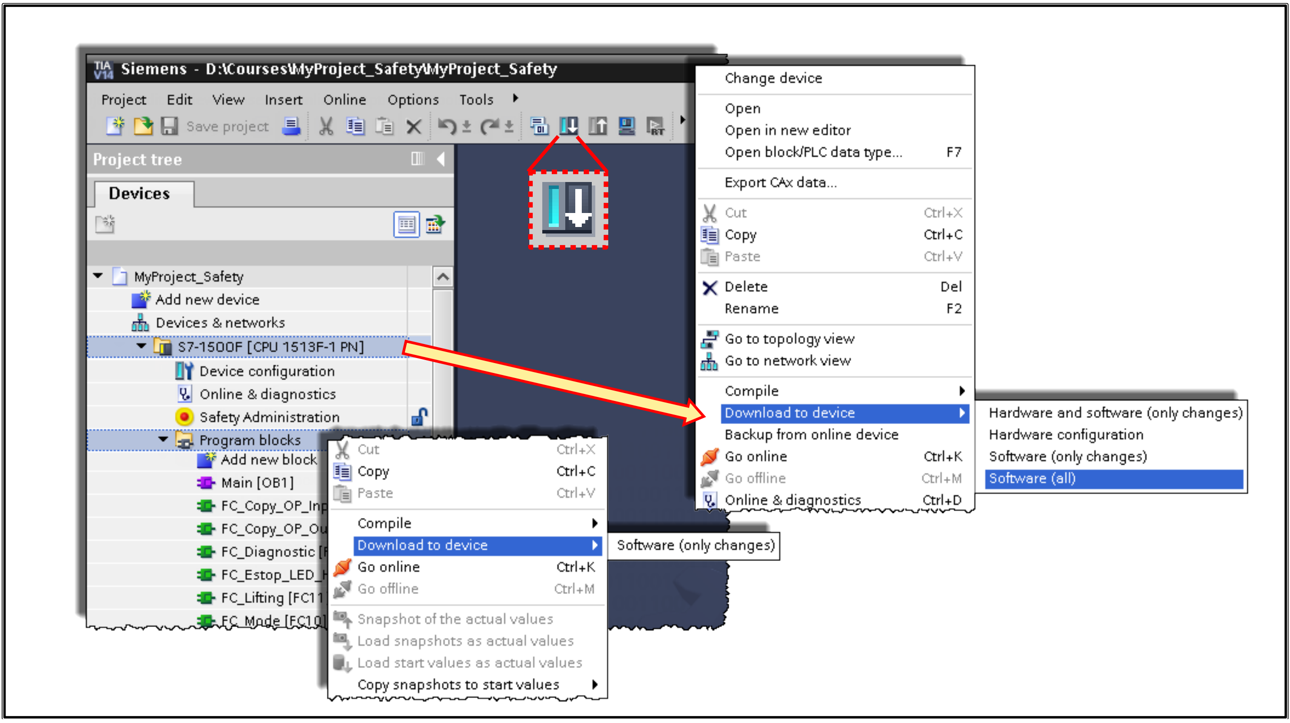
To download a safety program, you follow essentially the same approach as for downloading a standard user program, via different starting points in STEP 7:

- In the "Load preview" dialog, enter data (for example, password for the F-CPU) and set the requirements for downloading (for example, that the F-CPU is switched to STOP mode before downloading).
- The "Load results" dialog shows the results after downloading.

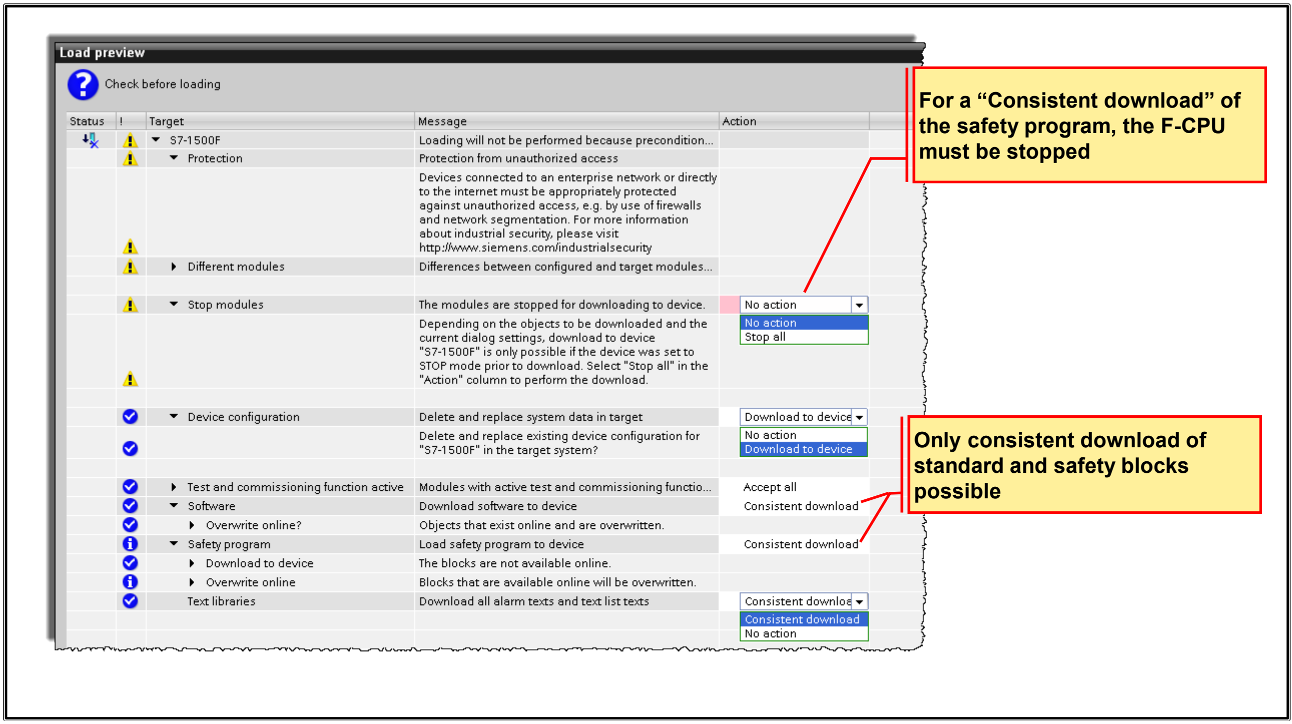
Downloading the Safety Program into the CPU

The consistency of the CPU safety program exists only if the safety program is completely compiled after every safety-relevant change – whether the change is in the hardware configuration or parameter assignment, or, in the safety program itself – and downloaded into the CPU. This is only possible when the CPU is in the STOP state. Only a consistent safety program is given an online signature.

6.13.2. Downloading the Safety Program into the CPU (2)



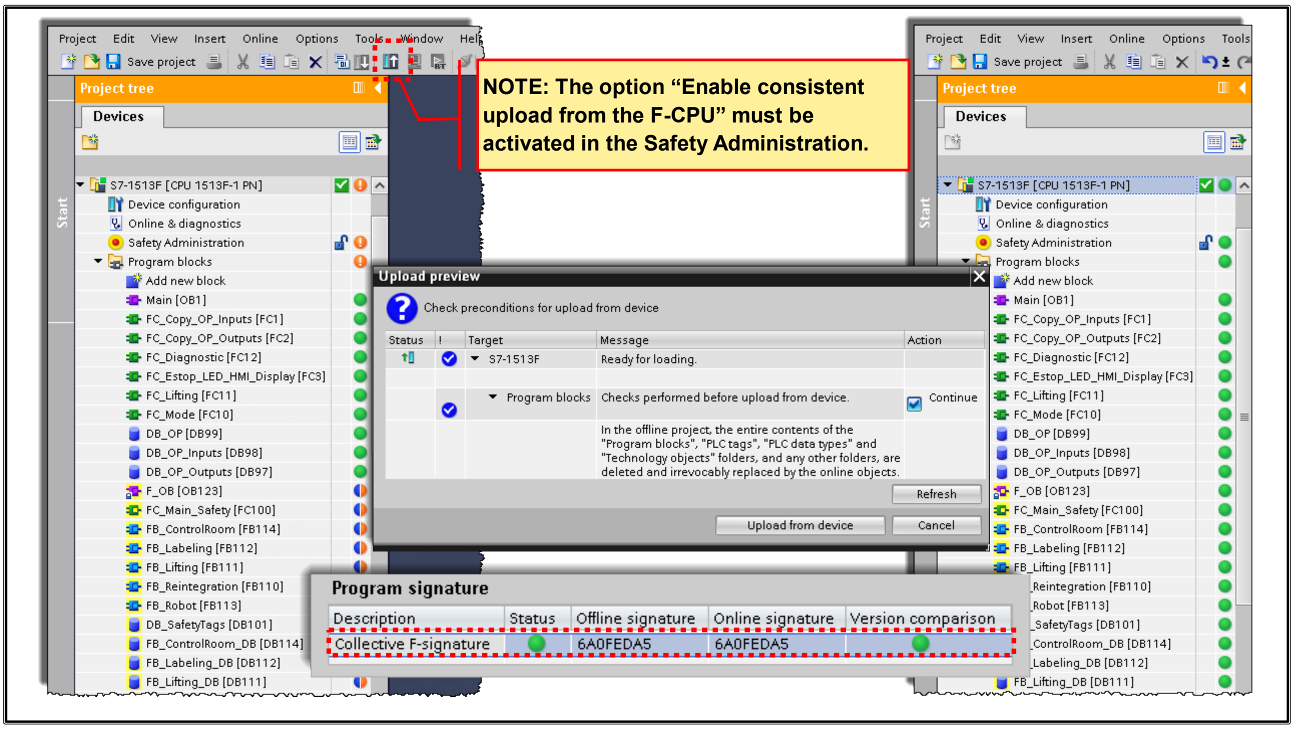
6.13.3. Downloading the Safety Program into the CPU (3)



For S7-1200/1500 F-CPUs, only the "Consistent download" value is possible as an action in the "Load preview" dialog. It is not possible to select separate loading of standard program or safety program. The complete user program is automatically, consistently downloaded as soon as changes have been made in both the standard program and in the safety program.

6.14. Uploading into the PG

6.14.1. Uploading the Safety Program into the PG



Uploading the Safety Program into a PG/PC (S7-1200, S7-1500)

The "Upload from device (software)" or "Upload device as new station (hardware and software)" function is only possible S7-1500 F-CPUs if the "Enable consistent upload from the F-CPU" option is activated for the F-CPU in the Safety Administration Editor and the project data is loaded to the F-CPU afterwards.

To load the project data (including safety-relevant project data) to a PG/PC, proceed as for standard blocks. If several F-CPUs can be reached over a network (for example, Industrial Ethernet) by the PG/PC, ensure that the project data is downloaded from the correct F-CPU, for example, with "Online & diagnostics" > "Online access" > "Flash LED". After successful loading from the device, you can continue working just as with a project that was created offline. You can load individual F-blocks into a PG/PC irrespective of the "Enable consistent upload from the F-CPU" option. You cannot upload individual know-how protected F-blocks to a PG/PC.

6.15. Testing the Safety Program

Monitoring

Read-only test functions (such as monitoring tags of the safety program) are available for safety programs as in the standard.

Modifying

Read and write test functions (such as controlling tags of the safety program) are only available to a limited extent for safety programs and only in disabled safety mode.

Rules for testing

- **Forcing** of F-I/O inputs and F-I/O outputs is **not possible**.
- Controlling F-I/O outputs in connection with the function “Enabling F-I/O outputs" is not possible.
- Setting breakpoints in the standard user program will cause errors in the safety program (see also Testing the safety program.

Testing the Safety Program

After creating a safety program, you must carry out a complete function test in accordance with your automation task. For changes made to a safety program that has already undergone a complete function test, only the changes need to be tested.

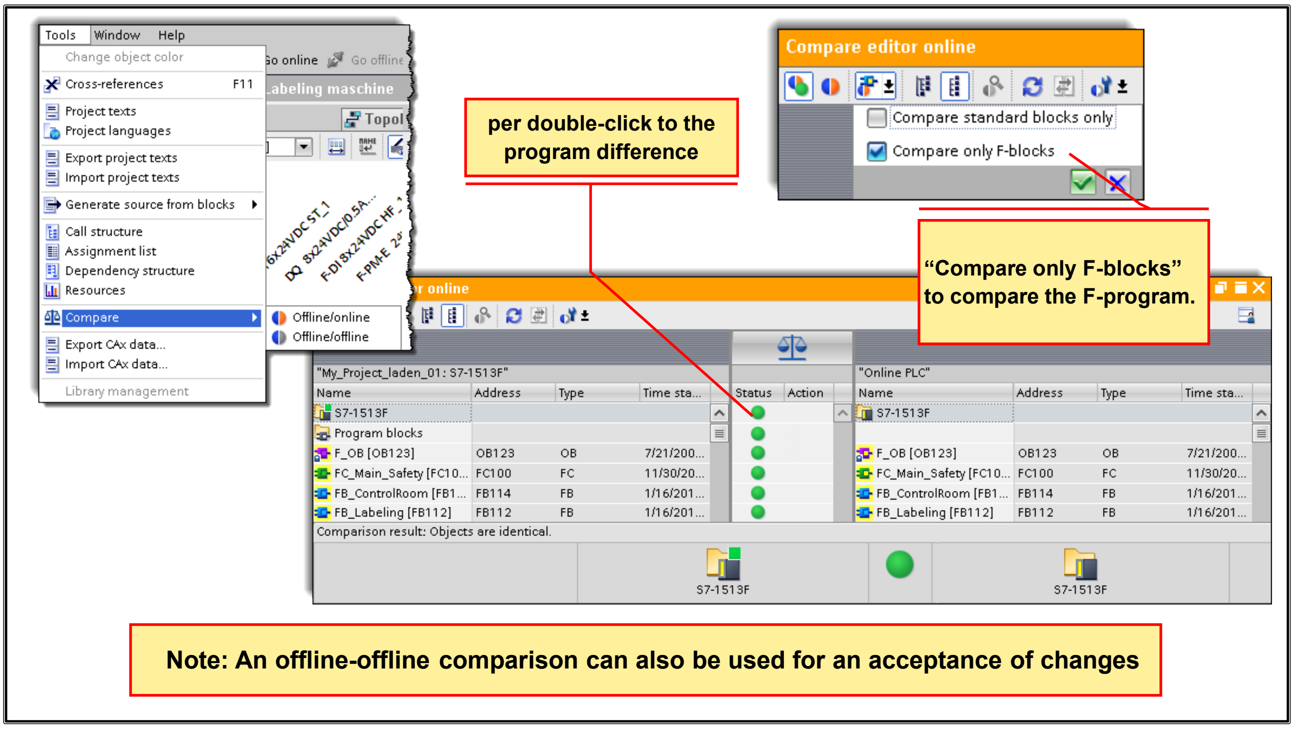
Monitoring

All read-only test functions (for example, monitoring tags) are generally also possible for safety programs and in safety mode.

Modifying

Modifying data of the safety program and write accesses to the safety program are only possible with limitations and in disabled safety mode.

6.16. Comparing Safety Programs



Comparing Safety Programs just as in Standard Programs

You can use the Compare editor in STEP 7 for offline-online or offline-offline comparison of safety programs. The procedure is the same as for standard user programs. The contents of F-blocks are also compared for the comparison of safety programs. As a result, an offline-offline comparison can also be used for an acceptance of changes. You enable this comparison by selecting the "Safety" comparison criterion and disabling all other comparison criteria.

Comparison Result of Safety Programs

You receive information about whether the safety program is consistent. If you interrupt the connection to the F-CPU during the online/offline comparison, the comparison result will be incorrect.

Comparison Filter Options

You can use filters in the Compare editor to limit the comparison result to the following block groups:

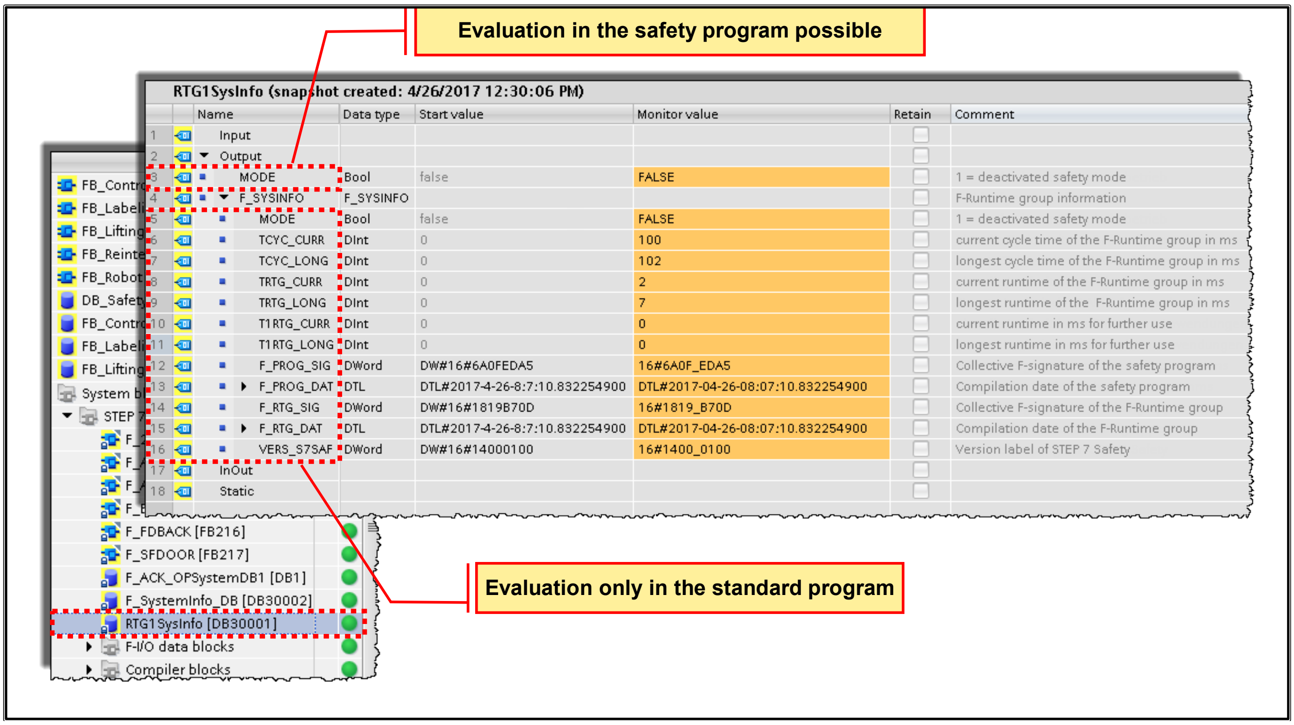
- Compare only F-blocks
- Compare only F-blocks relevant for certification
- Compare all blocks
- Compare only standard blocks

You also have the STEP 7 filter options "Show only objects with differences" and "Show identical and different objects". For comparison of safety programs, F-blocks in the "System blocks" folder are also relevant.

Printing Result of Comparison

The comparison result can be printed via "Project > Print" in the menu bar or the "Print" icon in the toolbar. Select: "Print objects/area" "All" and "Properties" "All".

6.17. RTG1SysInfo Data Block



F-Runtime Group Information DB

The F-runtime group information DB provides key information on the corresponding F-runtime group and on the safety program as a whole.

The F-runtime group information DB is generated automatically when an F-runtime group is created. A symbol, for example, "RTG1SysInfo", is assigned for the F-runtime group information DB. You can change the name in the Safety Administration Editor.

You access the contents of the F-runtime group information DB with fully qualified addressing. Either collectively with the F_SYSINFO PLC data type (UDT), for example, "RTG1SysInfo.F_SYSINFO", provided by the F-system or individual information, for example, "RTG1SysInfo.F_SYSINFO.MODE".

Note

The data blocks "T1RTG_CURR" and "T1RTG_LONG" are currently not supported in STEP 7 Safety V14.

6.18. Data Types and Operations

Standard Program

- can be changed without influencing the integrity of the safety program
- may read all data of the safety program, but cannot write to it
- must not call any F-blocks

Safety Program

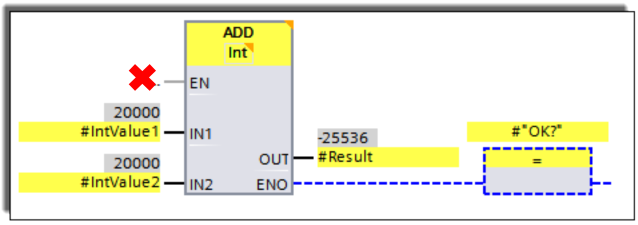
- Programming languages: FBD / LAD
- Supported data types: BOOL / WORD / INT / DINT / TIME
UDT / ARRAY (restricted)
(not Byte, Real, complex data types)
- Supported operations: just like standard FBD / LAD

6.19. Special Issues of Safety Program

Enable input EN and enable output ENO

Enable input EN and enable output ENO cannot be connected. .

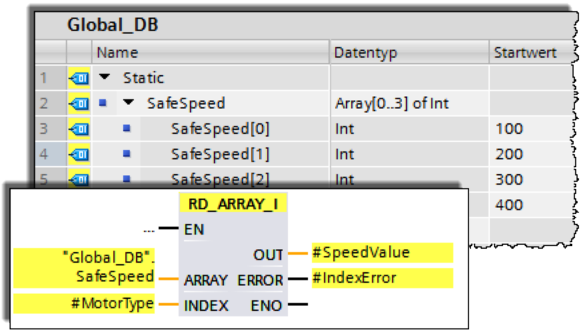
Exception(S7-1200, S7-1500):
With the following instructions you can program overflow detection by connecting the enable output ENO:
ADD, SUB, MUL, DIV. NEG, ABS, CONVERT



Use of data types F-ARRAY

- Only data types INT and DINT
- Only in F-global DBs
- Read-only function in safety program by using the instructions RD_ARRAY_I / RD_ARRAY_DI
- ARRAY limits: 0 up to max. 10000

.



6.20. Data Exchange between Standard Program and Safety Program

Allowed in the Standard Program:

- Read-only access to F-data such as:
  - Fail-safe data blocks
  - Process image of F-modules
- For evaluations of the current signal and operating statuses
- Write access to F-data is not permitted

Allowed in the Safety Program:

- Reading OR writing access to standard data such as:
  - Data block
  - Memory bits
  - Standard process image
- non-safe data must not change for the duration (execution) of the safety program → can lead to data corruption and the STOP of the CPU

Data Transfer from the Safety Program to the Standard User Program

The standard user program can read all data of the safety program, for example, using symbolic (fully qualified) accesses to:

- The instance DBs of the F-FBs ("Name of Instance DB".Signal_x)
- F-DBs (for example, "Name of F_DB".Signal_1)
- The process image for inputs and outputs of F-I/O (for example, "Emergency_Stop_Button_1" (I 5.0))

Data Transfer from the Standard User Program to the Safety Program

As a basic principle, only fail-safe data or fail-safe signals from F-I/O and other safety programs (in other F-CPUs) may be processed in the safety program, since all standard tags are unsafe.

If you must process tags from the standard user program in the safety program, however, you can evaluate either memory bits from the standard user program, tags from a standard DB, or the process image for inputs (PII) of standard I/O in the safety program (In the Safety manual: also see the table of supported operand areas in: Restrictions in the programming languages FBD/LAD).

Note that structural changes to standard DBs which are used in the safety program lead to inconsistencies of the safety program and possibly to the password being requested. In this case, the collective F-signature is once again the same as the original after compilation. To prevent this effect, use "interprocess communication blocks" between the standard user program and the safety program.

6.21. Access to the Process Image

		From the standard program		From the safety program	
		reading	writing	reading	writing
Standard process image	Inputs	✓	✓	✓	✗
	Outputs	✓	✓	✗	✓
Fail-safe process image	Inputs	✓	✗	✓	✗
	Outputs	✓	✗	✗	✓

6.22. Access to Data Blocks

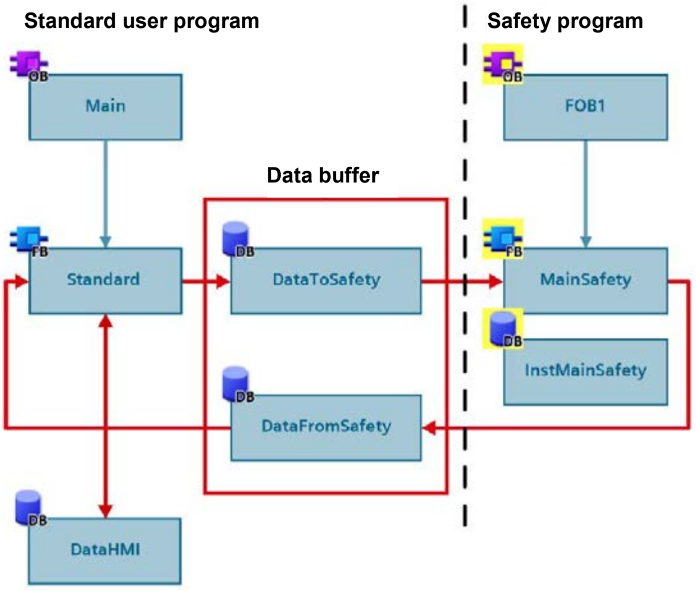
	From the standard program		From the safety program	
	reading	writing	reading	writing
Standard data block	✓	✓	✓ ✗	✗ ✓
Fail-safe data block	✓	✗	✓	✓

Data Block/Memory Bit

In order to write safety program data directly to the standard user program (for example, DIAG output of the SENDDP instruction), you can write to data blocks of the standard user program from the safety program. However, a written tag must not be read in the safety program itself.

You can also write to memory bits in the safety program. However, a written memory bit must not be read in the safety program itself.

6.23. Recommendation data exchange between standard user program and safety program



Empfehlung:

- Use global standard data blocks to exchange data between the standard user program and the safety program.
- To ensure a good overview of which program part reads and which one writes, it is recommended to create two data blocks for the two directions.
- You should not store any other information (e.g., diagnostic data from the standard user program) in the data blocks as each modification of the data block involves a modification of the safety program.

Advantages

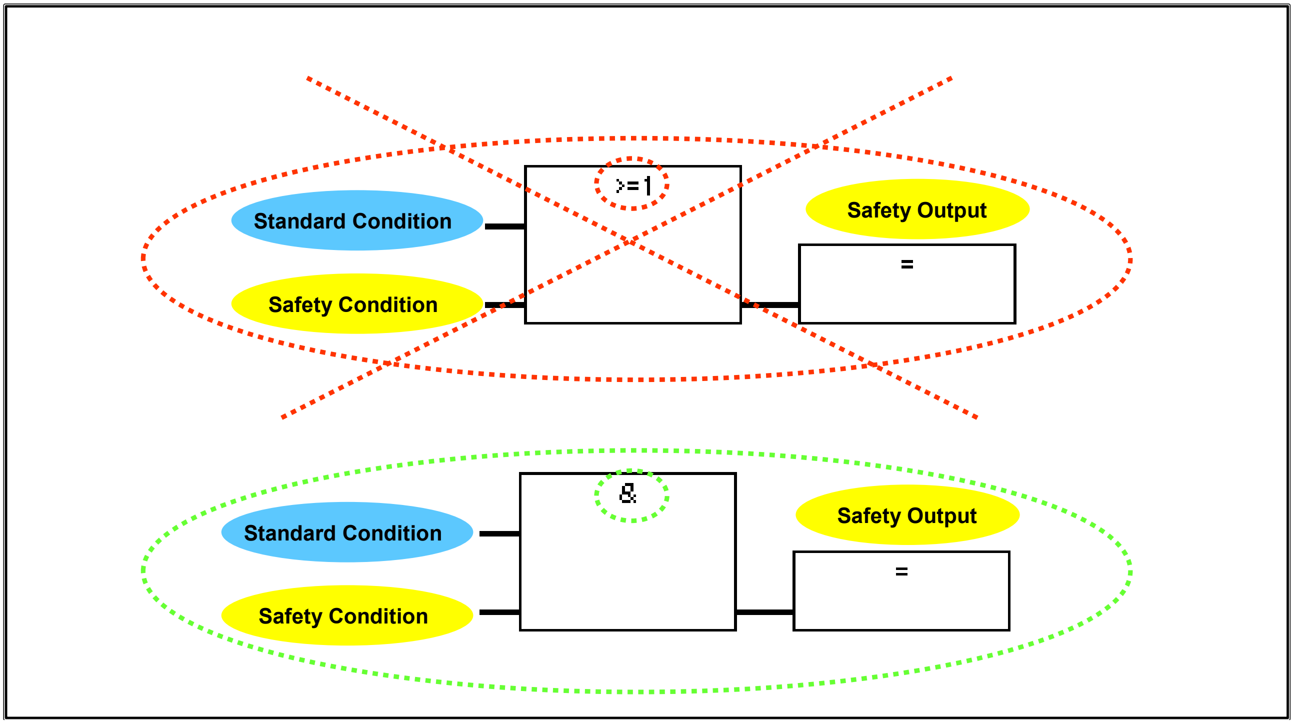
- Lean F-runtime group
- Better overview of the exchanged data
- Changes of the diagnostic and signaling concept in the standard user program do not affect the safety program's signature
- Minimized risk of downtimes caused by data corruption due to write access to the safety program
- Simplified typing of F-blocks
- Changes to the standard user program can be loaded without stopping the CPU
- Standard user program and safety program can be created independently of each other, provided that interfaces have already been defined

Using non-safe inputs in the safety program

Standard inputs that are required directly in the safety program must be read directly in the safety program. A "detour" via the standard user program should be avoided.

The background to this is that non-safety-related signals are also included in the application's systematic integrity. Typical examples are acknowledgment / reset buttons or mode selectors. Which button / switch is allowed to reset which safety function is a direct result of the risk assessment. A change of the command devices must therefore influence the signature and must be made only accompanied by a reassessment and an acceptance test for changes.

6.24. Plausibility Checks



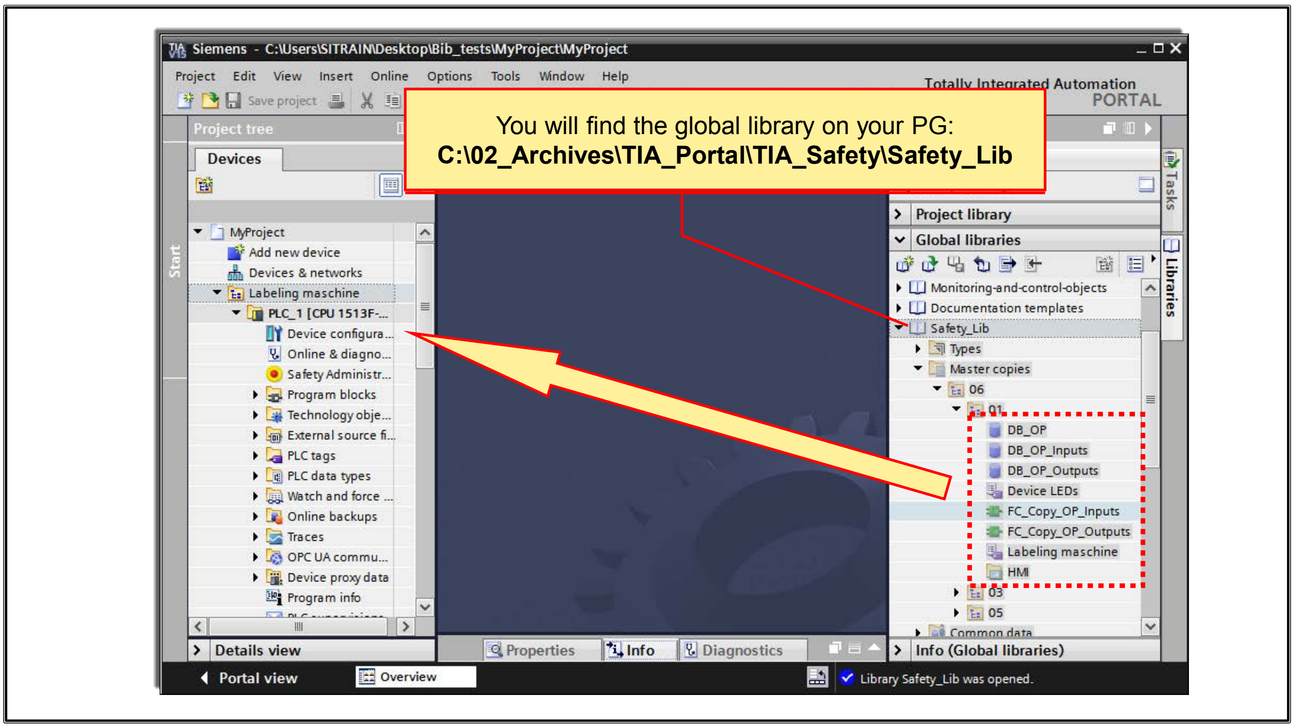
Programming Plausibility Checks

- Use Comparison instructions to check whether tags from the standard user program exceed or fall below permitted high and low limits. You can then influence your safety function with the result of the comparison.
- Use the ---(S)---: Set output, ---(R)---: Reset output or SR: Set/reset flip-flop instructions, for example, with tags from the standard user program to allow a motor to be switched off, but not switched on.
- For switch-on sequences, use the AND logic operation instruction, for example, to logically combine tags from the standard user program with switch-on conditions that you derive from fail-safe tags.

If you want to process tags from the standard user program in the safety program, please bear in mind that there is not a simple method of checking plausibility for all tags.

6.25. Exercise 1: Configuring the Touchpanel

6.25.1. Re: Exercise 1: Copying a Touchpanel Project, Interface DBs and FCs from the Library



Task

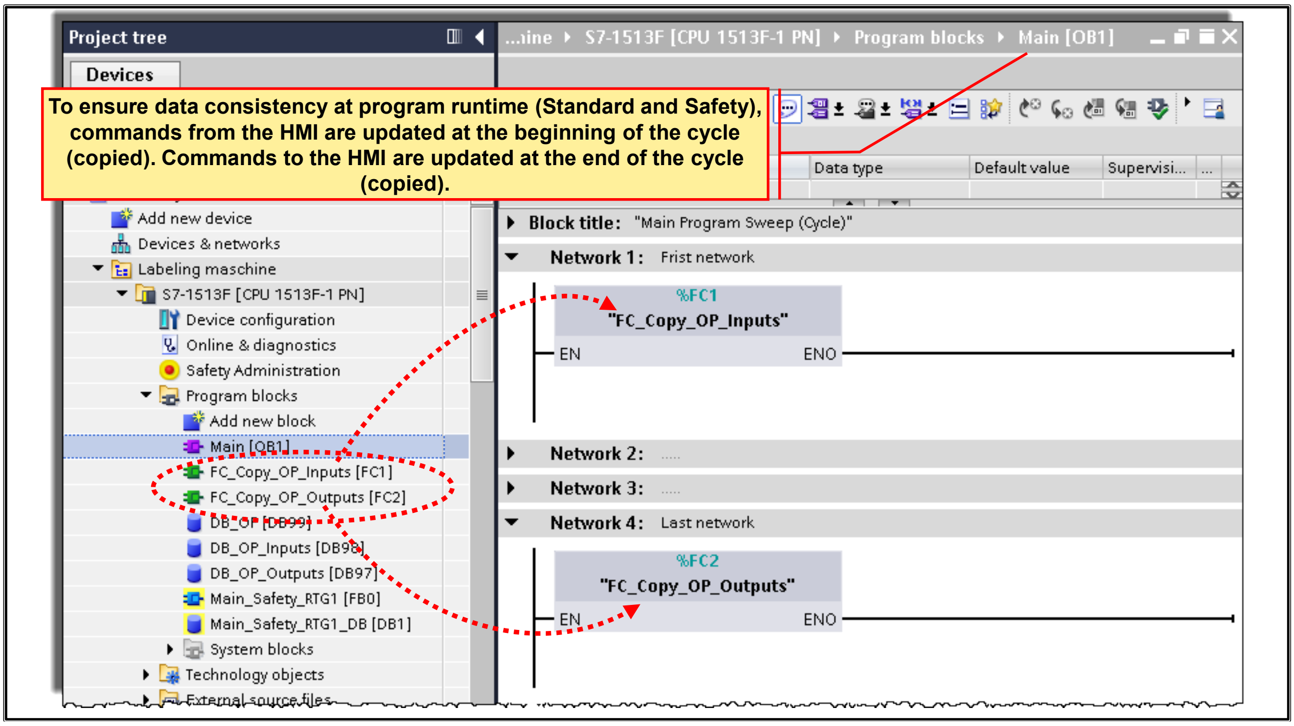
So far, your project does not contain an HMI device. Instead of creating a completely new configuration, you are to copy a prepared Panel project and the data block "DB_OP", which is to serve as the interface between the controller and the touchpanel, from the global library "Safety_Lib" into your project. You will find the global library under:

"C:\02_Archives\TIA_Portal\TIA_SAFETY\Safety_Lib"

What to Do

1. Open the global library "C:\02_Archives\TIA_Portal\TIA_SAFETY\Safety_Lib".
2. Using drag & drop, copy the library elements found in the folder "06" -> "01" to the appropriate locations in your project.
3. Assign the HMI to the device group "Labeling machine" by dragging it there using drag & drop.
4. Save your project.

6.25.2. Re: Exercise 1: Ensuring Data Consistency



Task

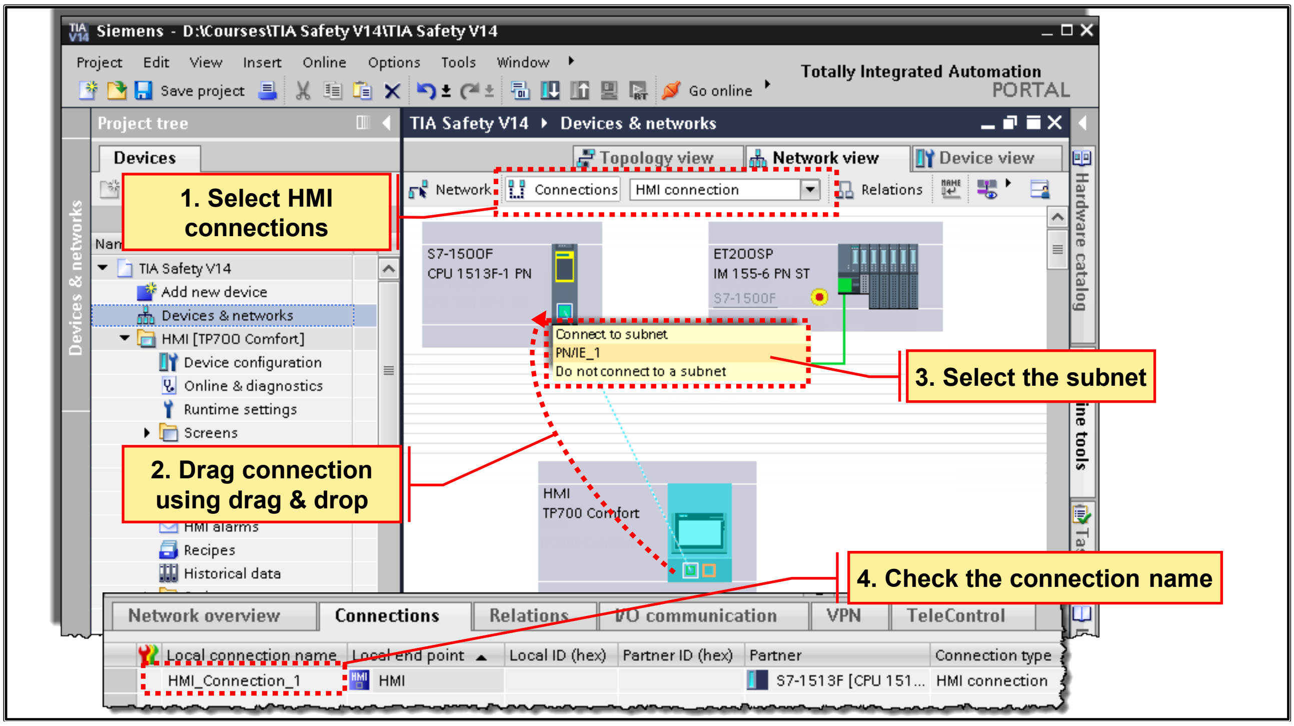
To ensure a data consistency, data which is written from the HMI into the user program at the beginning of the cycle are to be copied in a separate data block (DB_OP -> DB_OP_Inputs). Data which is read by the HMI is only to be transferred into the relevant data block (DB_OP_Outputs -> DB_OP) at the end of the program cycle.

Note: The 1200/1500 CPU no longer works with a cycle control point (300/400) to update HMI tags. The tags are updated at runtime.

What to Do

1. Call the "FC_Copy_OP_Inputs" (FC1) block in the first network of your cyclic OB1.
2. Call the "FC_Copy_OP_Outputs" (FC2) block in the last network of your cyclic OB1.
3. Save your project.

6.25.3. Re: Exercise 1: Configuring, Networking and Adjusting the HMI Connection



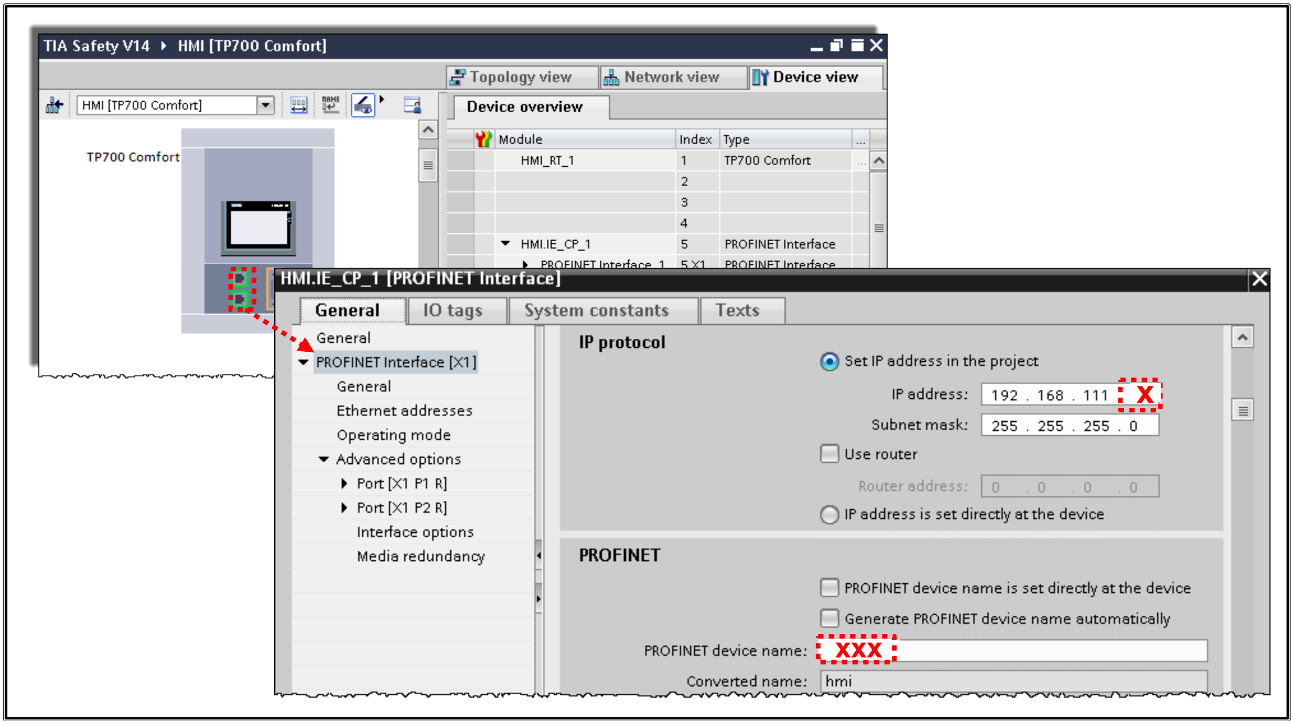
Task

The touchpanel, which was added, is to be networked and connected offline to the Ethernet network.

What to Do

1. In the Project tree, start the "Devices and networks" editor. Switch to the "Network view" and there select "Connections".
2. Position the mouse pointer on the Ethernet interface of the HMI device and, while keeping the left mouse button pressed down, drag a connection to the CPU. The connection is created. The associated subnet and the parameters (IP address and subnet mask) appropriate for the networking are automatically created.
3. If the current IP address of the HMI device does not match any subnet of the CPU, then the subnet must be selected.
4. Check the local connection name of the just created HMI connection. It must match the name preconfigured in the HMI project.

6.25.4. Re: Exercise 1: Adjusting the IP Address and PROFINET Device Name



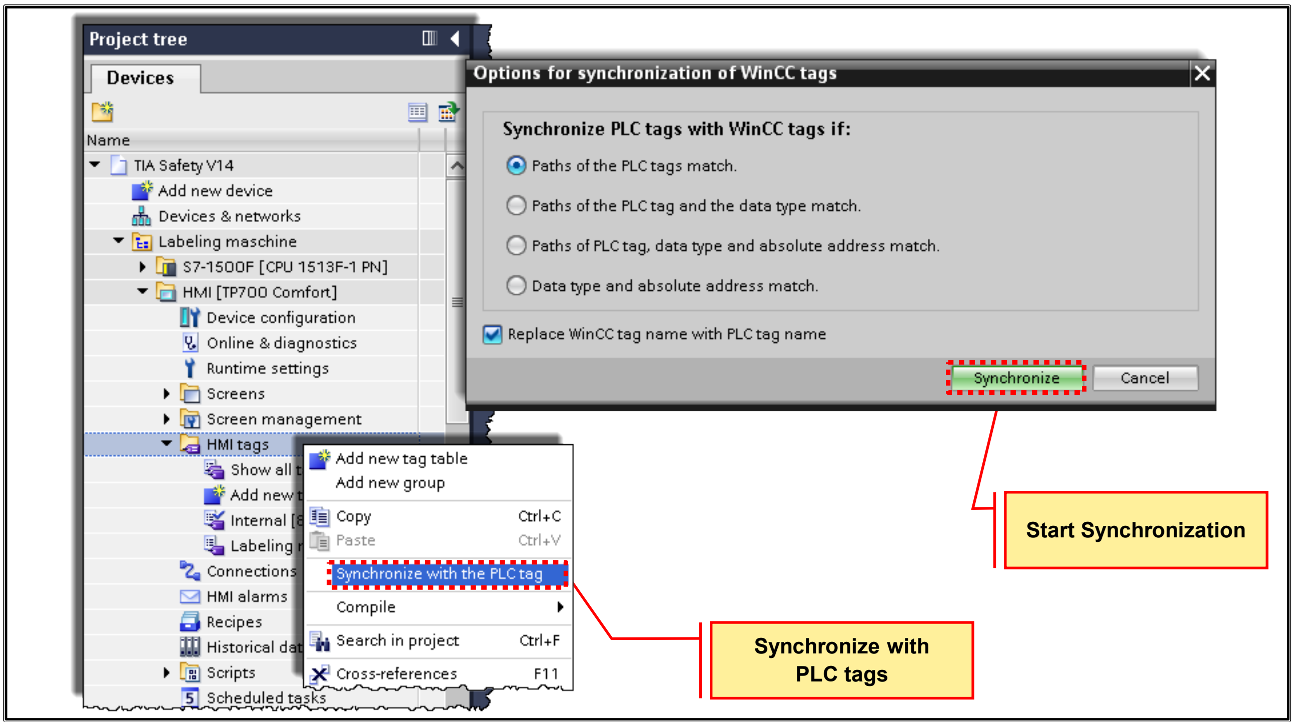
Task

Now that the HMI is networked and connected, the IP address and the PROFINET device name are to be adjusted.

What to Do

1. Assign the touchpanel the appropriate IP address. This can be set via the ‘Properties’ in the Inspector window.
2. Also assign the appropriate PROFINET device name. You can let it be automatically generated from the Station name by setting the checkmark at "Generate PROFINET device name automatically" or you can manually define it by removing the checkmark.

6.25.5. Re: Exercise 1: Comparing the HMI / PLC Tags and Compiling



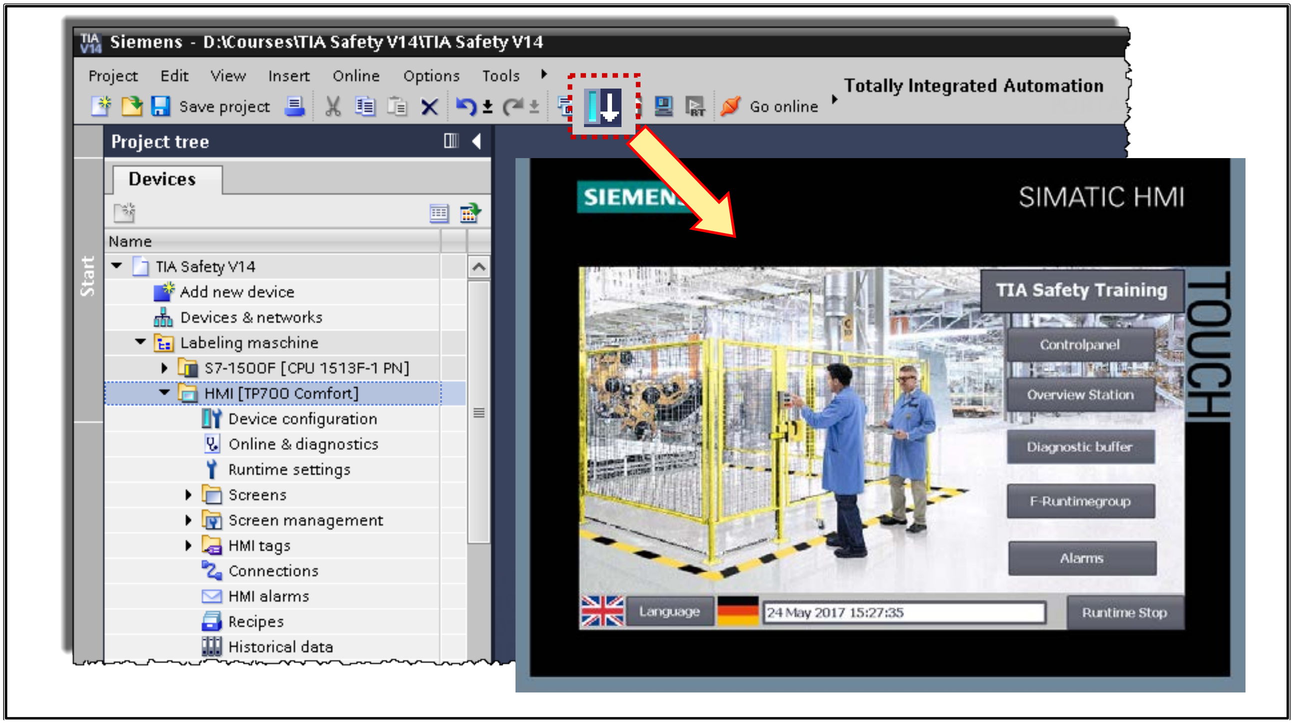
Task

To make sure that every HMI tag is correctly connected to the corresponding PLC tag, you are to carry out a synchronization between the HMI tags and the PLC tags.

What to Do

1. Open the "HMI tags" of the HMI device.
2. Then synchronize the WinCC tags (see picture).
3. Compile the HMI project by selecting the touchpanel in the Project tree and then clicking the "Compile" button.
4. Save your project.

6.25.6. Re: Exercise 1: Downloading to the HMI and CPU



Task

The now completed HMI and PLC projects are now to be downloaded.

What to Do

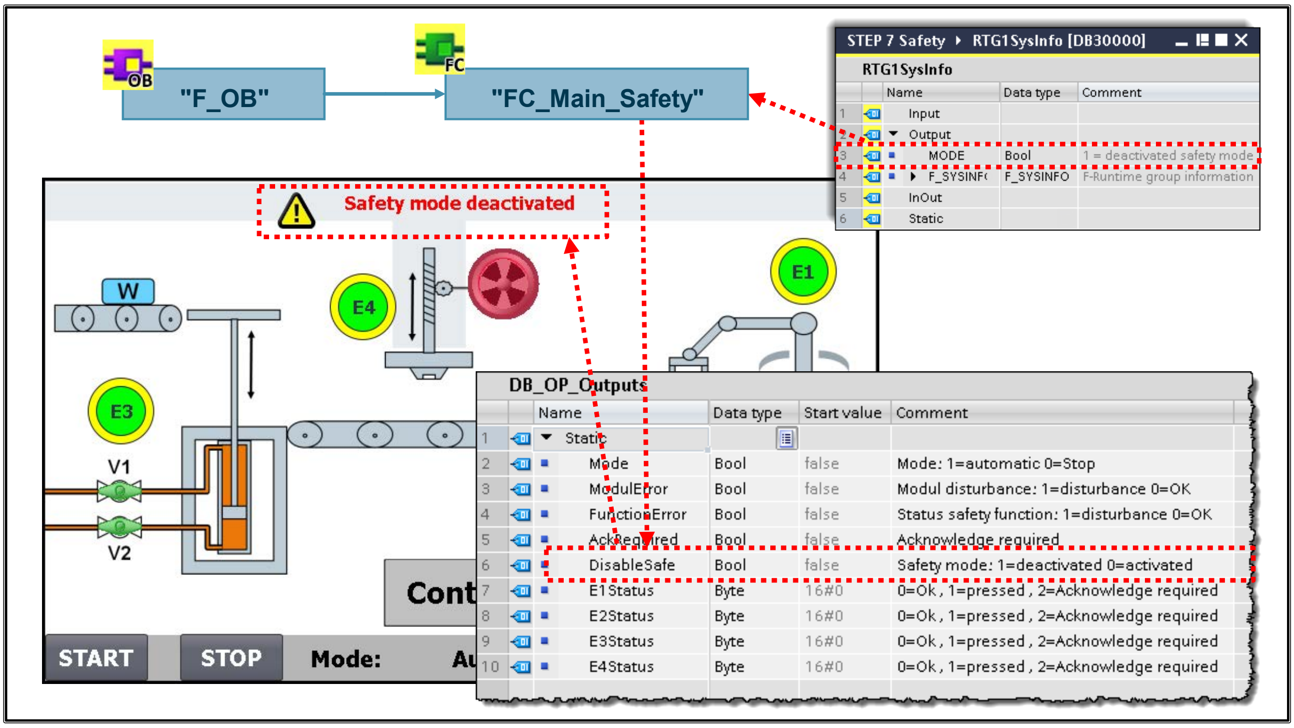
1. Download the Panel project into the touchpanel.
2. Compile the PLC project and download it to the CPU.
3. Save your project.

Result

The touchpanel should now be connected to your CPU. You can control the CPU tags of the "DB_OP" data block with the touchpanel.

To check if it is working properly, switch to the "Controlpanel" screen on the Panel and there press the "Start" button. In monitoring mode, you should see that the tag "Start" assumes the value "1" in the data block "DB_OP".

6.26. Exercise 2: "Safety Mode Deactivated" Display



Task Description

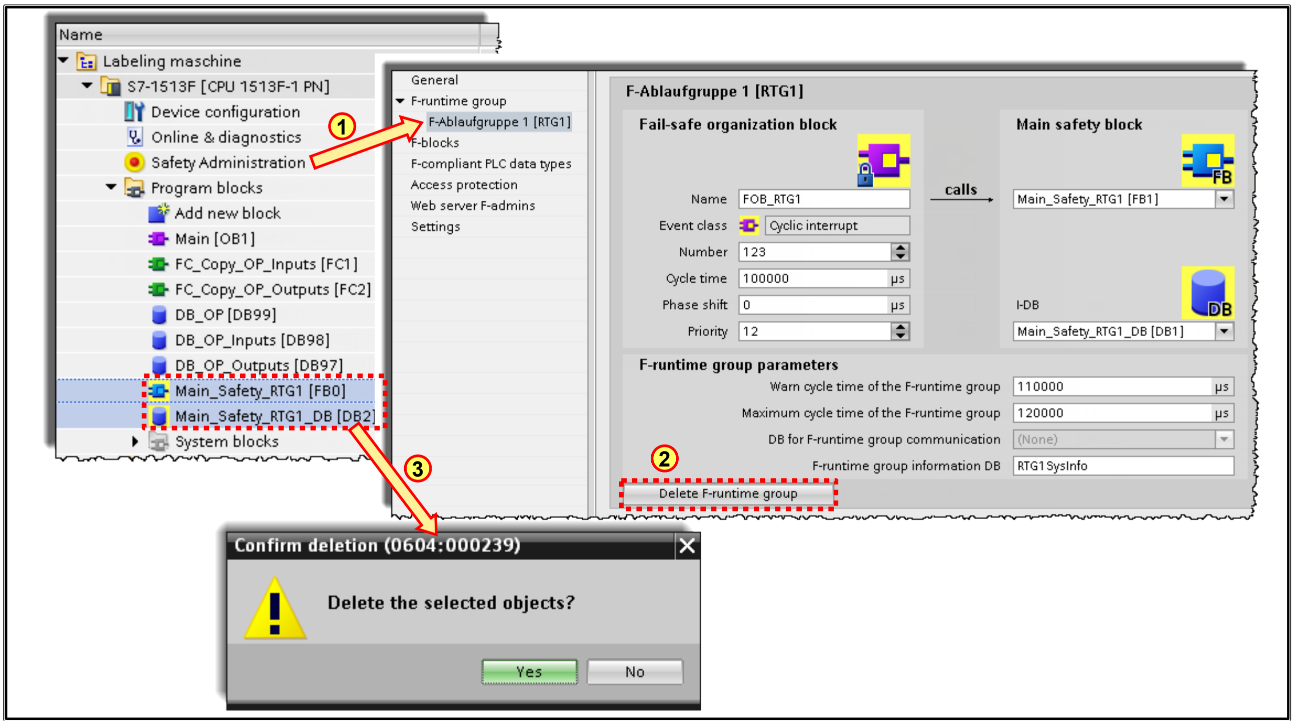
You are to program the safety-related block "FC_Main_Safety" (FC100) which, through evaluation of the RTG1Sys-DB, controls and displays the "Safety mode deactivated" display on the Panel as long as the safety mode of the CPU is deactivated.

Note:
The evaluation of the RTG1Sys-DB could also be programmed in the standard program.

What to Do

The following pages explain what has to be done.

6.26.1. Re: Exercise 2: Deleting the Existing Runtime Group



Because a runtime group is automatically created when an F-CPU is created in TIA Portal, you must delete this group and the associated F-blocks.

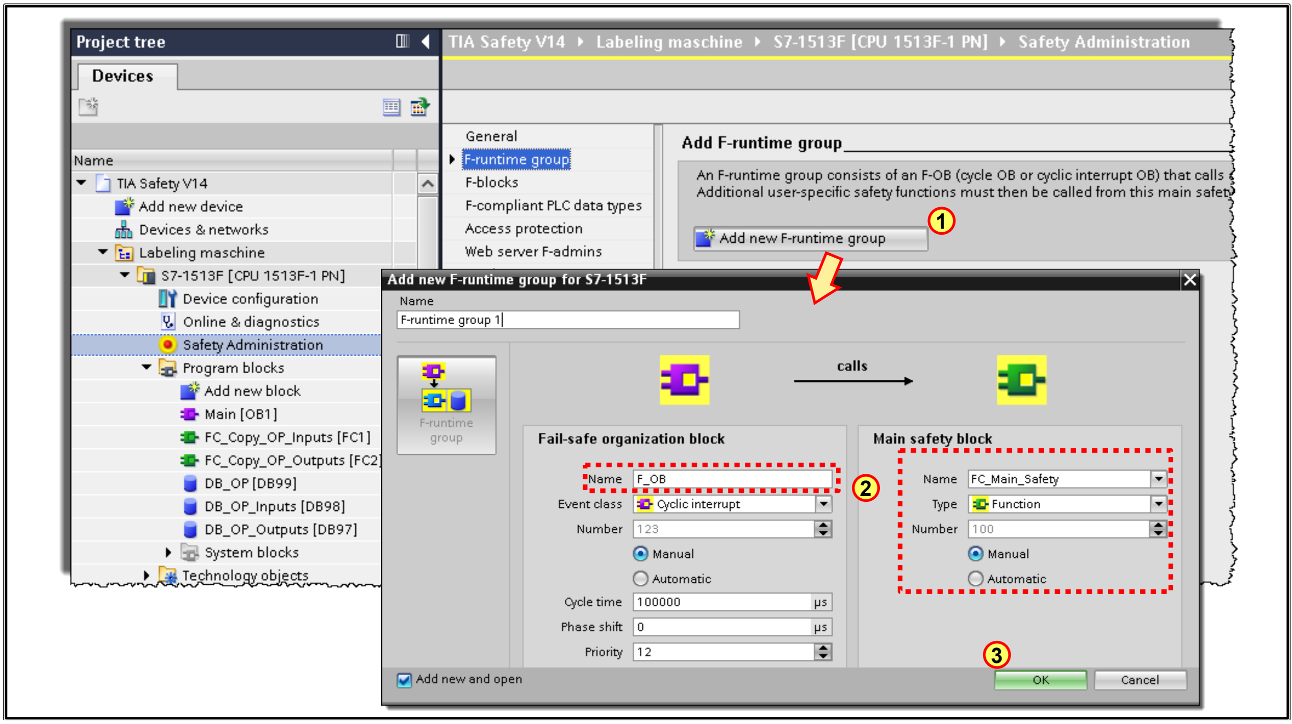
Note:

At this point, deleting the automatically created runtime group is only carried out as an exercise in order to illustrate the creating of a new runtime group.

What to Do

1. Open the currently existing runtime group
   "Safety Administration" -> "F-runtime group" -> "F-runtime group 1".
2. Delete the runtime group.
3. Delete the still existing F-blocks of the deleted runtime group.
4. Save your project.

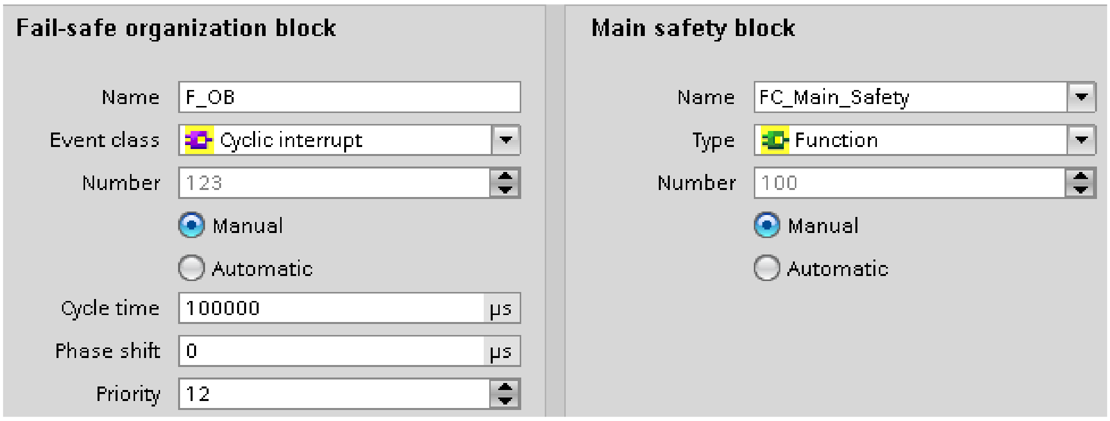
6.26.2. Re: Exercise 2: Manually Creating a New Runtime Group



You are now to create a new runtime group. This runtime group will later contain your entire safety program.

What to Do

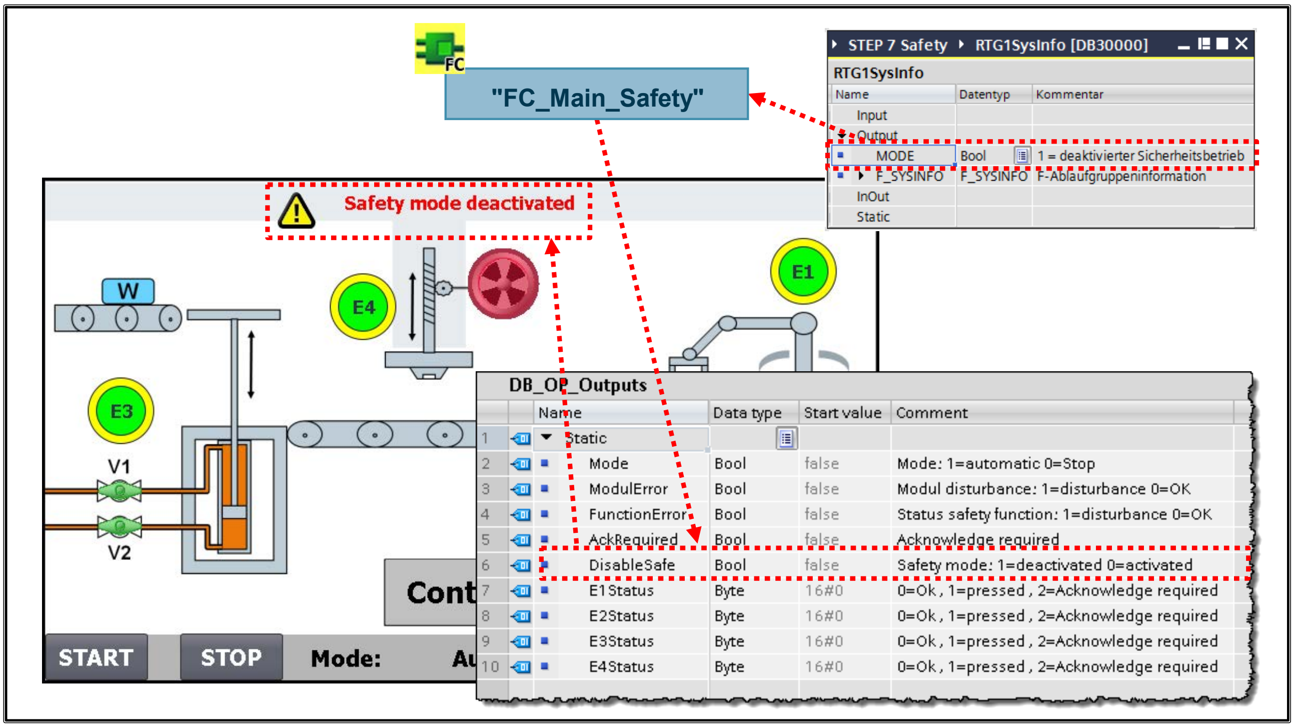
1. Create a new runtime group
   "Safety Administration" -> "F-runtime group" -> "Add new F-runtime group".
2. Select the name and the settings as shown in the picture.



3. Create the configured runtime-group.
4. Activate the option "Safety mode can be disabled"
   "Safety Administration" -> "Settings" -> "Advanced settings".

   Note: This option is required for Exercise 5 (Wiring Test) later on.
5. Save and compile your project.

6.26.3. Re: Exercise 2: "FC_Main_Safety"



Task

The user must be informed immediately when the safety mode of the CPU is deactivated. This is to be implemented via a display on the Panel.

What to Do

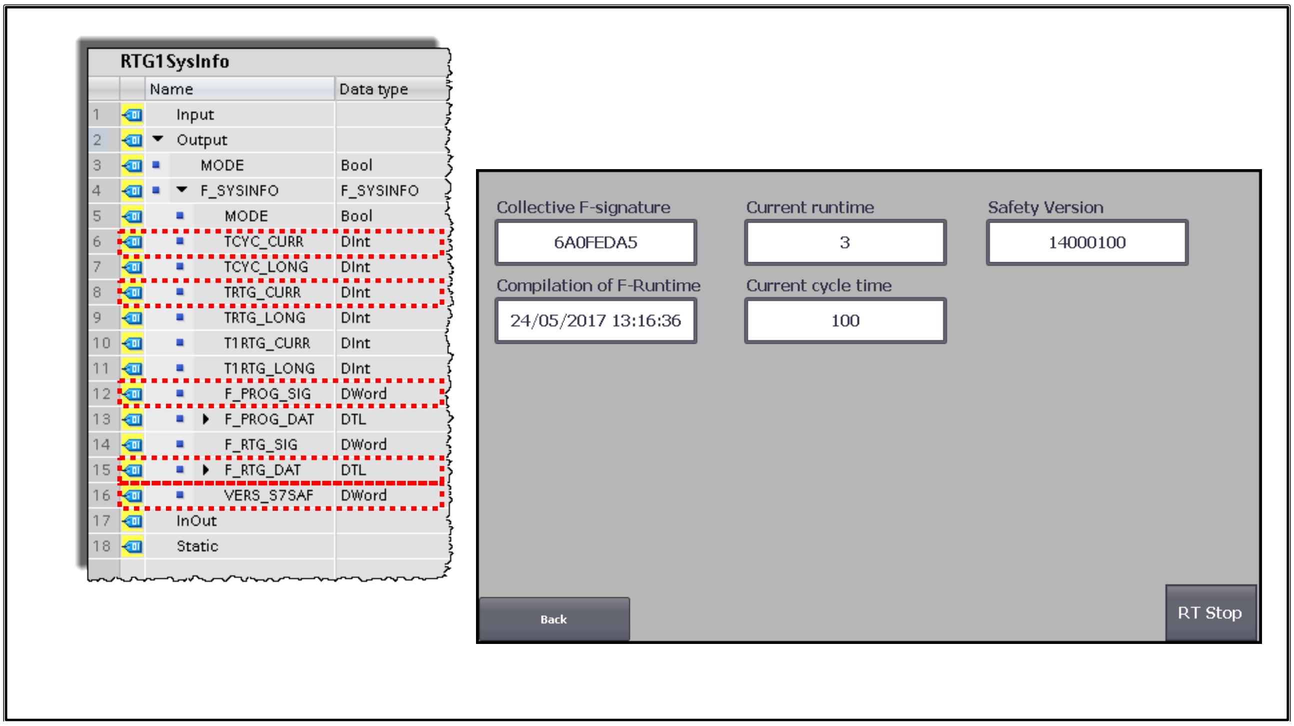
1. Program the "FC_Main_Safety" (FC100) in such a way that the "Safety mode deactivated" (DB_OP_Outputs.DisableSafe) Display is displayed on the Panel as long as the safety mode of the CPU is deactivated (RTG1SysInfo.MODE).
2. Download all blocks into the CPU.
3. Save your project.

Relevant Interfaces		
Inputs	**Standard**	**Fail-safe**
	-	-
Outputs	**Standard**	**Fail-safe**
	-	-
Data blocks	**Global**	**System**
	DB_OP_Outputs.DisableSafe (DB99)	RTG1SysInfo.MODE

Note

You will find the system data block RTG1SysInfo in the Program blocks folder under "Program blocks" -> "System blocks" -> "STEP 7 Safety"

6.26.4. Exercise 2.1 (Optional): Displaying the Runtime Group Information



Task

All relevant information about the safety program is to be provided to the user on the Panel.

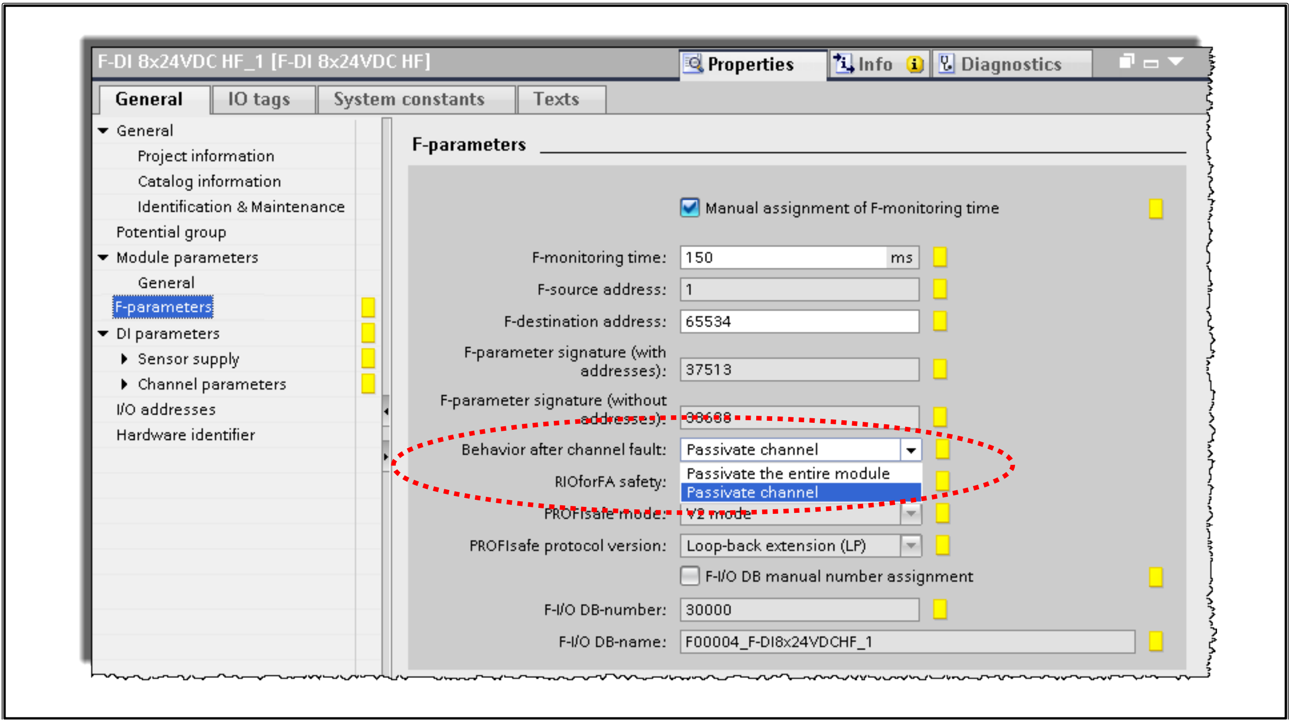
What to Do

1. The current HMI project contains the "Runtimegroup Info" screen (see picture). On the Panel, this screen is called via the "F-Runtimegroup" button. Configure individual output fields that have the correct tag connection to the system data block "RTG1SysInfo" from the CPU.
2. Download your HMI project into the Panel.
3. Save your project.

Relevant Interfaces		
Inputs	**Standard**	**Fail-safe**
	-	-
Outputs	**Standard**	**Fail-safe**
	-	-
Data blocks	**Global**	**System**
	-	RTG1SysInfo.TCYC_CURR
		RTG1SysInfo.TRTG_CURR
		RTG1SysInfo.F_PROG_SIG
		RTG1SysInfo.F_RTG_DAT
		RTG1SysInfo.VERS_S7SAF

6.27. F-Module Passivation

6.27.1. Principle



Passivation

The safety concept is based on the existence of a safe state for all process variables. With safety-related I/O modules, this "Fail-safe value" is the status '0'. If the safety-related I/O module detects a fault, it passivates the channel involved or the entire module (all channels), which means the channels are switched to the safe state.

The **passivation** of a channel or F-module occurs …

- During startup of the F-system
- In case of communication errors between the F-CPU and F-I/O
- In case of faults detected by the F-I/O (wire break, short-circuit, cross-circuit, etc.)
- Via the F-program (must be programmed by the user)

For passivated channels, a **passivated F-DI module** signals the logic state '0' to the process image for inputs (PII) of the CPU, regardless of the actual sensor signals from the system.

A **passivated F-DO module** de-energizes passivated output channels regardless of the output states transferred by the CPU from the process image for outputs (PIQ).

Depassivation

The **depassivation** of a channel or an F-module can occur …

- By a restart of the F-CPU automatically after fault elimination (not for communication errors)
- Via the F-program (must be programmed by the user)

6.27.2. F-I/O Data Block

F-I/O DB

- Is generated for every F-module when it is inserted in the Device view
- Contains tags for evaluating the module status
- Is supplied with valid data by the PROFIsafe driver

Using the tags in the F-I/O DB

- Evaluating whether process or substitute values are output
- Reintegration of the F-I/O (ACK_REI) after:
  - PROFIsafe communication errors
  - F-module and channel faults
- Manual passivation, dependent on certain states in the safety program ("Group passivation", PASS_ON)

F-I/O DB

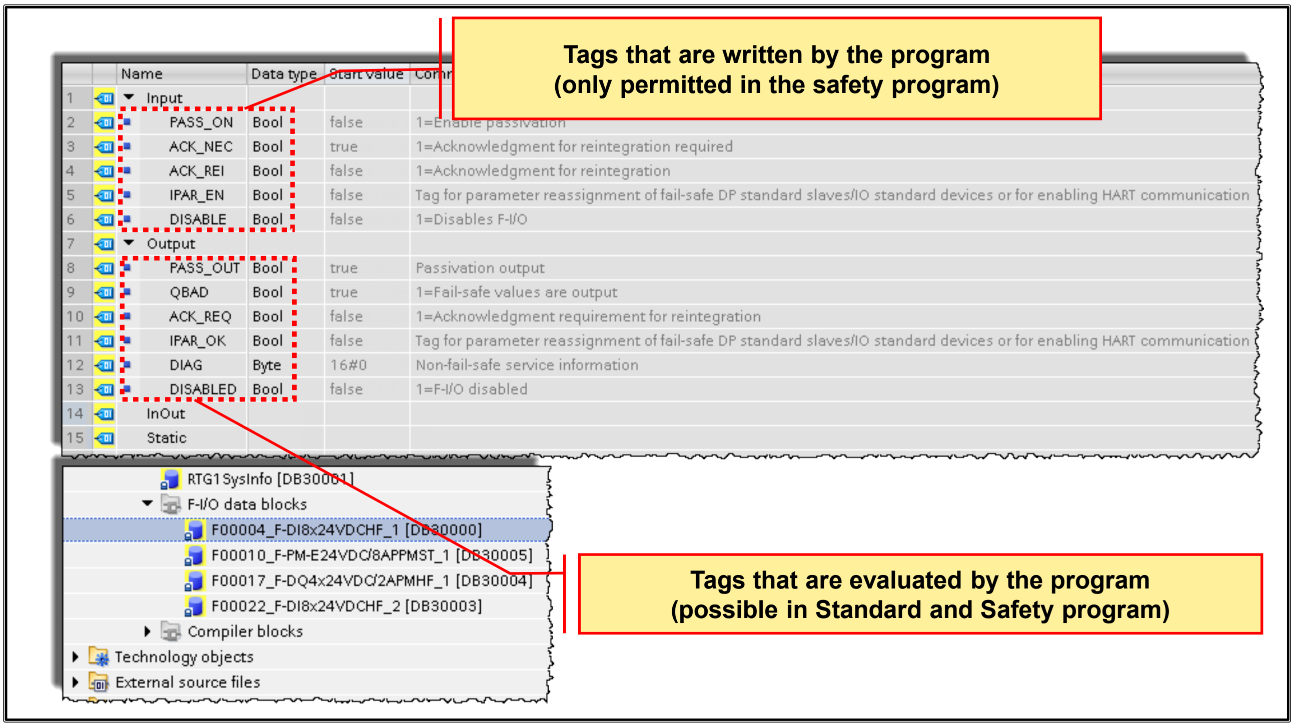
For each F-I/O (in safety mode), an F-I/O DB is created automatically when the F-I/O are configured in the Hardware and Network editor. The F-I/O DB contains tags that you can evaluate in the safety program, or, that you can or must write in the safety program. A change of the start values of the tags directly in the F-I/O DB is not permitted. When an F-I/O is deleted, the associated F-I/O DB is also deleted.

Using the Access to an F-I/O DB

You access tags of the F-I/O DB:

- For reintegration of the F-I/O after communication errors, F-I/O faults or channel faults
- If you want to passivate the F-I/O dependent on certain states of your safety program (for example, group passivation)
- For reassignment of parameters of fail-safe standard DP slaves/IO devices
- If you want to evaluate whether substitute values or process values are being output

6.27.3. I/O DB Tags



PASS_ON

You can use the PASS_ON tag to enable passivation of an F-I/O, for example, dependent on certain states in your safety program. You can only passivate the entire F-I/O using the PASS_ON tag in the F-I/O DB; channel-selective passivation is not possible. Passivation of the associated F-I/O occurs as long as PASS_ON = 1.

ACK_NEC, ACK_REI

The depassivation (reintegration) of the module can be done manually or automatically. If the initial value of the ACK_NEC tag remains '1', the module must be reintegrated manually. For this purpose, the F-program assigns the state '1' to the ACK_REI tag. If the ACK_NEC tag is overwritten with state "0", the module is depassivated or reintegrated automatically once the fault has been eliminated (not after communication errors).

IPAR_EN

The IPAR_EN tag corresponds to the iPar_EN_C tag in the PROFIsafe bus profile as of PROFIsafe Specification V1.20, fail-safe standard DP-slaves/IO-devices. To find out when you must set/reset this tag when parameters of fail-safe standard DP slaves/IO devices are reassigned, refer to the PROFIsafe specification V1.20 or higher or the documentation for the fail-safe standard DP slave/IO device. Note that the passivation of the F-I/O involved is not triggered by IPAR_EN = 1. If passivation is to occur when IPAR_EN = 1, you must also set the tag PASS_ON = 1.

PASS_OUT

With state '1', the module indicates that it passivated itself due to a detected fault. If the module was passivated by the PASS_ON tag via the F-program, the module leaves the PASS_OUT tag in '0' state.

QBAD

With state '1', the module indicates that at least one channel is passivated. It does not matter in this case whether passivation was brought about by the module itself or by the F-program using the PASS_ON tag.

ACK_REQ

After a fault is eliminated, the still passivated module indicates that it is ready for reintegration with ACK_REQ= '1'.

IPAR_OK

The IPAR_OK tag corresponds to the iPar_OK_S tag in the PROFIsafe bus profile as of PROFIsafe Specification V1.20, fail-safe standard DP-slaves/IO-devices. To find out how you can evaluate this tag when parameters of fail-safe standard DP slaves/IO devices are reassigned, refer to the PROFIsafe specification V1.20 or higher or the documentation for the fail-safe standard DP slave/IO device.

DIAG

The DIAG tag is used for service purposes to provide non-fail-safe information (1 byte) regarding faults that have occurred. You can read out this information using operator control and monitoring systems or evaluate it in your standard user program, if necessary. The DIAG bits remain saved until you carry out an acknowledgement with the ACK_REI tag or an automatic reintegration occurs. You can assign this tag to a standard tag in the safety program using the MOVE instruction

.

6.27.4. Value Status of the 1200/1500 F-CPUs

Value status

- Additional information about the value of an F-I/O channel.
- Is supported by modules of the ET 200SP, ET 200S, ET 200iSP, ET 200pro, and ET 200MP.
- The value status provides information about the validity of the associated channel value:
  - **1**: A **valid process value** is being output for the channel.
  - **0**: A **substitute value** is being output for the channel.
- The channel value and value status of an F-I/O may only be accessed from the same F-runtime group.
- The value status **is entered in the process image for inputs** (PII).

Value status

The value status is additional binary information for a channel value of an F-I/O. The value status is entered in the process image for inputs (PII).

The value status is supported by fail-safe modules S7-1500/ET 200MP, ET 200SP, ET 200S, ET 200iSP, ET 200pro, S7-1200 or S7-300 F-SMs, fail-safe standard IO-devices as well as fail-safe standard DP-slaves which support the "RIOforFA-Safety" profile.

We recommend the assignment of a symbolic name for the value status, consisting of the name of the channel value supplemented by "_VS", for example, "TagIn_1_VS".

The value status provides information about the validity of the associated channel value:

- 1: A valid process value is being output for the channel.
- 0: A substitute value is being output for the channel.

The channel value and value status of an F I/O may only be accessed from the same F-runtime group.

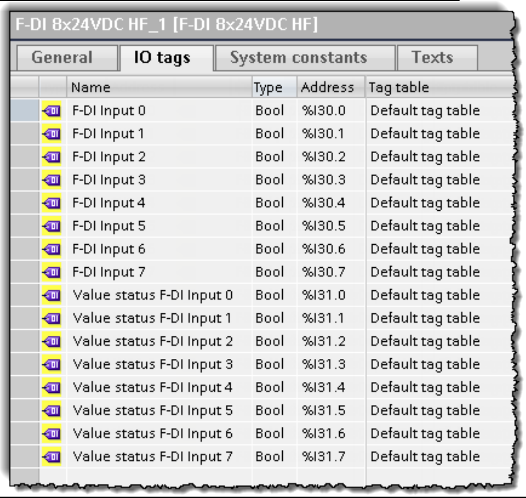
6.27.5. Value Status Bits for F-DI

Byte in the F-CPU	Assigned bits in F-CPU per F-module:							
	7	6	5	4	3	2	1	0
x + 0	DI_7	DI_6	DI_5	DI_4	DI_3	DI_2	DI_1	DI_0
x + 1	Value status for DI_7	Value status for DI_6	Value status for DI_5	Value status for DI_4	Value status for DI_3	Value status for DI_2	Value status for DI_1	Value status for DI_0

Address assignment in the PII

x = Module start address

- The value status bits directly follow the channel value in the PII.



F-DI 8x24VDC HF_1 [F-DI 8x24VDC HF]

General | IO tags | System constants | Texts

Name	Type	Address	Tag table
F-DI Input 0	Bool	%I30.0	Default tag table
F-DI Input 1	Bool	%I30.1	Default tag table
F-DI Input 2	Bool	%I30.2	Default tag table
F-DI Input 3	Bool	%I30.3	Default tag table
F-DI Input 4	Bool	%I30.4	Default tag table
F-DI Input 5	Bool	%I30.5	Default tag table
F-DI Input 6	Bool	%I30.6	Default tag table
F-DI Input 7	Bool	%I30.7	Default tag table
Value status F-DI Input 0	Bool	%I31.0	Default tag table
Value status F-DI Input 1	Bool	%I31.1	Default tag table
Value status F-DI Input 2	Bool	%I31.2	Default tag table
Value status F-DI Input 3	Bool	%I31.3	Default tag table
Value status F-DI Input 4	Bool	%I31.4	Default tag table
Value status F-DI Input 5	Bool	%I31.5	Default tag table
Value status F-DI Input 6	Bool	%I31.6	Default tag table
Value status F-DI Input 7	Bool	%I31.7	Default tag table

Value Status for the Digital Input and Output Modules

The value status is influenced by the wire break check, short-circuit, chatter monitoring, pulse stretching and plausibility check.

Note

You may only access the addresses occupied by user data and value status. The other address ranges occupied by the F-modules are assigned, among other things, for safety-related communication between the F-modules and F-CPU in accordance with PROFIsafe. For 1oo2 evaluation of the sensors, the two channels are combined. For 1oo2 evaluation of the sensors, you may only access the low-order channel in the safety program.

6.27.6. Value Status Bits for F-DQ

Byte in the F-CPU	Assigned bits in F-CPU per F-module:							
	7	6	5	4	3	2	1	0
x + 0	—	—	—	—	Value status DQ_3	Value status DQ_2	Value status DQ_1	Value status DQ_0

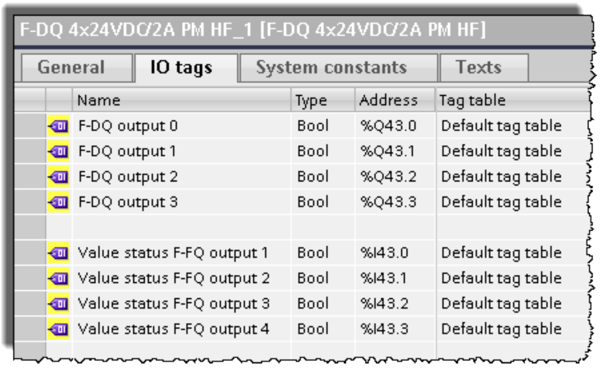
Address assignment in the PII

Byte in the F-CPU	Assigned bits in F-CPU per F-module:							
	7	6	5	4	3	2	1	0
x + 0	—	—	—	—	DQ_3	DQ_2	DQ_1	DQ_0

Address assignment in the PIQ

x = Module start address

- The value status bits are mapped in the PII with the same structure as the channel values in the PIQ.



Name	Type	Address	Tag table
F-DQ output 0	Bool	%Q43.0	Default tag table
F-DQ output 1	Bool	%Q43.1	Default tag table
F-DQ output 2	Bool	%Q43.2	Default tag table
F-DQ output 3	Bool	%Q43.3	Default tag table
Value status F-FQ output 1	Bool	%I43.0	Default tag table
Value status F-FQ output 2	Bool	%I43.1	Default tag table
Value status F-FQ output 3	Bool	%I43.2	Default tag table
Value status F-FQ output 4	Bool	%I43.3	Default tag table

6.27.7. Value Status Bits for F-PM

Byte in the F-CPU	Assigned bits in F-CPU per F-module:							
	7	6	5	4	3	2	1	0
x + 0	—	—	—	—	—	—	DI_1	DI_0
x + 1	—	—	—	—	—	—	Value status for DI_1	Value status for DI_0
x + 2	—	—	—	—	—	—	—	Value status DQ_0

Address assignment in the PII

Byte in the F-CPU	Assigned bits in F-CPU per F-module:							
	7	6	5	4	3	2	1	0
x + 0	—	—	—	—	—	—	—	DQ_0

Address assignment in the PIQ

x = Module start address

F-PM-E 24VDC/8A PPM ST_1 [F-PM-E 24VDC/8A PPM ST]

General | IO tags | System constants | Texts

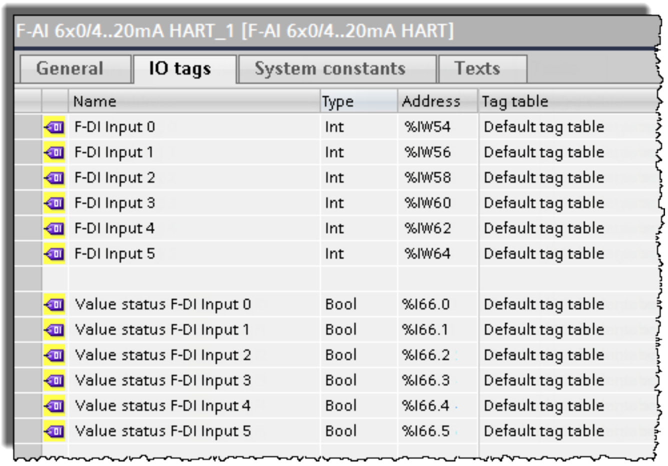
Name	Type	Address	Tag table
F-PM Input 0	Bool	%I36.0	Default tag table
F-PM Input 1	Bool	%I36.1	Default tag table
F-PM Output 1	Bool	%Q36.0	Default tag table
Value status F-PM Input 0	Bool	%I37.0	Default tag table
Value status F-PM Input 1	Bool	%I37.1	Default tag table
Value status F-PM Input 2	Bool	%I38.0	Default tag table

6.27.8. Value Status Bits for F-AI

Byte in the F-CPU	Assigned bytes/bits in the F-CPU per F-I/O:							
	7	6	5	4	3	2	1	0
x + 0	Channel value AI_0							
...	...							
x + 10	Channel value AI_5							
x + 12	—	—	Value status AI_5	Value status AI_4	Value status AI_3	Value status AI_2	Value status AI_1	Value status AI_0

x = Module start address

Address assignment in the PII

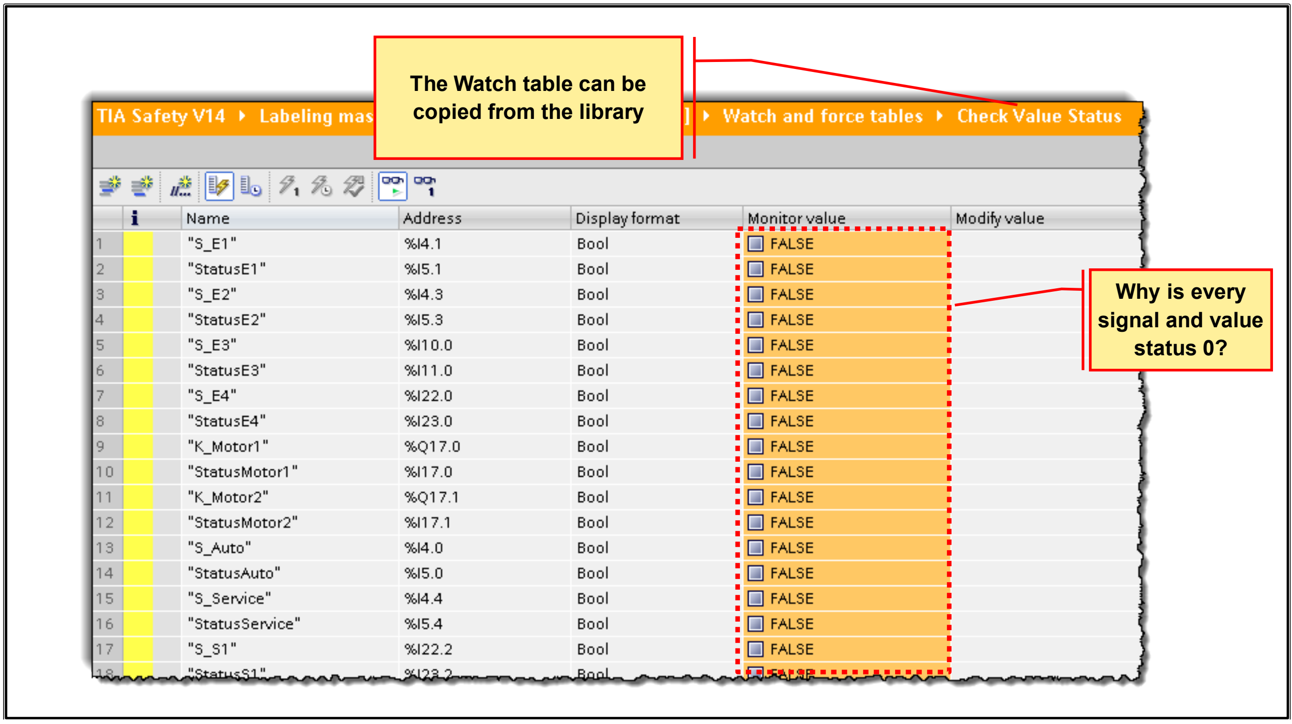


F-AI 6x0/4..20mA HART_1 [F-AI 6x0/4..20mA HART]

General | IO tags | System constants | Texts

Name	Type	Address	Tag table
F-DI Input 0	Int	%IW54	Default tag table
F-DI Input 1	Int	%IW56	Default tag table
F-DI Input 2	Int	%IW58	Default tag table
F-DI Input 3	Int	%IW60	Default tag table
F-DI Input 4	Int	%IW62	Default tag table
F-DI Input 5	Int	%IW64	Default tag table
Value status F-DI Input 0	Bool	%I66.0	Default tag table
Value status F-DI Input 1	Bool	%I66.1	Default tag table
Value status F-DI Input 2	Bool	%I66.2	Default tag table
Value status F-DI Input 3	Bool	%I66.3	Default tag table
Value status F-DI Input 4	Bool	%I66.4	Default tag table
Value status F-DI Input 5	Bool	%I66.5	Default tag table

6.28. Exercise 3: Understanding the Value Status



	i	Name	Address	Display format	Monitor value	Modify value
1		"S_E1"	%I4.1	Bool	FALSE	
2		"StatusE1"	%I5.1	Bool	FALSE	
3		"S_E2"	%I4.3	Bool	FALSE	
4		"StatusE2"	%I5.3	Bool	FALSE	
5		"S_E3"	%I10.0	Bool	FALSE	
6		"StatusE3"	%I11.0	Bool	FALSE	
7		"S_E4"	%I22.0	Bool	FALSE	
8		"StatusE4"	%I23.0	Bool	FALSE	
9		"K_Motor1"	%Q17.0	Bool	FALSE	
10		"StatusMotor1"	%I17.0	Bool	FALSE	
11		"K_Motor2"	%Q17.1	Bool	FALSE	
12		"StatusMotor2"	%I17.1	Bool	FALSE	
13		"S_Auto"	%I4.0	Bool	FALSE	
14		"StatusAuto"	%I5.0	Bool	FALSE	
15		"S_Service"	%I4.4	Bool	FALSE	
16		"StatusService"	%I5.4	Bool	FALSE	
17		"S_S1"	%I22.2	Bool	FALSE	
18		"StatusS1"	%I23.2	Bool	FALSE	

Task

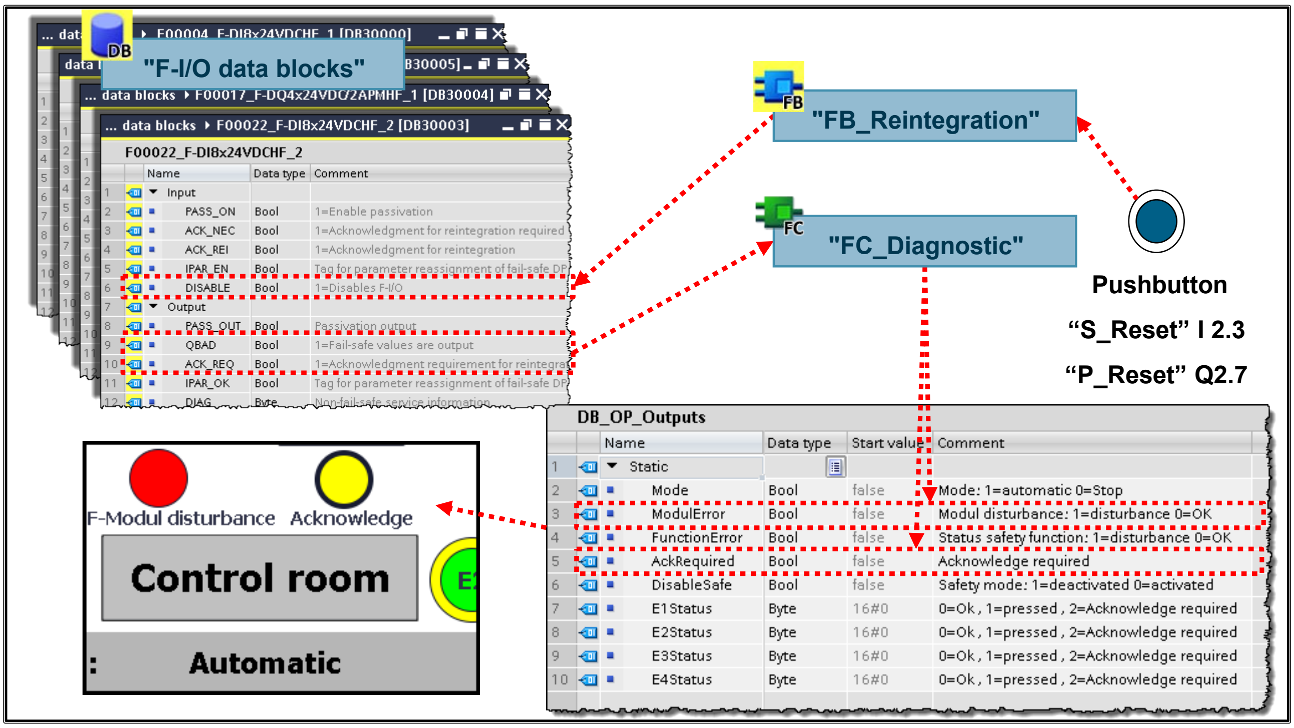
The behavior of the channel-specific value status of the fail-safe inputs / outputs of the training device is now to be checked.

What to Do

1. Using drag & drop, copy the Tag table "Value Status F-Channels" and the Watch table "Check Value Status" from the library into you project.
   Safety_Lib: "06"->"03"
2. Monitor the value status and the process signal of the individual channels when you trigger individual sensors (E1, E2, RFID, etc.).
3. Think about why all channels are currently passivated (value status = 0).

6.29. Exercise 4: Evaluating the F-Modules

6.29.1. Re: Exercise 4: "FC_Diagnostic" (FC12) and "FB_Reintegration" (F-FB110)



Task

The user is to be signaled via the Panel as soon as a channel of an F-module has failed or is passivated. In addition, the user is to receive a message as soon as a fault has gone and can be acknowledged. So that the user can acknowledge a fault that has been eliminated, he is provided with an acknowledgement button.

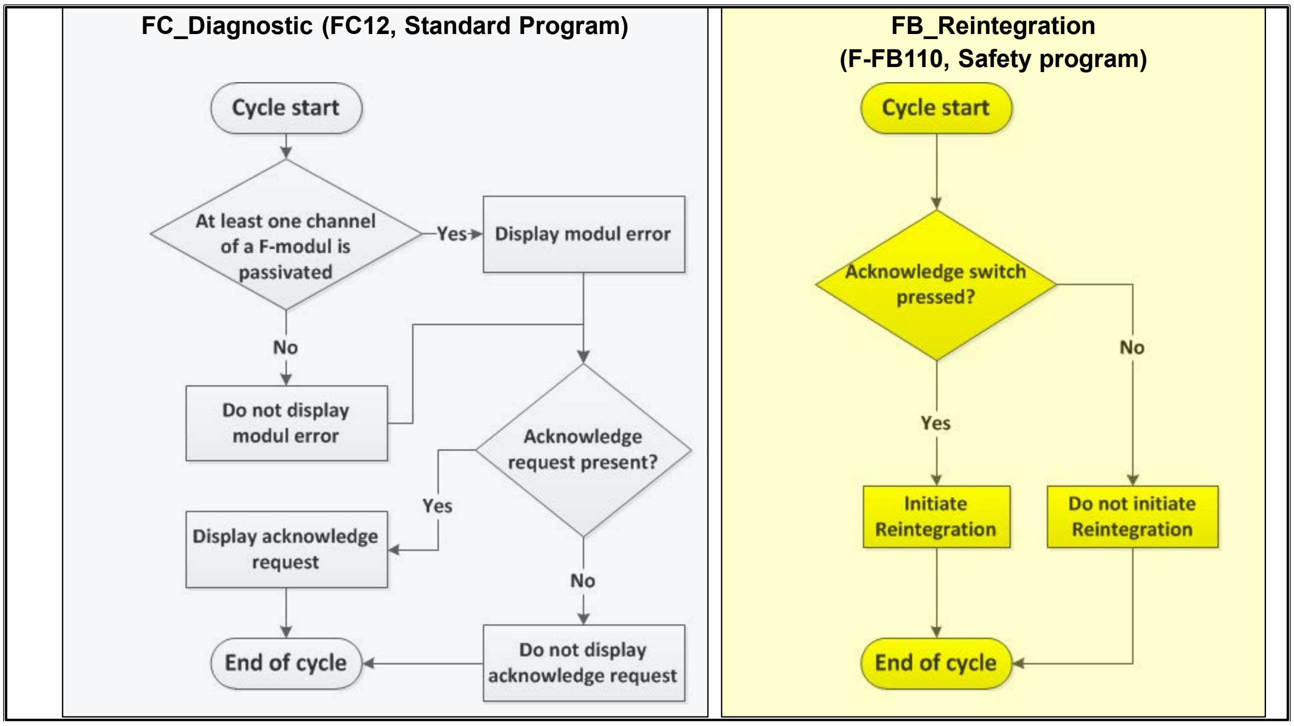
NOTE: For this exercise, please do not use the "ACK_GL" block from the Safety library. To illustrate, the acknowledgement is to be triggered directly via the I/O DBs.

What to Do

1. Generate the safety block "FB_Reintegration" (FB110) and the standard block "FC_Diagnostic" (FC12). Call these blocks in your program OB1->FC12 and FC100->FB110.

Continued on the next page

6.29.2. Re: Exercise 4: Flow Chart



2. Functionality "FB_Reintegration":

   The reintegration (depassivation) of all F-modules is to be programmed in this block. As soon as the acknowledgement button ("S_Reset") is pressed, a reintegration ("ACK_REI" of each F-I/O data block) is to be triggered for each F-module.

3. Functionality "FC_Diagnostic":

   The block is to read-in the passivation of at least one channel ("QBAD" of each F-I/O data block) and display it on the Panel ("DB_OP_Outputs.ModulError"). In addition, the reintegration request ("ACK_REQ" of each F-I/O data block) of an F-module is to be read-in and displayed on the Panel ("DB_OP_Outputs.AckRequired") as well as via the LED of the acknowledgement button ("P_Reset").

4. Download all blocks into the CPU.

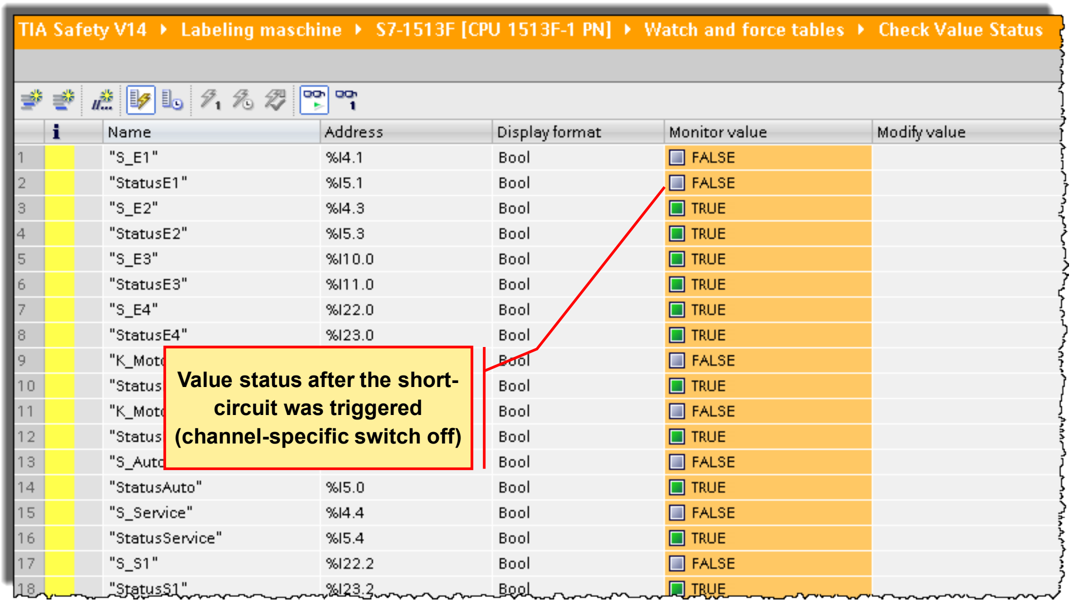
5. Save your project and test the functionality.

Relevant Interfaces		
Inputs	**Standard**	**Fail-safe**
	"S_Reset" (I 2.3)	-
Outputs	**Standard**	**Fail-safe**
	"P_Reset" (Q2.7)	-
Data blocks	**Global**	**System**
	DB_OP_Outputs.ModulError (DB99)	F_Peripherie DB.ACK_REI
	DB_OP_Outputs.AckRequired (DB99)	F_Peripherie DB.ACK_QBAD
		F_Peripherie DB.ACK_REQ

Note

All four F-I/O data blocks must be evaluated.

6.30. Exercise 5: Once Again Understanding the Value Status



Task

The behavior of the channel-specific value status of the fail-safe inputs / outputs of the training device is now to be checked once again.

What to Do

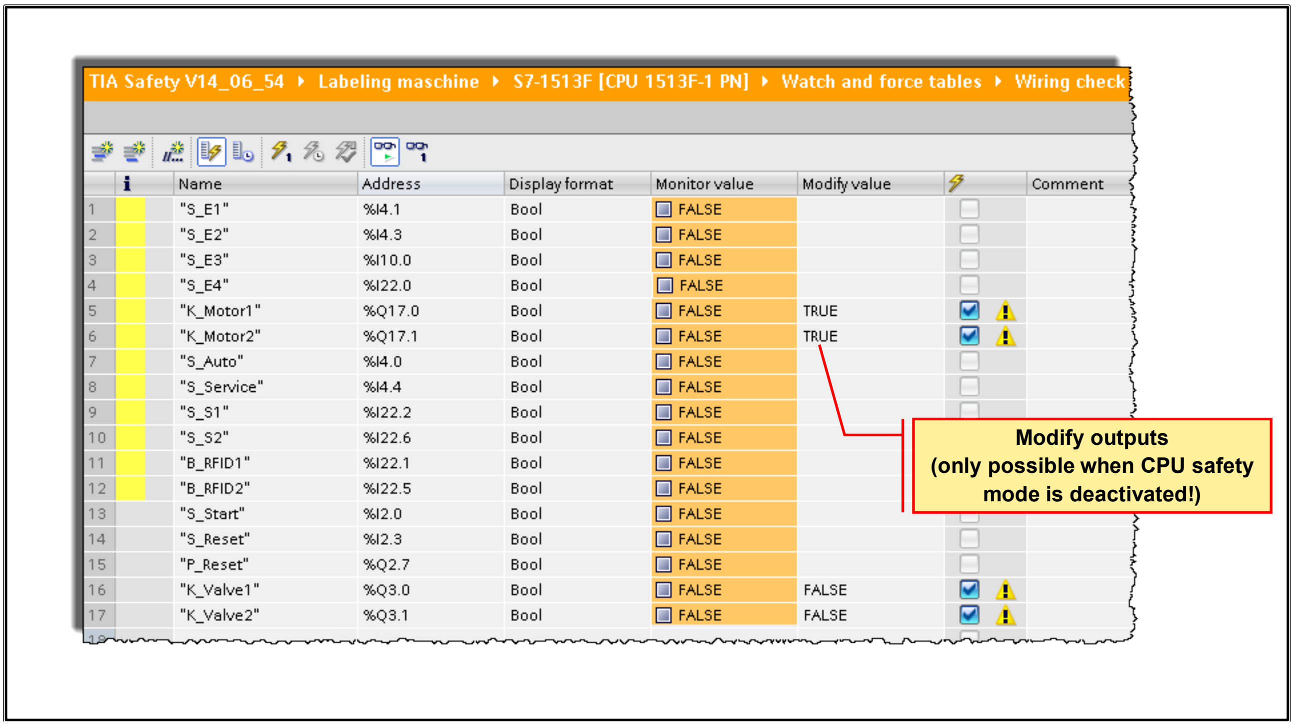
1. Monitor the reaction of the tags when:

- a protective device is triggered (E-Stop, safety door, etc.)
- you press the short-circuit switch ("Short circuit") on the training device.

Result

All F-modules are now (because of Exercise 4) used in the safety program and are depassivated after CPU startup and supply valid process values.

6.30.1. Re: Exercise 5: Wiring Test of the Inputs and Outputs



Task

You are now to check the wiring of all inputs and outputs of the training device.

What to Do

1. Using drag & drop, copy the Watch table "Wiring check" from the library into your project. Safety_Lib: "06"->"05"
2. Check the wiring of the inputs by activating the corresponding operating elements on the training case and comparing them with the monitoring values displayed on the PG.
3. Check the wiring of the fail-safe outputs by setting the control values on the PG and comparing them with the reactions of the actuators on the training case.

- Acknowledge the message "Safety mode active"
- Confirm that you want to deactivate the safety mode

Result

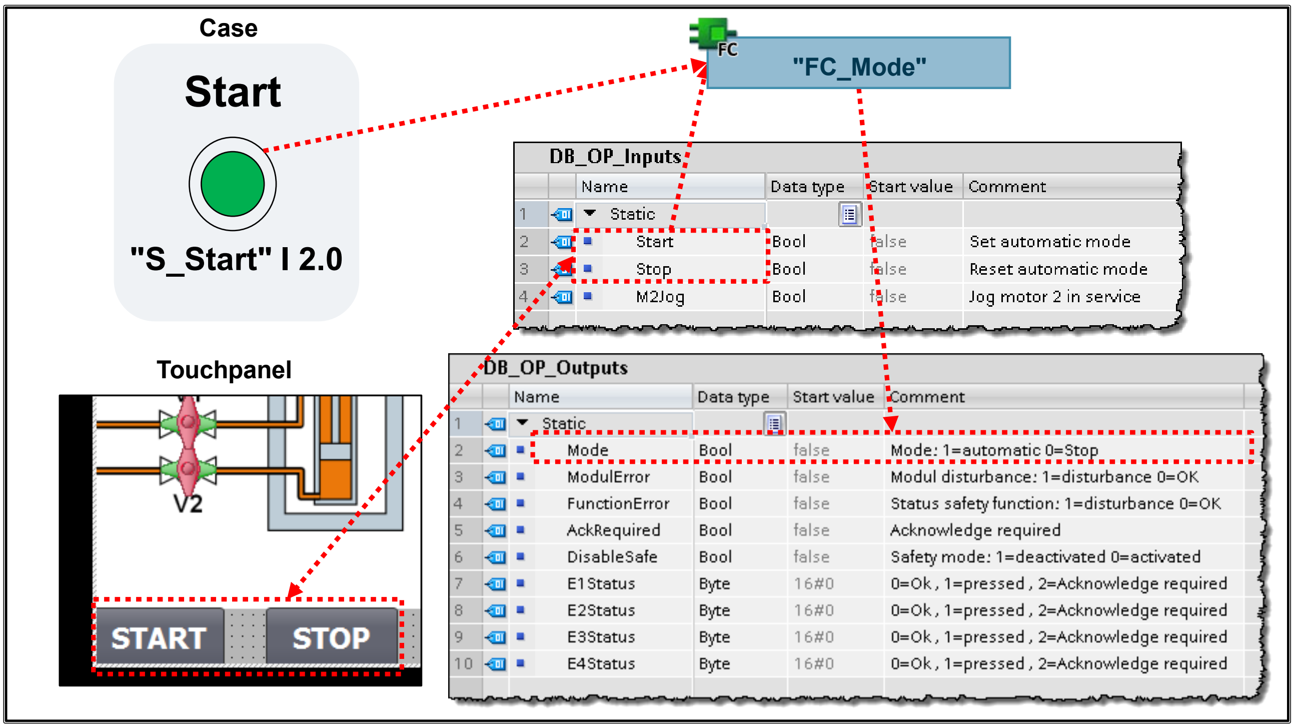
All inputs and outputs of the training device should be correctly connected. If not, check the parameter assignments of the channels concerned and also the process image assignment.

Caution!

Please do not change the existing wiring in any way. If you are of the opinion that a wiring error exists, please discuss it with your instructor.

6.31. Exercise 6: Operating Mode

6.31.1. Re: Exercise 6: "FC_Mode" (FC10)



Task

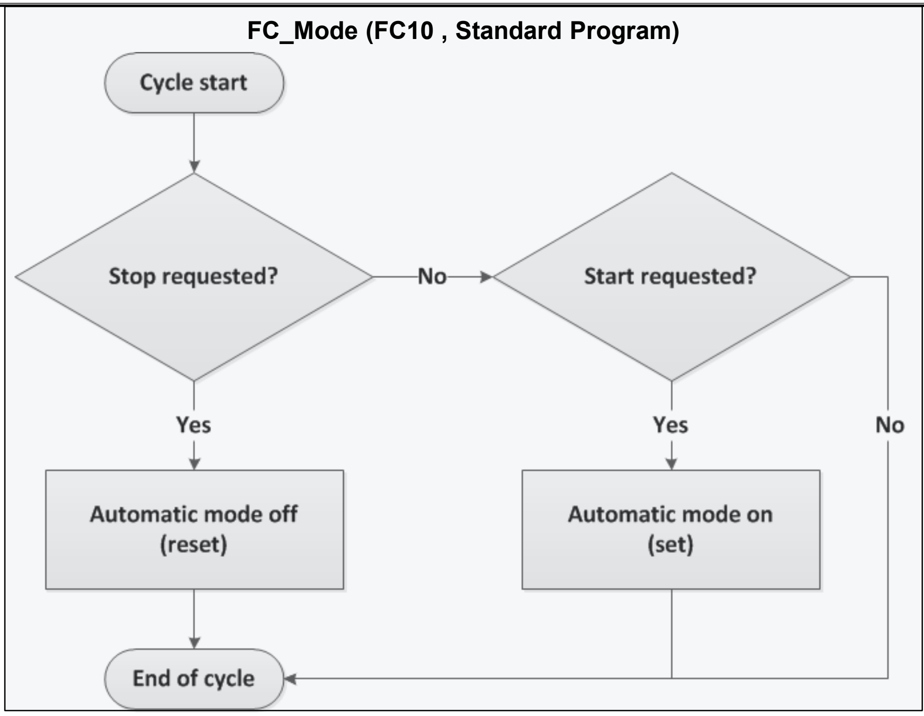
The machine "Labeler" is to be considered as a stand-alone and independent system. As operating mode, only an Automatic mode is to be implemented that simultaneously affects all parts of the system. The user is to be able to switch the Automatic mode on and off via the Panel. In addition, the user can trigger a Start command via a Start button on the station. With a simultaneous Start and Stop command, the Stop command is to dominate.

What to Do

1. Generate the standard block "FC_Mode" (FC10). Call this block in your program OB1->FC10

Continued on the next page

6.31.2. Re: Exercise 6: Flow Chart



2. Functionality "FC_Mode":

You are to program the block in such a way that the Automatic mode is reset ("DB_OP_Outputs.mode" = 0) for a Stop command ("DB_OP_Inputs.stop" =1).
When a Start command ("DB_OP_Inputs.start"=1 or "S_Start" =1) is triggered, the Automatic mode is to be switched on ("DB_OP_Outputs.mode" = 1).
Keep in mind that the Stop command is to dominate with a simultaneous activation.

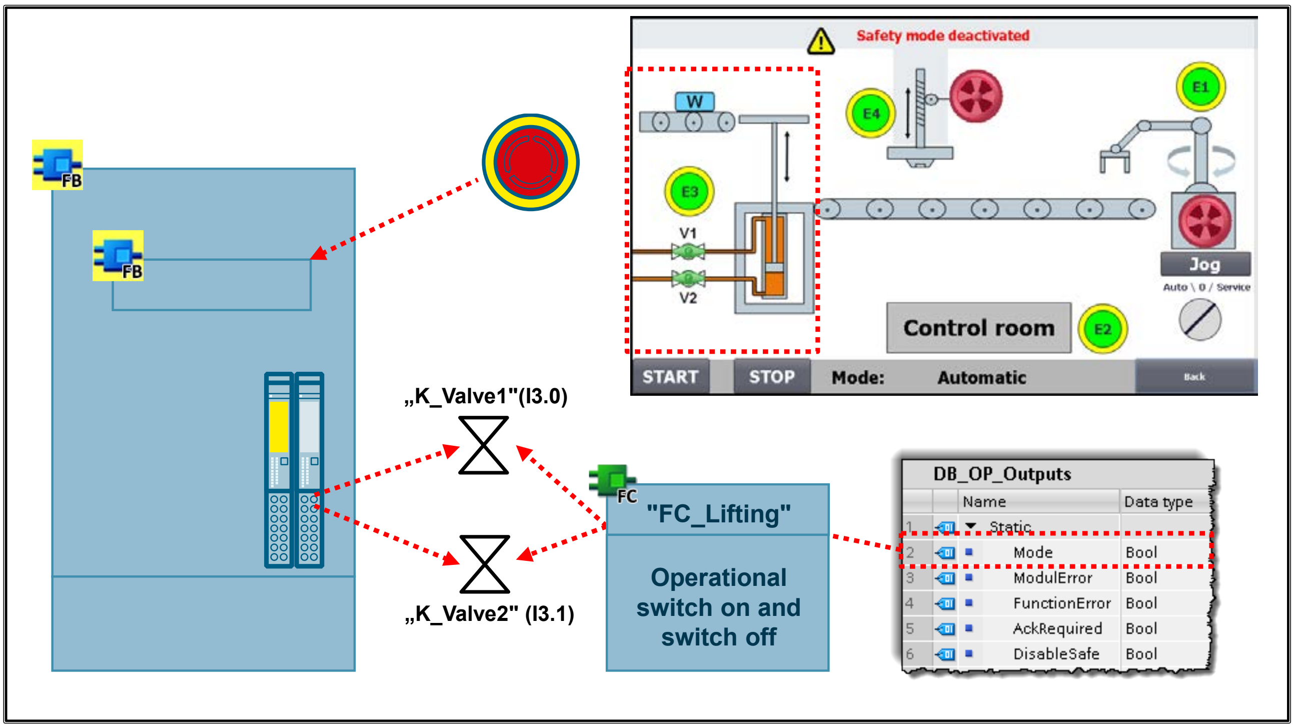
3. Download all blocks into the CPU.

4. Save your project and test the functionality.

Relevant Interfaces		
Inputs	**Standard**	**Fail-safe**
	"S_Start" (I 2.0)	-
Outputs	**Standard**	**Fail-safe**
	-	-
Data blocks	**Global**	**System**
	DB_OP_Inputs.start (DB99)	
	DB_OP_Inputs.stop (DB99)	
	DB_OP_Outputs.mode (DB99)	

6.32. Exercise 7: Lifting Device

6.32.1. Re: Exercise 7: "FC_Lifting" (FC11) and "FB_Lifting" (F-FB111)



Task

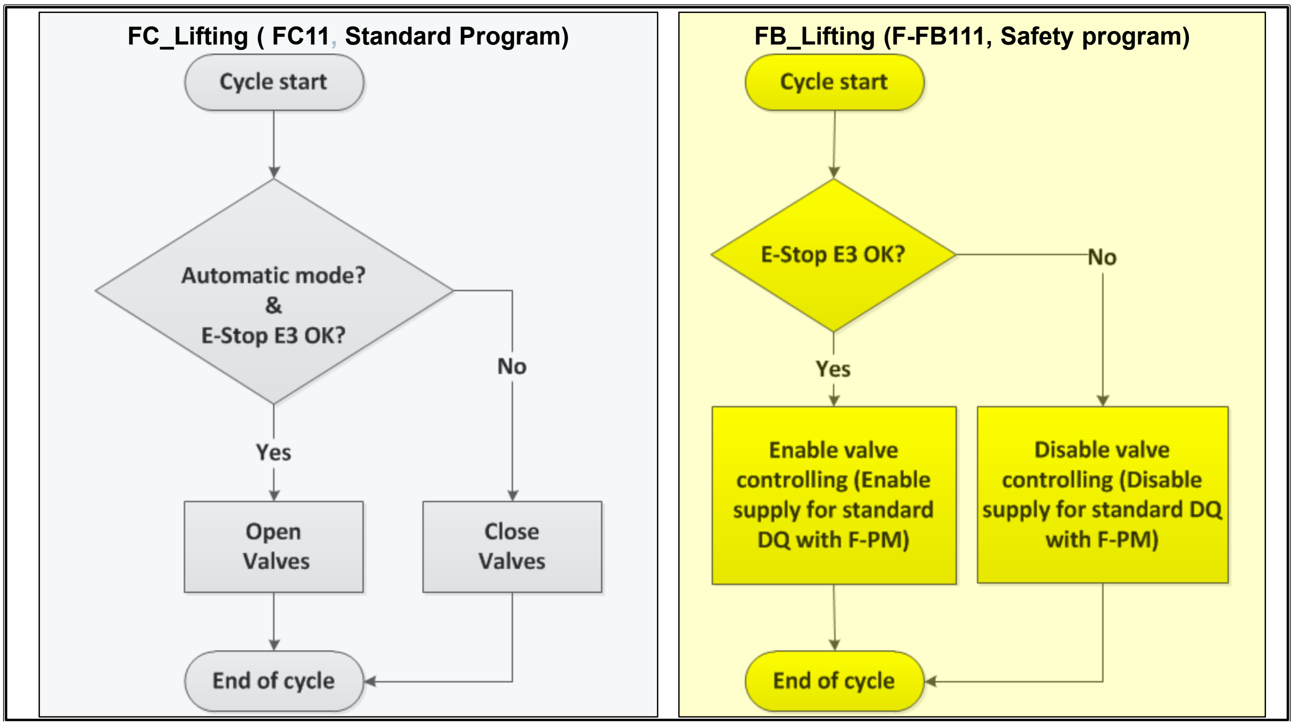
The lifting device part of the system serves to feed a workpiece to the labeling device. At this point, we are only considering the functionality of the safety-relevant shut-off valves. The functions 'lower' and 'lift' of the lifting device are not considered in this exercise.
The shut-off valves are to be operationally switched. In Automatic mode, the valves are to be enabled and in Stop they are to be disabled. A safety-related shutdown is to be realized via an E-OFF set-up. The safety program is to inhibit the operational control of the valves via the shutdown of the energy supply. After triggering the E-STOP, an energy supply enable is only to occur after an acknowledgement.

What to Do

1. Generate the safety block "FB_Lifting" (FB111) and the standard block "FC_Lifting" (FC11). Call these blocks in your program OB1->FC11 and FC100->FB111.

Continued on the next page

6.32.2. Re: Exercise 7: Flow Chart



1. Functionality "FB_Lifting":

   The block is to monitor the E-Stop E3 ("S_E3") by means of the safety function "ESTOP". As soon as the E-Stop E3 is pressed ("S_E3" =0) the shutdown of the power supply for the subsequent standard module DO (Slot 5) is to be triggered immediately ("K_PowerValves" =0). After the E-Stop E3 ("S_E3" =1) is unlocked, the power supply is once again to be switched-on ("K_PowerValves" =1) after the acknowledgement button ("S_Reset" =1) is pressed.

2. Functionality "FC_Lifting":

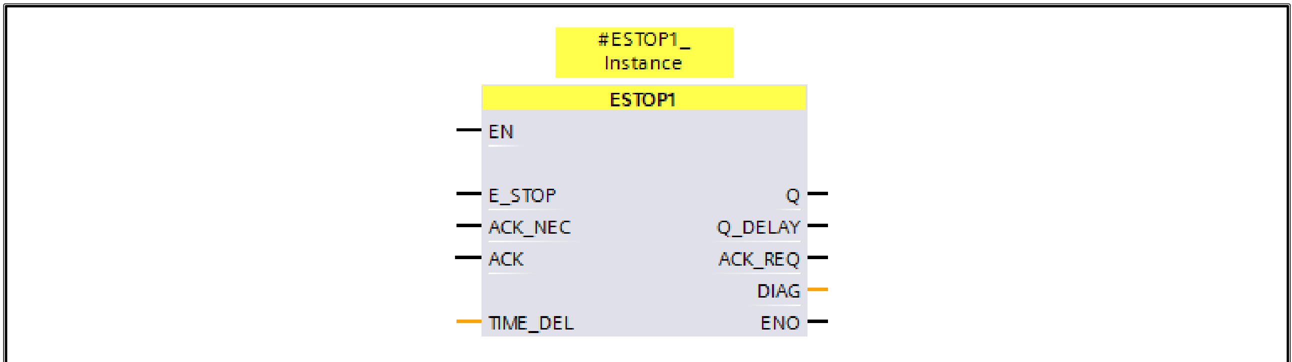
   The block is to check whether the Automatic mode switches on ("DB_OP_Outputs.mode" =1) and the safety program supplies an enable for the valve control ("K_PowerValves" =1). If these two conditions are fulfilled, both shut-off valves are to be energized ("K_Valve1"=1 and "K_Valve2"=1).
   If not, both valves are to be de-energized ("K_Valve1"=0 and "K_Valve2"=0).

3. Download all blocks into the CPU.

4. Save your project and test the functionality.

Relevant Interfaces		
Inputs	**Standard**	**Fail-safe**
	"S_Reset" (I 2.3)	"S_E3" (I 10.0)
Outputs	**Standard**	**Fail-safe**
	"K_Valve1" (Q3.0)	"K_PowerValves" (Q10.0)
	"K_Valve2" (Q3.1)	
Data blocks	**Global**	**System**
	"DB_OP_Outputs.mode" (DB99)	

6.32.3. ESTOP (FB215)



Static			
ESTOP1_Instance	ESTOP1		
Input			
E_STOP	Bool	false	Emercency STOP
ACK_NEC	Bool	true	1=Acknowledgment necessary
ACK	Bool	false	1=Acknowledgment
TIME_DEL	Time	0	Time delay
Output			
Q	Bool	false	1=Enable
Q_DELAY	Bool	false	Enable is OFF delayed
ACK_REQ	Bool	false	1=acknowledgment request
DIAG	Byte	B#16#00	Service information
InOut			

This instruction implements an emergency STOP/emergency OFF shutdown with acknowledgement for Stop Categories 0 and 1.

The enable signal Q is reset to 0 as soon as input E_STOP assumes the signal state 0 (Stop Category 0). The enable signal Q_DELAY is reset to 0 after the delay time set at input TIME_DEL (Stop Category 1).

The enable signal Q is not reset to 1 until input E_STOP assumes signal state 1 and an acknowledgment occurs. The acknowledgment for the enable is dependent on the parameter assignment at input ACK_NEC:

- If ACK_NEC = 0, the acknowledgment is automatic.
- If ACK_NEC = 1, you must use a rising edge at input ACK for acknowledging the enable.

The output ACK_REQ is used to signal that a user acknowledgment is required at input ACK for the acknowledgment. The instruction sets the output ACK_REQ to 1 as soon as input E_STOP = 1.

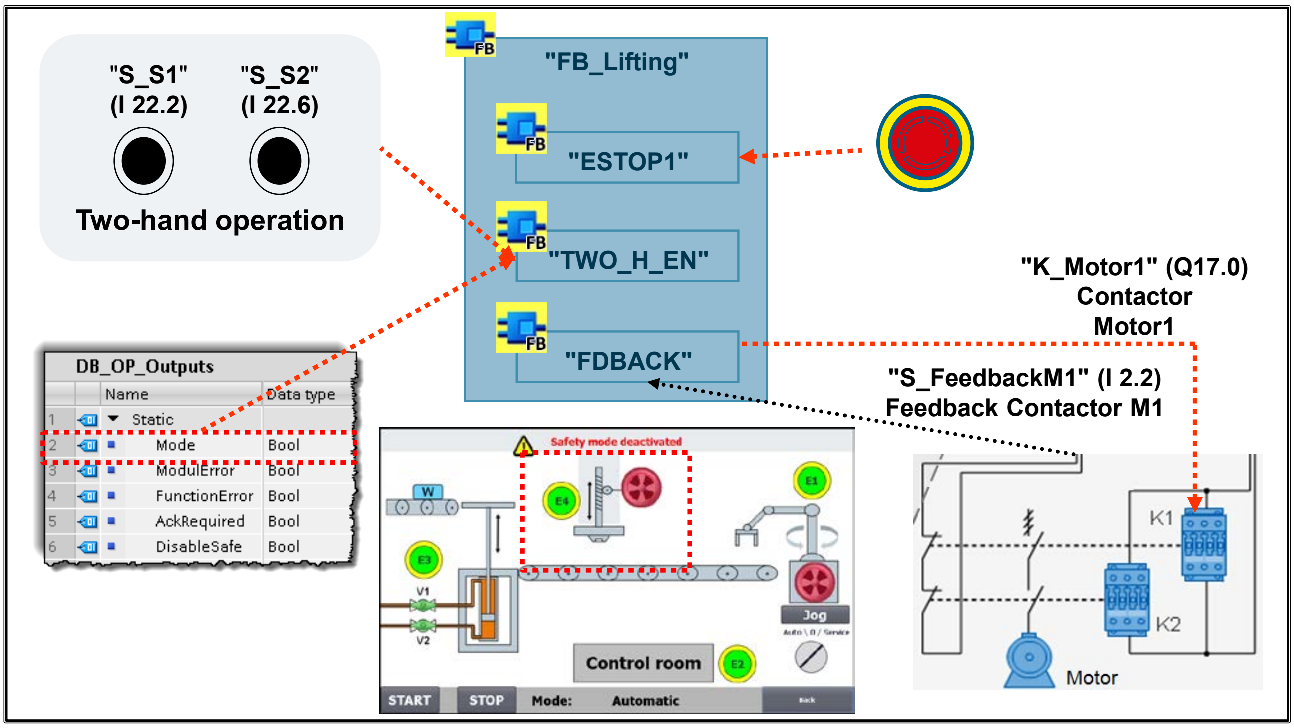
After acknowledgment, the instruction resets ACK_REQ to 0.

Warning:

The ACK_NEC tag must not be assigned a value of 0 unless an automatic restart of the affected process is otherwise excluded.

6.33. Exercise 8: Labeler

6.33.1. Re: Exercise 8: "FB_Labeling" (F-FB112)



Task

In the Labeler part of the system, the supplied part is labelled. Just as in the Lifting device part of the system, at this point, we are only considering the safety-relevant functionality.
The motor of the labeler is only to be energized if the following conditions are fulfilled:

- E-Stop (E4) is OK
- Two-hand operation is properly activated (t< 300ms)
- Automatic mode is active

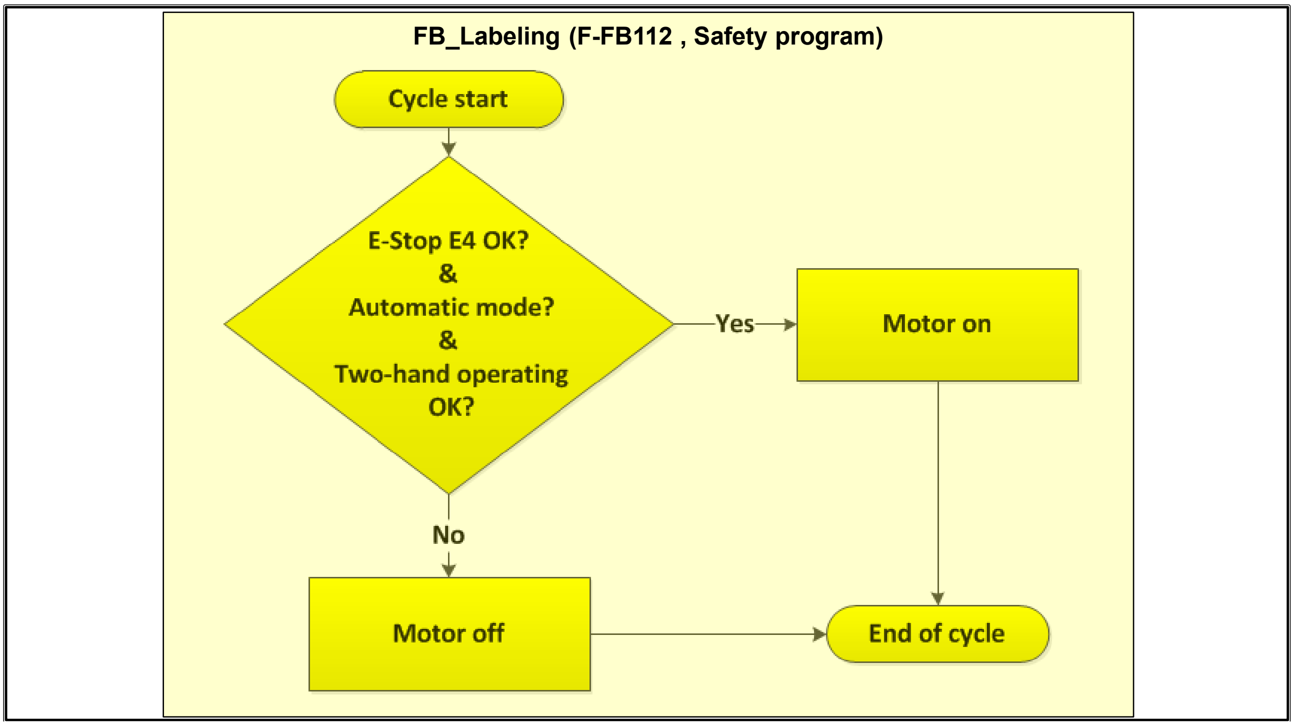
After the E-Off is triggered, an enable for the energizing of the motor is only to occur after an acknowledgement.

What to Do

1. Generate the safety block "FB_Labeling" (FB112). Call this block in your program FC100->FB112

Continued on the next page

6.33.2. Re: Exercise 8: Flow Chart



1. Functionality "FB_Labeling":

The block is to monitor the enable for energizing Motor1 by means of the safety functions "ESTOP", "TWO_H_EN" and the standard function "Mode". Collect all enable conditions ("ESTOP.Q", "TWO_H_EN.Q" and "DB_OP_Outputs.mode") and with it energize Motor 1 by means of the safety function "FDBACK".

"ESTOP":
As soon as the E-Stop E4 is pressed ("S_E4" =0) the enable of ESTOP is to be inhibited immediately ("ESTOP.Q" =0). After the E-Stop E4 ("S_E4" =1) is unlocked, the enable of the ESTOP is once again to occur ("ESTOP.Q" =1) after the acknowledgement button ("S_Reset" =1) is pressed.

"TWO_H_EN":
An enable ("TWO_H_EN.Q" = 1) is only to occur when Button1 ("S_S1") and Button2 ("S_S2") assume the value 1 within 300ms.

"Mode":
It is only to be possible to energize the motor in Automatic mode ("DB_OP_Outputs.mode" =1). For this, use the enable function of the two-hand monitoring ("TWO_H_EN.ENABLE").

"FDBACK":
As soon as the safety function receives the enable ("FDBACK.ON" =1) Motor 1 is to be energized ("K_Motor1" =1). Connect all relevant interfaces of "FDBACK" correctly (Help function with "F1"). The monitoring time "FDB_TIME" is to be set to 200ms.

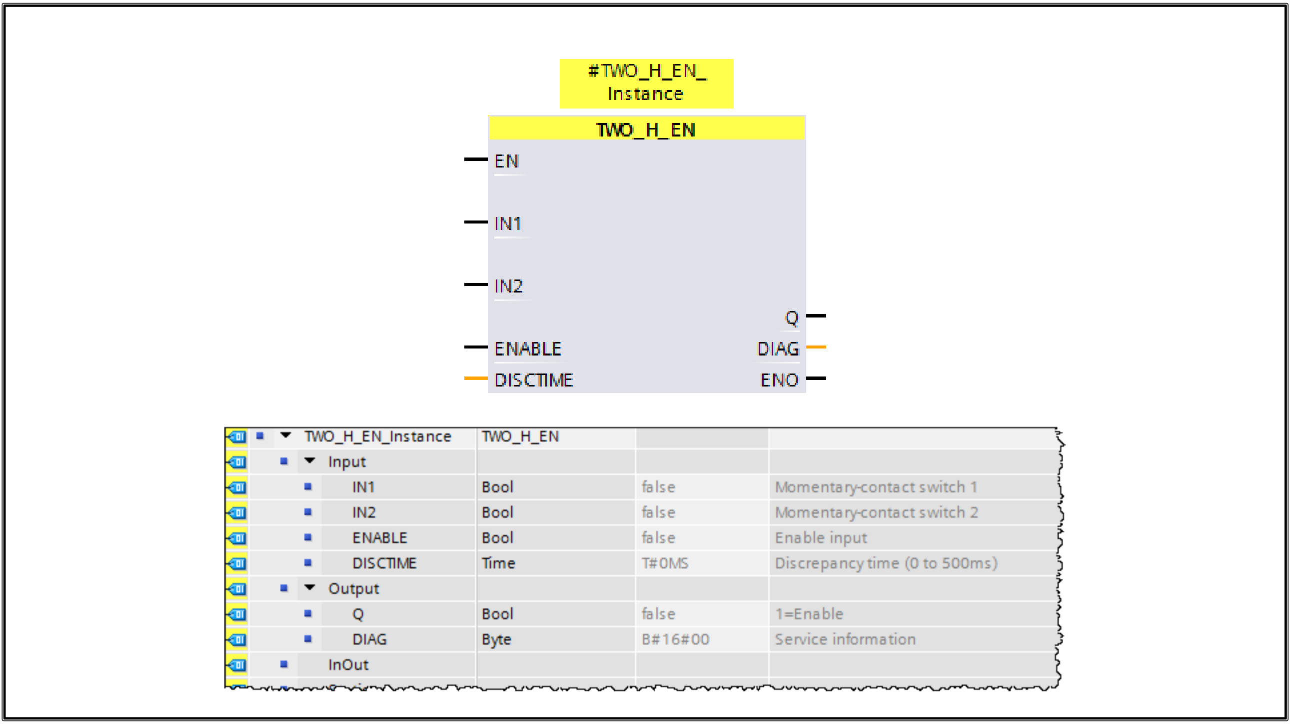
2. Download all blocks into the CPU.

3. Save your project and test the functionality.

Note: You will find the description of the relevant interfaces on the next page.

Relevant Interfaces		
Inputs	**Standard**	**Fail-safe**
	"S_Reset" (I 2.3)	"S_E4" (I 22.0)
	"S_FeedbackM1" (I 2.2)	"S_S1" (I 22.2)
		"S_S2" (I 22.6)
Outputs	**Standard**	**Fail-safe**
		"K_Motor1" (Q17.0)
Data blocks	**Global**	**System**
	"DB_OP_Outputs.mode" (DB99)	

6.33.3. TWO_H_EN (FB211)

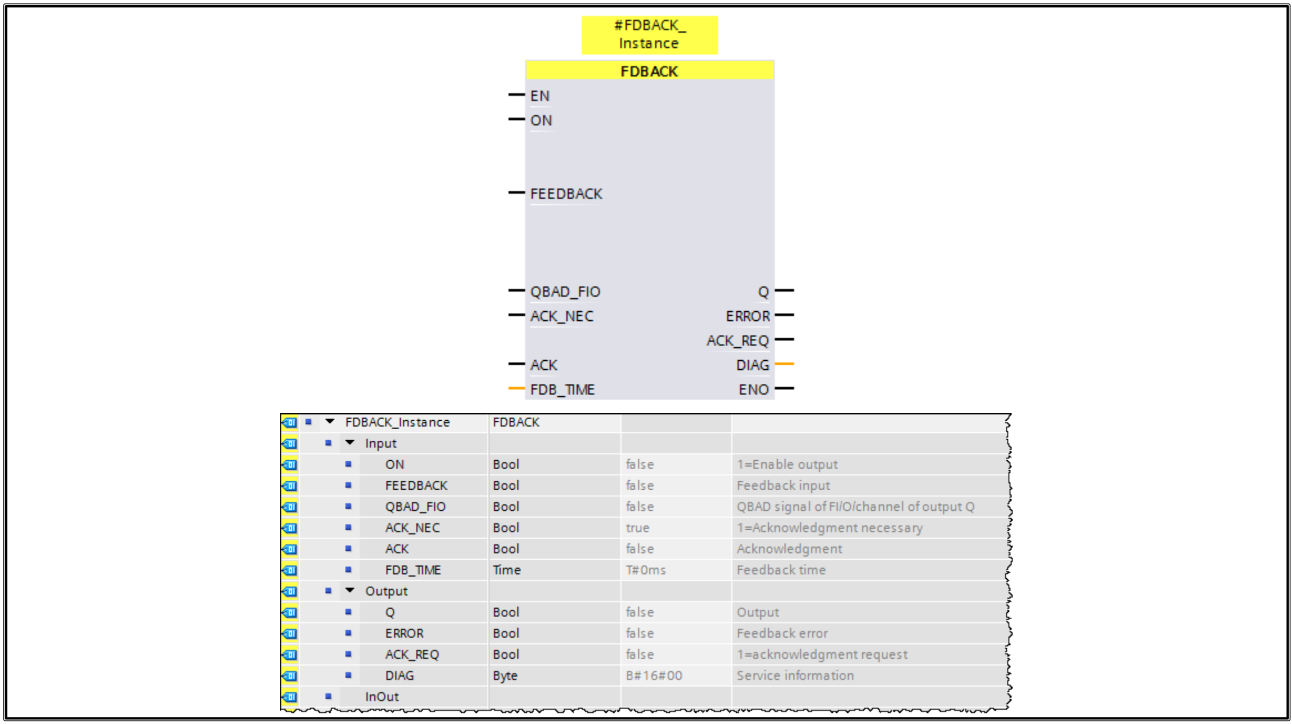


This instruction implements a two-hand monitoring with enable.

If the IN1 and IN2 buttons are pressed within the permitted discrepancy time DISCTIME ≤ 500 ms (IN1/IN2 = 1) (synchronous pressing), the enable signal Q is set to 1 when ENABLE = 1 is present. If the time difference between pressing the IN1 button and IN2 button was greater than DISCTIME, the buttons must be released and then pressed again.

Q is reset to 0 as soon as one of the buttons is released (IN1/IN2 = 0) or ENABLE = 0. The enable signal Q can then only be set to 1 again if the other button has also been released and, when afterwards, both buttons are pressed again within the discrepancy time when ENABLE = 1 is present.

6.33.4. FDBACK (FB216)



FDBACK_Instance	FDBACK		
Input			
ON	Bool	false	1=Enable output
FEEDBACK	Bool	false	Feedback input
QBAD_FIO	Bool	false	QBAD signal of FI/O/channel of output Q
ACK_NEC	Bool	true	1=Acknowledgment necessary
ACK	Bool	false	Acknowledgment
FDB_TIME	Time	T#0ms	Feedback time
Output			
Q	Bool	false	Output
ERROR	Bool	false	Feedback error
ACK_REQ	Bool	false	1=acknowledgment request
DIAG	Byte	B#16#00	Service information
InOut			

This instruction implements feedback loop monitoring.

The signal state of output Q is checked to see whether it corresponds to the inverse signal state of the feedback input FEEDBACK. Output Q is set to 1 as soon as input ON = 1. Requirement for this is that the feedback input FEEDBACK = 1 and no feedback error is saved. Output Q is reset to 0, as soon as input ON = 0 or if a feedback error is detected.

A feedback error ERROR = 1 is detected if the inverse signal state of the feedback input FEEDBACK (to input Q) does not follow the signal state of output Q within the maximum tolerable feedback time. The feedback error is saved.

If a discrepancy is detected between the feedback input FEEDBACK and the output Q after a feedback error, the feedback error is acknowledged in accordance with the parameter assignment of ACK_NEC:

- If ACK_NEC = 0, the acknowledgment is automatic.
- If ACK_NEC = 1, you must acknowledge the feedback error with a rising edge at input ACK.

The ACK_REQ = 1 output then signals that a user acknowledgment is necessary at input ACK to acknowledge the feedback error. Following an acknowledgment, the instruction resets ACK_REQ to 0.

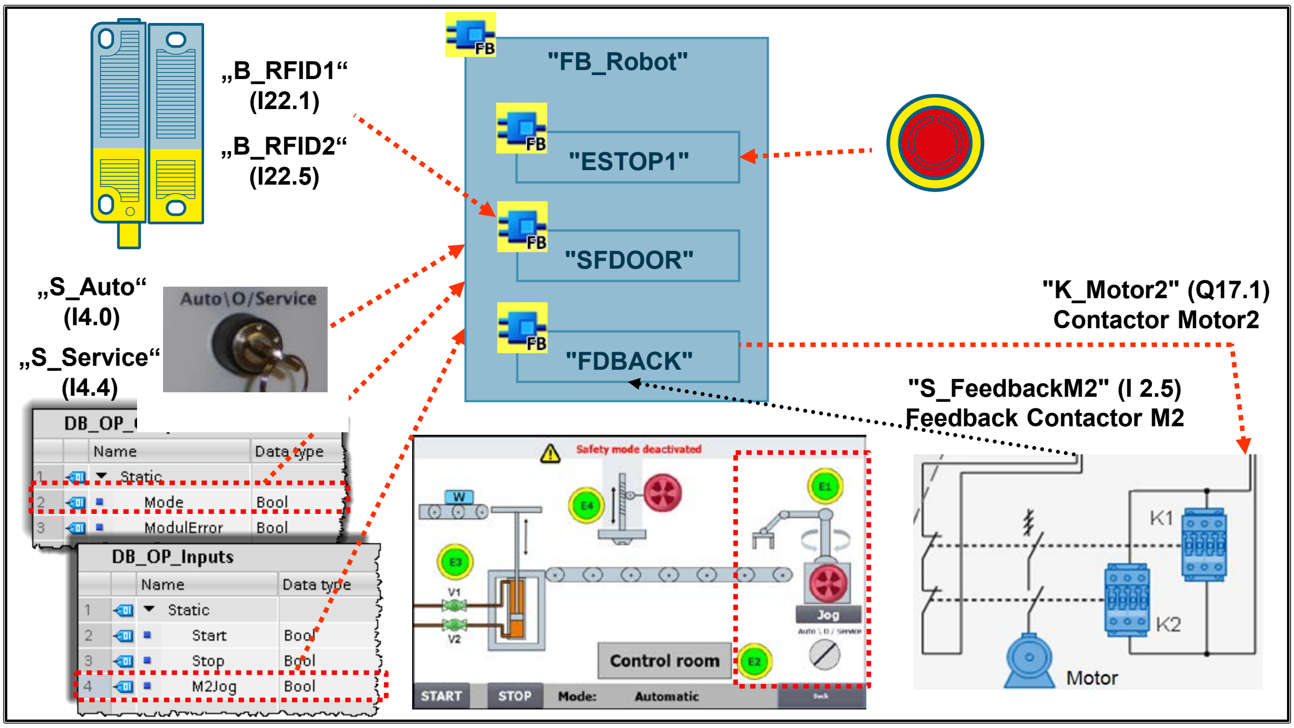
To prevent feedback errors from being detected and acknowledgments from being required when the F-I/O controlled by the Q output are passivated, you need to supply input QBAD_FIO with the QBAD signal of the associated F-I/O or the QBAD_O_xx signal/ with the inverted value status of the associated channel.

Warning:

The ACK_NEC tag must not be assigned a value of 0 unless an automatic restart of the affected process is otherwise excluded.

6.34. Exercise 9: Robot

6.34.1. Re: Exercise 9: "FB_Robot" (F-FB113)



Task

In the Robot part of the system, the processed workpiece is to be removed. Here we are only considering the safety-relevant functionality.
The motor of the robot is only to be energized when the following conditions are fulfilled:

- E-Stop (E1) is OK
- Safety door is closed
- Safety switch is set to Automatic mode
- Automatic mode is active

In addition - for Service / Commissioning work - it should be possible to control the robot in jog mode even if the safety door is open when the following conditions are fulfilled:

- E-Stop (E1) is OK
- Safety switch is set to Service mode
- Automatic mode is not active
- The "Jog" button on the Panel is pressed

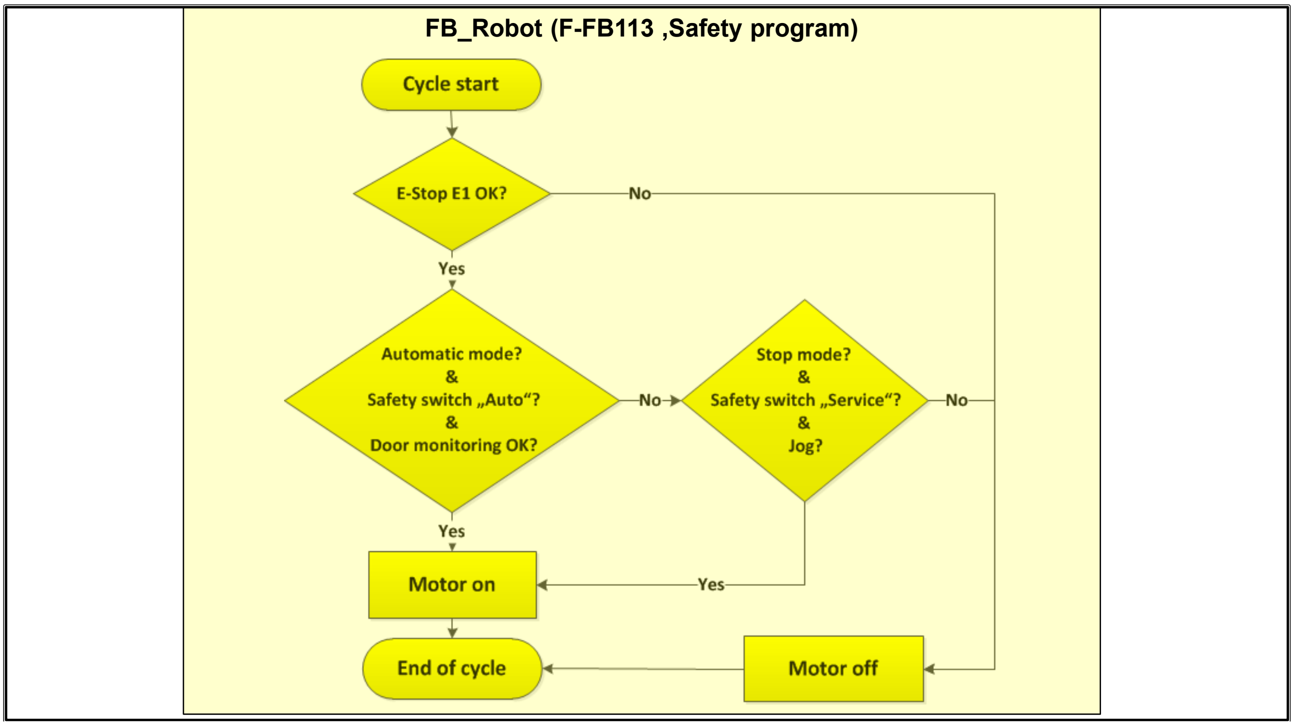
After the E-Stop or the safety door monitoring is triggered, an enable for the control of the motor is only to occur after an acknowledgement.

What to Do

1. Generate the safety block "FB_Robot" (FB113). Call this block in your program FC100->FB113.

Continued on the next page

6.34.2. Re: Exercise 9: Flow Chart



2. Functionality "FB_Robot":

The block is to monitor the enable for energizing Motor1 by means of the safety functions "ESTOP", "SFDOOR", the safety switch, the standard function "Mode" and the "Jog" button on the Panel. Collect all enable conditions ("ESTOP.Q", "SFDOOR.Q" etc.) and with it energize Motor 2 by means of the safety function "FDBACK".

"ESTOP":
As soon as the E-Stop E1 is pressed ("S_E1" =0) the enable of ESTOP is to be inhibited immediately ("ESTOP.Q" =0). After the E-Stop E1 ("S_E1" =1) is unlocked, the enable of the ESTOP is once again to occur ("ESTOP.Q" =1) after the acknowledgement button ("S_Reset" =1) is pressed.

"SFDOOR":
An enable ("SFDOOR.Q" = 1) is only to occur when the safety door is completely closed ("B_RFID1" =1 and "B_RFID2" =1). The functionality "Opening necessary after startup" is not required ("SFDOOR.OPEN_NEC" = 0). After the safety door is closed, the enable is only to occur after the acknowledgement button ("S_Reset" =1) is pressed.

"FDBACK":
As soon as the safety function receives the enable ("FDBACK.ON" =1) Motor 2 is to be energized ("FDBACK.Q" = "K_Motor2"). Connect all relevant interfaces of "FDBACK" correctly (Help function with "F1"). The monitoring time "FDB_TIME" is to be set to 200ms.

An enable for the energizing ("FDBACK.ON") of Motor 2 via the safety function "FDBACK" is now formed via two possible paths:

Automatic mode:

- Enable E-Stop ("ESTOP.Q" =1)
- Enable Safety door ("SFDOOR.Q" =1)
- Safety switch is set to Automatic mode ("S_Auto" =1)
- Automatic mode is active ("DB_OP_Outputs.mode" =1)

Continued on the next page

Service mode:

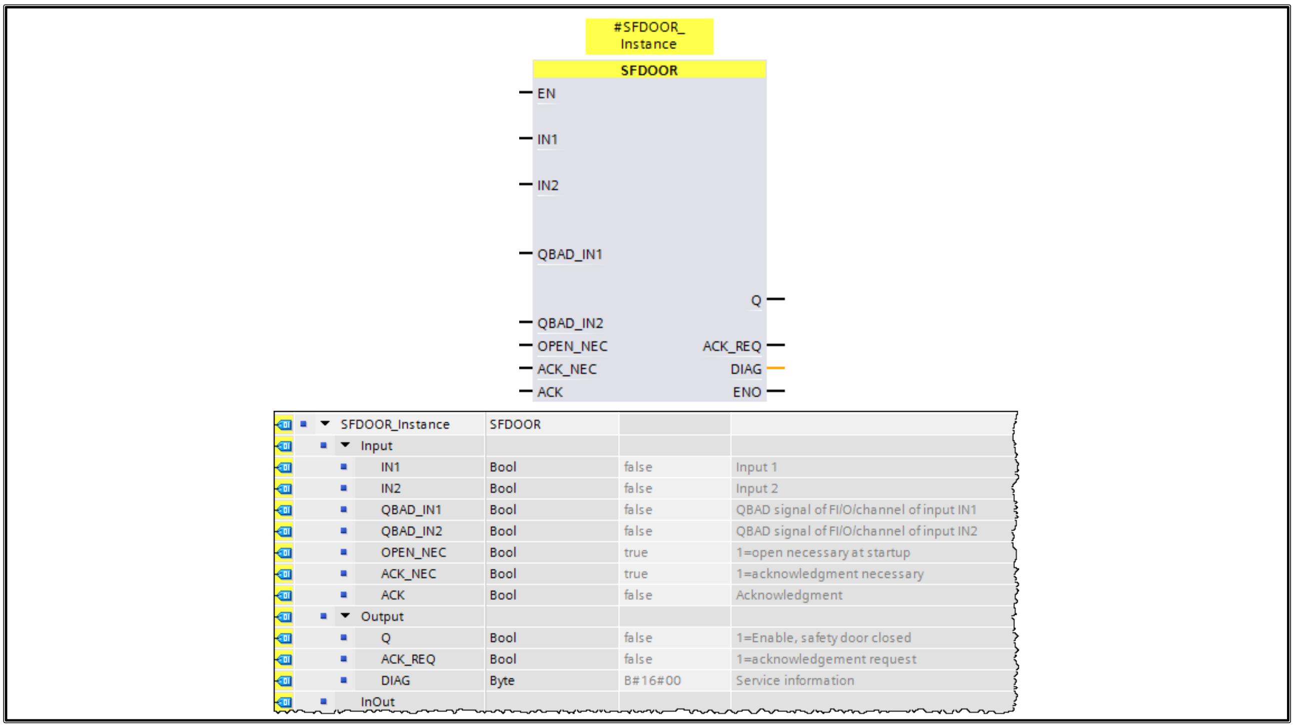
- Enable E-Stop ("ESTOP.Q" =1)
- Safety switch is set to Service mode ("S_Service" =1)
- Automatic mode is not active ("DB_OP_Outputs.mode" =0)
- The "Jog" button on the Panel is pressed ("DB_OP_Inputs.M2_Jog" =1)

3. Download all blocks into the CPU.

4. Save your project and test the functionality.

Relevant Interfaces		
Inputs	**Standard**	**Fail-safe**
	"S_Reset" (I 2.3)	"S_E1" (I 4.1)
	"S_FeedbackM2" (I 2.5)	"B_RFID1" (I 22.1)
		"B_RFID2" (I 22.5)
		"S_Auto" (I 4.0)
		"S_Service" (I 4.4)
Outputs	**Standard**	**Fail-safe**
		"K_Motor2" (Q17.1)
Data blocks	**Global**	**System**
	"DB_OP_Outputs.mode" (DB99)	-
	"DB_OP_Inputs.M2_Jog" (DB99)	

6.34.3. SFDOOR (FB217)



This instruction implements a safety door monitoring.

The Enable signal Q is reset to 0 as soon as one of the inputs IN1 or IN2 take a signal state of 0 (safety door is opened). The enable signal can only be reset to 1, if:

- Both inputs IN1 and IN2 have assumed signal state 0 before the door is closed (safety door had been completely open)
- Subsequently both inputs IN1 and IN2 assume signal state 1 (safety door is closed)
- An acknowledgement occurs

The acknowledgment for the enable takes place according to the parameter assignment at input ACK_NEC:

- If ACK_NEC = 0, the acknowledgment is automatic.
- If ACK_NEC = 1, you must use a rising edge at input ACK for acknowledging the enable.

Output ACK_REQ = 1 is used to signal that a user acknowledgment is required at input ACK for the acknowledgment. The instruction sets ACK_REQ = 1 as soon as the door is closed. Following an acknowledgment, the instruction resets ACK_REQ to 0.

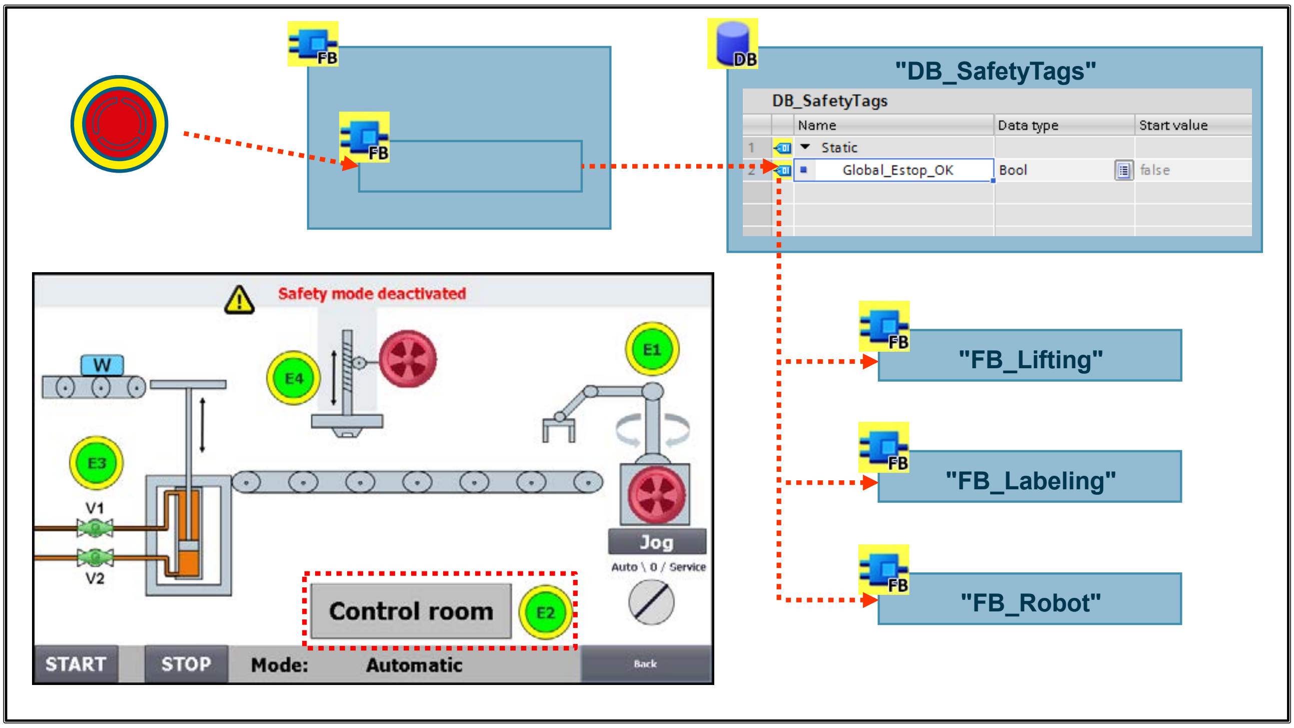
So that the instruction recognizes whether the inputs IN1 and IN2 are 0 merely due to passivation of the associated F-I/O, you must supply the inputs QBAD_IN1 or QBAD_IN2 with the QBAD signal of the associated F-I/O or QBAD_I_xx signal/ with the inverted value status of the associated channel. Among other things, this will prevent you from having to open the safety door completely prior to an acknowledgment in the event the F-I/O are passivated.

Warning:

The ACK_NEC tag must not be assigned a value of 0 unless an automatic restart of the affected process is otherwise excluded.

6.35. Exercise 10: Service Control Room

6.35.1. Re: Exercise 10: "FB_ControlRoom" (F-FB114) and "DB_SafetyTags" (F-DB101)



Task

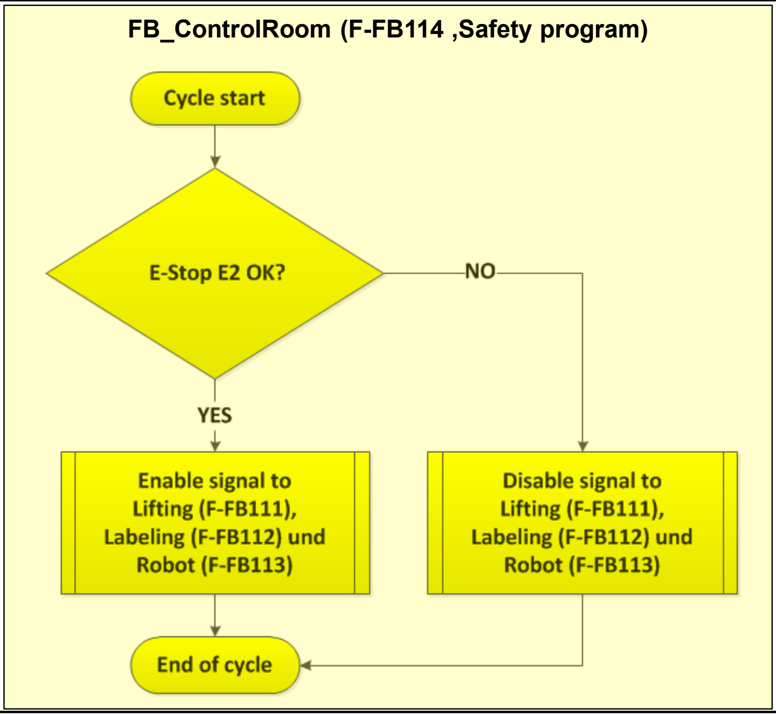
The Service Control room serves to monitor the entire system. The Control room should be able to bring the system to the safe state by means of the E-STOP. When the E-Stop is pressed, all system parts (lifting device, labeler and robot) are to switch to the safe state.
After the E-Stop is triggered, an enable is only to occur after an acknowledgement.

What to Do

1. Generate the safety block "FB_ControlRoom" (FB114). Call this block in your program FC100->FB114.
2. Generate the global fail-safe data block "DB_SafetyTags" (DB101) and create the Boolean tag "Global_Estop_OK" (see picture).

Continued on the next page

6.35.2. Re: Exercise 10: Flow Chart



3. Functionality "FB_ControlRoom":

The block is to monitor the E-Stop E2 ("S_E2") by means of the safety function "ESTOP". As soon as the E-Stop E2 is pressed ("S_E2" =0) the shutdown of all system parts is to be executed immediately. The enable of ESTOP ("ESTOP.Q") is to be stored in the previously created global fail-safe data block ("DB_SafetyTags.Global_Estop_OK"). After the E-Stop E2 ("S_E2" =1) is unlocked, the enable of the ESTOP is once again to occur ("ESTOP.Q" =1) after the acknowledgement button is pressed ("S_Reset" =1).

The global enable signal ("DB_SafetyTags.Global_Estop_OK") is now to be included in all parts of the system. Expand the blocks "FB_Lifting", "FB_Labeling" and "FB_Robot" to include this new enable condition.

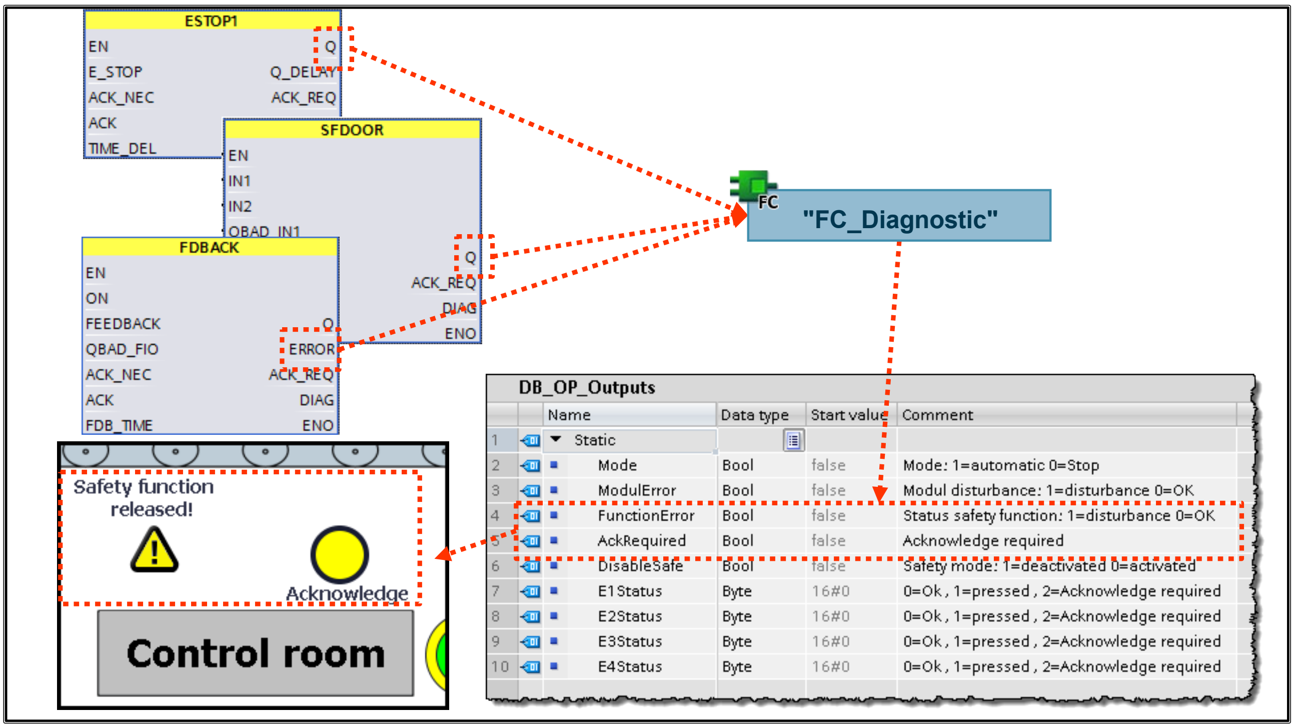
4. Download all blocks into the CPU.

5. Save your project and test the functionality.

Relevant Interfaces		
Inputs	**Standard**	**Fail-safe**
	"S_Reset" (I 2.3)	"S_E2" (I 4.3)
Outputs	**Standard**	**Fail-safe**
Data blocks	**Global**	**System**
	"DB_SafetyTags" (DB101)	

6.36. Exercise 11: Status Safety Functions

6.36.1. Re: Exercise 11: Expansion of "FC_Diagnostic" (FC12)



Task

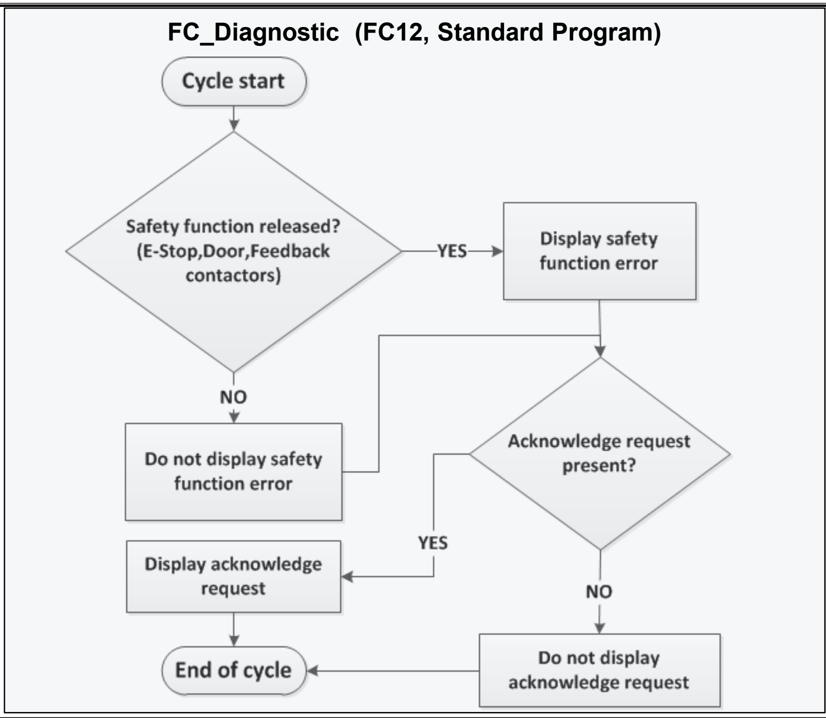
Currently, the user is informed via the Panel as soon as an F-module/channel has a problem and is passivated. The display is to be expanded with a status display of the safety functions. In addition, the user is also to receive a message as soon as an error of a safety function has gone and it can be acknowledged.

What to Do

1. Open the block "FC_Diagnostic" (FC12).

Continued on the next page

6.36.2. Re: Exercise 11: Flow Chart



2. Functionality "FC_Diagnostic":

The existing block is to be expanded with the status display of the safety functions. The block is to read-in the triggering of at least one safety function and display it on the Panel ("DB_OP_Outputs.FunctionError"). The trigger of a safety function can be implemented via the negated enable signal or an existing error bit.
In addition, the reintegration request (for example: "ESTOP.ACK_REQ") of every safety function is to be read-in and displayed on the Panel ("DB_OP_Outputs.AckRequired").

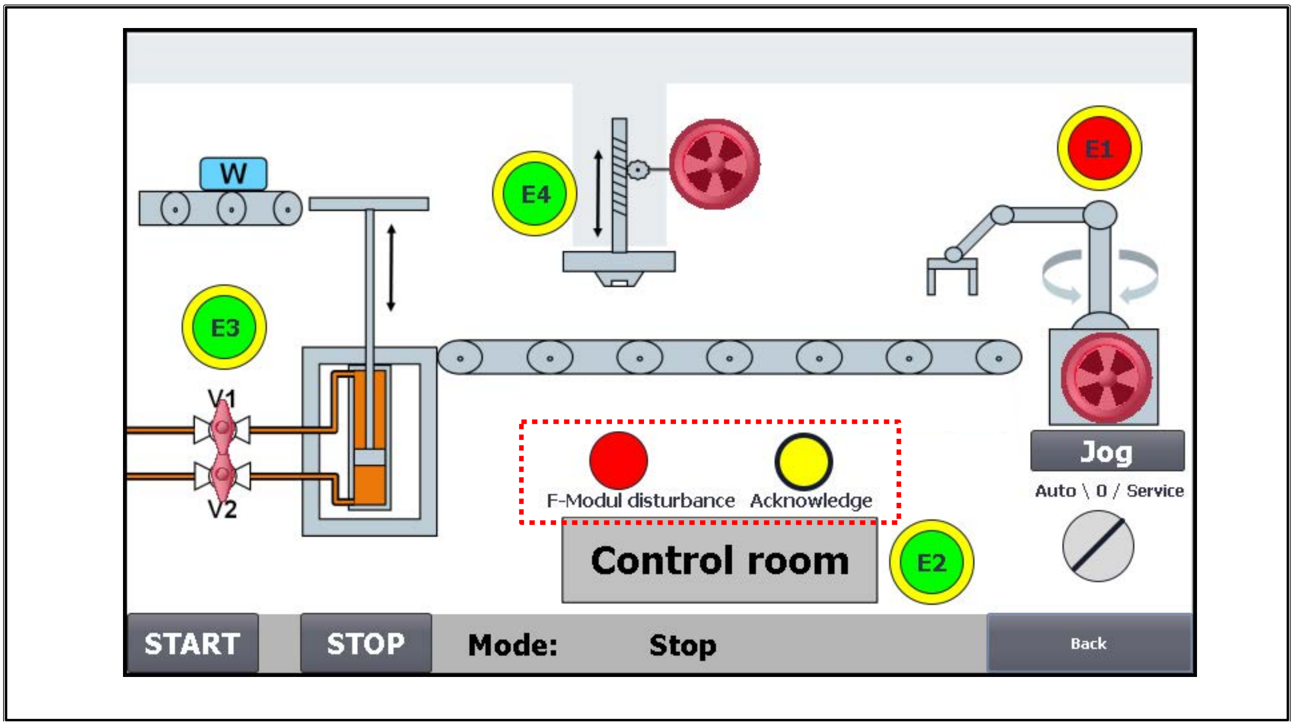
Note:
The explicit acknowledgement for each safety function should have already been implemented in the previous exercises.

3. Download all blocks into the CPU.

4. Save your project and test the functionality.

Relevant Interfaces		
Inputs	**Standard**	**Fail-safe**
	-	-
Outputs	**Standard**	**Fail-safe**
	-	-
Data blocks	**Global**	**System**
	"DB_OP_Outputs.FunctionError" (DB99)	
	"DB_OP_Outputs.AckRequired" (DB99)	

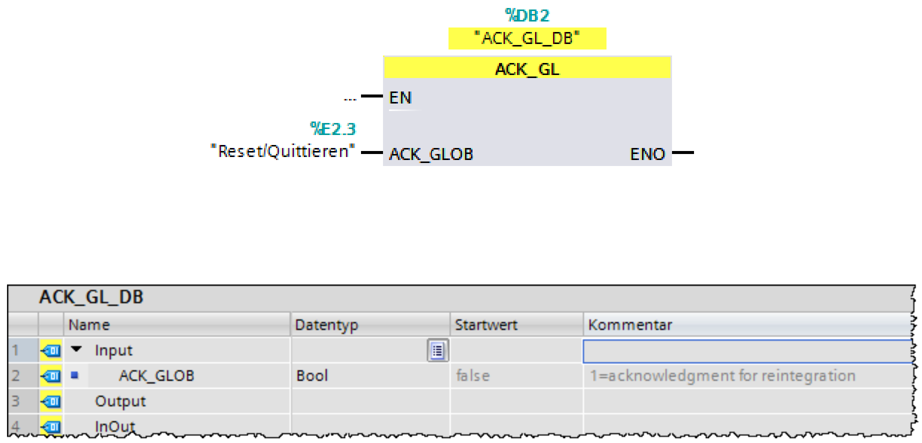
6.37. Exercise 12: Using the Safety Function "ACK_GL"



Task Description

Currently, the acknowledgement of all F-I/Os is implemented in the "FB_Reintegration" safety block through the direct control of the individual F-I/O DBs. You are to replace the current acknowledgement programming with the safety function "ACK_GL".

6.37.1. ACK_GL (FB187)

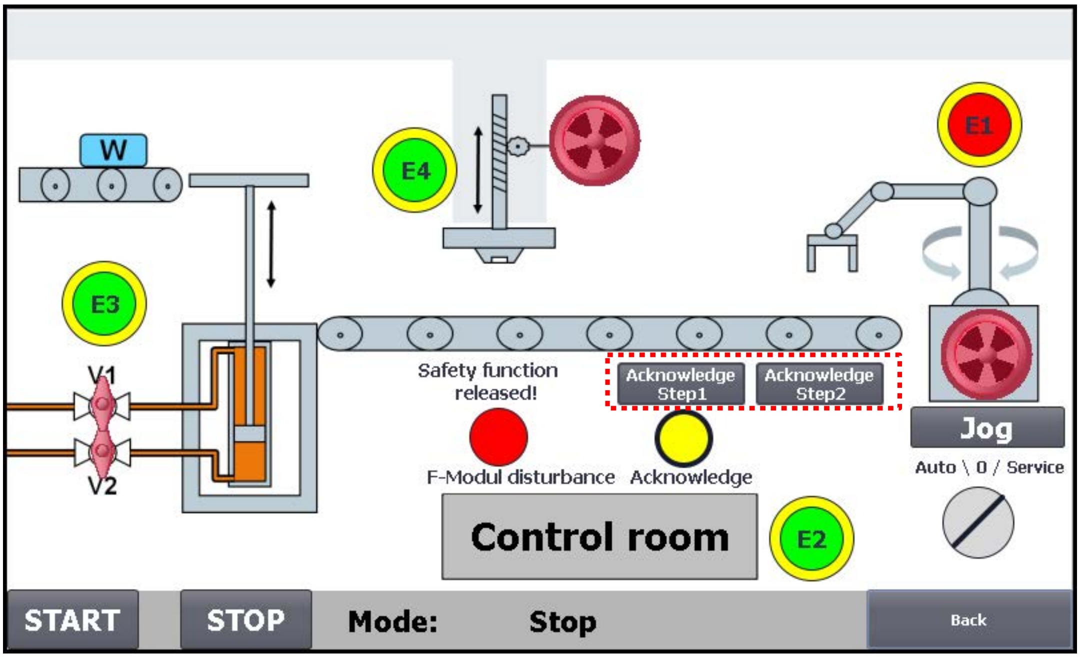


This instruction creates an acknowledgment for the simultaneous reintegration of all F-I/O or channels of the F-I/O of an F-runtime group after communication errors, F-I/O errors, or channel faults.

A user acknowledgment with a positive edge at input ACK_GLOB is required for reintegration. The acknowledgment occurs analogously to the user acknowledgment via the ACK_REI tag of the F-I/O DB, but it acts simultaneously on all F-I/O of the F-runtime group in which the instruction is called.

If you use the instruction ACK_GL, you do not have to provide a user acknowledgment for each F-I/O of the F-runtime group via the ACK_REI tag of the F-I/O DB.

6.38. Exercise 13 (Optional): Using the Safety Function "ACK_OP"



Task

Currently, the acknowledgement of an F-module error or a safety function is only possible via the acknowledgement button "S_Reset". You are to expand the Panel with a fail-safe acknowledgement. For this, use the safety function "ACK_OP".

Note: In the "DB_OP" data block, a tag "Ackfailsafe" of the type Integer is already created. This tag can be used for the safe acknowledgement.

Requirements:

- The acknowledgement on the Panel is to occur via 2 independent buttons
- The 1st. button is only to be visible when an acknowledgement request is pending
- The 2nd. button is only to be visible when the first acknowledgement step has been completed successfully (see Help "ACK_OP")
- Acknowledgement via the "S_Reset" button is still to be possible.

6.38.1. ACK_OP (FB187)

ACK_OP_DB

	Name	Datentyp	Startwert	Kommentar
1	▼ Input			
2	ACK_ID	Int	9	Identifier of acknowledgement (9 ... 30000)
3	▼ Output			
4	OUT	Bool	false	Output for acknowledgment
5	Q	Bool	false	Time status
6	▼ InOut			
7	IN	Int	0	Input variable from operator control and monitoring system
8	Static			

This instruction enables a fail-safe acknowledgment from an HMI system.

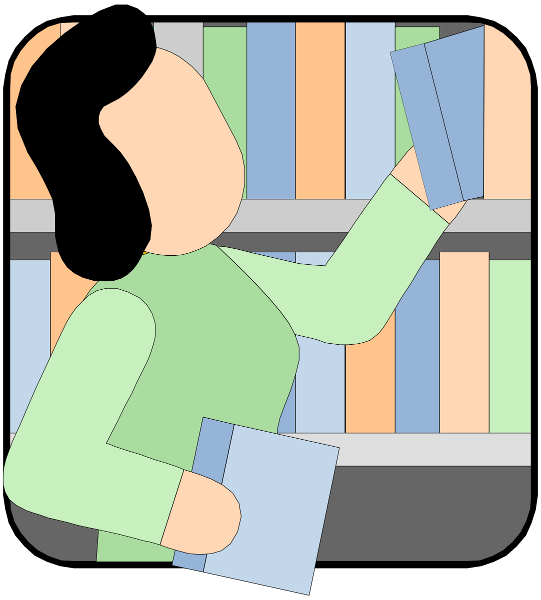
It allows, for example, reintegration of F-I/O to be controlled from the HMI system. Acknowledgment takes place in two steps:

- Input/output parameter IN changes to the value of 6 for exactly one cycle
- Input/output parameter IN changes to the value at the ACK_ID input within a minute for exactly one cycle

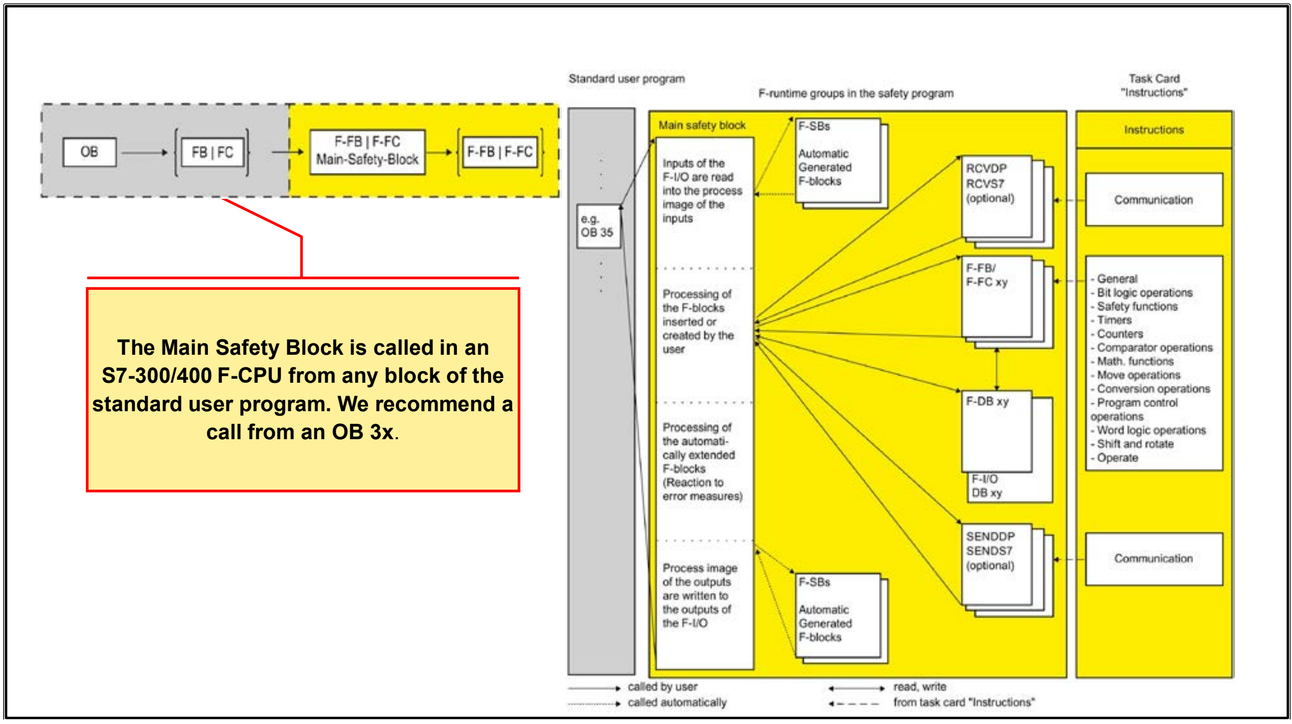
Once the in/out parameter IN has changed to the value of 6, the instruction evaluates whether this parameter has changed to the value at the ACK_ID input after 1 second, at the earliest, or one minute, at the latest. Output OUT (output for acknowledgment) is then set to 1 for one cycle.

If an invalid value is input or if in/out parameter IN has not changed to the value at the ACK_ID input within one minute or the change occurred before one second has elapsed, then in/out parameter IN is reset to 0, and both steps listed above must be repeated. During the time in which in/out parameter IN must change from 6 to the value at the ACK_ID input, output Q is set to 1. Otherwise, Q has a value of 0.

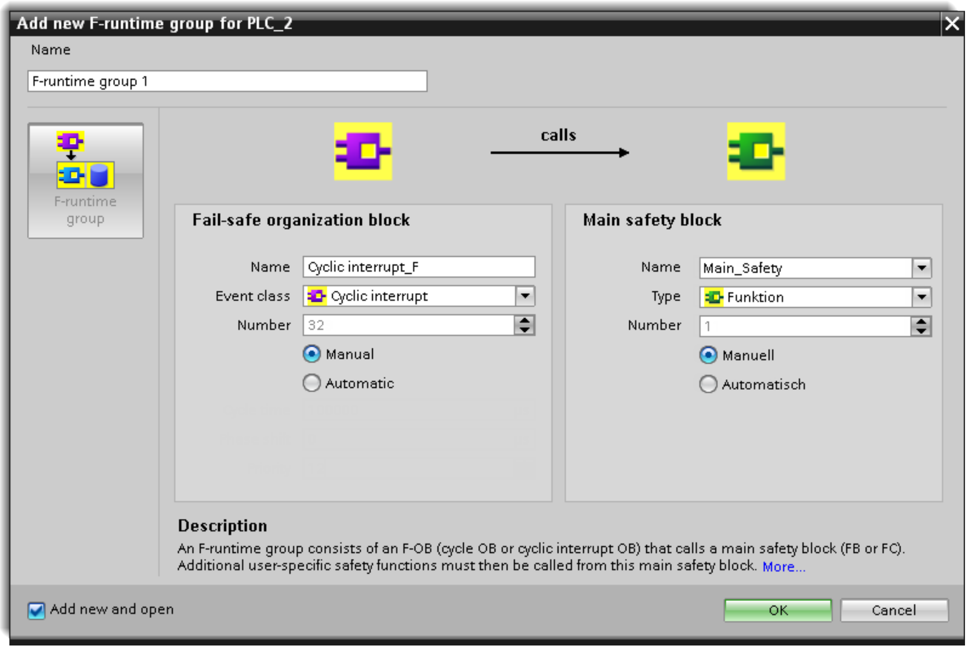
6.39. Additional Information



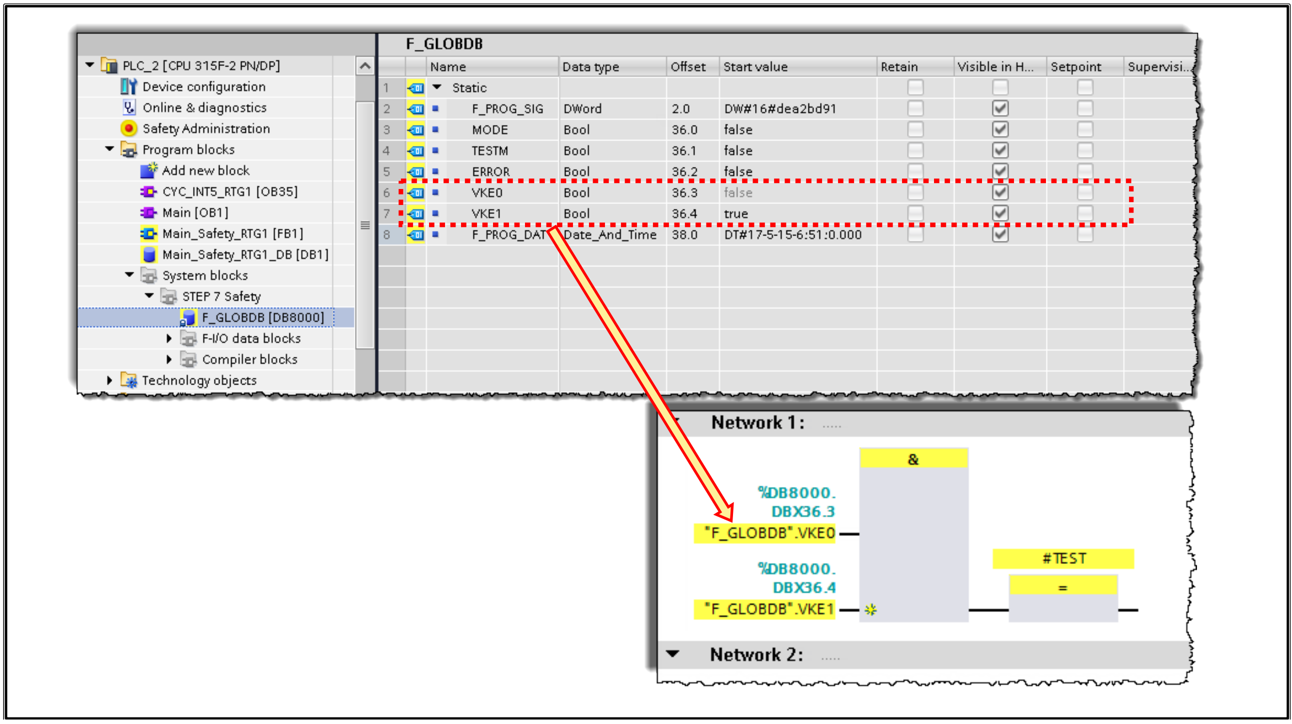
6.39.1. Structure and Execution of the Safety Program (300F/400F)



6.39.2. Runtime Group (300F/400F)



6.39.3. F_GLOBDB (300F/400F)



The F-shared DB (global) is a fail-safe data block that contains all of the shared data of the safety program and additional information needed by the F-system. The F-shared DB is automatically inserted when the hardware configuration is compiled.

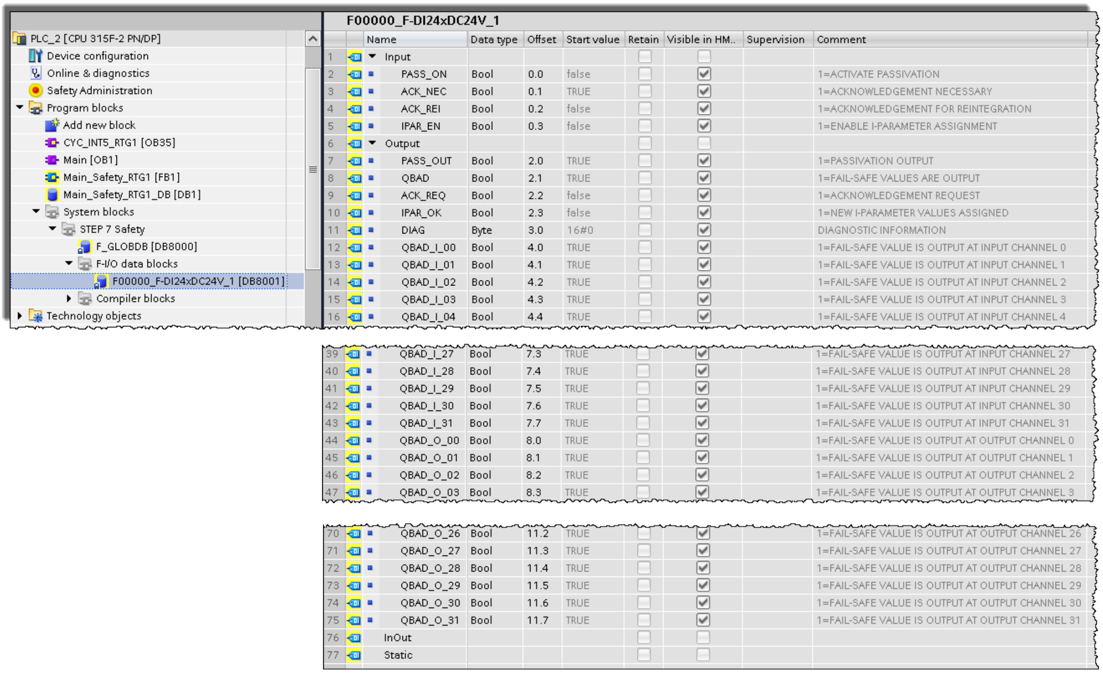
Using its name F_GLOBDB, you can evaluate certain data elements of the safety program in the standard user program.

You can read out the following information in the F-shared DB in the standard user program or on an operator control and monitoring system:

- The operating mode: safety mode or disabled safety mode ("MODE" tag)
- Error information "Error occurred when executing safety program" ("ERROR" tag)
- The collective F-signature ("F_PROG_SIG" tag)
- The compilation date of the safety program ("F_PROG_DAT" tag, Data type DATE_AND_TIME)

You use fully qualified access to access these tags (for example, "F_GLOBDB".MODE).

6.39.4. F-I/O DB Tags (300F/400F)



QBAD_I_xx and QBAD_O_xx display the validity of the channel value channel-specific and thus correspond to the inverted value status with S7-1200/1500. Value status or QBAD_I_xx and QBAD_O_xx are not available with fail-safe standard DP-slaves and fail-safe standard IO-devices without the "RIOforFA-Safety" profile.

6.39.5. F-I/O DB / Differences in the Evaluation (1)

Differences in the evaluation in S7-1500F and S7-300F/400F

Tag in the F-I/O DB or Value status in the PII	F-I/O with F-CPU S7-1500	F-I/O with F-CPU S7-300/400
ACK_NEC	✓	✓
QBAD	✓	✓
PASS_OUT	✓	✓
QBAD_I_xx *	✗	✓
QBAD_O_xx *	✗	✓
Value status	✓	✗

6.39.6. F-I/O DB / Differences in the Evaluation (2)

Differences in the evaluation in S7-1500F and S7-300F/400F

Scenario	Value status (S7-1500F)	Q_BAD (S7-300F/400F)
Valid values to F-I/O (no error)	✓	✗
Channel fault occurs	✗	✓
Channel fault is gone (ACK_REQ)	✗	✓
Error acknowledgement (ACK_REI)	✓	✗

Contents

7

7. TIA Safety: Response Times

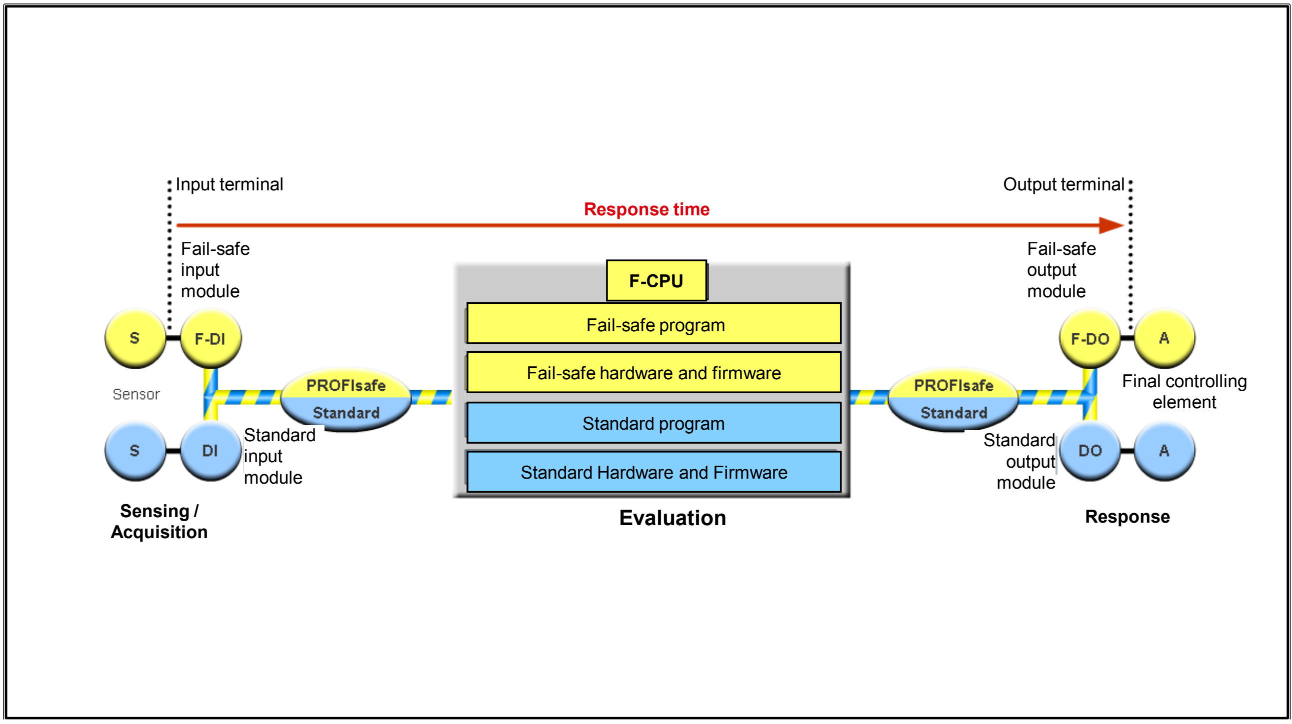
At the end of the chapter the participant will ...

… be able to explain which times make up the total response time

… be able to explain why the response time of a controller is safety-relevant

… be familiar with the S7Safety_RTT table and will be able to use it

7.1. Response Time of the F-System: Overview



Response Time

The response time is the period that elapses between the detection of an input signal and the change of a connected output signal. The safety clearances within danger zones depend mainly on the approach speed and the stopping time of the machine. For time-critical applications, an estimation of the response time of the fail-safe controller may be necessary for optimization of safety clearances. Ultimately, smaller safety clearances usually also mean smaller plant areas and with that reduced costs.

Fluctuation Range

The actual response time lies between the minimum and the maximum response time. You must always take the maximum response time into account in your system configuration.

Maximum Response Time

The maximum response time of the F-system is the "worst-case time" from acquisition of a safety-relevant signal from the safety-related input module up to the output of a signal to the safety-related output module.

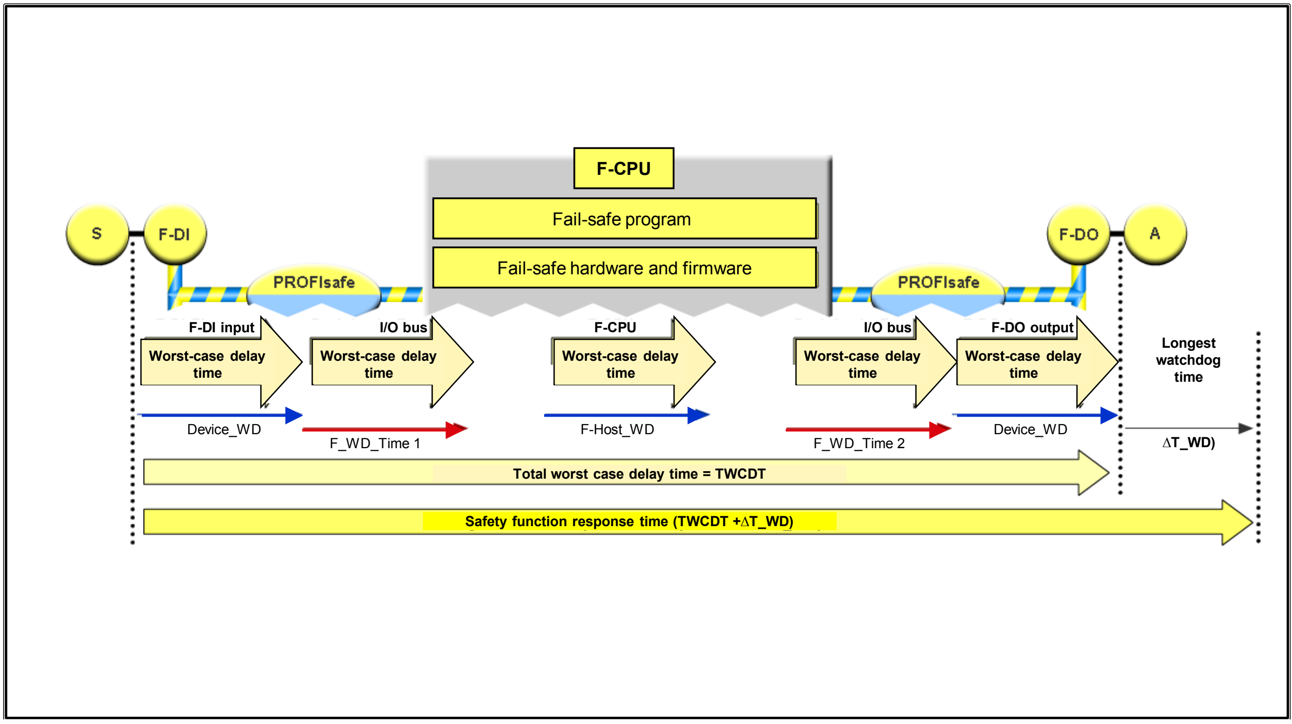
Standard Program

The F-CPU executes the standard program and the safety program independently of one another. The maximum possible (OB1) cycle time and thus the response time of the standard program is extended due to execution of the safety program. This depends on the size of the safety program and how often it must be executed by the CPU.

F-Program

The response time of the safety program, however, does not depend on the size or execution time of the standard program. Thus, the response time in the safety-related part of the system does not depend on the execution time of the standard program.

7.1.1. Response Time if there is No fault



Response Time of the Safety Function

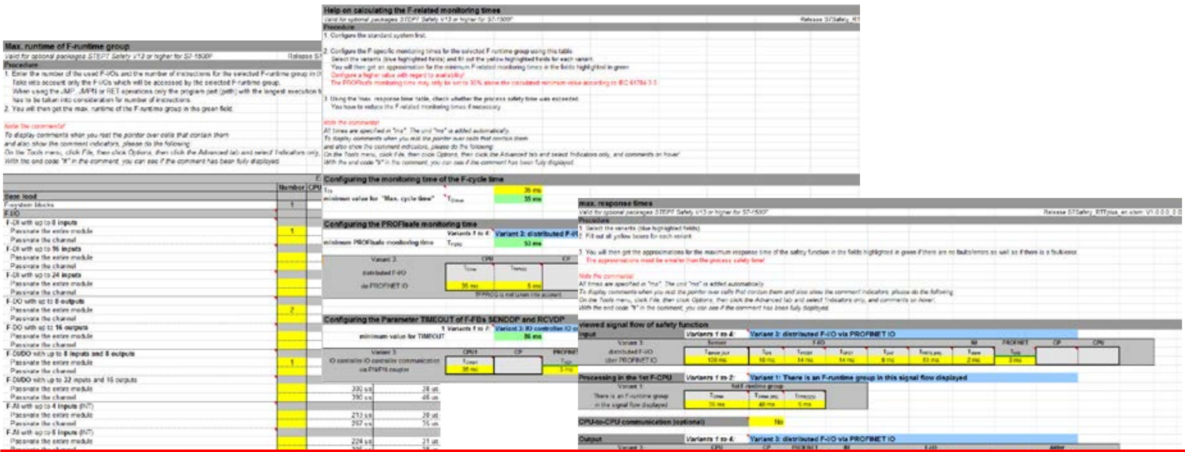
The time TWCDT + ΔT_WD shown in the picture correspond to the "Safety function response time". The time "ΔT_WD" takes into account the signal delays at the interchange points that may cause the signal to be forwarded only in the next cycle (worst-case consideration).

The "(max.) Safety function response time" is composed of the following …

- Maximum acknowledgment time of the F I/O (Device_WD)
- Execution of the F program (F-Host_WD)
  (call interval and runtime of the runtime group)
- Maximum target rotation time of the PROFIBUS DP master system or the maximum update time of PROFINET IO systems (F_WD_Time 1/2)

7.2. S7Safety_RTT

As a support, the Excel file is available on the internet
http://support.automation.siemens.com/WW/view/de/49368678/133100
with which you can approximately calculate the runtimes of the F-runtime groups, the F-specific minimum monitoring times and the maximum response times of your F-System.



Provision must still be made for measurement of the actual values in the ‘real’ system, taking into consideration all actuators, sensors and possible conditions. The S7Safety_RTTplus*.xls is not legally binding and must not replace a system acceptance or be included in its documentation.

S7Safety_RTT

SIEMENS AG provides the Excel sheet "S7Safety_RTT" as a free download with which, in addition to the "(max.) Safety function response time ", the "F-monitoring times" can also be calculated for configuration and programming.

7.2.1. Max. Runtime of the F-Runtime Group (1)

Basic instructions			
General			
-o| (Invert power flow)		0,45 us	0,04 us
Bit logic operations			
FUP: & , >=1; KOP: parallel connection, series connection per Operand	70	1,4 us	0,1 us
X per Operand		1,6 us	0,1 us
=	10	0,14 us	0,01 us
R, S		2,0 us	0,2 us
SR, RS	50	3,1 us	0,3 us
P_TRIG, N_TRIG	10	2,0 us	0,2 us
Safety function			
ESTOP1	4	59 us	5,4 us
TWO_H_EN	1	55 us	5,1 us
MUT_P		199 us	18 us
EV1oo2DI		59 us	5,4 us
FDBACK	2	64 us	5,9 us
SFDOOR	1	41 us	3,7 us
ACK_GL		5,6 us	0,5 us
Timer operation, IEC timers			
TP		60 us	5,5 us
TON		62 us	5,7 us
TOF		63 us	5,8 us
Counter operation, IEC counters			
CTU		35 us	3,2 us
CTD		36 us	3,3 us
CTUD		62 us	5,7 us
Comparator operations			
CMP ==, <>		3,8 us	0,4 us
CMP > , < , >= , <=		2,5 us	0,2 us
Math functions			
ADD		1,2 us	0,11 us
SUB		1,7 us	0,2 us
MUL		2,6 us	0,2 us
DIV		6,8 us	0,6 us
NEG		1,4 us	0,1 us
Move operations			
MOVE	2	0,2 us	0,02 us
Conversion operations			
CONVERT INT-->DINT		1,0 us	0,1 us
BO_W		21 us	2,0 us
W_BO		27 us	2,5 us
SCALE		50 us	4,6 us

SIMATIC STEP 7 Safety V14 Reaction Time Table SIMATIC S7-1500F

The S7Safety Reaction Time Table (S7Safety_RTTplus*.xls) is used for theoretical estimation of F-execution times, F-runtimes, F- monitoring times and F-response times in conjunction with the SIMATIC S7-1500 F-CPU during system layout. The execution times of the F-application blocks, the F-FBD/F-LAD elements and the runtime of the F-runtime group were determined based on SIMATIC STEP 7 Safety Advanced V14. Provision must still be made for measurement of the actual values in the real system, taking into consideration all actuators, sensors and possible conditions. The S7Safety_RTTplus*.xls is not legally binding and must not replace system acceptance testing or be incorporated in the system's documentation.

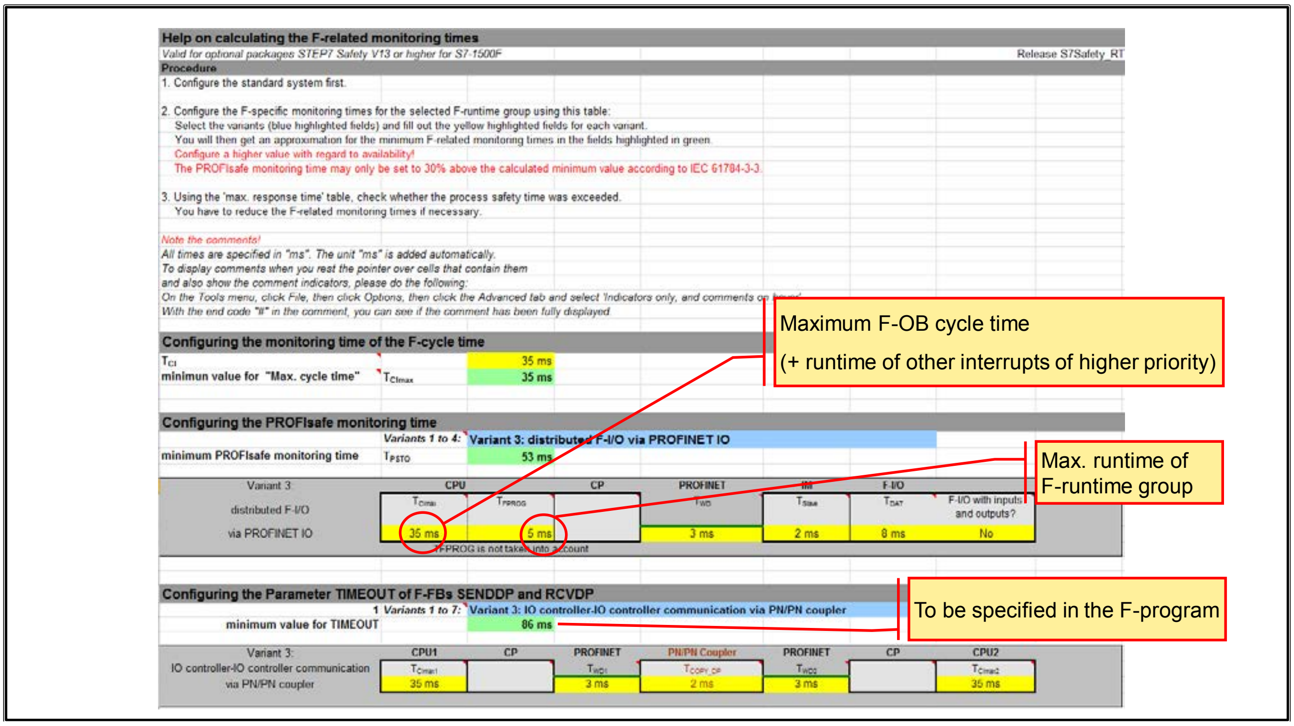
7.2.2. Max. Runtime of the F-Runtime Group (2)

Program control operations			
JMP, JMPN, RET		7,9 us	0,7 us
Word logic operations			
AND, OR, XOR		3,2 us	0,3 us
Shift and rotate			
SHR		16 us	1,5 us
SHL		19 us	1,7 us
Operate			
ACK_OP		42 us	3,8 us
Communication			
PROFIBUS / PROFINET			
SENDDP	1	143 us	23 us
RCVDP	1	172 us	26 us
F-FBs/F-FCs from another F-library or instructions from another optional package			
Total of the execution times	1	0 us	0 us
Block calls			
CALL F-FB / F-FC	3	1,9 us	0,2 us
Input parameter		0,2 us	0,02 us
Output parameter		0,1 us	0,01 us
IN_OUT parameter		0,3 us	0,03 us
Static local data		0,1 us	0,01 us
Data type conversion at divergent data type			
The number of parameters of the data type INT or WORD that are interconnected an operand with a different data type (WORD instead of INT or INT instead of WORD).		1,9 us	0,2 us
max. runtime of F-runtime group		**4 ms**	**1 ms**

Conditions for the Runtime Specifications

The "max. runtime of F-runtime group" can be extended due to, among other things, the communication load (e.g. S7 communication, PROFINET IO communication, PG/OP communication), the processing of higher-priority interrupts and the testing and commissioning functions.
You can determine the effect of these factors based on the documentation and configuration of the standard system and add it to the value calculated up to now.

7.2.3. Min. F-Monitoring Times



Parameter "F-Monitoring Time"

You have two options for configuring the monitoring time of the safety-related communication between the F-CPU and F-I/O:

- Centrally in the Hardware and Network editor when assigning the F-CPU parameters, in the Properties of the F-CPU or
- when assigning the F-I/O parameters in the Hardware and Network editor; in the Properties of the F-I/O

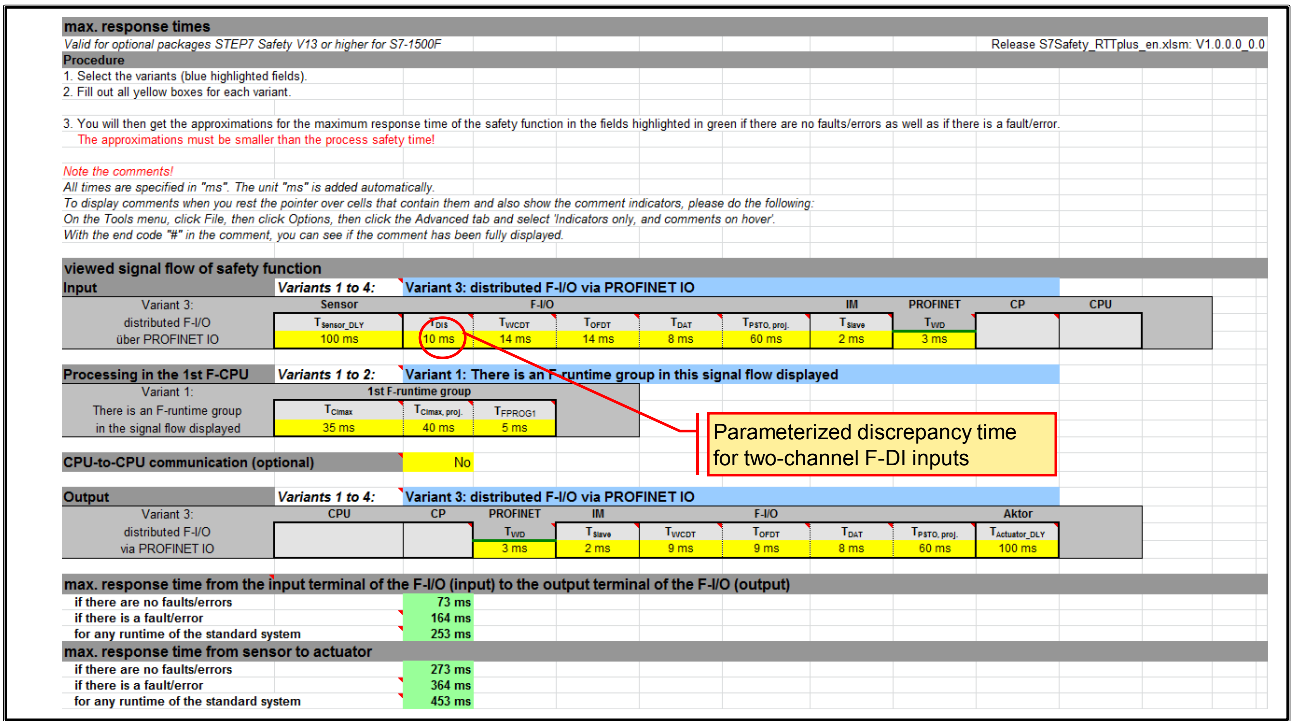
"F-Monitoring Time" = PROFIsafe Monitoring Time TPSTO

The PROFIsafe monitoring time TPSTO must be specified high enough to prevent the monitoring function from being triggered when no faults are present.

Parameter TIMEOUT to SENDDP and RCVDP

The time monitoring is performed in the SENDDP and RCVDP instructions of the communication partner. You must assign the time monitoring with identical monitoring time for both instructions at the TIMEOUT parameter. The TIMEOUT monitoring time must be specified high enough to prevent the monitoring function from being triggered when no faults are present.

7.2.4. Max. Response Times


max. response times
Valid for optional packages STEP7 Safety V13 or higher for S7-1500F
Release S7Safety_RTTplus_en.xlsm: V1.0.0.0_0.0
Procedure
1. Select the variants (blue highlighted fields).
2. Fill out all yellow boxes for each variant.
3. You will then get the approximations for the maximum response time of the safety function in the fields highlighted in green if there are no faults/errors as well as if there is a fault/error.
The approximations must be smaller than the process safety time!
Note the comments!
All times are specified in "ms". The unit "ms" is added automatically.
To display comments when you rest the pointer over cells that contain them and also show the comment indicators, please do the following:
On the Tools menu, click File, then click Options, then click the Advanced tab and select 'Indicators only, and comments on hover'.
With the end code "#" in the comment, you can see if the comment has been fully displayed.
viewed signal flow of safety function
Input | Variants 1 to 4: | Variant 3: distributed F-I/O via PROFINET IO
Variant 3: distributed F-I/O über PROFINET IO
Sensor: T_{Sensor_DLY} 100 ms
F-I/O: T_{DIS} 10 ms | T_{WCDT} 14 ms | T_{OFDT} 14 ms | T_{DAT} 8 ms | $T_{PSTO,proj.}$ 60 ms
IM: T_{Slave} 2 ms
PROFINET: T_{WD} 3 ms
CP | CPU
Processing in the 1st F-CPU | Variants 1 to 2: | Variant 1: There is an F-runtime group in this signal flow displayed
Variant 1: There is an F-runtime group in the signal flow displayed
1st F-runtime group: T_{CImax} 35 ms | $T_{CImax,proj.}$ 40 ms | T_{FPROG1} 5 ms
Parameterized discrepancy time for two-channel F-DI inputs
CPU-to-CPU communication (optional) | No
Output | Variants 1 to 4: | Variant 3: distributed F-I/O via PROFINET IO
Variant 3: distributed F-I/O via PROFINET IO
CPU | CP
PROFINET: T_{WD} 3 ms
IM: T_{Slave} 2 ms
F-I/O: T_{WCDT} 9 ms | T_{OFDT} 9 ms | T_{DAT} 8 ms | $T_{PSTO,proj.}$ 60 ms
Aktor: $T_{Actuator\_DLY}$ 100 ms
max. response time from the input terminal of the F-I/O (input) to the output terminal of the F-I/O (output)
if there are no faults/errors | 73 ms
if there is a fault/error | 164 ms
for any runtime of the standard system | 253 ms
max. response time from sensor to actuator
if there are no faults/errors | 273 ms
if there is a fault/error | 364 ms
for any runtime of the standard system | 453 ms

Maximum Response Times

The maximum response time of the F-system is the "worst-case time" from acquisition of a safety-relevant signal from the safety-related input module up to the output of a signal at the safety-related output module.

Rule for the Maximum Response Time of a Safety Function

The maximum response time of a safety function must be less than the fault tolerance time of the process.

"Response Time if there are No Faults/Errors"

This is the time that must be used for the practical design. The following measures are suitable for optimizing the response times:

- Shorten the call interval of the runtime group
- Faster bus transmission (e.g. increase the baud rate of the PROFIBUS)
- Use of module-wide passivation
- Time-optimized parameter assignment of the F-DI modules (e.g. optimize discrepancy time if appropriate for the safety function)
- Use faster F-CPUs

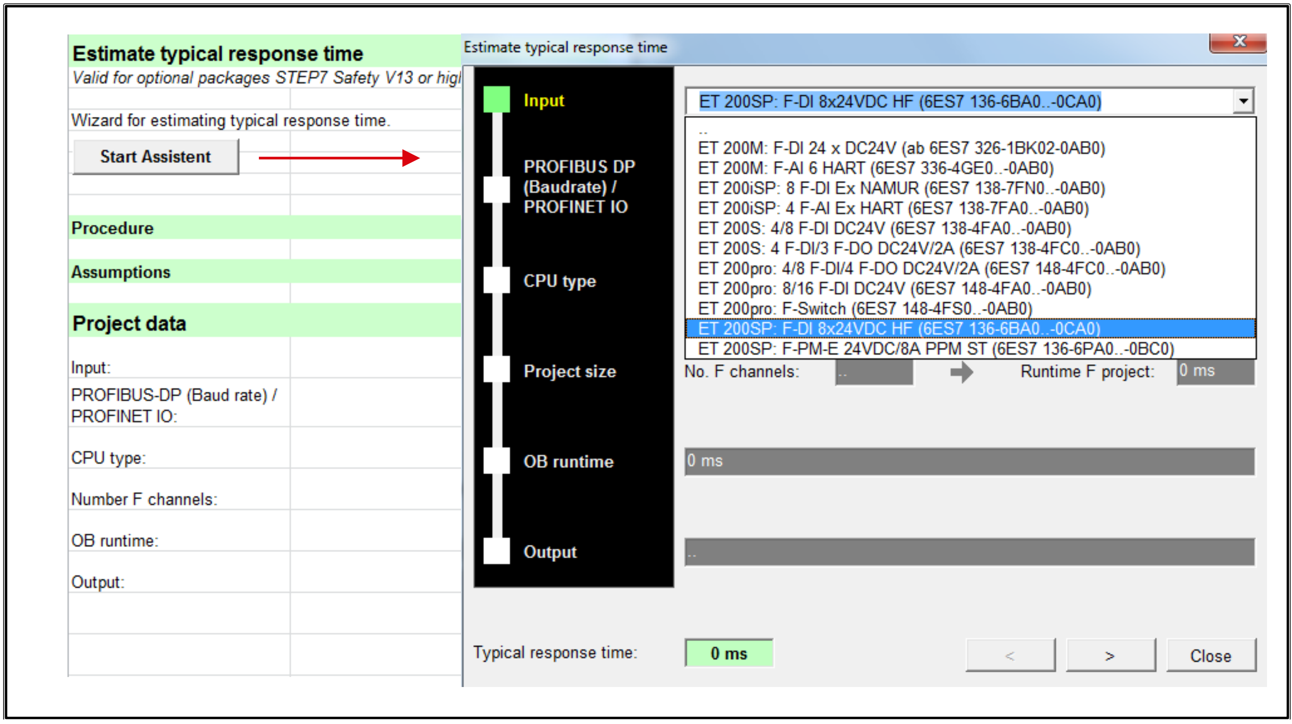
"...if there is a Fault/Error"

This time is only relevant for multiple error considerations in accordance with IEC61508.

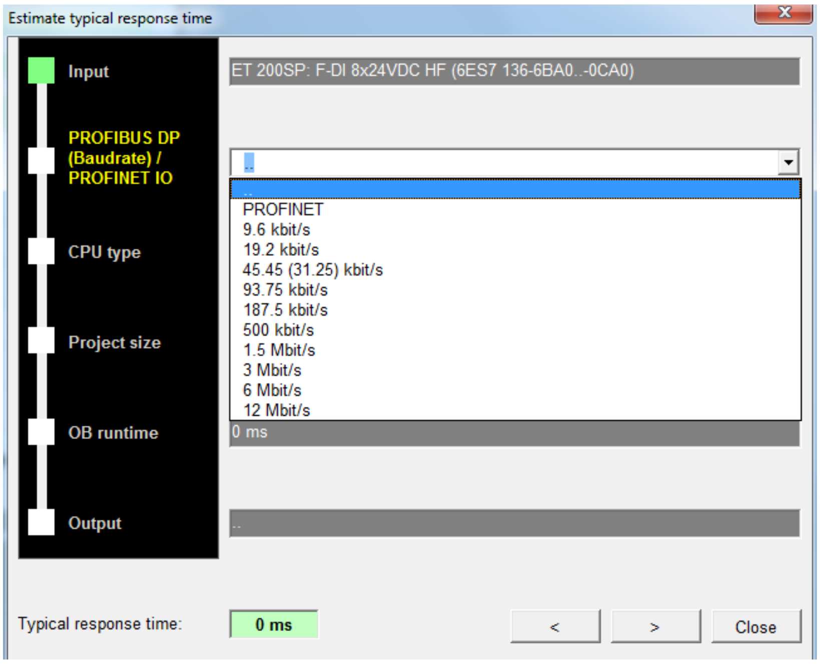
...for any Runtime of the Standard System

This time is only relevant if the F-runtime group is called from lower-priority OBs (for example, OB1) and so can be interrupted by higher priority OBs (for example, F-OB).

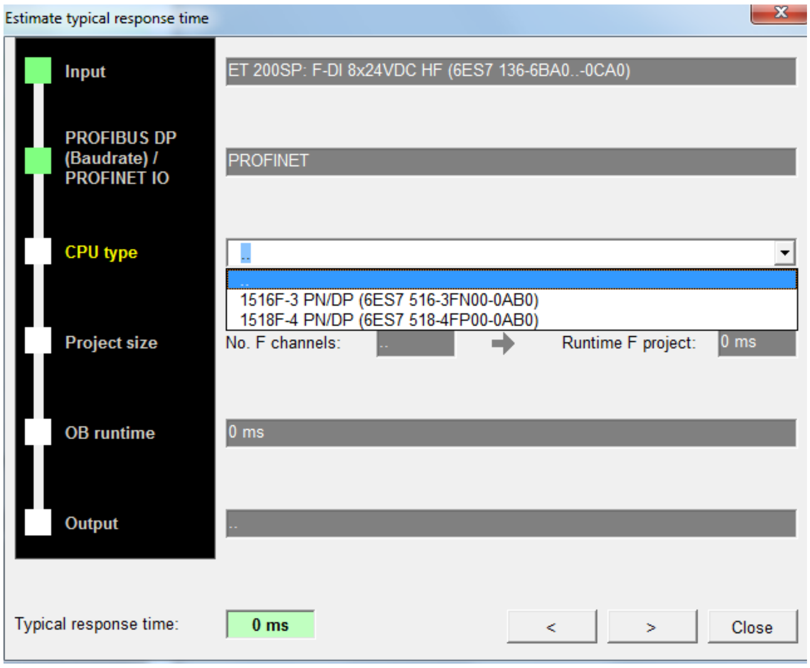
7.2.5. Typical Response Times (1)



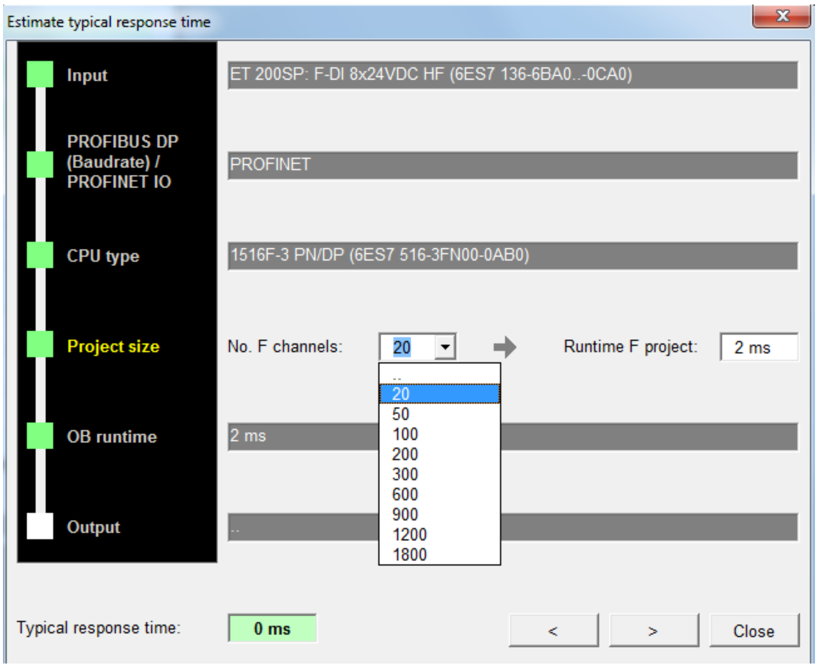
7.2.6. Typical Response Times (2)



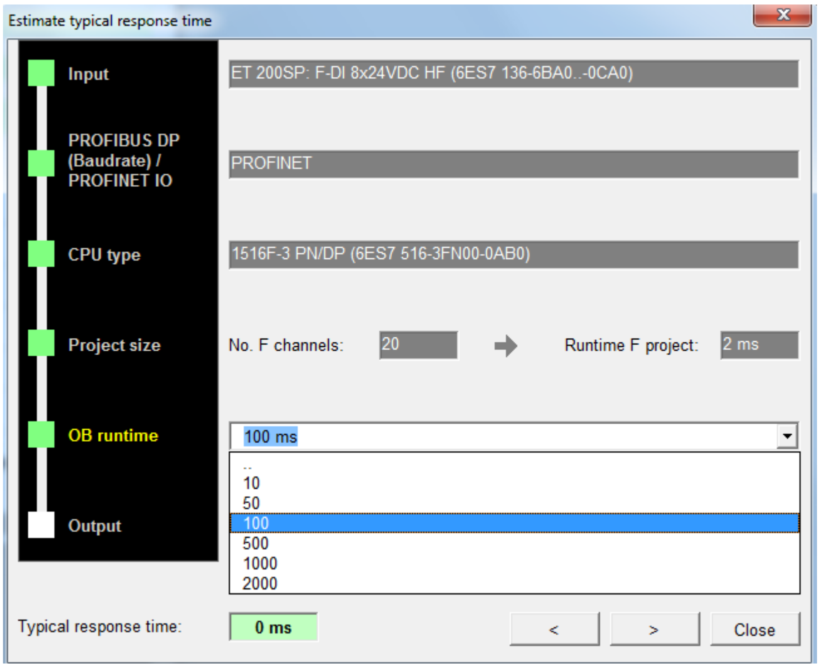
7.2.7. Typical Response Times (3)



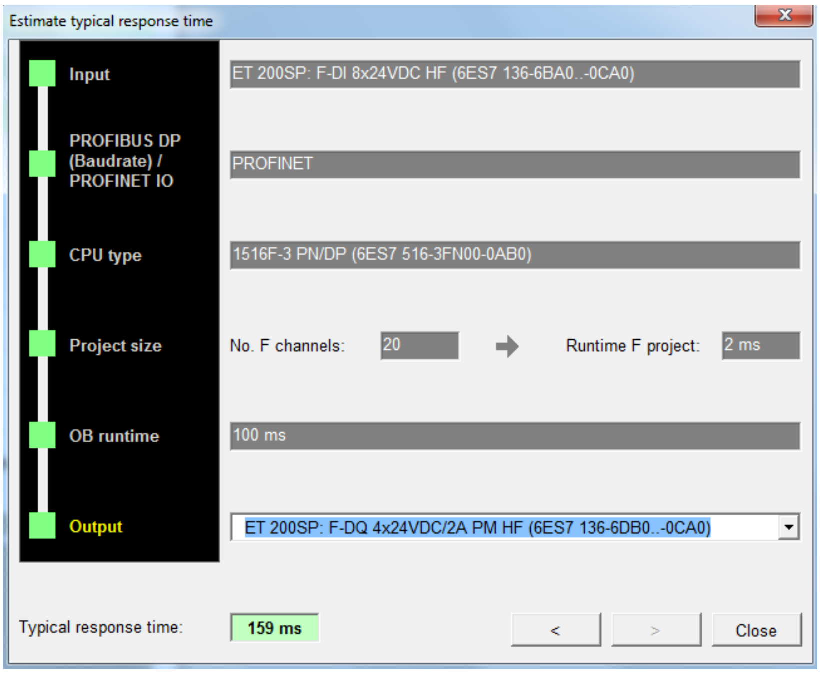
7.2.8. Typical Response Times (4)



7.2.9. Typical Response Times (5)



7.2.10. Typical Response Times (6)



7.2.11. Typical Response Times / Result

Estimate typical response time

Valid for optional packages STEP7 Safety V13 or higher Release S7Safety_RTTplus_en.xlsm: V1.0.0.0_0.0

Wizard for estimating typical response time.

Start Assistent

Procedure

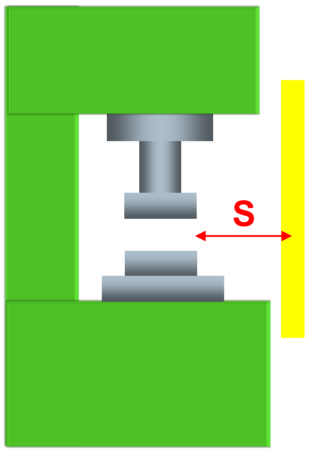
Assumptions

Project data

Input:	ET 200SP: F-DI 8x24VDC HF (6ES7 136-6BA0..-0CA0)
PROFIBUS-DP (Baud rate) / PROFINET IO:	PROFINET
CPU type:	1516F-3 PN/DP (6ES7 516-3FN00-0AB0)
Number F channels:	20
OB runtime:	100 ms
Output:	ET 200SP: F-DQ 4x24VDC/2A PM HF (6ES7 136-6DB0..-0CA0)

Typical response time: **159 ms**

7.3. Response Time and Safety Distance according to ISO 13855



General Formula:

$$S = K \times T + C$$

For right-angled approach

S	**= Minimum safety distance in mm**
K	**= 2 mm/ms Approach speed**
T	**= t1 + t2 + t3 in ms**
	t1: Response time of the AOPD
	t2: Response time of the safety interface
	t3: Stopping time of the machine
C	**= 8 x (d - 14) in mm**
d	**= Resolution of the AOPD (range 14 to 40 mm)**

Minimum Distances and Positions of the Components

Optical protective devices can only perform their protective effect/function if they are installed with a sufficient safety distance. The calculation formulas for the safety distance depend on the type of safeguard. The harmonized standard ISO 13855 "Positioning of protective equipment with respect to the approach speeds of parts of the human body" (formerly EN 999 describes installation situations and calculation formulas for the safety distances for the aforementioned types of safeguards.

The safety distances within danger zones depend mainly on the approach speed and the stopping time of the machine.

For time-critical applications, an estimation of the response time of the fail-safe controller may be necessary for optimization of safety distances (see formula in the picture: t2, Response time of the safety interface).

Definition of Process Safety Time (Fault Tolerance Time)

The process safety time is the time interval during which the process can be left on its own without risk to life and limb of the operating personnel or risk of damage to the environment. Within the process safety time, any type of F-system process control is tolerated. That is, during this time, the F-system can control its process incorrectly or it can even exercise no control at all. The process safety time depends on the process type and must be determined on a case-by-case basis.

Contents

8

8. Acceptance Test of a System

8.1. Legal Basis: Machinery Directive

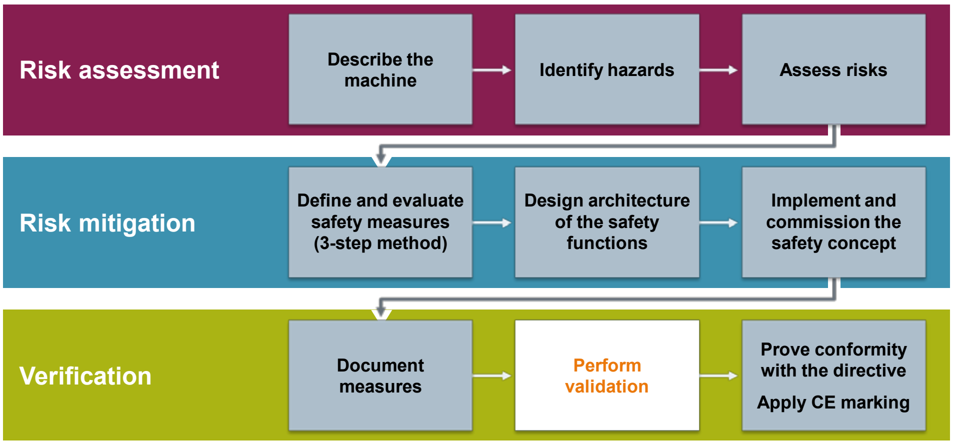
DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of May 17, 2006 on machinery, and amending Directive 95/16/EC (revised version)

(19) In view of the nature of the risks involved in the use of machinery covered by this Directive, **procedures for assessing conformity to the essential health and safety requirements should be established.** These procedures should be devised in the light of the extent of the danger inherent in such machinery. Consequently, each category of machinery should have its appropriate procedure in conformity with Council Decision 93/465/EEC of 22 July 1993 concerning the modules for the various phases of the conformity assessment procedures and the rules for the affixing and use of the CE conformity marking, which are intended to be used in the technical harmonization directives (2), taking account of the nature of the verification required for such machinery.

Acceptance Test of a System

During a system acceptance test, all the standards and guidelines relevant to the specific application must be complied with. This also applies to systems that are not "subject to acceptance". For the acceptance, you must consider the requirements in the Certification Report. As a general rule, the acceptance of an F-System is performed by an independent expert.

8.2. The Route to a Safe Machine According to the Machinery Directive



Validation is a phase in the process model for the development of a safe machine. The validation, therefore, applies to the entire machine. This phase includes validation of the safety system.

8.3. What is Validation?

According to EN ISO 13849-2 (2012 edition) and EN 62061, validation is a confirmation by examination of a safety-related system according to the following aspects:

- Are the requirements of the **safety requirements specification (SRS)** correctly and effectively implemented?
- Are the **safety functions for the machine** correctly implemented?
- Does the implementation meet the required **safety quality**?

Aim of Validation

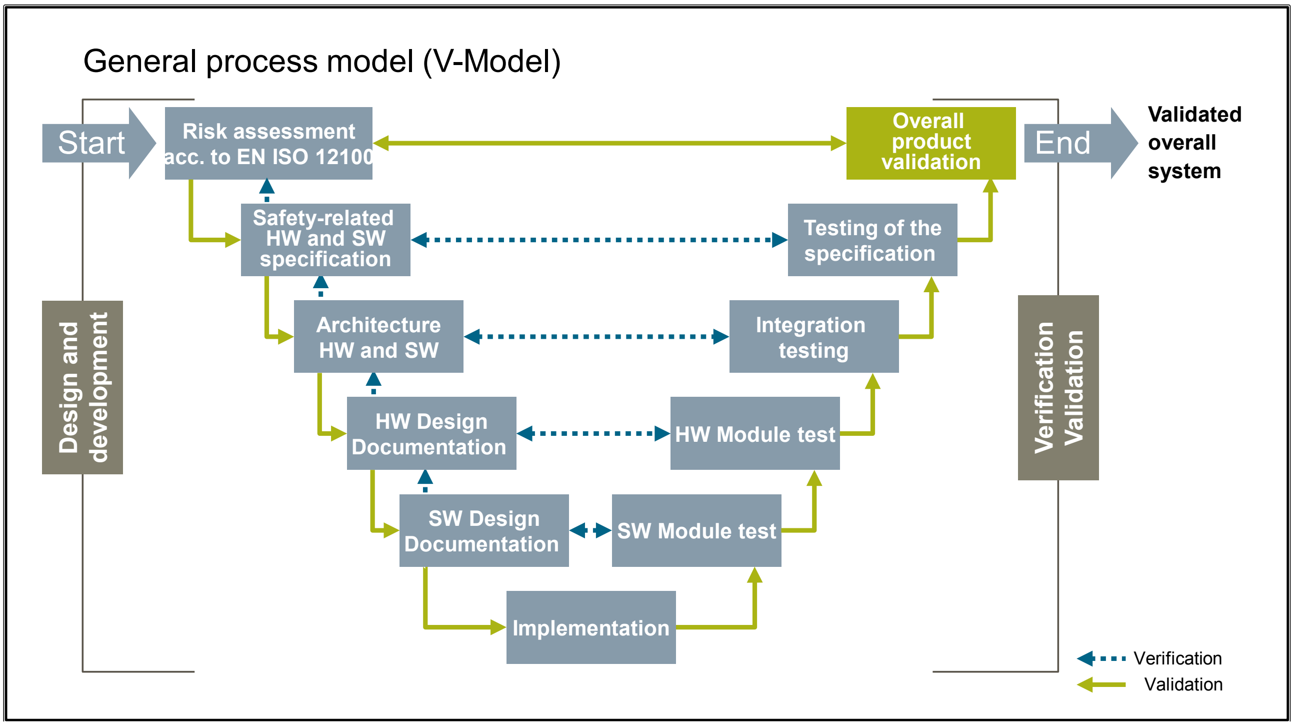
The aim of validation is to verify that the implemented safety functions make the required contribution to risk mitigation so that the machine becomes and remains safe.

Risk mitigation is achieved by the safety functions as well as other measures (design, technical, organizational).

SRS stands for Safety Requirements Specification

Moreover, IEC 51508-2 (Annex B) and IEC 61508-3 (Annex A) each describe techniques and measures for avoiding systematic failures. Compliance with them increases the quality of the safety function and aids successful validation.

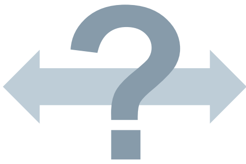
8.4. Position of the Overall Validation (Acceptance Tests) in the Process Model



The V-model shown is the generic model for the development and release of a safety system.

8.5. Verification < > Validation

Analogous definition of verification and validation from EN 62061:



Verification

Confirmation by examination (**for example, tests, analyses**) that the safety-related system and the parts of the safety-related system meet the requirements of the **respective (associated) specification**.

Blue dashed line, activities in the V-model (checking of individual phases for **correct implementation**)

Validation

Confirmation by examination (**for example, tests, analyses**) that the safety-related system meets the requirement for functional safety for the **respective application**.

Green unbroken line, activities in the V-model (checking the **suitability of the application**)

Verification:

From the Latin **Veritas**:
proving the **truth**

Validation:

From the Latin **Validus**:
checking **effectiveness**

8.6. Validation Measures before the Overall Product Validation

What do you have to validate?

1. **Specification of the safety functions**
   -> for example, Review of the specification
2. **Implementation concept, architecture and reliability**
   -> for example, SET (Safety Evaluation Tool)
3. **Hardware implementation**
   -> Analysis of circuit diagram and cabling/HW configuration
4. **Software implementation**
   -> Review Software documentation and flow charts
5. **Overall application (Acceptance test)**

8.7. Validation of the Overall Application

What do you have to validate?

1. Implementation and functionality of the safety functions
2. Robustness of implementation of the safety functions when faults occur

Aim of validation:

The aim is to prove that the safety functions have been implemented correctly according to the requirements and that the (application) software supports the execution of the safety functions and that the planned measures for error prevention have been effectively implemented.

How to validate:

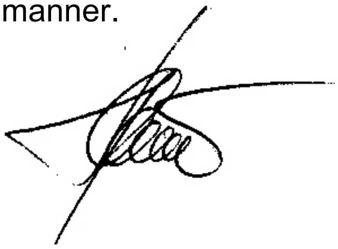
Perform a functional test of the safety functions by means of a black-box test. Perform selected fault simulations (fault seeding tests) based on the results of the analyses performed.

Before performing the functional tests, you must check that the correct configuration in the safety device (MSS) is active. This is done by checking the displayed checksum of the configuration.

8.8. Authorized Persons and Acceptance Report

The test for each SI function must be conducted, **recorded in the acceptance report and signed** by a person authorized to do this. The acceptance report must be kept in a machine logbook.

In this context, an authorized person is **a person who is authorized by the machine manufacturer** and who has suitable professional training and knowledge of the safety functions to conduct the acceptance test in a proficient manner.



Note

The guidelines and specifications for commissioning must be observed for this.
If parameters of SI functions are changed, the acceptance test must be conducted again and documented in the acceptance report.

Authorized Person

An authorized person can, therefore, also be an employee of another company commissioned to perform the test, if the requirements described above are met. In a practical sense, this means, for example, that a SIEMENS service technician can be involved in carrying out the acceptance test for an OEM and even provide his/her signature on the acceptance report. In addition, however, a responsible employee of the machine manufacturer must always confirm the correctness of the acceptance report. As a rule, this is the assigned safety officer of the company.

8.9. Contents of a Complete Acceptance Test

1. Documentation
- (1) Machine description and overview image
- (2) SI functions in the PLC program / printout
- (3) Description of the safety equipment

2. Function test with check of each individual SI function used
- (1) For example, safety door monitoring
- (2) For example, Emergency Off function

3. Report completion – Documentation of commissioning and signatures from parties involved
- (1) Check of program printouts
- (2) Recording of checksums
- (3) Proof of data backups
- (4) Signatures

4. Appendix – Measurement recordings of function tests

Contents of an Acceptance Test

The complete acceptance of a machine also includes corresponding documentation on the safety-relevant mechanical components, controllers, structures, process description, etc. Furthermore, particularly strict provisions apply to machines and systems that are subject to FDA conformity requirements.

8.10. Safety Summary

The safety summary generates a documentation of the safety program and provides support for the acceptance test of the system!

The safety summary includes:

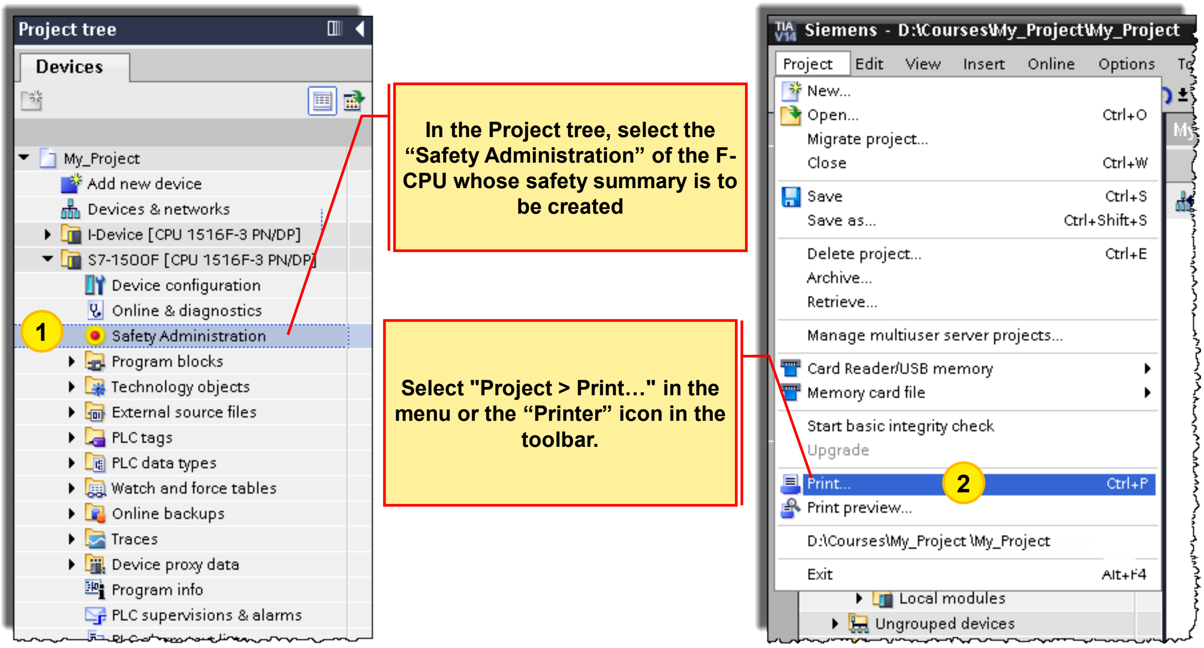
- General information on the **program identification**, such as,
  - Software versions used
  - Collective F-signature and time stamp of generation
- Information on the **hardware**, such as,
  - F-CPU with which firmware version
  - F-I/Os used and their parameter assignments
- Information on the **safety program**, such as,
  - User program blocks with offline signature
  - Library blocks used with offline signature

Safety Summary

You can print out all important project data of the hardware configuration of the F-I/O and the safety program. As a result, you receive a "safety summary" that serves not only as documentation but also as a basis for checking for correctness of the individual components of the system. The correctness is a requirement for acceptance of the system. The declaration of the collective F-signature in the footer of the printout pages guarantees a clear assignment of the printout to a safety program.

8.10.1. Creating a Safety Summary

Procedure for creating a safety summary (printout)

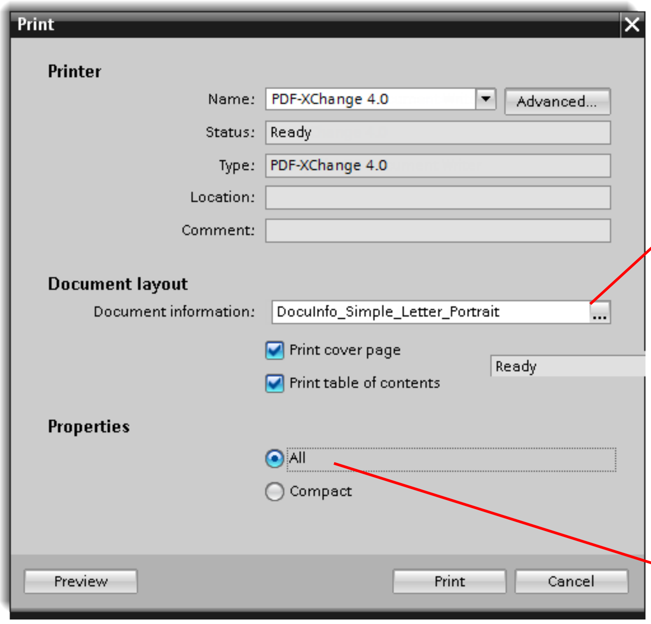


Safety Summary (Printout)

The safety summary is the project documentation which supports you for the acceptance test of the system.

8.10.2. Procedure for Creating a Safety Summary (Printout)

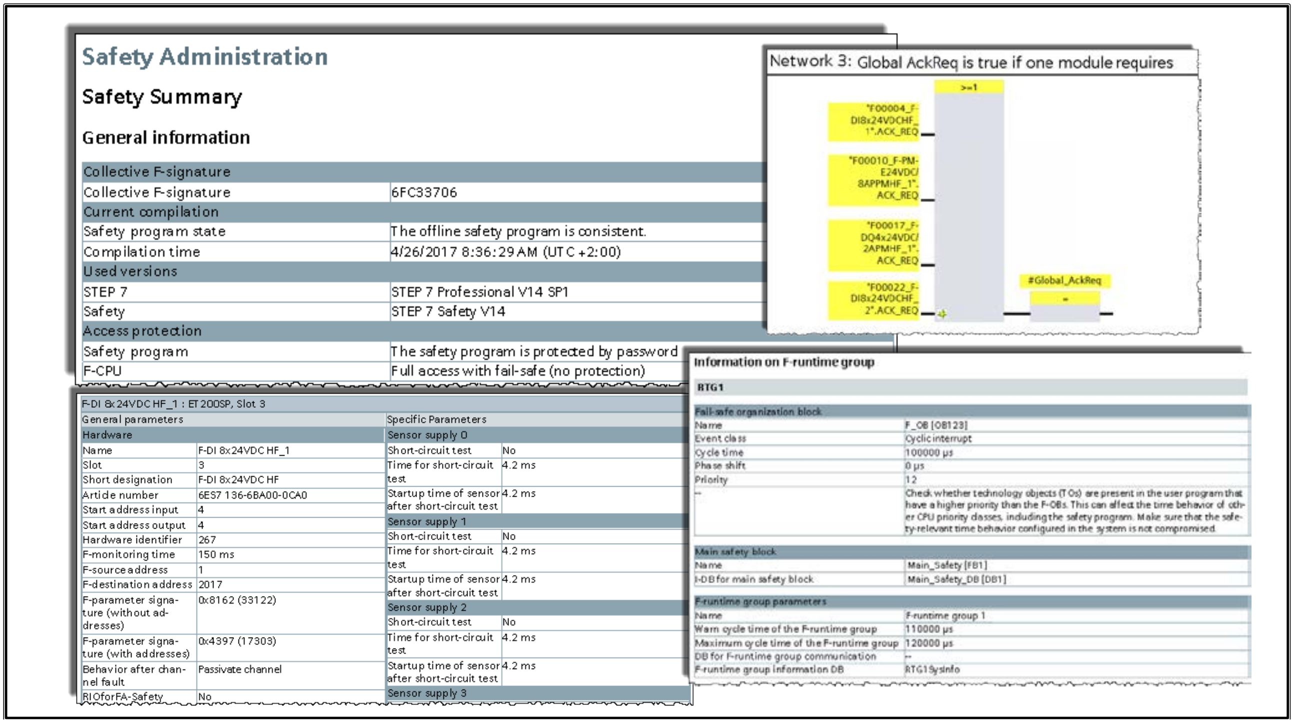
Procedure for creating a safety summary (printout)



In the dialog that appears, you can, among other things, make layout settings for the printout and define the scope of the printout.

Activate the "All" option! This is necessary to document the program code for the acceptance test

8.10.3. Example of a Safety Summary



8.11. Acceptance of Changes

For negligible changes, you do not have to have the entire system re-accepted, only the changes!

For an acceptance of changes, the following tests are necessary:

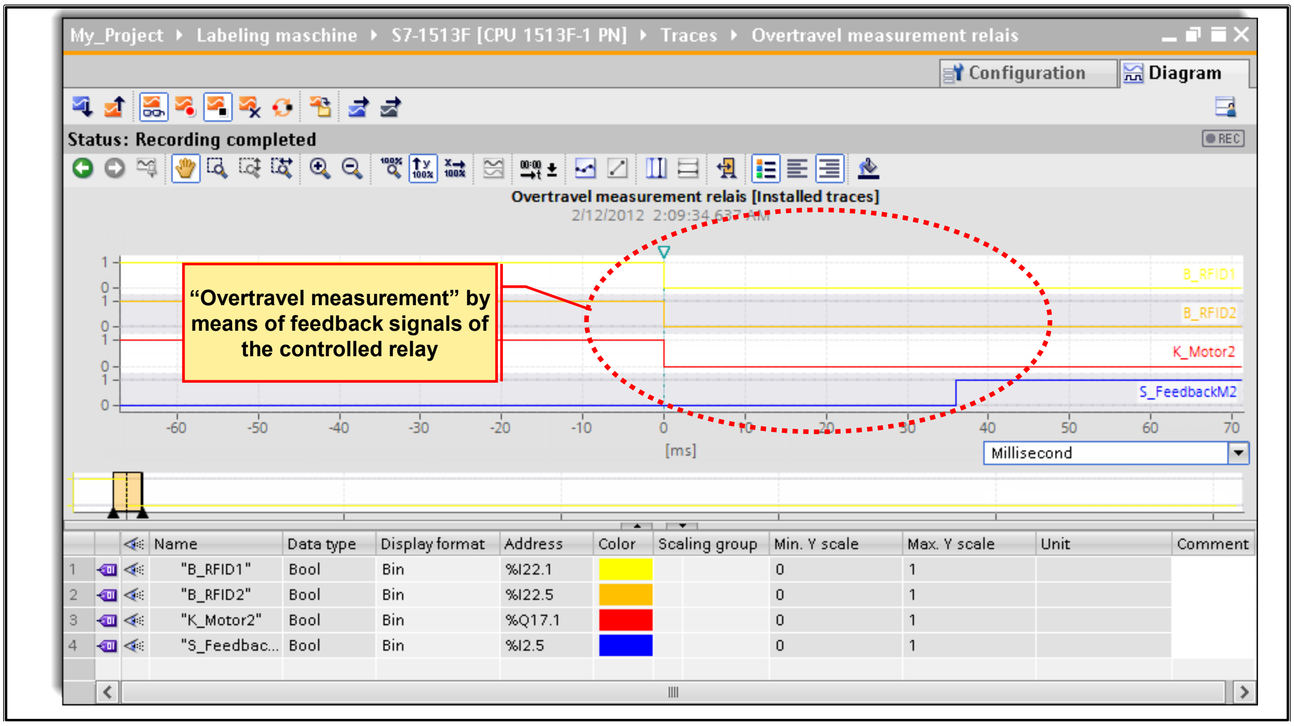
- Risk Impact Assessment (assess the effect of the change)
- Checking the changed or newly added F-blocks
- Checking the changed or newly added instructions and F-system blocks
- Checking the safety-relevant parameters of the changed or newly added F-I/O

The Risk Impact Assessment also determines to what extent the function tests have to be repeated or expanded.

Acceptance of Changes

In general, you can adopt the same approach for the acceptance of changes as the initial acceptance. However, so that you can avoid the acceptance of the entire system in case of negligible changes, STEP 7 Safety Advanced helps you to identify those parts of your safety program that have changed. For an acceptance of changes, the tests shown in the picture are necessary.

8.12. Exercise 1: “Overtravel Measurement” Motor 2 Using a Trace



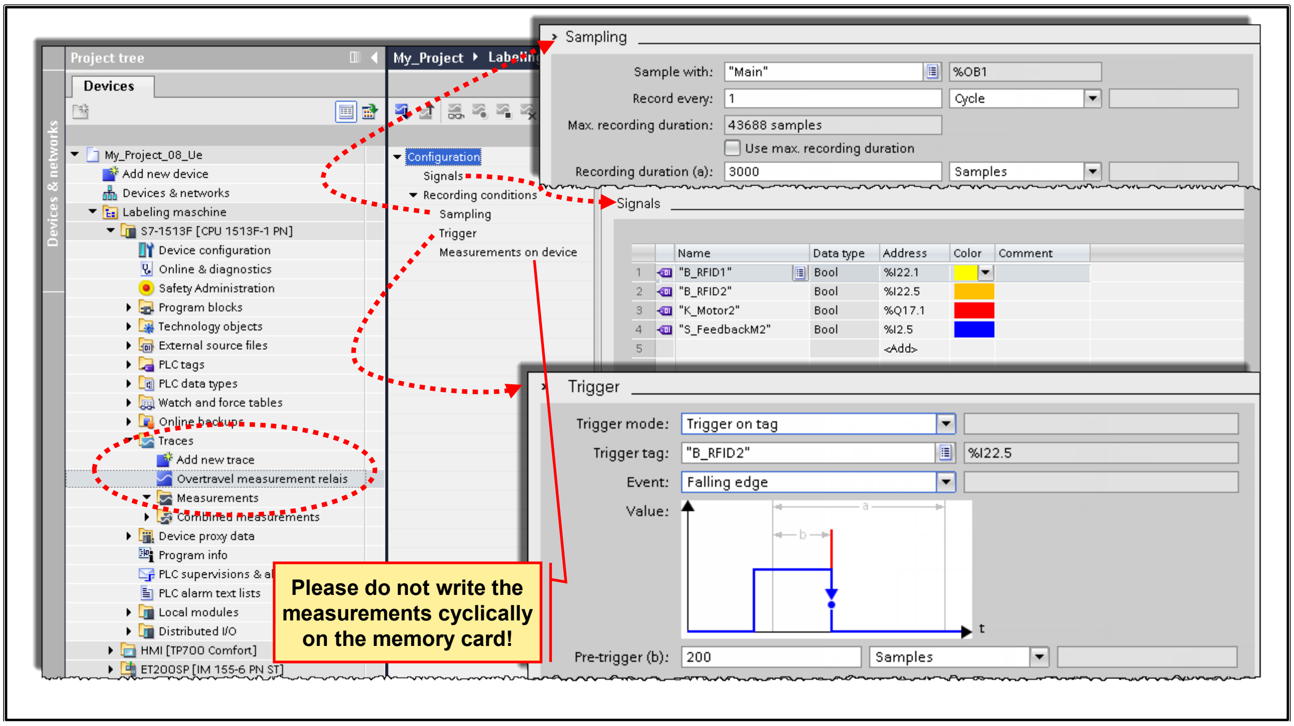
Task Description

An “Overtravel measurement” of Motor 2 is to be carried out using a Trace. The feedback signals (“S_FeedbackM2”) of the relay are to be evaluated when Motor 2 is switched off. You are to determine how long it takes for the feedback signal (“S_FeedbackM2”) to change after Motor 2 is switched off. The switch off is to occur as a result of the opening of the safety door in Automatic mode.

What to Do

Continued on the next page

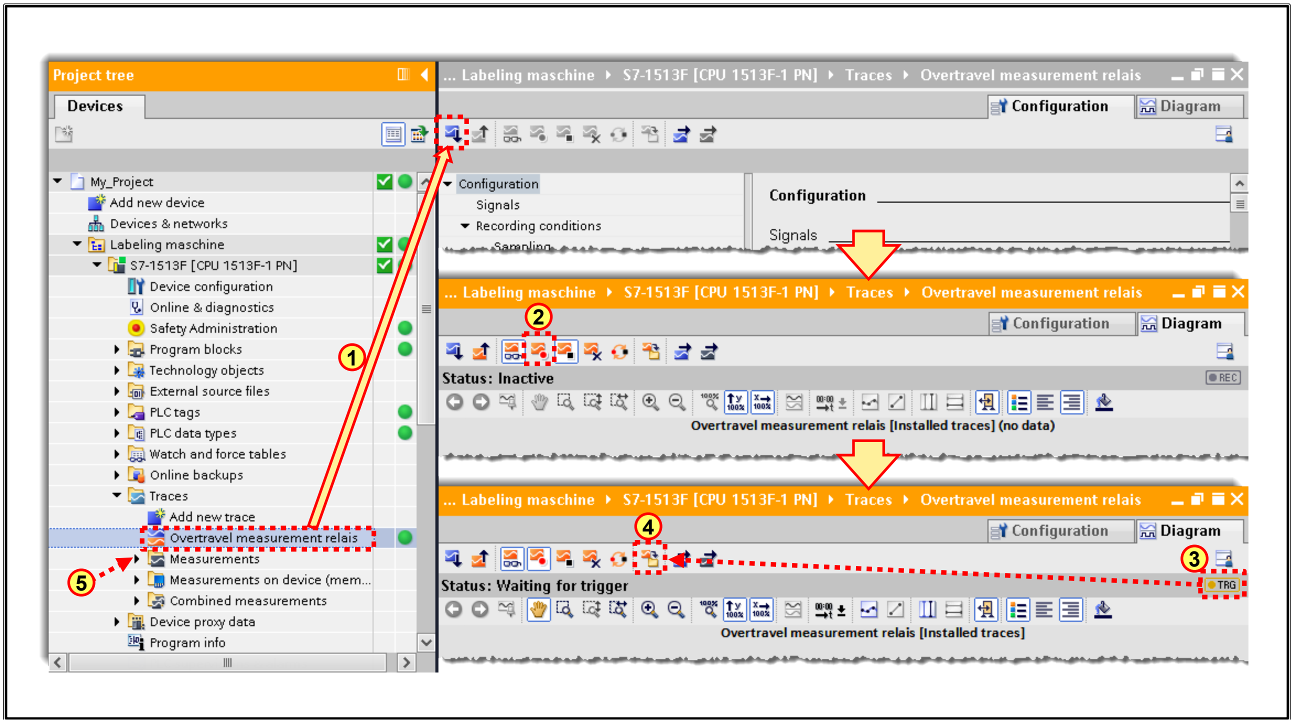
8.12.1. Re: Exercise 1: Creating a Trace



What to Do

1. Create a Trace with the name “Overtravel measurement relays”.
2. Select the required signals that you want to monitor (see picture)
3. Set a Sampling and Trigger tag that makes sense (see picture)
4. Save your project.

8.12.2. Re: Exercise 1: Downloading, Starting and Saving the Trace



What to Do

1. Download the Trace into the CPU.
2. Activate the recording. The recording is now temporarily stored in a ring buffer.
3. After activation, the recording waits until the Trigger is tripped (TRIG=yellow). After the Trigger has been tripped, the recording (REC=red) starts. Wait until the recording is completed (REC=gray).
4. The measurement is now available online in the CPU and is to be saved in the offline project for evaluation.
5. Analyze the measurement and find out the “Overtravel time” of the feedback signal.

8.13. Exercise 2(Optional): Performing an Acceptance Test

You are to perform a function test of the safety functions of a partner station using the black-box test.

In addition, selected fault simulations (fault seeding tests) are performed based on the results of the analyses performed.

8.13.1. Re: Exercise 2: Description of the Test Documentation

Cons. No.	Inputs affected	Outputs affected	Test case	Test requirement	Test description/ Performance	Expected result	Test result Tester / Date
1.0			What is to be tested?	Particular requirements for the test case (for example, variations of the configuration)	Description of the test performance	What is expected as the result of the test?	Was the test successful?

Cons. No.:
For each test case, a consecutive test number is assigned in the test tables in order to be able to exactly subdivide and quantify each test.
Inputs affected:
To provide a better overview, the inputs to be monitored in the test case are noted here
Outputs affected:
To provide a better overview, the outputs to be monitored in the test case are noted here
Note: If neither inputs nor outputs are entered in this column, then you are dealing with internal signals of the CPU which must be monitored per program or must be checked per tag table.
Test case:
In the test case, the test object is described, that is, what is to be tested. Here, which behavior is to be tested or was checked is briefly presented.
Test description/Performance:
The test description explains how the test case is to be tested, that is, which action must be performed by the tester.
Expected result:
After a test is performed, this can be used to check whether the test was successful or not by checking whether the result matches the expected result described here.
Test result:
The test result is completed by the tester. Here, whether the expected result was achieved or not is entered during the test. If the module / the system misses the test goal, then the reason or the erroneous behavior is briefly noted here.

8.13.2. Re: Exercise 2: Test Cases before Startup Operation

Function	Cons. No.	Inputs affected	Outputs affected	Test case	Test requirement	Test description/ Performance	Expected result	Test result Tester / Date
Wiring	0.0			Test the wiring according to the circuit diagram		A test must be made (visible test) that cables (supply, signal lines, bus lines) are properly laid and connected according to the circuit diagram	All cables are laid and connected according to the circuit diagram.	OK Eberle Thomas 01.01.2017

Function	Cons. No.	Inputs affected	Outputs affected	Test case	Test requirement	Test description/ Performance	Expected result	Test result Tester / Date
System restart	0.1			System restart	Test case 0.0 is completed	The system is disconnected from the power and then reconnected	System is ready for operation (CPU in RUN, no SF/BF)	

8.13.3. Re: Exercise 2: Test Cases during Operation: Lifting Device

Function	Cons No.	Inputs affected	Outputs affected	Test case	Test requirement	Test description/ Performance	Expected result	Test result Tester / Date
E-Stop Lifting Device	1.0	I 10.0	Q10.0 Q3.0 Q3.1	Press E-Stop	The system must be in operation and the valves controlled in the Automatic mode operating mode	Pressing the E-Stop at the valve field I 10.0 1->0	The shutdown of the F-PM must occur immediately. Both valves must close (signal state “0”) I 10.0 = 0 Q10.0 = 0 Q3.0 = 0 Q3.1 = 0	
	1.1	I 10.0	Q10.0 Q3.0 Q3.1	Unlock E-Stop	Test case 1.0 is completed.	The E-Stop is unlocked I 10.0 0->1	An automatic restart must not occur. I 10.0 = 1 Q10.0 = 0 Q3.0 = 0 Q3.1 = 0	
	1.2	I 2.3	Q10.0	Acknowledge	Test case 1.1 is completed.	The safety-related shutdown is acknowledged via the acknowledgement button I 2.3 0->1	The control of the valves is once again enabled for operation I 10.0 = 1 Q10.0 = 1	

8.13.4. Re: Exercise 2: Test Cases during Operation: Labeler (1)

Function	Cons No.	Inputs affected	Outputs affected	Test case	Test requirement	Test description/ Performance	Expected result	Test result Tester / Date
E-Stop Labeler	2.0	I 22.0	Q17.0	Press E-Stop	The system must be in operation and Motor 1 controlled	Pressing the E-Stop at Motor 1 I 22.0 1->0	Motor 1 must be de-energized immediately I 22.0 = 0 Q17.0 = 0	
	2.1	I 22.0	Q17.0	Unlock E-Stop	Test case 2.0 is completed.	The E-Stop is unlocked and then two-hand operation pressed I 22.0 0->1	An automatic restart must not occur. I 22.0 = 1 Q17.0 = 0	
	2.2	I 2.3	Q17.0	Acknowledge	Test case 2.1 is completed.	The safety-related shutdown is acknowledged via the acknowledgement button and two-hand operation pressed I 2.3 0->1	The control of Motor 1 is once again enabled for operation I 22.0 = 1 Q17.0 = 1	

8.13.5. Re: Exercise 2: Test Cases during Operation: Labeler (2)

Function	Cons No.	Inputs affected	Outputs affected	Test case	Test requirement	Test description/ Performance	Expected result	Test result Tester / Date
Two-hand monitoring Labeler	3.0	I 22.2 I 22.6	Q17.0	Two-hand monitoring within the discrepancy	The system must be in operation. Motor 1 is not switched on Q17.0 = 0	Pressing the S1 and S2 buttons within the discrepancy time of 200ms I 22.2 0->1 I 22.6 0->1	Motor 1 is controlled I 22.2 = 1 I 22.6 = 1 Q17.0 = 1	
	3.1	I 22.2 I 22.6	Q17.0	Two-hand monitoring outside of discrepancy (S1 comes too late)	The system must be in operation. Motor 1 is not switched on Q17.0 = 0	Pressing the S2 button and after the discrepancy pressing the S1 button I 22.6 0->1 Wait: > 200ms I 22.2 0->1	Motor 1 is controlled I 22.2 = 1 I 22.6 = 1 A17.0 = 0	
	3.2	I 22.2 I 22.6	Q17.0	Two-hand monitoring outside of discrepancy (S2 comes too late)	The system must be in operation. Motor 1 is not switched on Q17.0 = 0	Pressing the S1 button and after parameterized discrepancy pressing the S2 button I 22.2 0->1 Wait: > 200ms I 22.6 0->1	Motor 1 is controlled I 22.2 = 1 I 22.6 = 1 Q17.0 = 0	

8.13.6. Re: Exercise 2: Test Cases during Operation: Robot Automatic Mode (1)

Function	Cons No.	Inputs affected	Outputs affected	Test case	Test requirement	Test description/ Performance	Expected result	Test result Tester / Date
E-Stop Robot Automatic	4.0	I 4.1	Q17.1	Press E-Stop	The system must be in Automatic mode and Motor 2 controlled	Pressing the E-Stop at Motor 2 I 4.1 1->0	Motor 2 must be de-energized immediately I 4.1 = 0 Q17.1 = 0	
	4.1	I 4.1	Q17.1	Unlock E-Stop	Test case 4.0 is completed.	The E-Stop is unlocked I 4.1 0->1	An automatic restart must not occur. I 4.1 = 1 Q17.1 = 0	
	4.2	I 2.3	Q17.1	Acknowledge	Test case 4.1 is completed.	The safety-related shutdown is acknowledged via the acknowledgement button I 2.3 0->1	The control of Motor 2 is once again enabled for operation I 4.1 = 1 Q17.1 = 1	

8.13.7. Re: Exercise 2: Test Cases during Operation: Robot Automatic Mode (2)

Function	Cons No.	Inputs affected	Outputs affected	Test case	Test requirement	Test description/ Performance	Expected result	Test result Tester / Date
Safety door monitoring	5.0	I 22.1	Q17.1	Open safety door	The system must be in Automatic mode and Motor 2 controlled	The safety door is opened I 22.1 1->0	Motor 2 must be de-energized immediately I 22.1 = 0 Q17.1 = 0	
	5.1	I 22.1	Q17.1	Close safety door	Test case 5.0 is completed.	The safety door is closed again I 22.1 0->1	An automatic restart must not occur. I 22.1 = 1 Q17.1 = 0	
	5.2	I 2.3	Q17.1	Acknowledge	Test case 5.1 is completed.	The safety-related shutdown is acknowledged via the acknowledgement button I 2.3 0->1	The control of Motor 2 is once again enabled for operation I 22.1 = 1 Q17.1 = 1	

8.13.8. Re: Exercise 2: Test Cases during Operation: Robot Service Mode

Function	Cons No.	Inputs affected	Outputs affected	Test case	Test requirement	Test description/ Performance	Expected result	Test result Tester / Date
E-Stop Robot Service Mode	6.0	I 4.1	Q17.1	Press E-Stop	The system must be in Service mode and Motor 2 controlled	Pressing the E-Stop at Motor 2 I 4.1 1->0	Motor 2 must be de-energized immediately I 4.1 = 0 Q17.1 = 0	
	6.1	I 4.1	Q17.1	Unlock E-Stop	Test case 6.0 is completed.	The E-Stop is unlocked I 4.1 0->1	An automatic restart must not occur. I 4.1 = 1 Q17.1 = 0	
	6.2	I 2.3	Q17.1	Acknowledge	Test case 6.1 is completed.	The safety-related shutdown is acknowledged via the acknowledgement button I 2.3 0->1	The control of Motor 2 is once again enabled for operation I 4.1 = 1 Q17.1 = 1	

8.13.9. Re: Exercise 2: Test Cases during Operation: Fault Seeding Test

Function	Cons No.	Inputs affected	Outputs affected	Test case	Test requirement	Test description/ Performance	Expected result	Test result Tester / Date
Short-circuit at E-Stop	7.0	I 4.1	Q17.1	Activate short-circuit switch	The system must be in operation and Motor 2 controlled	Activate short-circuit switch	Motor 2 must be de-energized immediately I 4.1 = 0 Q17.1 = 0	
	7.1	I 4.1	Q17.1	Unlock short-circuit switch	Test case 7.0 is completed.	Short-circuit switch is unlocked	An automatic restart and depassivation must not occur. I 4.1 = 0 Q17.1 = 0	
	7.2	I 2.3	Q17.1	Acknowledge I/O	Test case 7.1 is completed.	The channel fault is acknowledged via the acknowledgement button I 2.3 0->1	An automatic restart must not occur. I 4.1 = 1 Q17.1 = 0	
	7.3	I 2.3	Q17.1	Acknowledge E-Stop	Test case 7.2 is completed.	The safety-related shutdown is acknowledged via the acknowledgement button I 2.3 0->1	The control of Motor 2 is once again enabled for operation I 4.1 = 1 Q17.1 = 1	

8.13.10. Re: Exercise 2: Result

Summary of the test(s)

Findings

Primary findings (requirements not fulfilled)

Secondary findings (requirements fulfilled to a limited extent)

Notes (requirements fulfilled)

Summary

Contents 9

9. Service and Diagnostics

At the end of the chapter the participant will ...

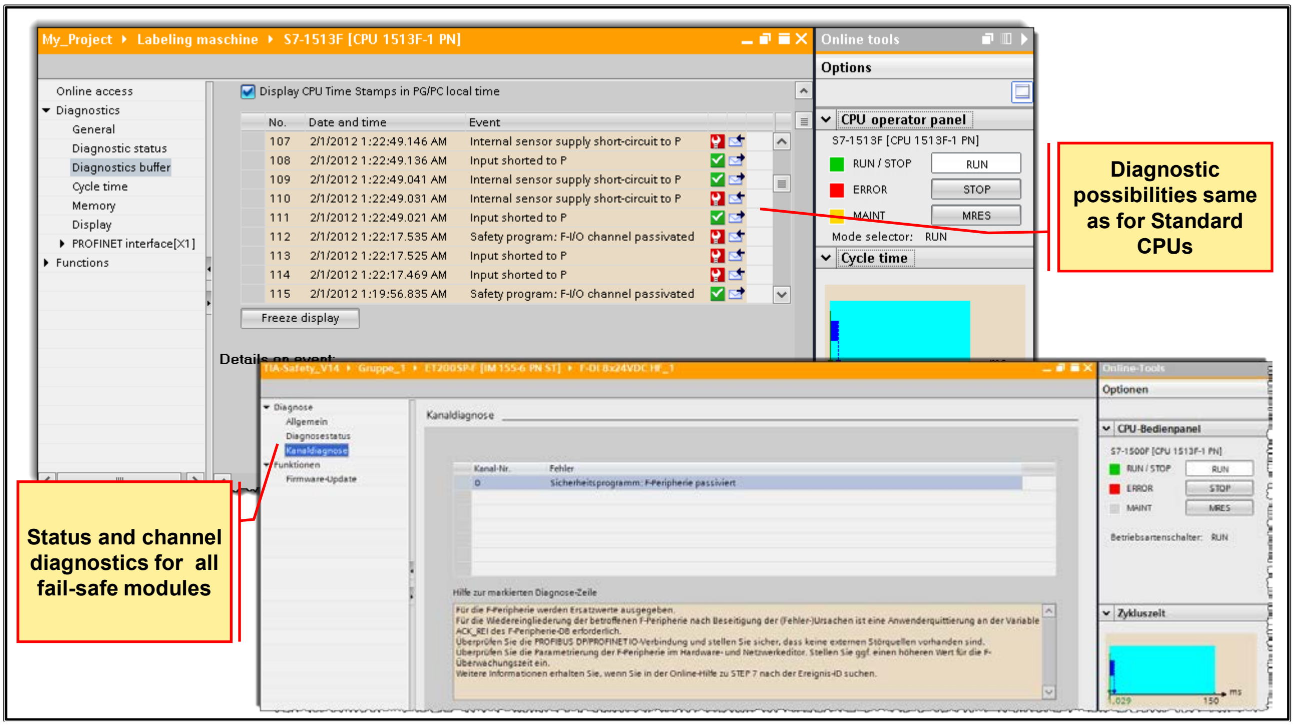
… be able to interpret LEDs of the fail-safe modules

… be able to operate the Display of the 1500 F-CPUs

… be able recognize and eliminate errors and diagnostic messages of Safety Advanced

… be able to carry out a module exchange and firmware update

9.1. General Diagnostics



System Diagnostics

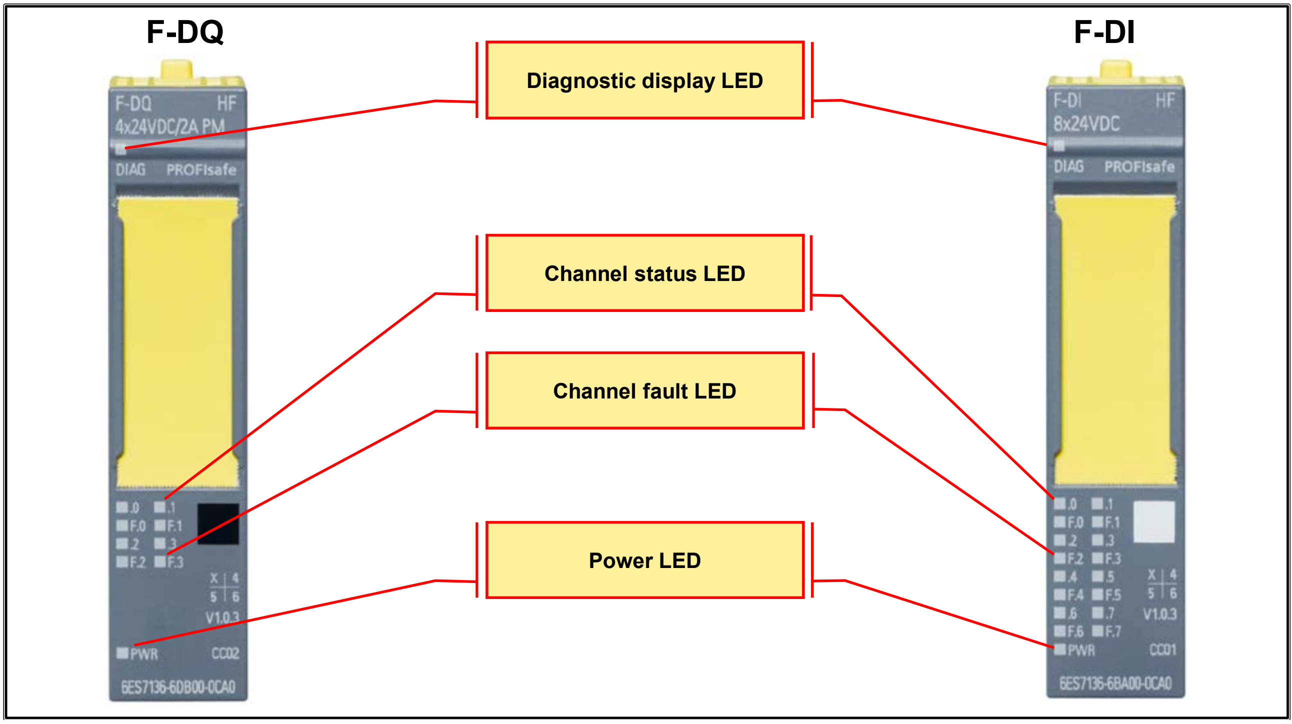
All SIMATIC products have integrated diagnostic functions with which you can recognize and eliminate faults. The components automatically signal a possible fault of the operation and provide additional detailed information. You can minimize unplanned downtimes through system-wide diagnostics. The SIMATIC automation system monitors the following states in the running system:

- Device failure/recovery
- Pull/plug event
- Module error
- I/O access error
- Channel fault
- Parameterization error
- Failure of the external auxiliary voltage

Diagnostic Messages

Module errors are displayed as diagnostics (module information). After error elimination, you must reintegrate the F-module in the safety program.

9.2. LED Displays



The LED DIAG and the LEDs channel status and channel fault of the inputs are not designed to be safety-related and must therefore not be evaluated for safety-related activities.

9.3. LED Evaluation (1)

F-DQ

F-DI

DIAG	Meaning
Off	Backplane bus supply of the ET 200SP not okay
Flashing	Module parameters not configured
On	Module parameters configured and no module diagnostics
Flashing	Module parameters configured and module diagnostics

PWR	Meaning
Off	Supply voltage L+ missing
On	Supply voltage L+ available

9.4. LED Evaluation (2)

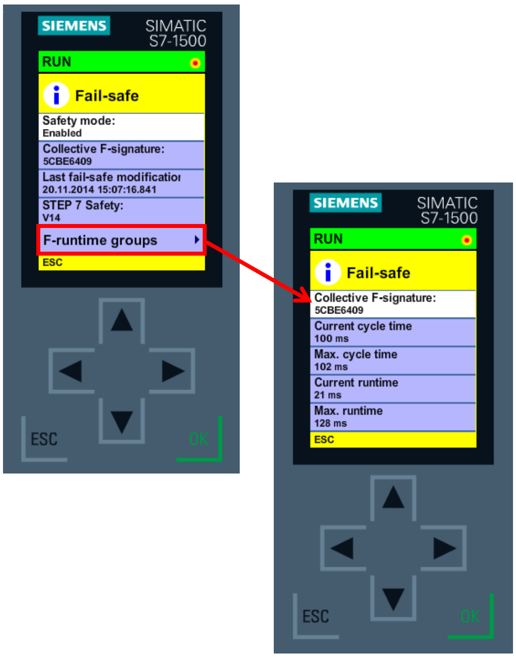
F-DQ

F-DI

Channel status	Channel fault	Meaning
Off	Off	Process signal = 0 and no channel diagnostics
On	Off	Process signal = 1 and no channel diagnostics
Off	On	Process signal = 0 and channel diagnostics
Alternately flashing		Channel waiting for user acknowledgment

Channel status	DIAG	Channel fault	Meaning
Off	Flashing	All On	The PROFIsafe address does not match the configured PROFIsafe address
Flashing	Flashing	Off	Identification of the F-module when assigning the PROFIsafe address

9.5. Display Expansions for 1500 F-CPU



S7-1500 F-CPUs with Display show the following in the menu “Overview” under “Fail-safe”:

- Safety mode enabled/disabled
- Collective F-signature
- Last fail-safe modification
- Version of STEP 7 Safety with which the safety program was compiled.
- Information about the F-runtime groups (RTGSYSInfo)

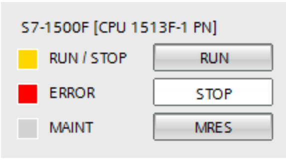
For each F-I/O, the menu "Status" under "Safety" displays the following:

- F-parameter signature (with address)
- Safety mode
- F-monitoring time
- F-source address
- F-destination address

9.6. Procedure for Diagnosis of Safety-relevant Errors (1)

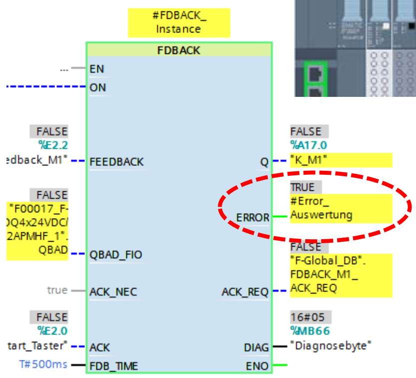
HOW does the error appear?

- Error detected by the system (module error, exceeding the cycle time)
- Functional error (Logic error, safety functions triggered)



WHERE does the error appear?

- In the program (safety blocks)
- At individual fail-safe modules
- At entire stations

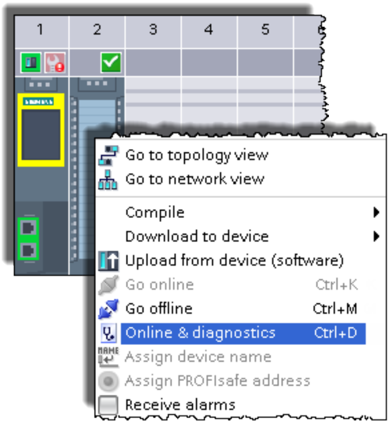


WHEN does the error appear?

- Permanently pending (immediately after CPU power up)
- Sporadic (in undefined intervals)
- Through certain signal changes (for example, special input signal changes)

9.7. Procedure for Diagnosis of Safety-relevant Errors (2)

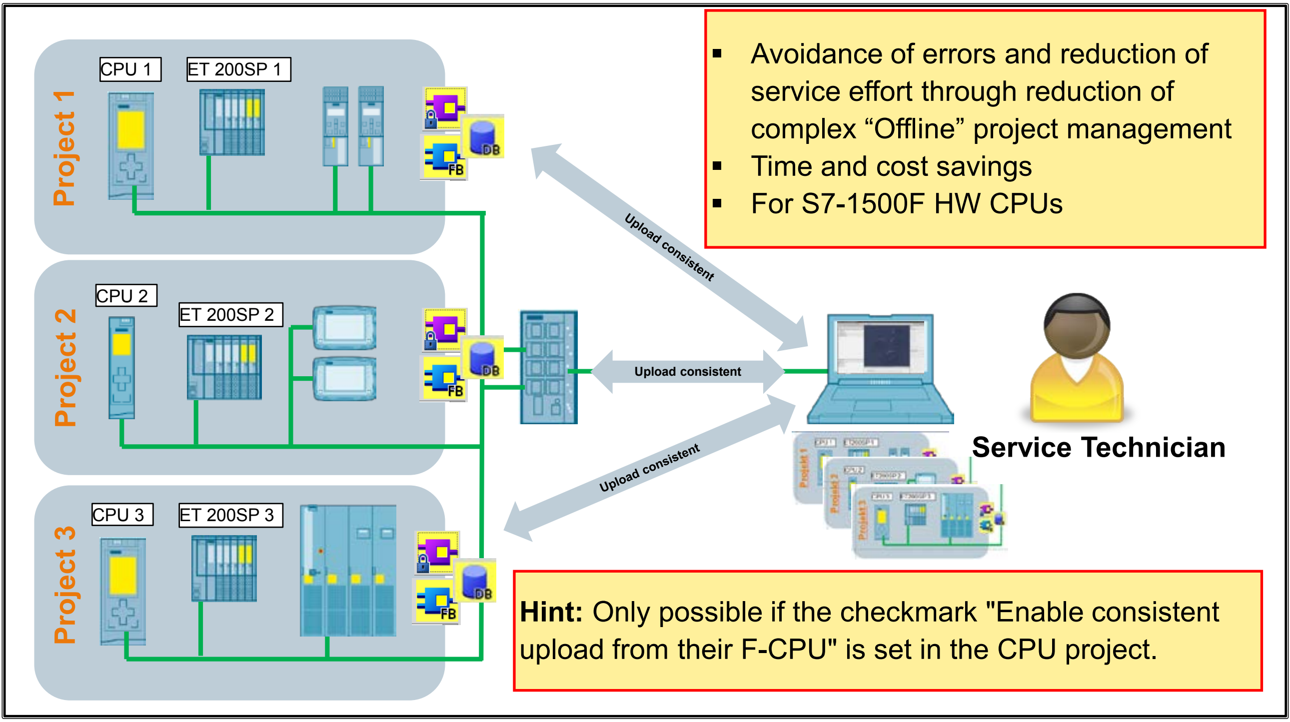
Troubleshooting



1. **Approach same as for Standard diagnosis**
   - Diagnostic messages
   - Test wiring
   - Cross-references
   - Watch table

   ...
2. **Special approach for Safety-relevant errors**
   - **Exceeding the monitoring time:**
     - Check PROFIsafe monitoring time of modules
   - **Parameter-assignment error:**
     - Check the destination addresses and coding elements of F-modules
   - **Data corruption, CRC-error:**
     - Do not execute standard program in order to detect possibly unallowed accesses
     - Inhibit standard communication in order to detect possibly unallowed accesses

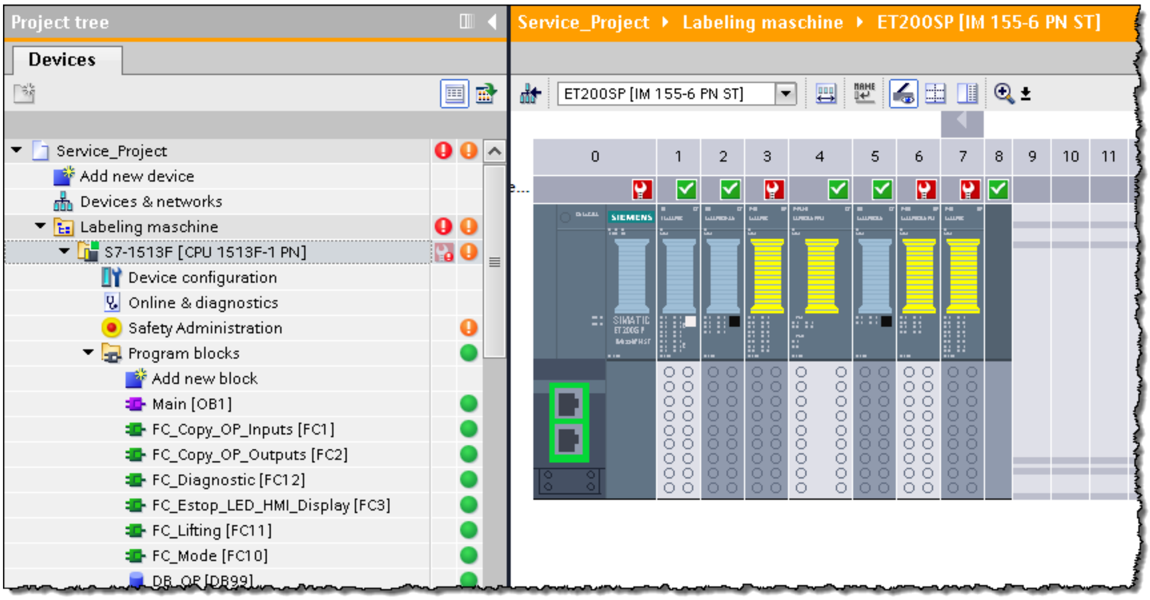
9.8. Consistent Upload of Safety Projects



- Avoidance of errors and reduction of service effort through reduction of complex “Offline” project management
- Time and cost savings
- For S7-1500F HW CPUs

Hint: Only possible if the checkmark "Enable consistent upload from their F-CPU" is set in the CPU project.

9.9. Exercise 1: Troubleshooting



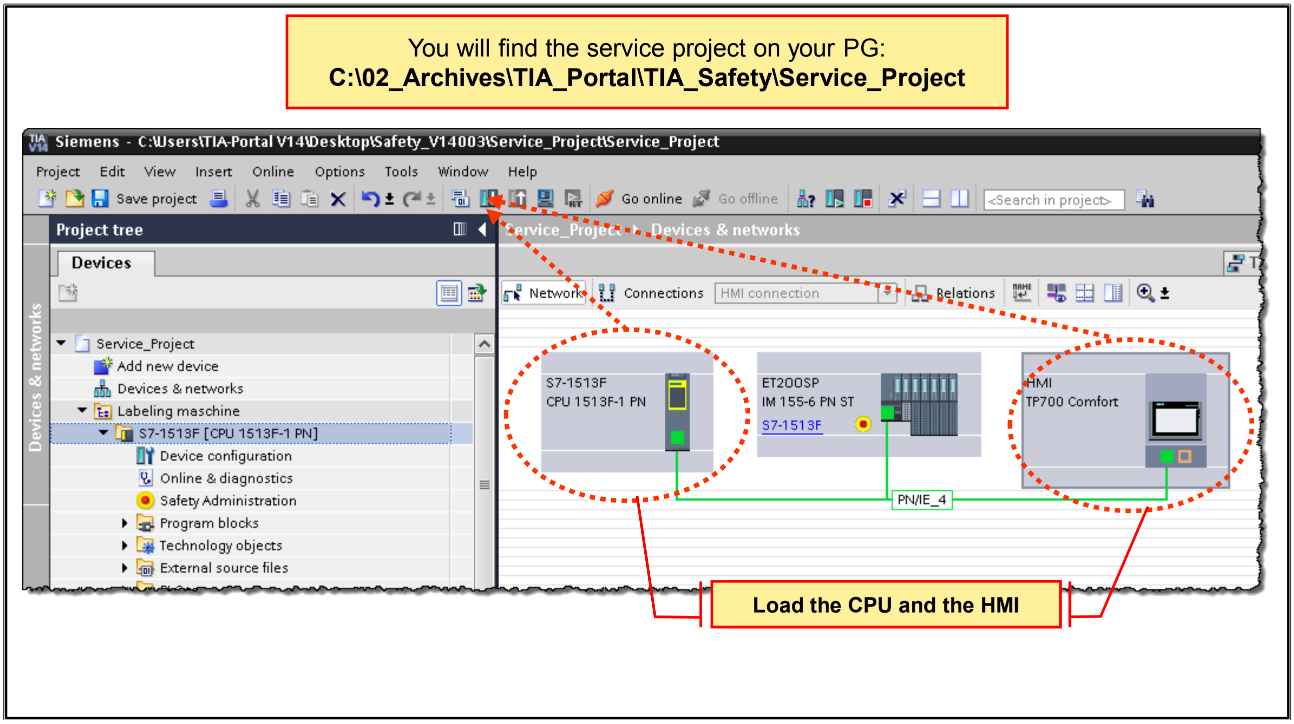
Task Description

A typical service case is to be simulated. You arrive on-site at the customer as a service technician and you find the system in fault. You are now to find all errors/faults and eliminate them so that the system is working again.

What to Do

See next page

9.9.1. Re: Exercise 1: Downloading the Service Project (CPU + HMI) into the Device



Task

In order to carry out troubleshooting, you must first load a faulty project into the system. Under "C:\02_Archives\TIA_Portal\TIA-SAFETY\Service_Project" you will find a prepared TIA V14SP1 project.

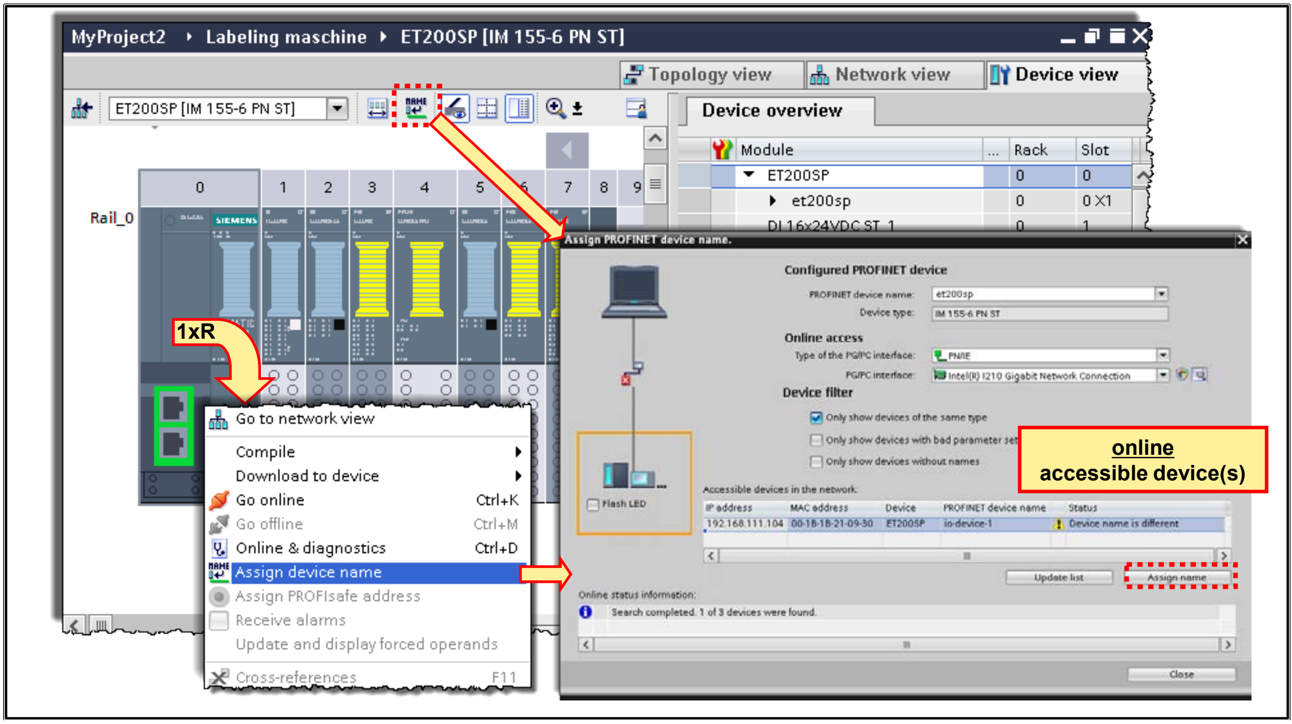
Note:

The service project does not contain an F-password and also no CPU protection. This is permitted for exercise purposes but for productive operation, the CPU and also the F-program must always be protected by a password.

What to Do

1. Save your current project "MyProject" and close the project.
2. Open the service project. You will find the project under the following path: **"C:\02_Archives\TIA_Portal\TIA-SAFETY\Service_Project"**
3. Load the CPU and the HMI in your device.

9.9.2. Re: Exercise 1: Assigning the ET 200SP Device Name ONLINE



Task

The PROFINET device name assigned offline in the service project must now be assigned to the ET 200SP online, so that the IO-Controller or the CPU can assign the offline-configured IP address during system startup of the ET 200SP.

What to Do

1. In the Hardware and Network editor, select the "Device view" of the ET 200SP.
2. Right-click on the Interface module or the module on Slot 0 and in the menu that appears, activate the item "Assign device name".
3. In the dialog that appears, check the (offline) PROFINET device name.
4. Under "Type of the PG/PC interface", select the interface through which you are connected to the PROFINET (see picture). Click on "Update list" to display all accessible devices.
5. In the lower part of the dialog, under the (online) "Accessible devices in the network", select the ET 200SP or the Interface module IM156-6 and activate "Assign name".
6. Save your project.

Result:

The CPU is in RUN mode and the ERROR-LED flashes red.

The ET 200SP has received its parameterization and the “RN-LED” (RUN) of the ET 200SP head station has a steady light. Through the “DIAG-LED”, several modules signal that an error/diagnosis exists.

9.9.3. Re: Exercise 1: Troubleshooting

Task

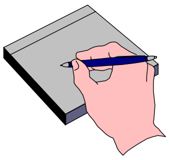
The service project contains two types of errors.

1. 3x system errors (errors detected by the system)
2. 3x functional errors (errors not detected by the system)

First, you are to find and eliminate all system errors. Then, you are to localize all functional errors and eliminate them. The correct functionality of the system is identical to the functionality in the programming exercises.

What to Do: Finding and Eliminating the System Errors

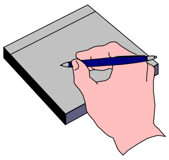
Using the online diagnostics possibilities (diagnostics buffer, module information, channel diagnostics…etc.) you are to find all system errors and eliminate them.



- **First error**:
  - Error
  - ....

    ....
  - Correction:
  - ....

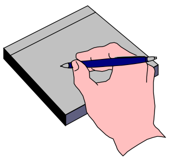
    ....



- **Second error:**
  - Error
  - ....

    ....
  - Correction:
  - ....

    ....



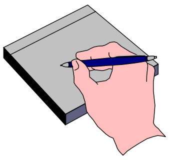
- **Third error:**
  - Error
  - ....

    ....
  - Correction:
  - ....

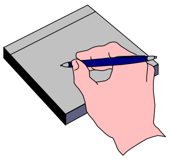
    ....

What to Do: Finding and Eliminating the Functional Errors

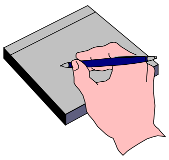
Using the diagnostic functions (monitor block, Watch tables, diagnostic byte of the safety functions…etc.) you are to find all functional errors and eliminate them.



- **First error:**
  The shut-off valves can no longer be shutdown via the local E-Stop “E3”
  - Error
  - ....
    ....
  - Correction:
  - ....
    ....

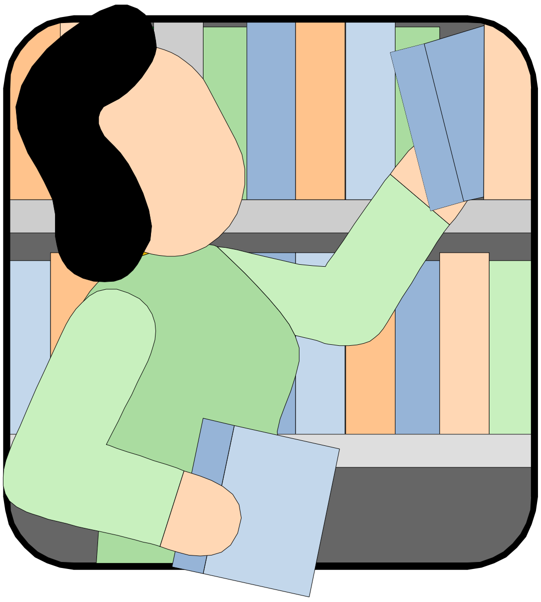


- **Second error:**
  Motor 1 can no longer be controlled via two-hand operation
  - Error
  - ....
    ....
  - Correction:
  - ....
    ....

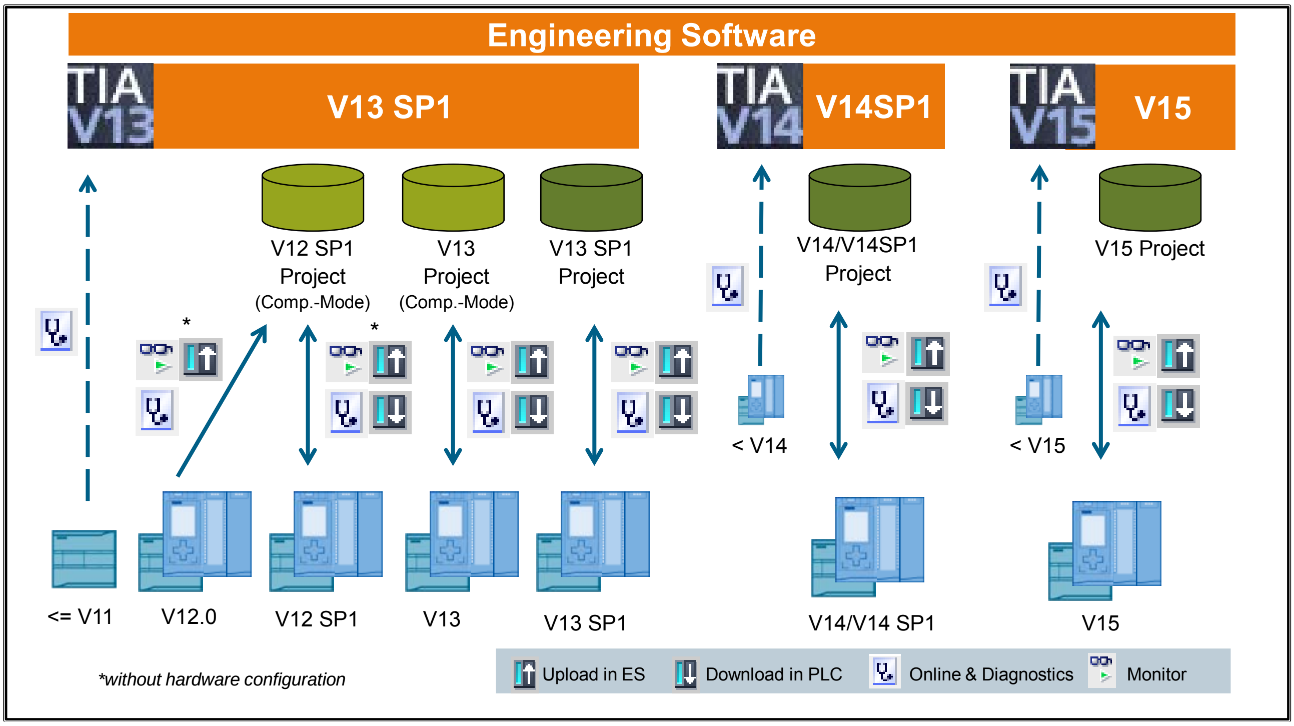


- **Third error:**
  Motor 2 can no longer be controlled in Automatic as well as Service mode (Jog)
  - Error
  - ....
    ....
  - Correction:
  - ....
    ....

9.10. Additional Information



9.10.1. TIA Portal – Compatibility Online



Contents 10

10. Fail-safe Communication

At the end of the chapter the participant will ...

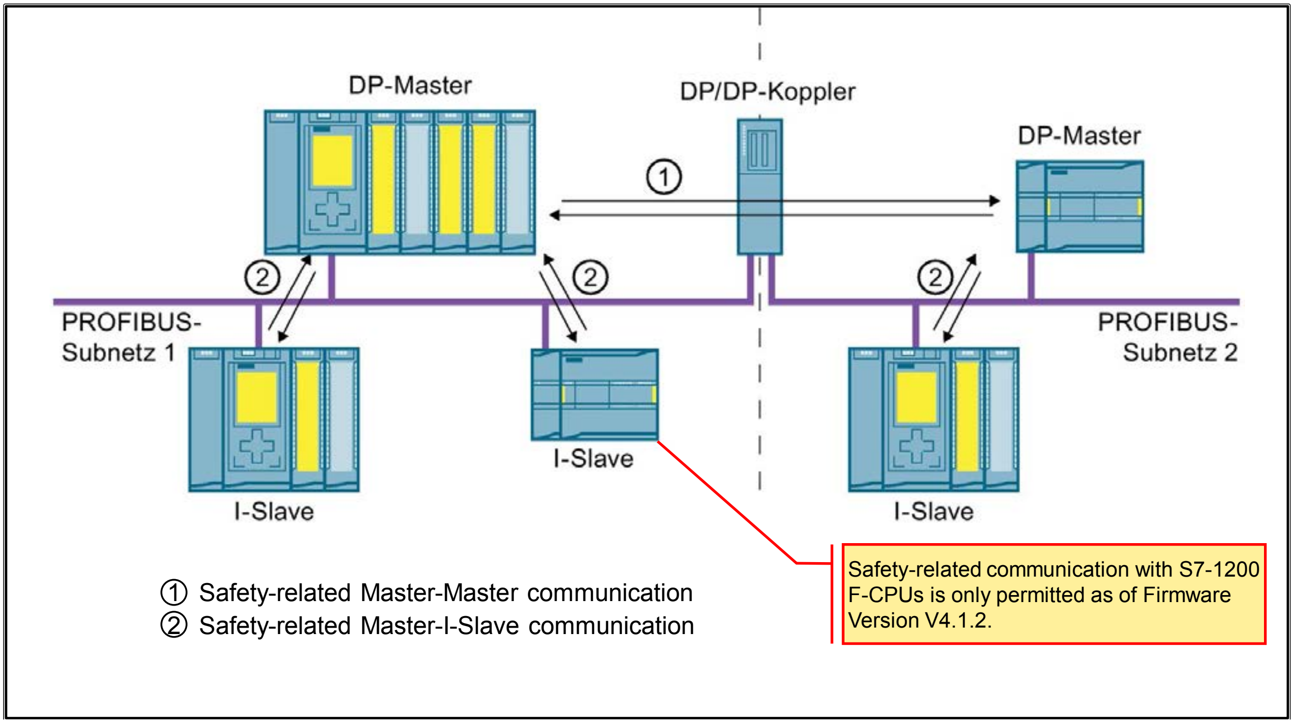
… have an overview of the different communication options via PROFIBUS and PROFINET

… be able explain and configure CPU communication via coupler modules

… be able explain and configure Controller I-Device communication

… be able explain and configure communication between Safety Advanced and Distributed Safety

10.1. Overview of Safety-related Communication via PROFIBUS DP



Fail-safe Communication

Fail-safe communications takes place with the PROFIsafe profile via PROFIBUS as well as PROFINET.

PROFIsafe was the first communication standard based on safety standard IEC 61508 that permit both standard and safety-related communication on the same bus. This not only brings an enormous savings potential with regard to cabling and part variety but also the advantage of retrofit ability.

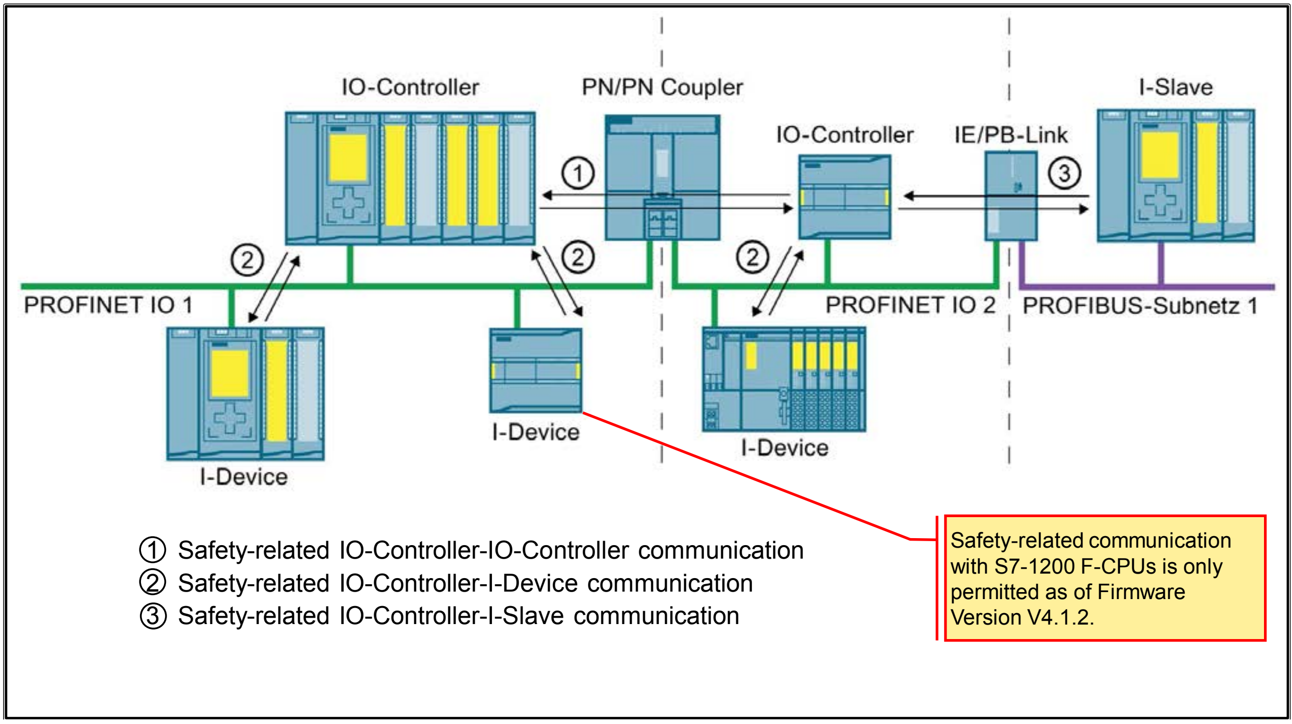
PROFIsafe is one of the open solutions for safety-related communication via standard fieldbuses. Numerous manufacturers of safety components and end users of safety technology have helped to develop this vendor-neutral and open standard of PROFIBUS International (PI).

The PROFIsafe profile enables safe communication for the open standard buses PROFIBUS and PROFINET on the basis of standard network components. In conjunction with PROFINET, PROFIsafe also supports fail-safe wireless communication via IWLAN.

Overview of Safety-related Communication via PROFIBUS DP

In the picture above, you will find an overview of the possibilities of safety-related communication via PROFIBUS DP in SIMATIC Safety F-systems with S7-1500 F-CPUs. In safety-related CPU-CPU communication, a fixed amount of data of data type BOOL or INT is transferred in a fail-safe manner between the safety programs in F-CPUs of DP masters. The data is transferred using the SENDDP instruction for sending and the RCVDP instruction for receiving. The data is stored in configured transfer areas of the devices. The hardware identifier (HW identifier) defines the configured transfer areas.

10.2. Overview of Safety-related Communication via PROFINET IO

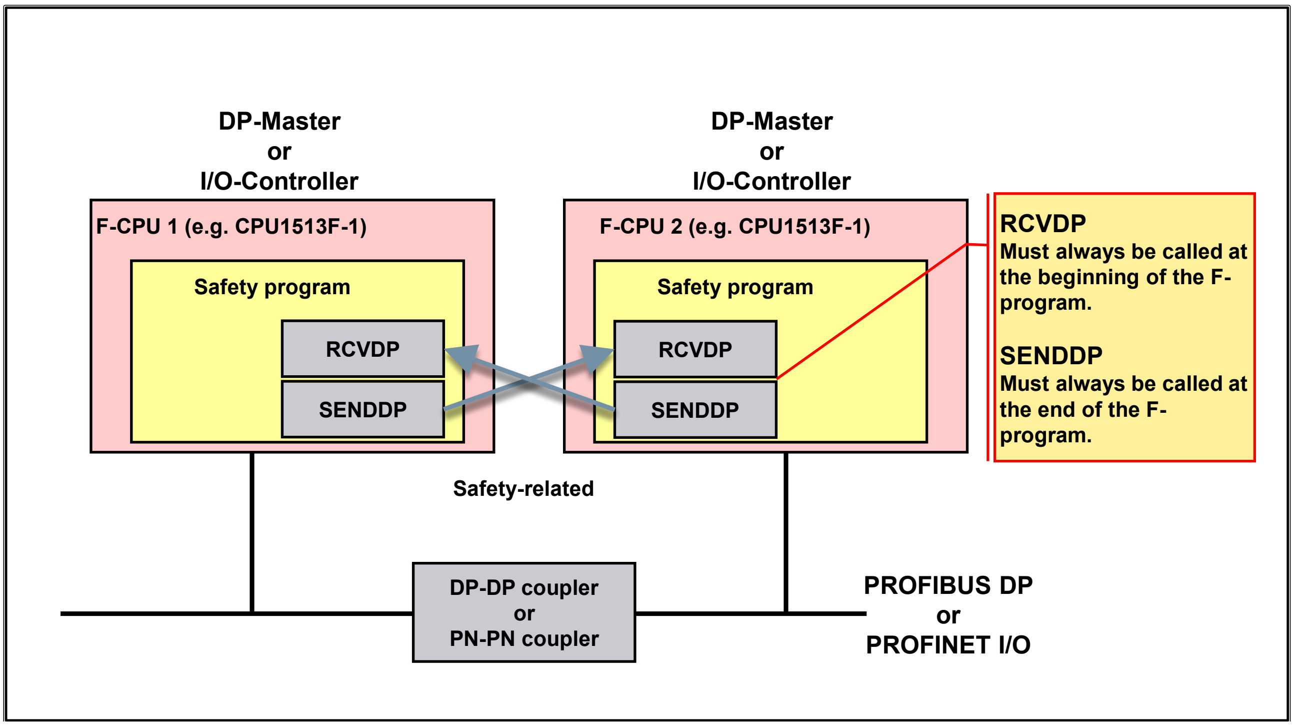


Safety-related CPU-CPU Communication via PROFINET IO

In safety-related CPU-CPU communication, a fixed amount of data of data type BOOL or INT is transferred in a fail-safe manner between the safety programs in F-CPUs of IO Controllers/ I-Devices. The data is transferred using the SENDDP instruction for sending and the RCVDP instruction for receiving. The data is stored in configured transfer areas of the devices. The hardware identifier (HW identifier) defines the configured transfer areas.

10.3. Fail-safe CPU-CPU Communication via Coupler

10.3.1. SENDDP / RCVDP Communication Blocks



Defining Transfer Areas

The transfer areas for input and output data for the PN/PN coupler must be configured. The transfer areas are assigned using the hardware identifier that is assigned automatically to the modules and devices. You need the HW identifier for programming the SENDDP and RCVDP blocks (LADDR input). For each HW identifier of the transfer area, a system constant is created in the respective F-CPU. You can assign these system constants to the SENDDP and RCVDP blocks symbolically or absolutely.

Communication using the SENDDP and RCVDP Instructions

The safety-related communication between the F-CPUs of the IO Controller is handled using the SENDDP instruction for sending and the RCVDP instruction for receiving. With them, a fixed amount of fail-safe data of data type BOOL or INT is transferred in a fail-safe manner. You can find these instructions in the "Instructions" task card under "Communication".

Note

You must call the RCVDP instruction at the beginning of the Main Safety Block. You must call the SENDDP instruction at the end of the Main Safety Block. Note that the send signals are sent only after the call of the SENDDP instruction at the end of execution of the corresponding F-runtime group.

10.3.2. SENDDP and RCVDP Overview

- Fail-safe data exchange between two safety programs via I/O coupling (PROFIBUS + PROFINET)

- Data transmission occurs through SENDDP and RCVDP combination

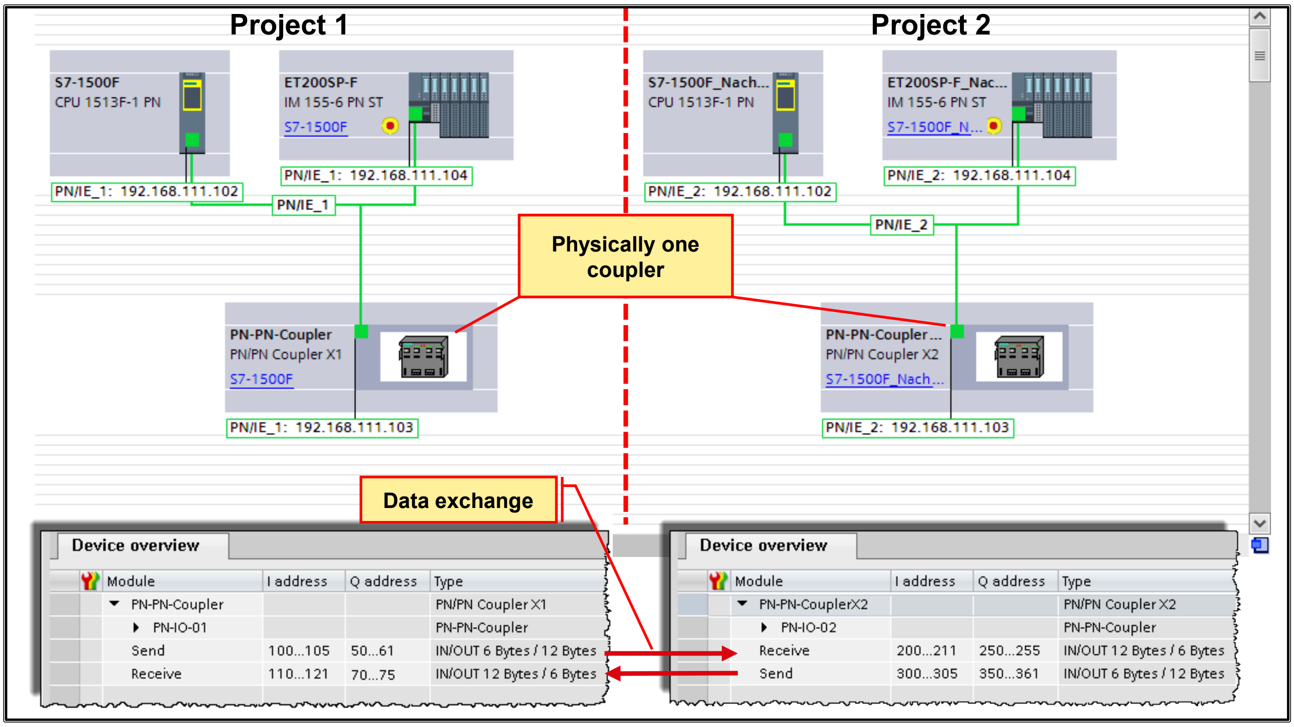
- Consistent transmission of a fixed amount of data
  - 16 BOOL values
  - 2 INT values/1 DINT value
  - F-parameters
  - F-parameters as acknowledgement

- Data is stored in configured address areas
  - Sender: 12 bytes output data 6 bytes input data
  - Receiver: 12 bytes input data 6 bytes output data

DP-DP or PN-PN Coupler

The fixed amount of 6 bytes of user data can be transferred during DP Master-DP Master or IO Controller-IO Controller communication via a DP-DP or PN-PN coupler module. When so-called universal modules of the coupler modules are configured, additional input and output bytes must be taken into account for safety-related communication with the PROFIsafe profile.

10.3.3. Defining Transfer Areas



Note

In the Hardware and Network editor, deactivate the parameter "Data validity display DIA" in the Properties of the PN/PN coupler. This corresponds to the default setting. Otherwise, a safety-related IO-Controller-IO-Controller communication is not possible.

Configuring Transfer Areas

For each safety-related communication connection between two F-CPUs in the PN/PN coupler, you must configure one transfer area for the output data and one transfer area for the input data in the Hardware and Network editor.

Rules for Defining the Transfer Areas

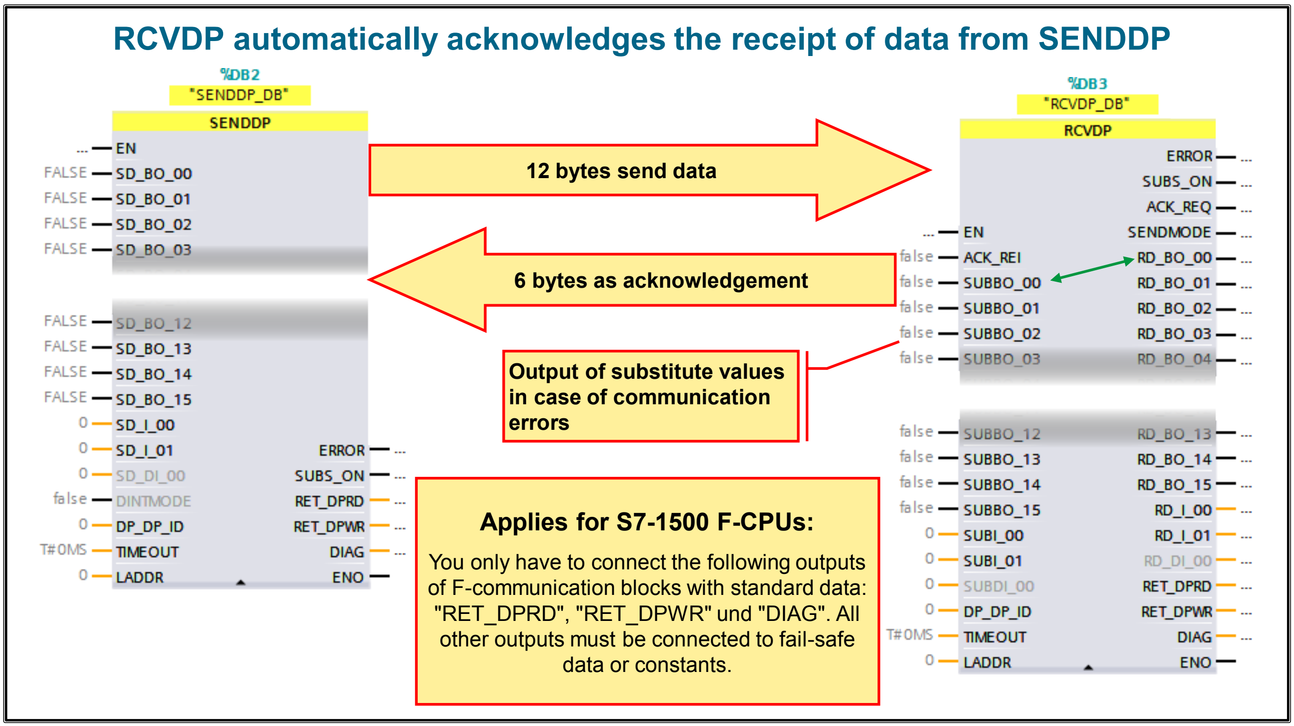
Data to be sent:

12 bytes (consistent) are required for the transfer area of the output data; 6 bytes (consistent) are required for the transfer area of the input data.

Data to be received:

12 bytes (consistent) are required for the transfer area of the input data; 6 bytes (consistent) are required for the transfer area of the output data.

10.3.4. SENDDP and RCVDP Parameters



"RCVDP", "SENDDP"

At SENDDP, the data to be sent is created at the "SD_..." parameters; at RCVDP, the received data is output to the "RD_..." parameter (under fault conditions, the substitute values "SUB_...").

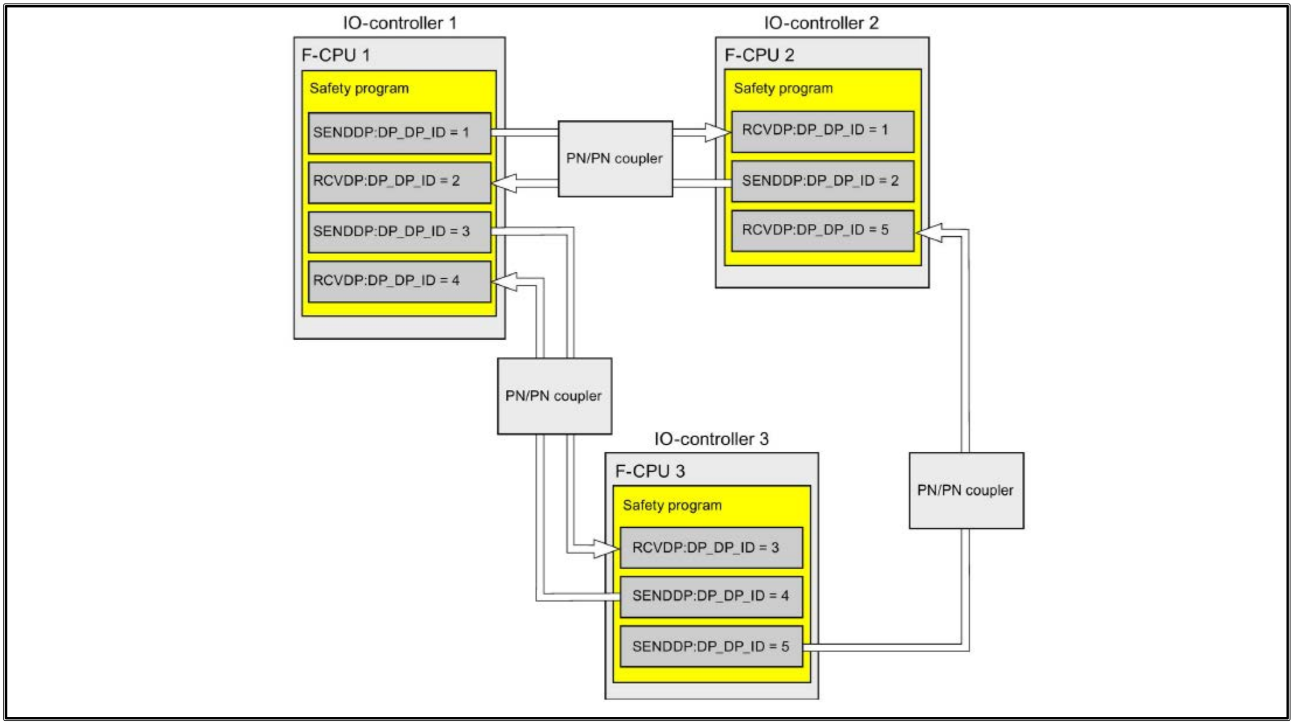
Input Parameters:

ACK_REI	BOOL	1 = Acknowledgment for reintegration of the send data after communication error
SUBBO_xx	BOOL	Substitute value for receive data BOOL xx (only RCVDP)
SUBI_xx	BOOL	Substitute value for receive data INT xx (only RCVDP)
SD_BO_xx	BOOL	Send data BOOL xx (only SENDDP)
SD_I_xx	INT	Send data INT xx (only SENDDP)
DP_DP_ID	INT	Network-wide unique identifier (user-assigned) for a SENDDP/RCVDP pair
TIMEOUT	TIME	Monitoring time [ms] for F-communication
LADDR	INT	Address of the HW identifier (defined in the Device configuration)

Output Parameters:

ERROR	BOOL	1 = Communication error
SUBS_ON	BOOL	SENDDP: 1 = Receiver outputs substitute values, RCVDP: 1 = Substitute values are output
ACK_REQ	BOOL	1 = Acknowledgment for reintegration of the received data required (only RCVDP)
SENDMODE	BOOL	1 = Sending F-CPU in deactivated F-mode
RD_BO_xx	BOOL	Receive data BOOL xx
RD_I_xx	INT	Receive data INT xx
RET_DPRD	WORD	Error code
RET_DPWR	WORD	Error code
DIAG	BYTE	Diagnostic data

10.3.5. Assignment of SENDDP and RCVDP via Unique ID



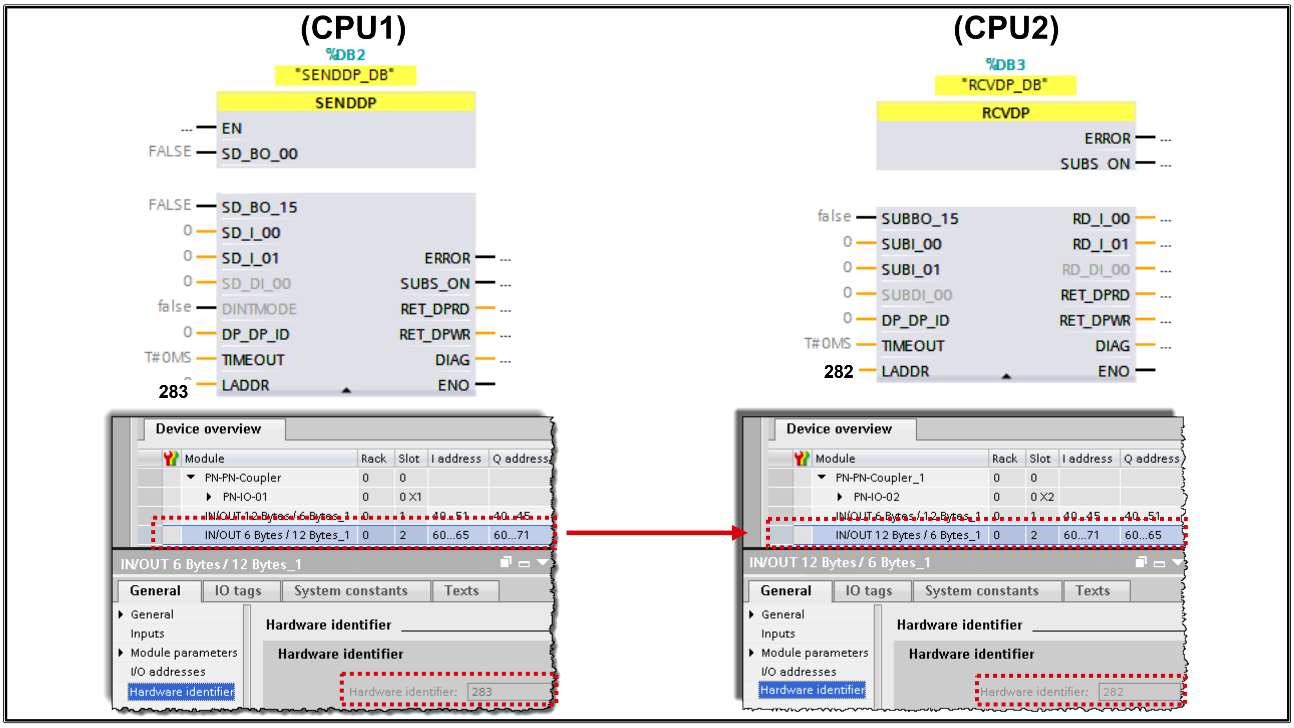
Parameter DP_DP_ID

You assign the value for the respective address relationship to the DP_DP_ID inputs. This establishes the communication relationship between the SENDDP instruction in one F-CPU and the RCVDP instruction in the other F-CPU: The associated instructions receive the same value for DP_DP_ID.

Note

The value for each address association (input DP_DP_ID; data type: INT) is user-defined; however, it must be unique from all other safety-related communication connections network-wide. The uniqueness must be checked in the (printout of the) safety summary during acceptance of the safety program. You must supply the inputs DP_DP_ID and LADDR with constant values when calling the instruction. Direct read or write access to the associated Instance DB is not permitted in the safety program!

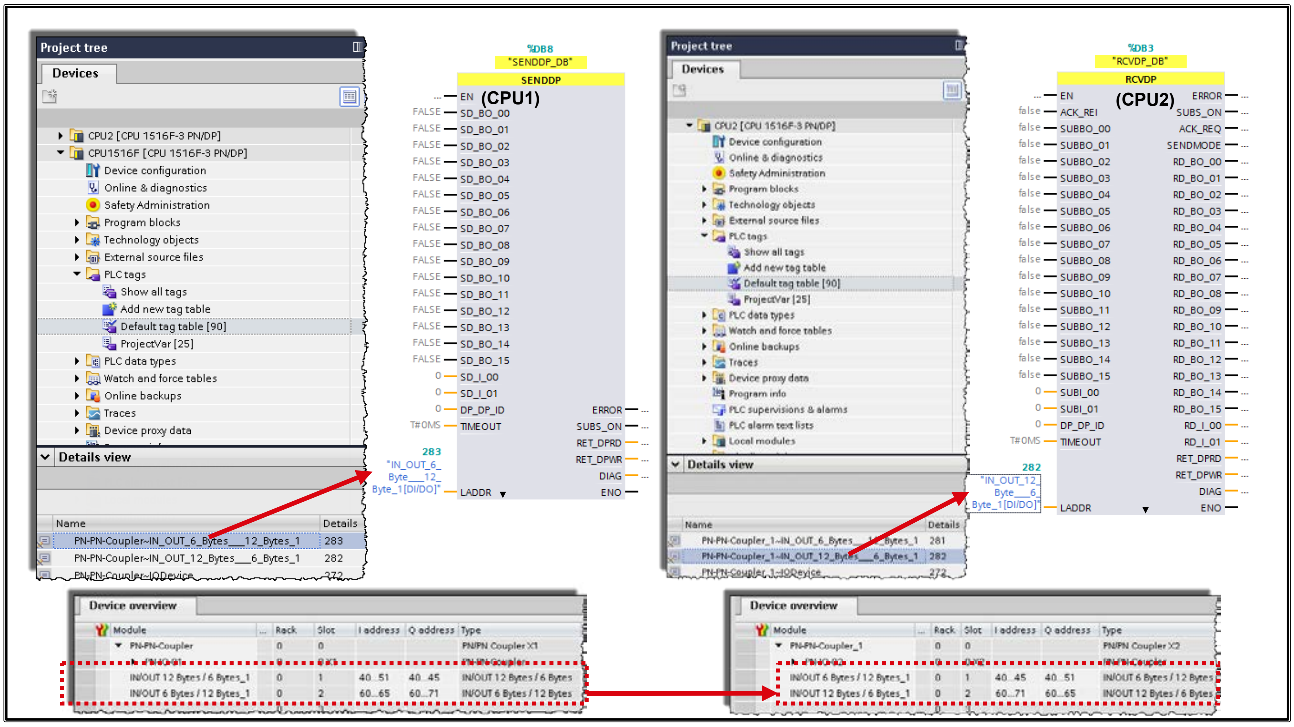
10.3.6. Parameter LADDR, Absolute



Parameter LADDR, Absolute

The transfer areas are assigned using the hardware identifier that is assigned automatically to the modules and devices. You need the HW identifier for programming the SENDDP and RCVDP blocks (LADDR input). For each HW identifier of the transfer area, a system constant is created in the respective F-CPU. You can assign these system constants to the SENDDP and RCVDP blocks as **absolute** constants.

10.3.7. Parameter LADDR, Symbolic



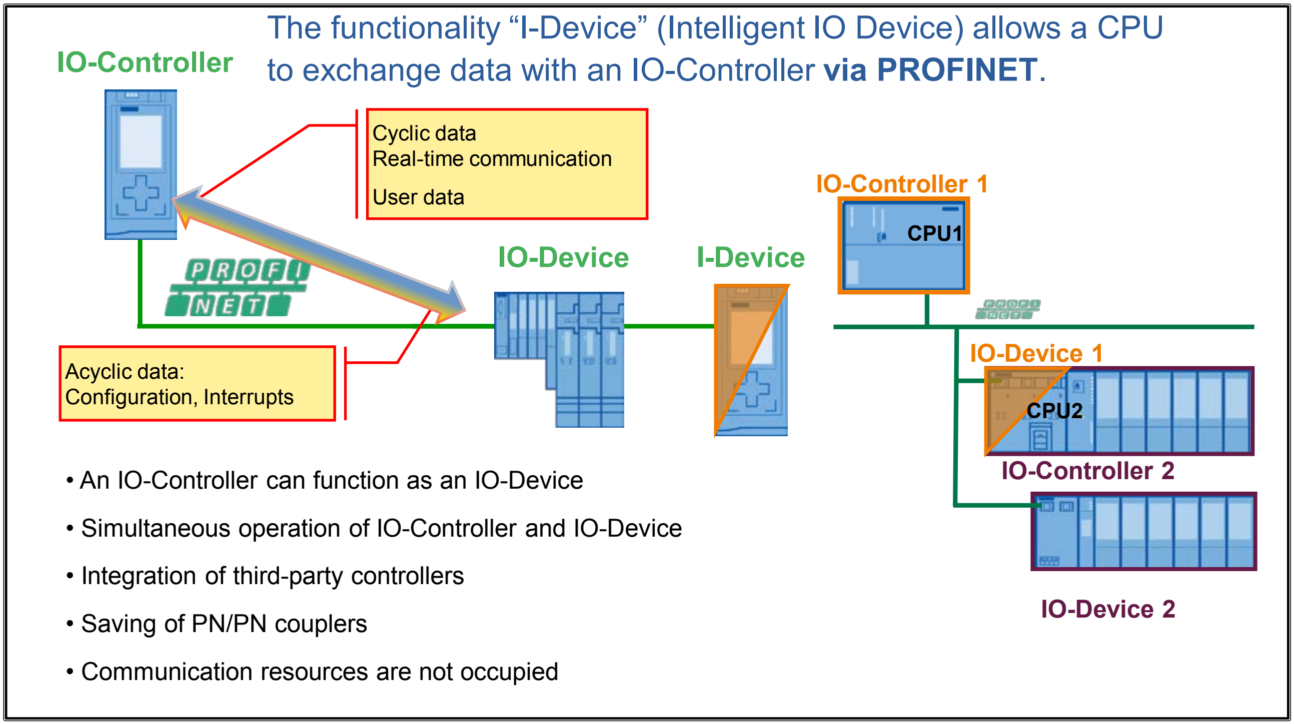
Parameter LADDR, Symbolic

The transfer areas are assigned using the hardware identifier that is assigned automatically to the modules and devices. You need the HW identifier for programming the SENDDP and RCVDP blocks (LADDR input). For each HW identifier of the transfer area, a system constant is created in the respective F-CPU. You can assign these system constants to the SENDDP and RCVDP blocks as **symbolic** constants.

Note

If the amount of data to be communicated is greater than the capacity of the associated SENDDP/RCVDP instructions, a second (or third) SENDDP/RCVDP call can also be used. Configure an additional communication connection via the PN/PN coupler for this. Whether or not this is possible with the same PN/PN coupler depends on the capacity limit of the PN/PN coupler.

10.4. Short and Sweet: PROFINET I-Device



Properties of the I-Device:

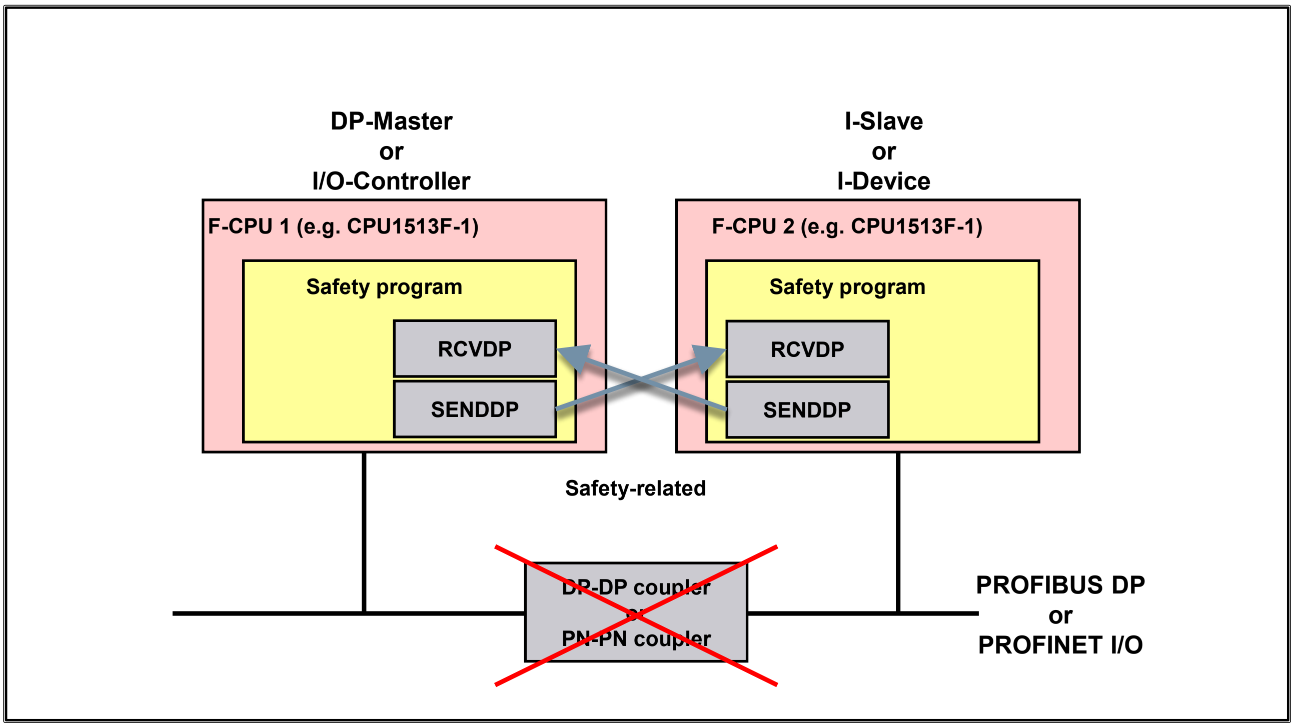
- Decoupling of STEP 7 projects
  Creators and users of an I-Device can have completely separate STEP 7 projects. The interface between the STEP 7 projects is the GSD file. This enables the connection to standard IO controllers via a standardized interface.
- Real-time communication
  The I-Device is made available to a deterministic PROFINET IO system via a PROFINET IO interface and therefore supports Real-Time (RT) and Isochronous Real-Time (IRT) communication.

The I-Device has the following advantages:

- Simple connection of IO Controllers without additional software tools
- Real-time communication between SIMATIC CPUs and to standard IO controllers
- By distributing the computing power among several I-Devices, the required computing power of the individual CPUs and the IO Controller can be reduced.
- Lower communication load through local processing of the process data.
- Clarity through processing of subtasks in separate STEP 7 projects.

10.5. Fail-safe I-Device/Slave Communication

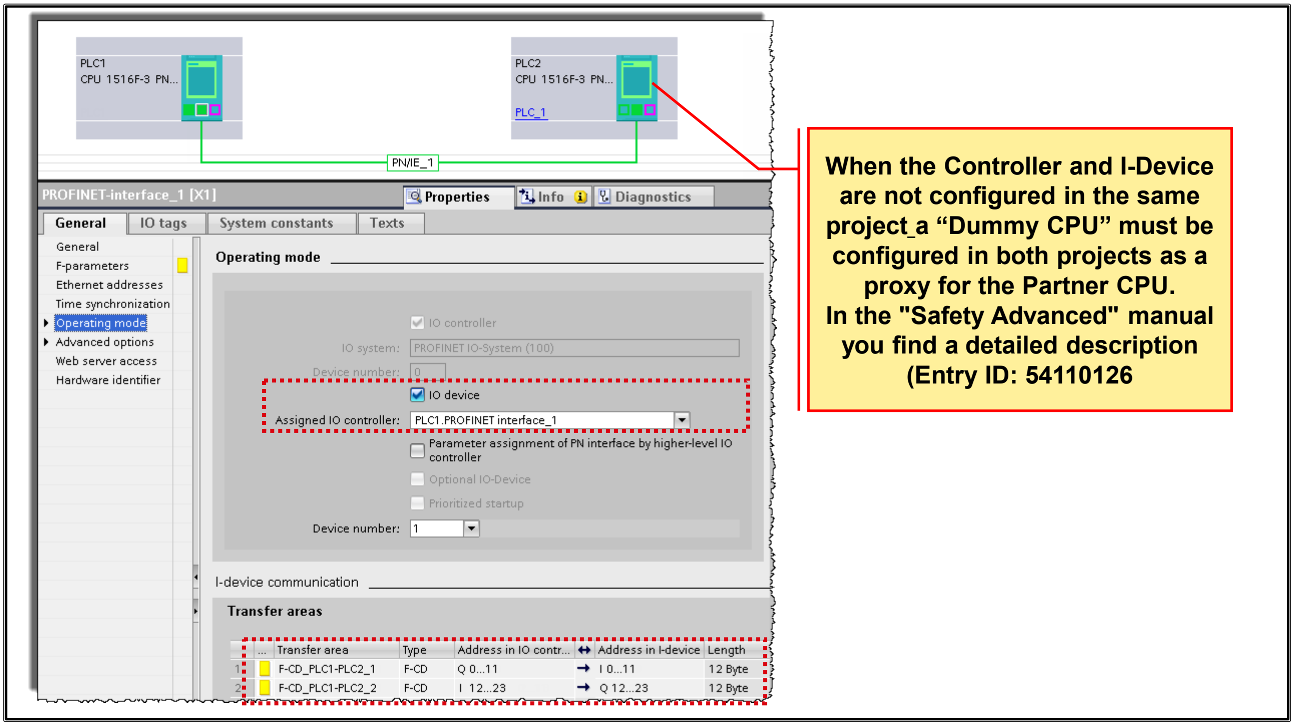
10.5.1. SENDDP / RCVDP Communication Blocks



Intelligent Device (I-Device)

With this functionality, PROFINET allows, in a typical automation solution with several networked controllers, not only communication with lower-level devices as an IO Controller, but also IO communication with other higher-level or centralized controllers as an IO Device. This communication takes place at the same time on the same bus. With an I-Device, the topology becomes leaner and more flexible. It enables the simple connection of controllers from different projects in exactly the same way as the integration of Siemens controllers and third-party controllers within one communication network.

10.5.2. Defining the Operating Mode, Assignment and Transfer Areas for an I-Device



Safety-related IO-Controller-I-Device Communication

The safety-related communication between the safety program of the F-CPU of an IO-Controller and the safety program(s) of the F-CPU(s) of one or more I-Devices takes place – just as in standard communication via PROFINET IO – via IO-Controller- I-Device connections (F-CD). You do not need any additional hardware for the IO-Controller-I-Device communication.

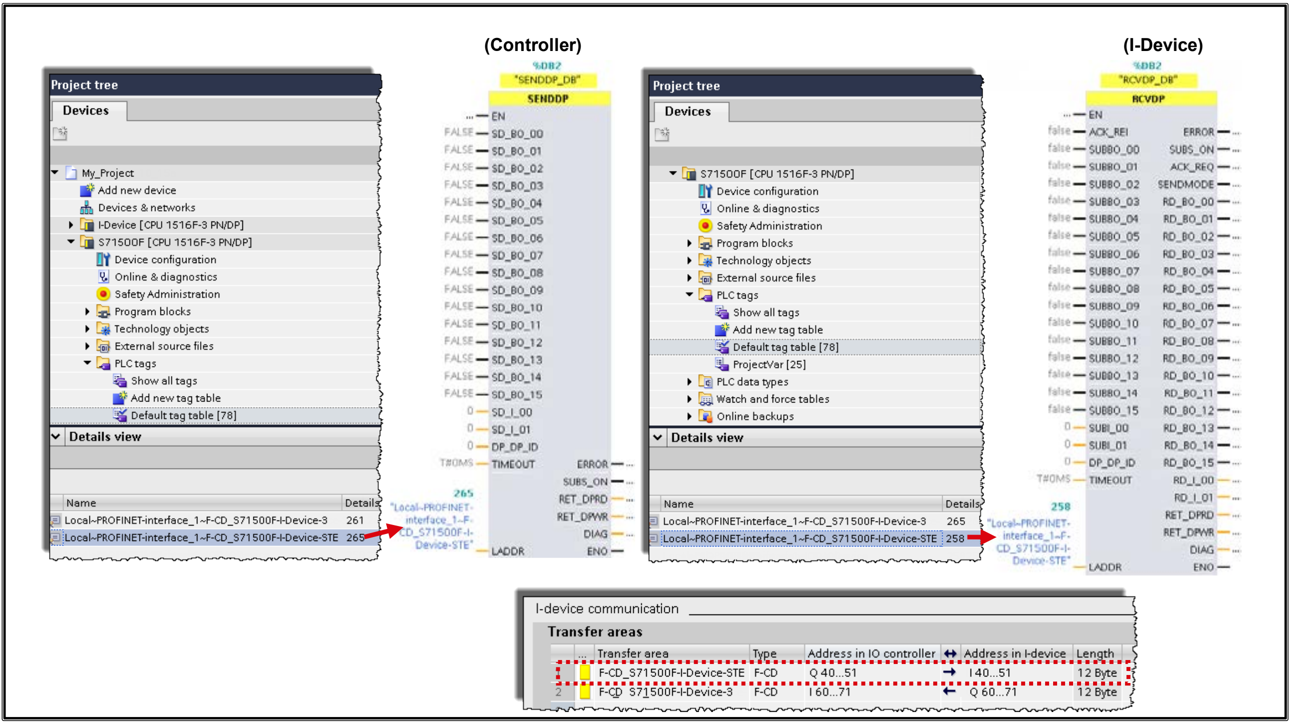
Defining the Operating Mode and Assignment for I-Device

For the Controller, you must set the Property that it is an I-Device. You must assign a controller to the I-Device.

Defining the Transfer Area

For each safety-related communication connection between two F-CPUs, you must configure transfer areas in the Hardware and Network editor. When created, the transfer area receives a name that designates the communication relationship, for example, "F-CD_PLC_2-PLC_1_1" for the first F-CD connection between IO-Controller F-CPU 1 and I-Device F-CPU 2. When a transfer area is created, a system constant with the same name as the transfer area is created both in the F-CPU of the IO-Controller and in the F-CPU of the I-Device. The system constant contains the HW identifier of the transfer area from the perspective of the respective F-CPU. In addition, an acknowledgment connection is created automatically for each F-CD connection.

10.5.3. SENDDP, RCVDP and LADDR Parameter



LADDR Parameter

You assign the HW identifiers (system constants from the standard tag table) of the transfer areas in the safety programs to the LADDR parameter of the SENDDP and RCVDP instructions symbolically.

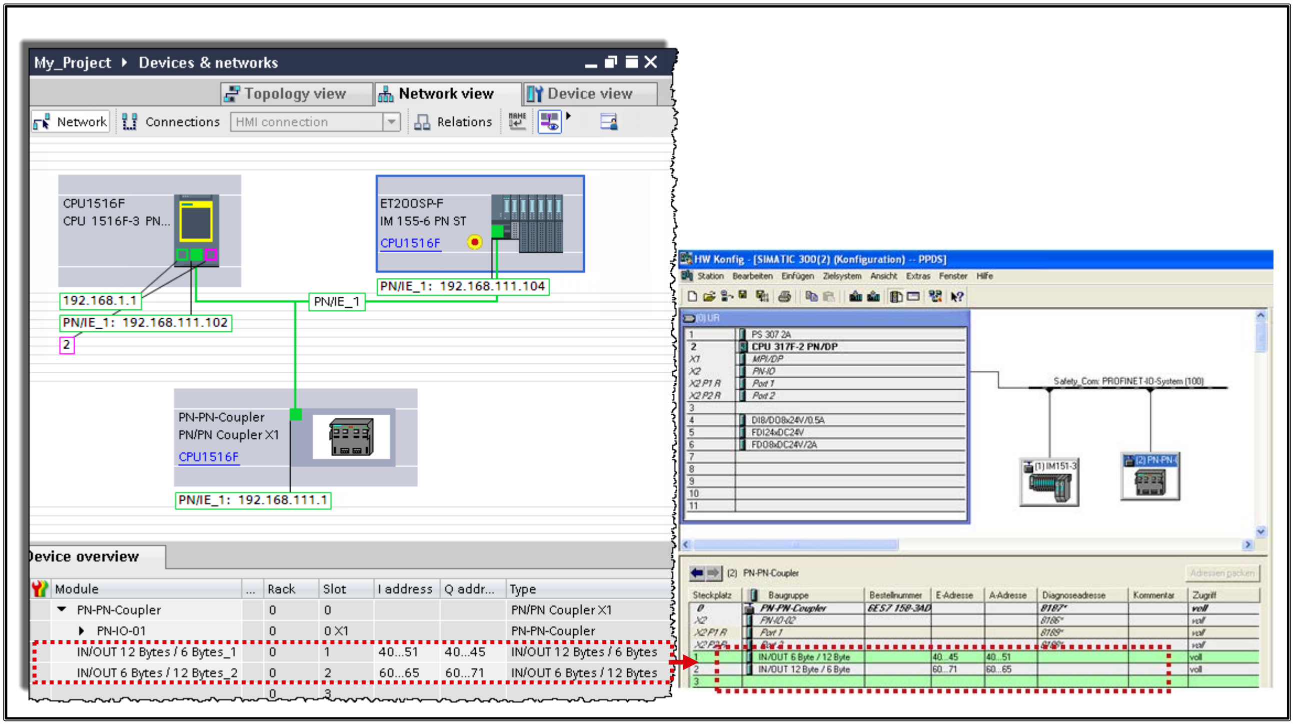
Communication using the SENDDP and RCVDP Instructions

The safety-related communication between the higher-level F-CPU and the I-Device also takes place with the help of the instructions SENDDP for sending and RCVDP for receiving. With them, a fixed amount of fail-safe data of the data type BOOL or INT can be transferred in a fail-safe manner. You can find these instructions in the "Instructions" task card under "Communication".

Note

If the amount of data to be communicated is greater than the capacity of the associated SENDDP/RCVDP instructions, you can use additional SENDDP/RCVDP instructions. Configure additional transfer areas for this. In doing so, heed the maximum limit of 1440 bytes of input data or 1440 bytes of output data for transfer between an I-Device and an IO-Controller. Take into account all other configured safety-related and standard communication connections (transfer areas of type F-CD and CD) in the maximum limit of 1440 bytes of input data and 1440 bytes of output data for transfer between an I-Device and an IO-Controller. In addition, data is allocated for internal purposes so that the maximum limit may be reached sooner. When the limit is exceeded, you receive a corresponding error message.

10.6. Fail-safe Communication with S7 F-Systems



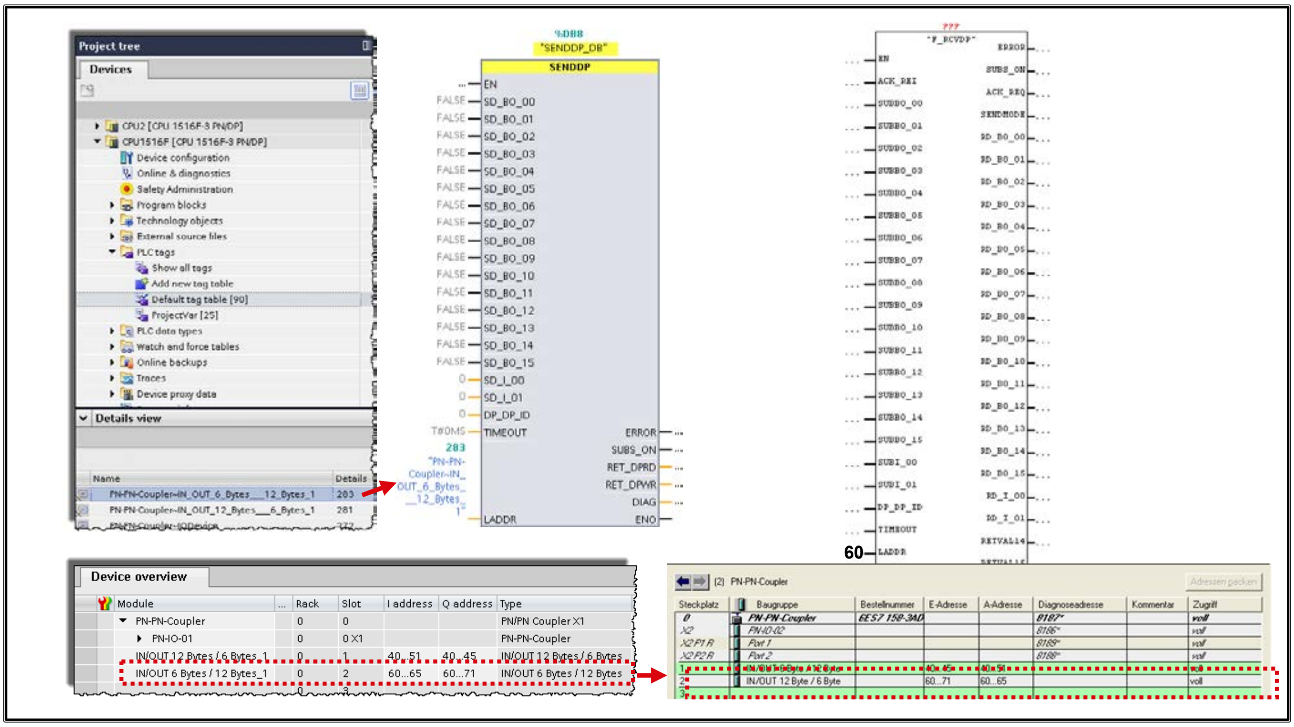
Safety-related Communication with S7 F-Systems

Safety-related communication of F-CPUs in SIMATIC Safety with F-CPUs in S7 Distributed Safety F-Systems is possible as IO-Controller-IO-Controller communication or Master-Master communication using a PN/PN or DP/DP coupler that you insert between the two F-CPUs.

Communication with S7 Distributed Safety

The communication is carried out between SENDDP/RCVDP instruction on the side of STEP 7 Safety Advanced and SENDDP/RCVDP F-application blocks on the side of S7 Distributed Safety.

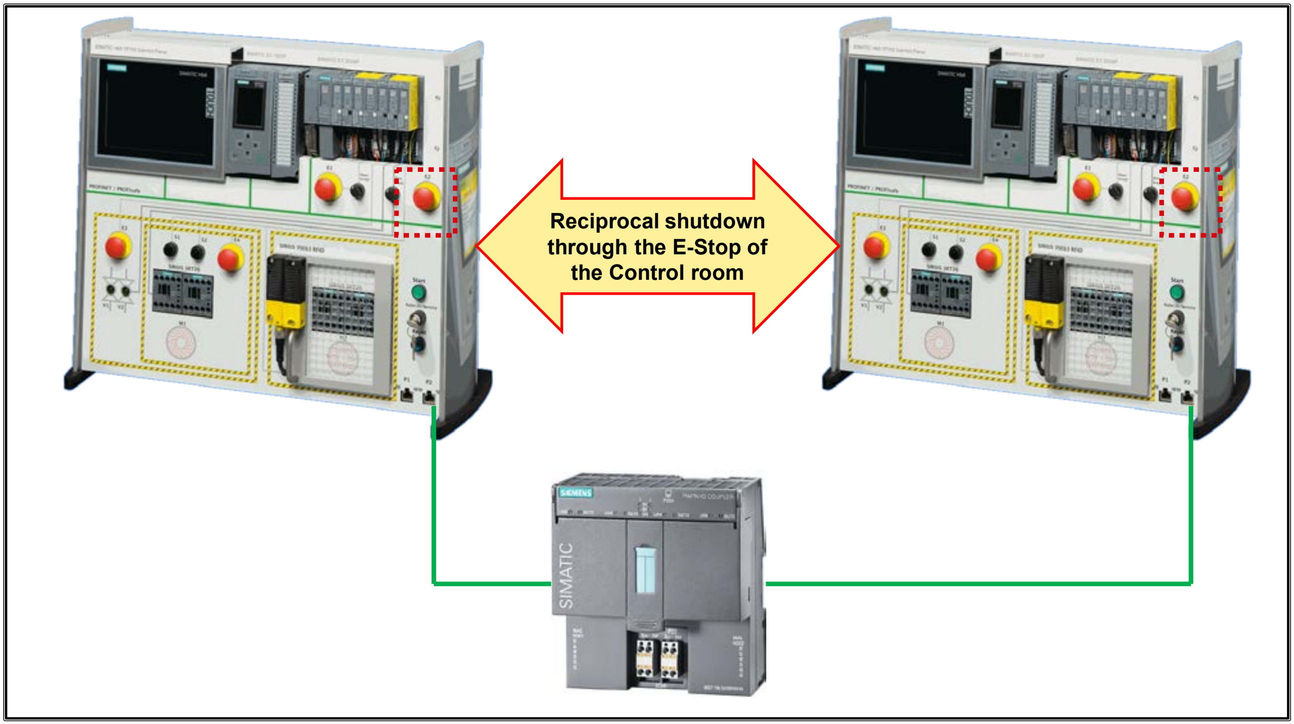
10.6.1. SENDDP, RCVDP and LADDR Parameter



SENDDP, RCVDP and LADDR Parameter

Use the start addresses of the transfer areas for programming an S7-300/400 F-CPU. Use the HW identifiers of the transfer areas for programming an S7-1500 F-CPU.

10.7. Exercise 1: "Total E-STOP" via PN-PN Coupler



Task

Currently, each individual system works separately without a connection to another station.
For this exercise you will set up fail-safe communication between 2 stations. Communication is via PN-PN coupler. Once this is done, it is will be possible to switch off the partner system via the E-Off of the Control Room. The partner system will also be able to do the same thing.

What to Do

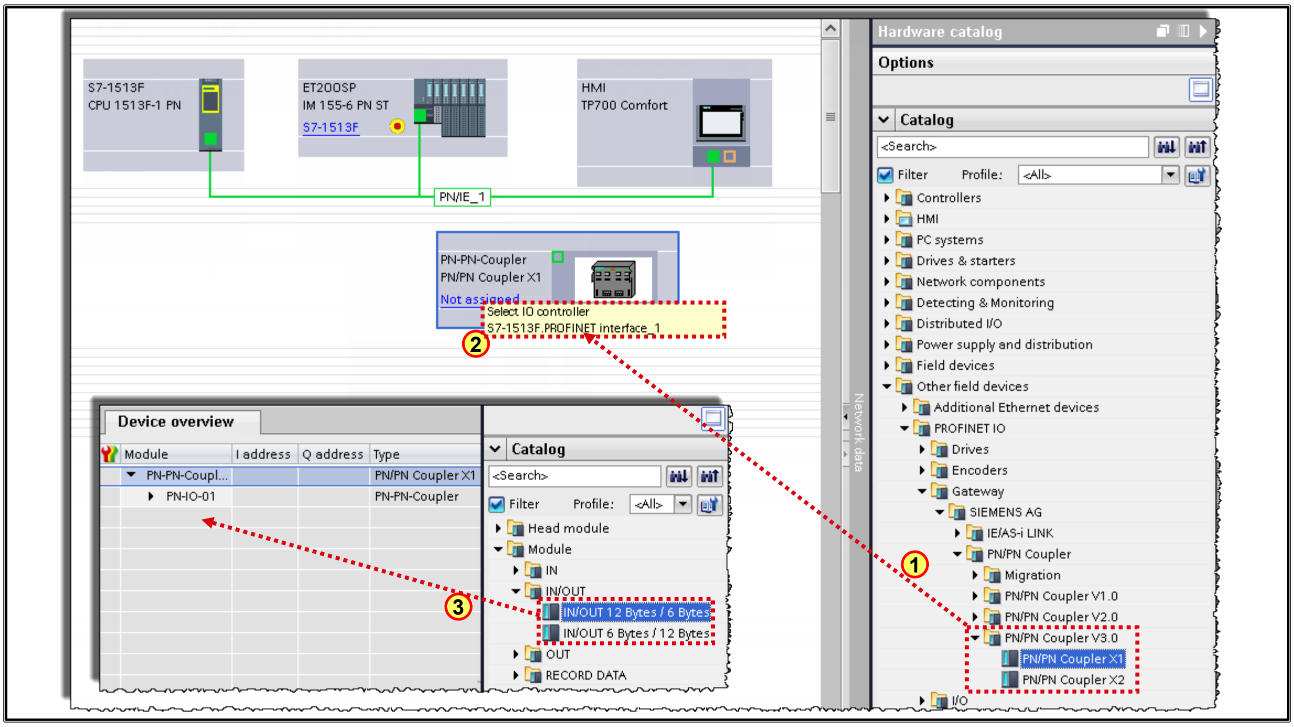
1. Establish a PROFINET connection with the PN-PN coupler.

   Note:

   Coordinate with your partner as to which coupler is used and who uses which interface (X1 or X2).

Continued on the next page

10.7.1. Re: Exercise 1: Configuring the PN-PN Coupler and Transfer Areas



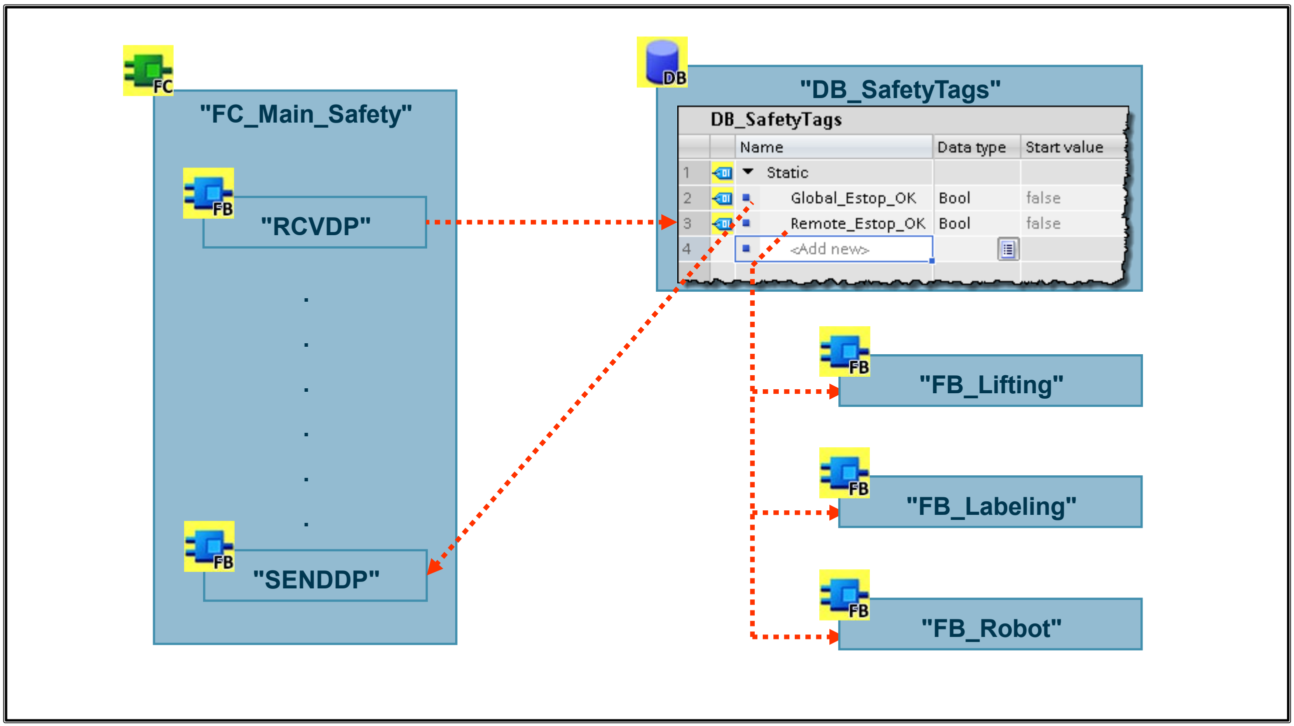
What to Do

1. Using drag & drop, copy the correct PN-PN coupler version and interface into your Network view.
2. Network the coupler with your CPU and adjust the device name and the IP address (see training case supplement)
3. Configure a Send module (IN/OUT 6Byte/12Byte)
   and a Receive module (IN/OUT 12Byte/6Byte)

   Caution: Coordinate with your partner on which slot the Send module and Receive module are configured!
4. Save and download your project.
5. As soon as the partner station has also been loaded, the entire station should be error-free. If not, check the parameterization and the connection of the PN-PN coupler again (both groups!)

Continued on the next page

10.7.2. Re: Exercise 1: Configuring RCVDP and SENDDP

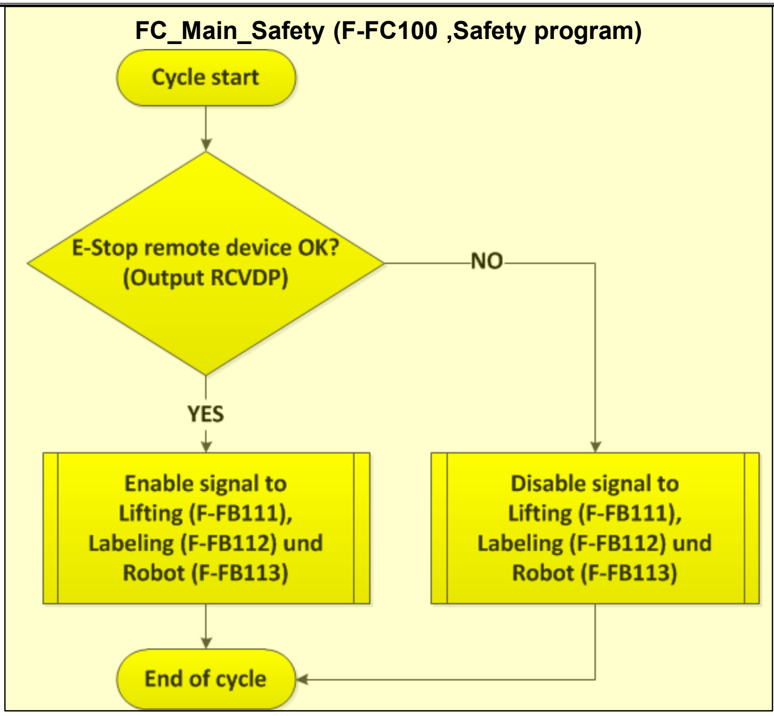


6. Generate a new tag "Remote_Estop_OK" in your fail-safe global data block "DB_SafetyTags" (DB101).
7. Call the "SENDDP" send block and the "RCVDP" receive block at the correct location in your safety program.
8. Connect your E-Off signal of the Service Control Room ("DB_SafetyTags.Global_Estop_OK") to the first send bit ("SENDDP.SD_BO_00").
9. At the first receive bit ("RCVDP.RD_BO_00") connect the E-Off signal of the partner station ("DB_SafetyTags.Remote_Estop_OK").
10. Parameterize the remaining necessary interfaces of the send and receive block according to your coupler configuration.

    Note: You may have to coordinate with your partner.

Continued on the next page

10.7.3. Re: Exercise 1: Flow Chart



11. The global enable signal of the partner station ("DB_SafetyTags.Remote_Estop_OK") is now to be included in all system sections. Expand the blocks "FB_Lifting", "FB_Labeling" and "FB_Robot" to include this new enable condition.

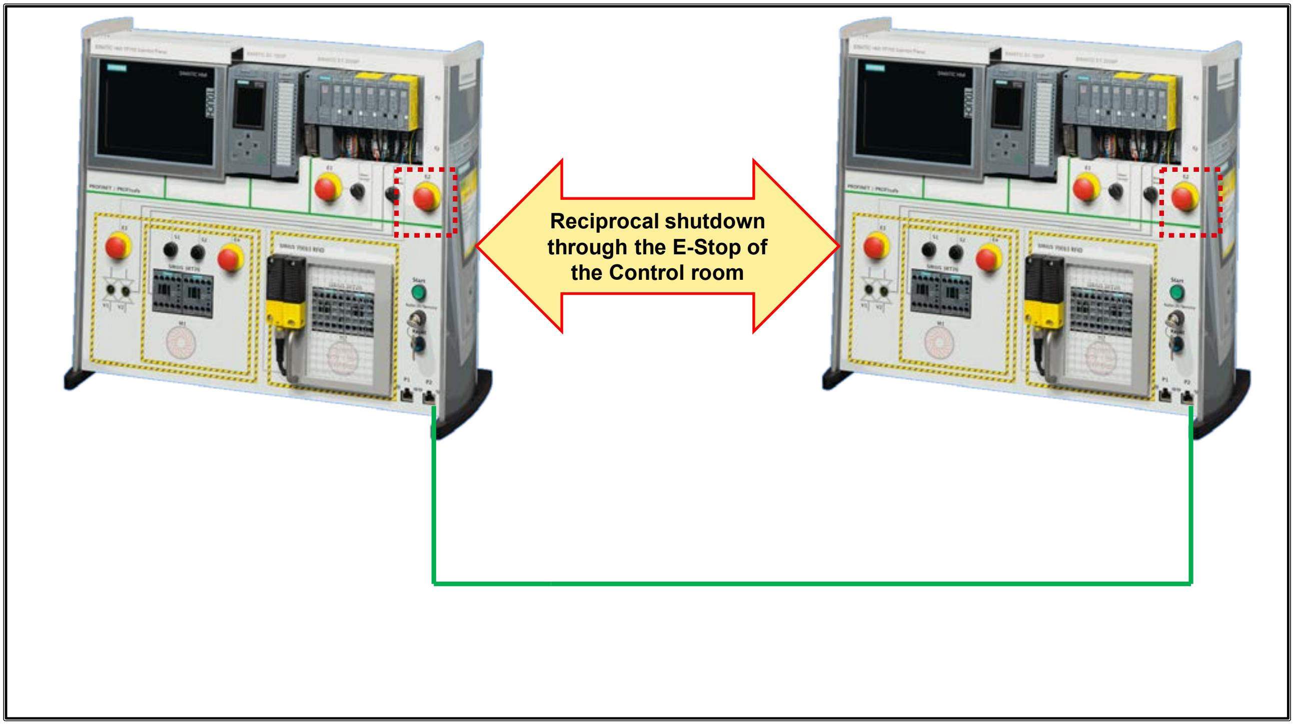
12. Download all blocks into the CPU.

13. Save your project and test the functionality.

Result:

Both stations should now be able to transfer the system of the partner into the safe state (shutdown) via the E-Off of the Service Control Room (E2).

10.8. Exercise 2 (Optional): "Total E-STOP" via I-Device



Task

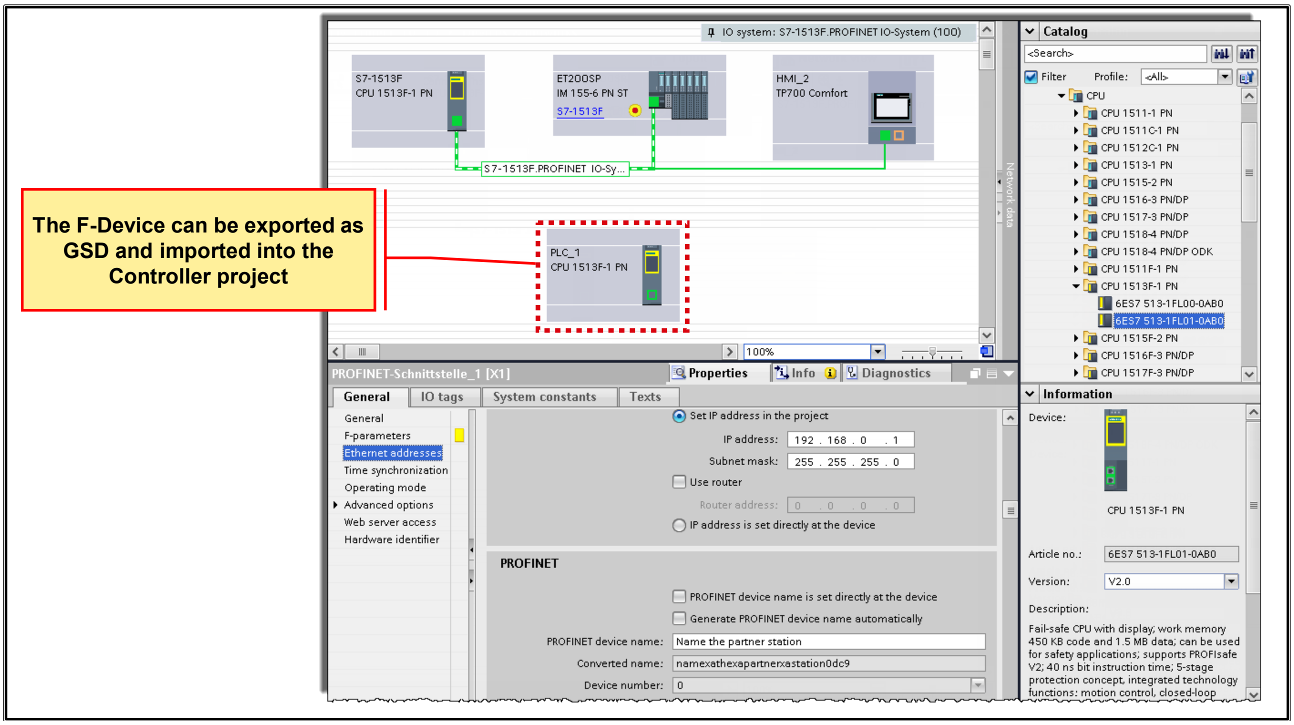
The existing F-communication via PN-PN coupler will be replaced with fail-safe I-Device communication. It will still be possible to shut down the partner system via the Control room.

What to Do

1. Establish a direct PROFINET connection to the Partner CPU.

Continued on the next page

10.8.1. Re: Exercise 2: Correctly Configuring a Dummy CPU



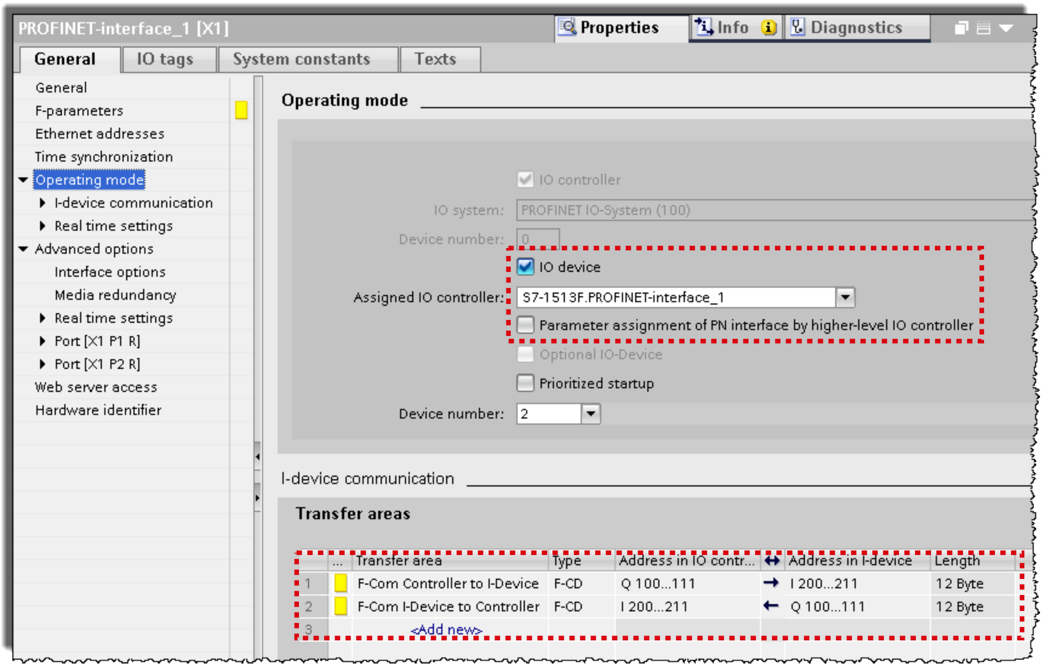
2. Define which group (CPU) is "I-Device" and which group (CPU) is "Controller".

   Note:
   The next steps are not always relevant for both groups. With the description "I-Device" or "Controller" you recognize which group has to do this step of the exercise.

3. **I-Device:** Configurate the partner CPU in your project as "Dummy CPU".

Continued on the next page

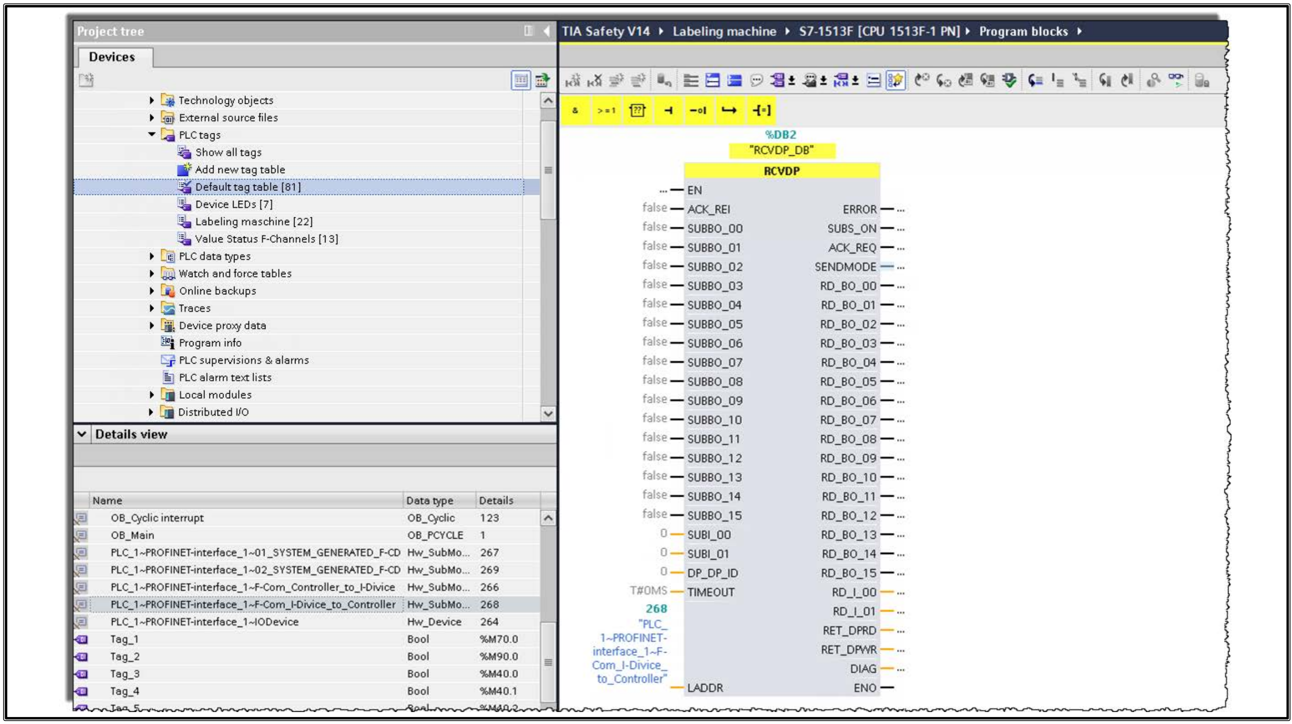
10.8.2. Re: Exercise 2: Defining the Transfer Areas



4. **I-Device:** Activate the I-Device functionality of **<u>your</u>** CPU.
5. **I-Device:** Define the required transfer areas for sending and receiving fail-safe data. You can use the process image in the screenshot.
   IMPORTANT: Pay attention with the communication direction (arrows) and use clear names!
6. **I-Device:** Check that the option
   "Parameter assignment of PN interface by higher-level IO controller" is **NOT** active.
7. **I-Device:** Export the I-device as a GSD file. Proceed as described in the STEP 7 help under "Configuring an I-device".
8. **Controller:** Import the GSD file in the project with the IO Controller. Proceed as described in the STEP 7 help under "Installing a GSD file".
9. **Controller:** Insert the I-device from the "Hardware catalog" task card into the project with the IO Controller.
10. **Controller:** Assign the F-CPU of the IO Controller to the I-device.

Continued on the next page

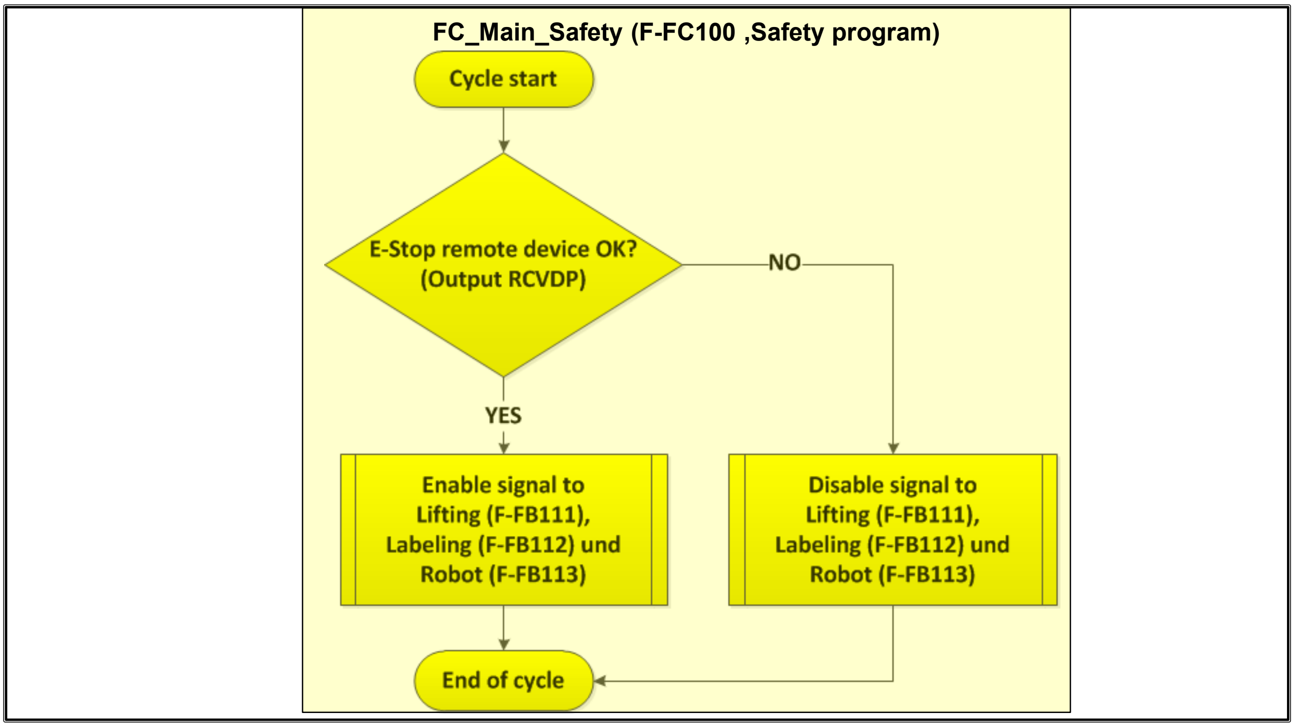
10.8.3. Re: Exercise 2: Addressing the Transfer Areas Symbolically



9. Parameterize the "SENDDP" and "RCVDP" blocks. You will find the HW identifier of the transfer areas in the standard tag table of your CPU.

Continued on the next page

10.8.4. Re: Exercise 2: Flow Chart



10. The functionality should be the same as in Exercise 1. The global enable signal of the partner station ("DB_SafetyTags.Remote_Estop_OK") will be included in all system sections. Expand the blocks "FB_Lifting", "FB_Labeling" and "FB_Robot" to include this new enable condition.

11. Download all into the CPU.

12. Save your project and test the functionality.

Result:

Both stations should now be able to transfer the system of the partner into the safe state (shutdown) via the E-Off of the Service Control Room (E2).

Contents

11

11. Appendix: Migration

At the end of the chapter the participant will ...

… be familiar with the particularities of the migration from Distributed Safety to Safety Advanced

… be familiar with the particularities of the migration from a 300F to a 1500F

… be familiar with the particularities of upgrading a Safety Advanced V1x to a Safety Advanced V14 project

11.1. Migration of Distributed Safety to STEP 7 Safety Advanced

11.1.1. Structure Change

In STEP 7 Safety Advanced V14, you can continue to use projects from S7 Distributed Safety V5.4 SP5.

Note: The safety program is only compiled if you enter the F-program password! If the password is not entered, only the standard user program is compiled!

Migration of Projects from S7 Distributed Safety V5.4 SP5 to STEP 7 Safety Advanced V15

In STEP 7 Safety Advanced V15, you can continue to use projects with safety programs which you created with S7 Distributed Safety V5.4 SP5. For this, you must have compiled the projects in S7 Distributed Safety V5.4 SP5 and then migrate them.

11.1.2. Acceptance?

As a result of the migration, you will have a complete STEP 7 Safety Project, which has **retained** the **program structure of S7 Distributed Safety and the collective F-signatures**.

As a result, the migrated project **does not have to be accepted again** and can be downloaded directly into the F-CPU without a recompilation.

The acceptance [safety] summary (printout) created with S7 Distributed Safety V5.4 SP5 retains its validity.

Only when the migrated project is **compiled again** with STEP 7 Safety Advanced V15, does it receive the **new program structures and a new collective F-signature.**

After the Migration

F-blocks from the S7 Distributed Safety (V1) F-library are converted into instructions which STEP 7 Safety Advanced provides. The migrated project does not have to be accepted again and can be downloaded into the F-CPU unchanged as long as it was not edited after the migration.

Safety Summary (Printout)

You cannot create a safety summary in STEP 7 Safety Advanced V15 for a migrated project. The summary of the project which was created with S7 Distributed Safety V5.4 SP5 and the associated acceptance documents continue to be valid because the collective F-signature was retained.

Note

After the migration of an SM 326; DI 24 x DC 24V (6ES7 326-1BK01-0AB0 and 6ES7 326-1BK02-0AB0), the following error message may be output when the hardware configuration is compiled: "F_IParam_ID_1: Value outside permissible range".

Solution:

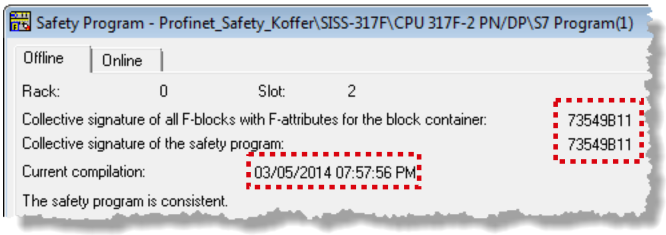
Delete the module and insert the module again. The error message "Internal error during CRC calculation. The CRC (F_Par_CRC) of the module (x) does not match the calculated value (y)." is a follow-on error and is eliminated when the original error is eliminated.

11.1.3. Signature

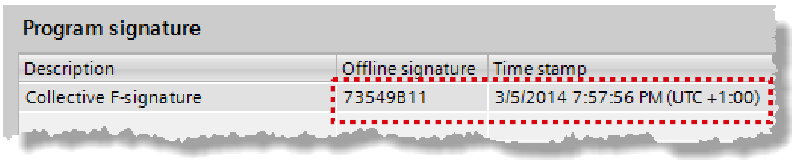
Download of the migrated project without changes

The signature of the migrated project is equal to the signature of the original project.

- Dialog in **Distributed Safety**:



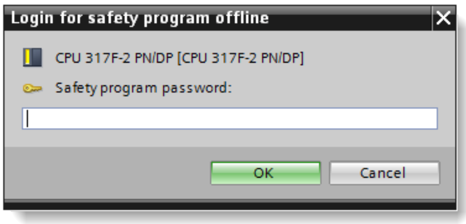
- Dialog in **Safety Advanced V14**:

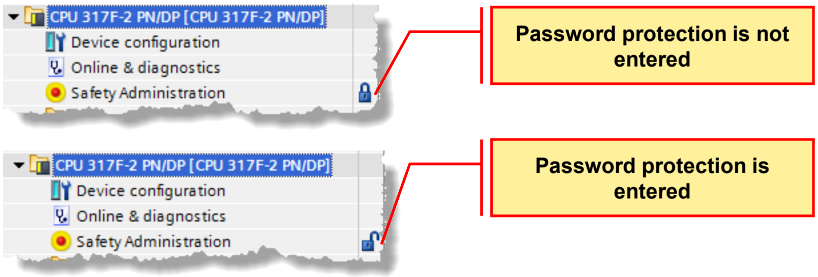


11.1.4. Download without Changes

Download of the migrated project without changes

When the project is compiled, the password for the safety program must not be entered!





11.1.5. Recompiling the Program

Compiling the migrated project

After the safety program is compiled, the structure changes and with that also the signature of the safety program.

- Before compilation:

Offline signature	Time stamp
73549B11	3/5/2014 7:57:56 PM (UTC +1:00)

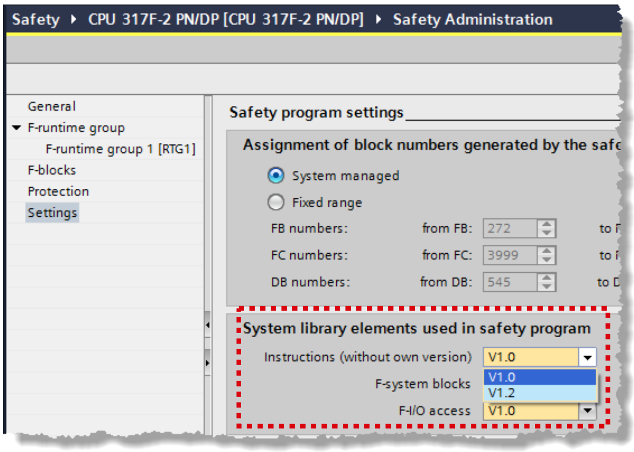
- After compilation:

Offline signature	Time stamp
9A8138AF	3/5/2014 9:18:01 PM (UTC +1:00)

11.1.6. Versions in the Safety Program (1)

Recommendation if changing the safety program:

Before you compile with STEP 7 Safety Advanced V14 for the first time, set **the elements of the system library used in the safety program** to the latest available version respectively. You do this in the Safety Administration Editor in the section “Settings".



Using the Latest Versions used in the Safety Program

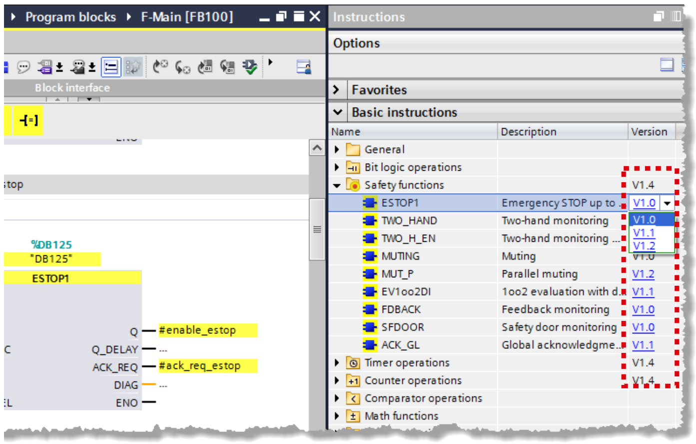
If you want to expand the migrated safety program, we recommend that you set the elements of the system library used in the safety program to the latest available version before you compile with STEP 7 Safety Advanced V15 the first time. You do this in the Safety Administration editor in the section "Settings".

11.1.7. Versions in the Safety Program (2)

Recommendation if changing the safety program:

Before you compile with STEP 7 Safety Advanced V14 for the first time, set the version of the **instructions used** to the latest available version.

Please pay attention to the information about the instruction versions for the respective instruction.



If you change the version of an instruction, you must compile twice in order to get a consistent safety program.

Using the Latest Instruction Versions

If you want to expand the migrated safety program, we recommend that you set the version of the instructions used to the latest available version respectively before you compile with STEP 7 Safety Advanced V15 the first time. Please pay attention to the information about the instruction versions for the respective instruction.

Compiling the Migrated Safety Program

When compiling the migrated project with STEP 7 Safety Advanced V15, the previous program structure (with F-CALL) is transferred into the new program structure of STEP 7 Safety Advanced V15 (with Main-Safety-Block). This changes the F-collective signature and the safety program must undergo acceptance again, if necessary.

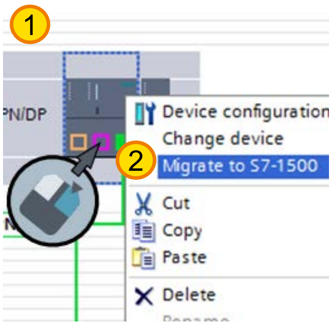
Note

Please note that the compiling of the migrated safety program could result in an extension of the runtime of the F-runtime group(s) and an increased work memory need of the safety program.

11.2. Migrating S7-300F to S7-1500F

Open and compile project with “Classic” hardware 1

Start migration to S7-1500 2



Migrating an F-CPU from S7-300F to S7-1500F

To migrate an F-CPU S7-300/400 onto an F-CPU S7-1500, proceed as with the migration of a standard CPU S7-300/400 onto a CPU S7-1500. After the migration note non-automatable actions.

- Creating an F-runtime group and assigning it to the Main-Safety-Block.
- The hardware configuration of the initial F-CPU is not automatically transferred to an S7-1500 F-CPU. Implement the hardware configuration of the new CPU manually after migration.

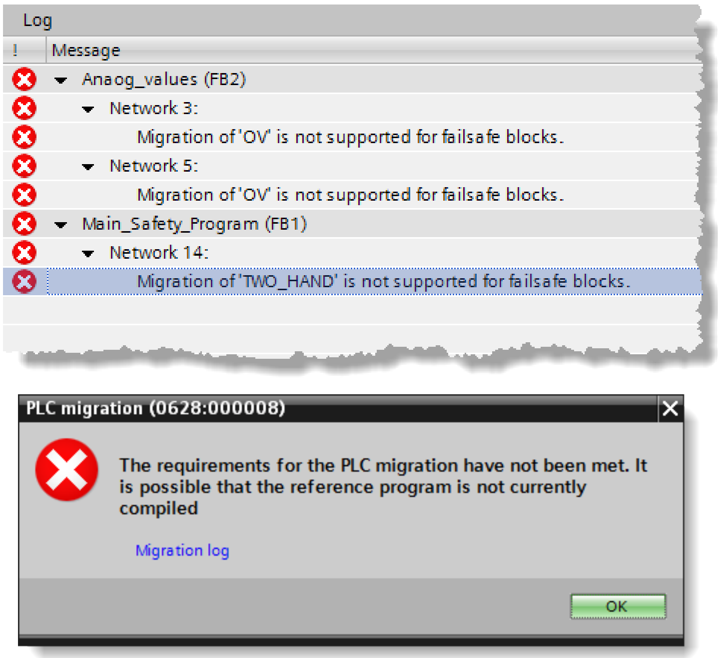
11.2.1. Instructions Not Supported

Instructions not supported

- OV
- MUTING
- TWO_HAND
- WR_FDB
- RD_FDB
- OPN
- SENDS7
- RCVS7

Caution:

If in the project with a “Classic” F-CPU, one of the blocks is used, the PLC migration cannot be carried out.
Adjust the block calls in the project!



Migrating an F-CPU from S7-300F to S7-1500F

Compile the safety program and eliminate any compilation errors displayed.

Note

A new acceptance must be carried out following F-CPU migration.

11.2.2. Changes to the Programming

Data types not supported

- DWORD

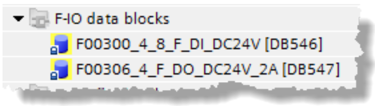
F-runtime group communication is not supported

- When using the S7-1500, a data exchange between two F-runtime groups is currently not possible

Changes to the names of F-I/O DBs

- The symbolic names of F-I/O DBs change after the migration. The names must be manually adjusted at the point of use.

S7-300 before Migration:



S7-1500 after Migration:

Changes to the Safety Program Programming

- F_GLOBDB.VKE0/1 replaced by FALSE/TRUE.
- The readable values from the F_GLOBDB replaced by the F-runtime group information DB.
- The QBAD_I_xx or QBAD_O_xx tag replaced by the value status.

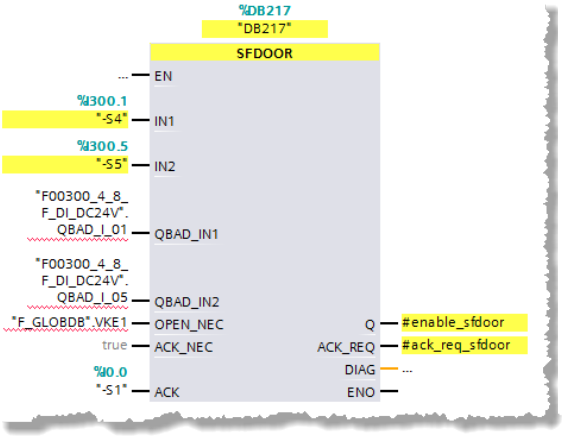
F-runtime group communication is not supported.

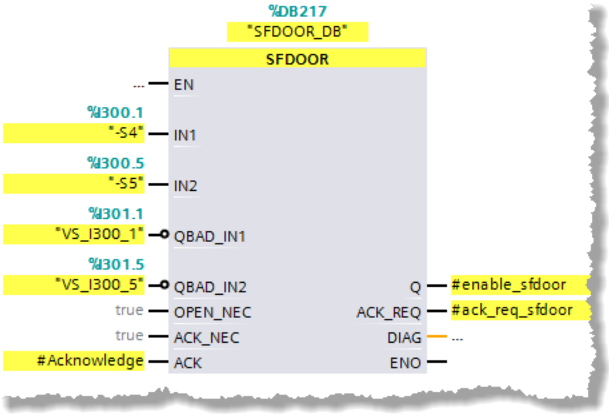
11.2.3. Changes to the Safety Functions (1)

Changes to the Safety Program Programming

- F_GLOBDB.VKE0/1 replaced by FALSE/TRUE
- The readable values from the F_GLOBDB are replaced by the F-runtime group information DB.
- The QBAD_I_xx or QBAD_O_xx tag replaced by the value status.

After migration to S7-1500: → changed programming

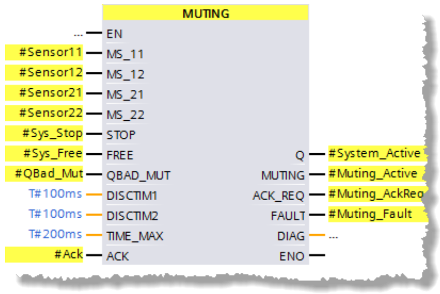


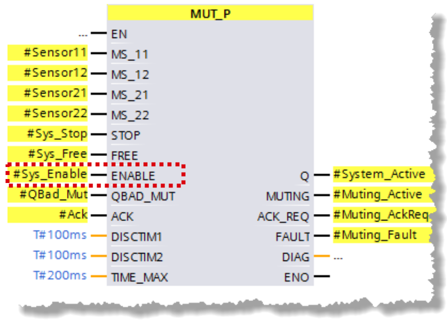


11.2.4. Changes to the Safety Functions (2)

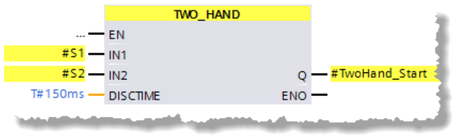
Instructions not converted

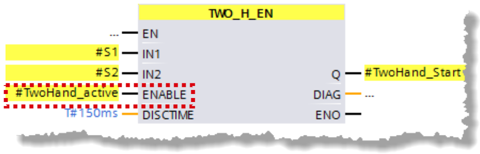
- Functions were expanded and can be implemented identically through successor functions. The adjustment must however be done manually.
  - MUTING → MUT_P (MUT_P additionally offers a FREE function)



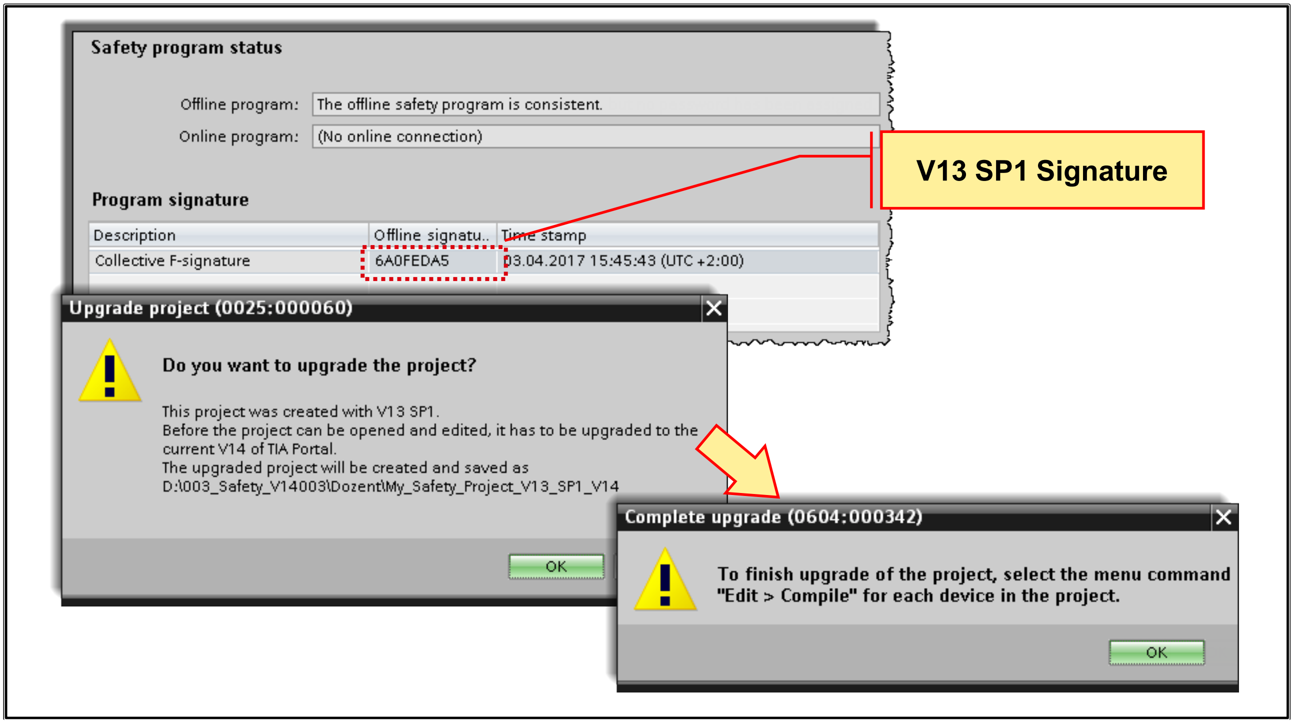


  - TWO_HAND → TWO_H_EN (Successor additionally offers an enable input)





11.3. Upgrading Projects from STEP 7 Safety V13 SP1 to V15

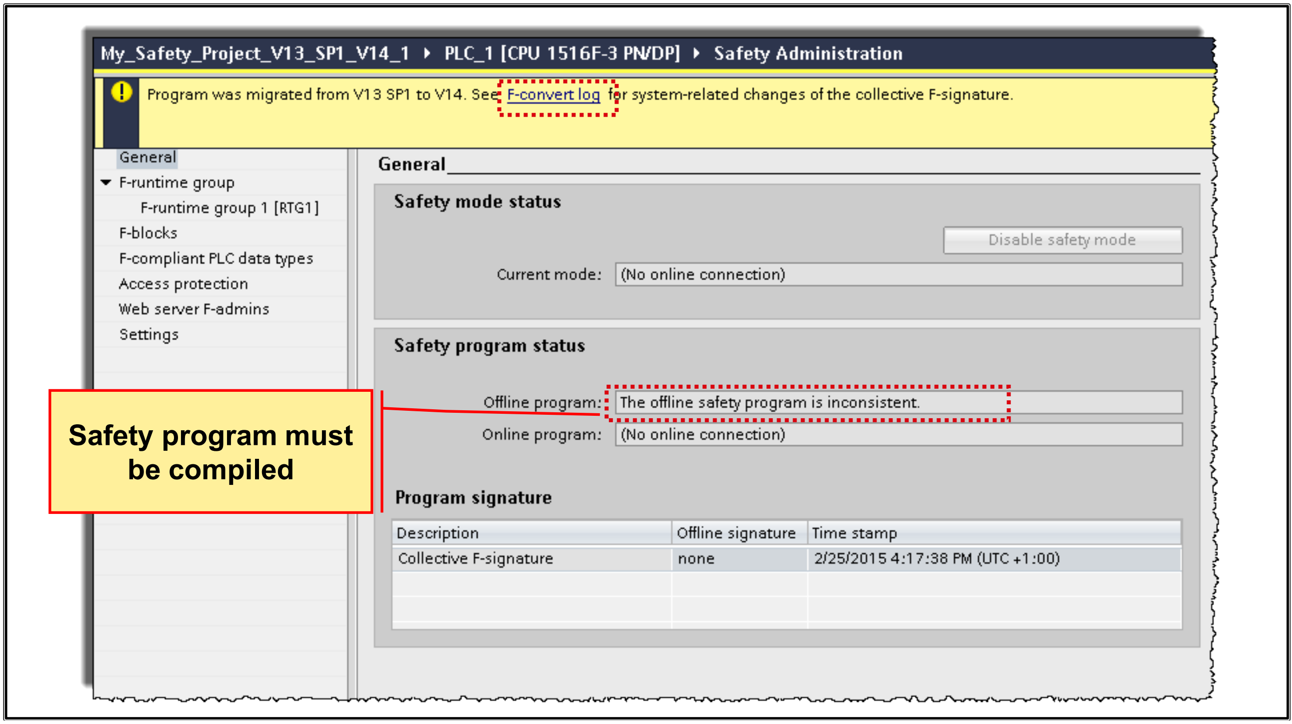


If you want to continue to work with a project from STEP 7 Safety V13 SP1, you must first upgrade the project to STEP 7 Safety V15.

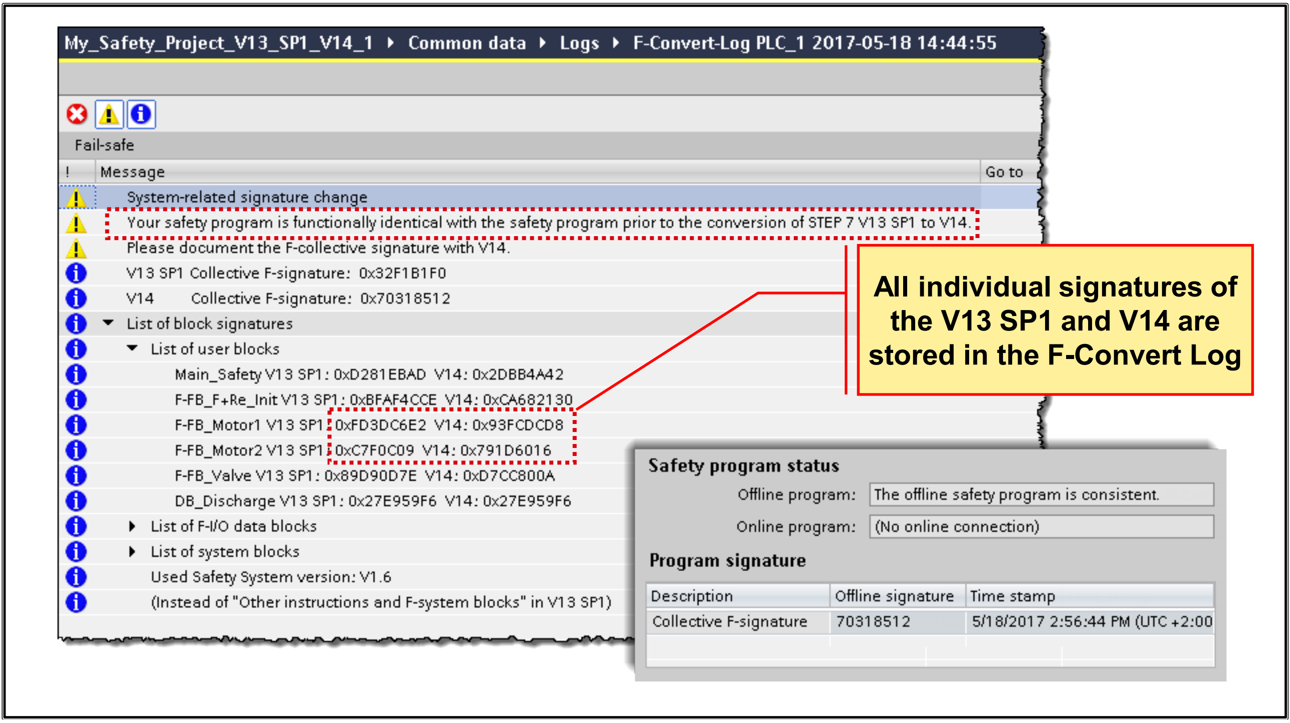
Perform the upgrade following the usual procedure for STEP 7. After upgrading to V15, you have to compile your safety program.

(S7-300/400): After compilation, the safety program is consistent and the collective F-signature of the migrated safety program corresponds to the collective F-signature of the safety program from V13 SP1. Acceptance of changes is not required.

11.3.1. New Compilation is Required



11.3.2. F-Convert Log

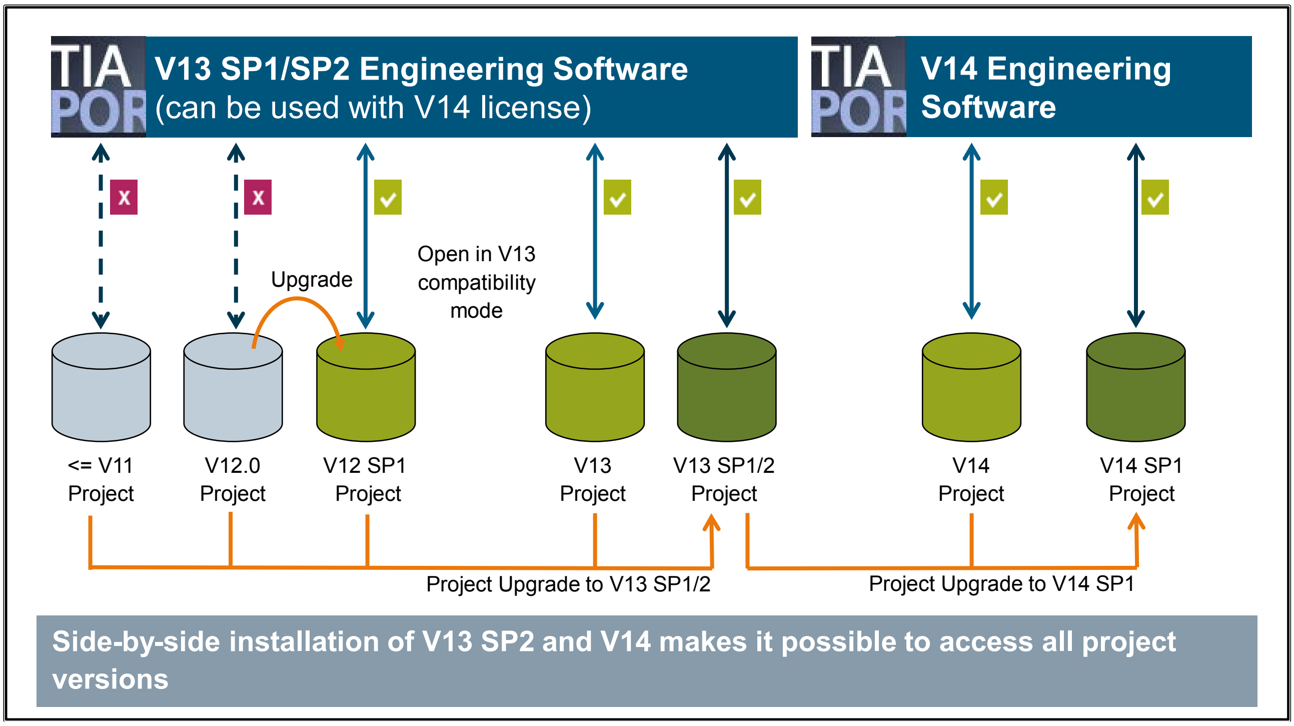


(S7-1200/1500): After compiling, your safety program is consistent and the collective F-signature of the migrated safety program has changed for system reasons. The new collective F-signature of the safety program with STEP 7 Safety V15 replaces the former collective F-signature of the safety program with STEP 7 Safety V13 SP1.

You can find an overview of all system-related changes under "Common data/Protocols/F-Convert Log+CPU name+time stamp". One of the system-related changes is that STEP 7 Safety V15 SP1 automatically replaces versions of instructions no longer supported with new, functionally identical versions. The overview contains a comparison of the previous signatures with STEP 7 Safety V13 SP1 to the new signatures with STEP 7 Safety V15 SP1 and displays the automatically changed instruction versions. Print out the overview and store this printout with your acceptance documents or your machine documentation. Change acceptance is not required, since the "Collective F-signature with STEP 7 Safety V13 SP1" contained in the overview matches the collective F-signature in your current acceptance documents.

Keep in mind that existing change histories are not upgraded. All previous entries are deleted after the upgrade. If necessary, print out the change log before you upgrade.

11.4. Upgrading STEP 7 Safety Projects before V13 SP1

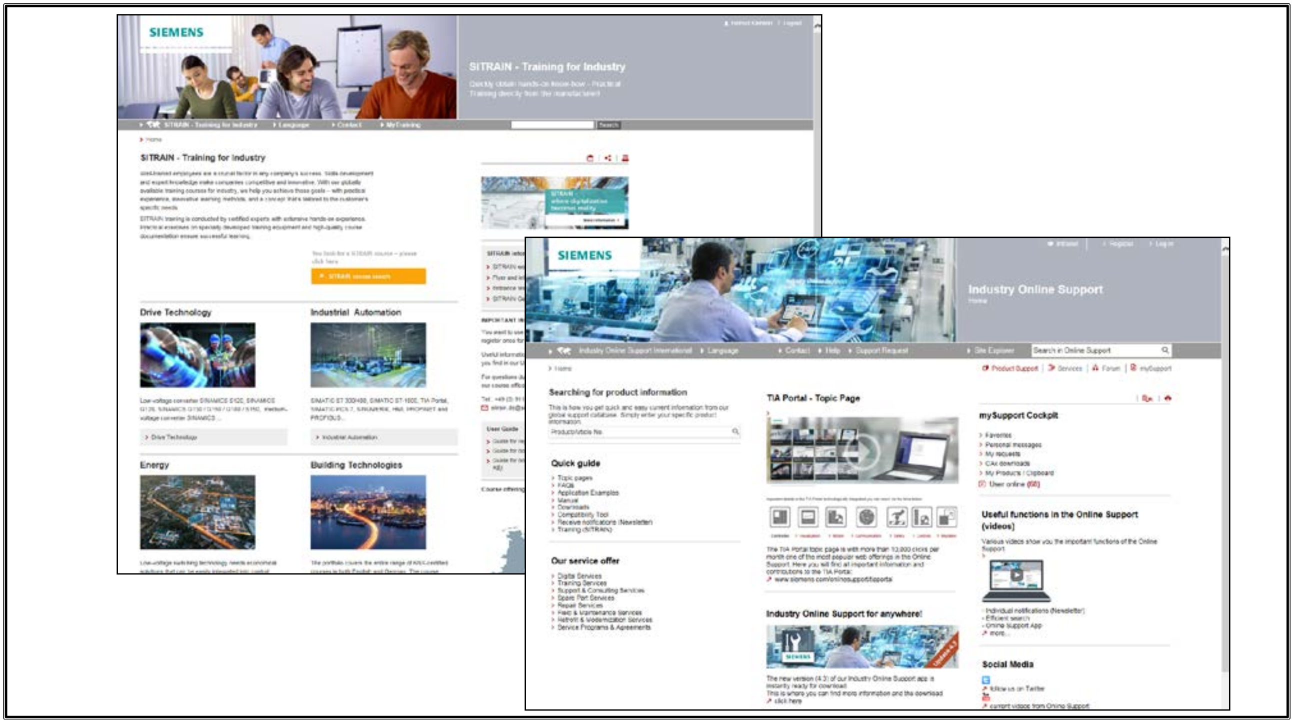


Projects of earlier versions must be upgraded to the V13SP1/SP2 version. This can be done with the help of the V13SP1/SP2 version which can be installed alongside V15.

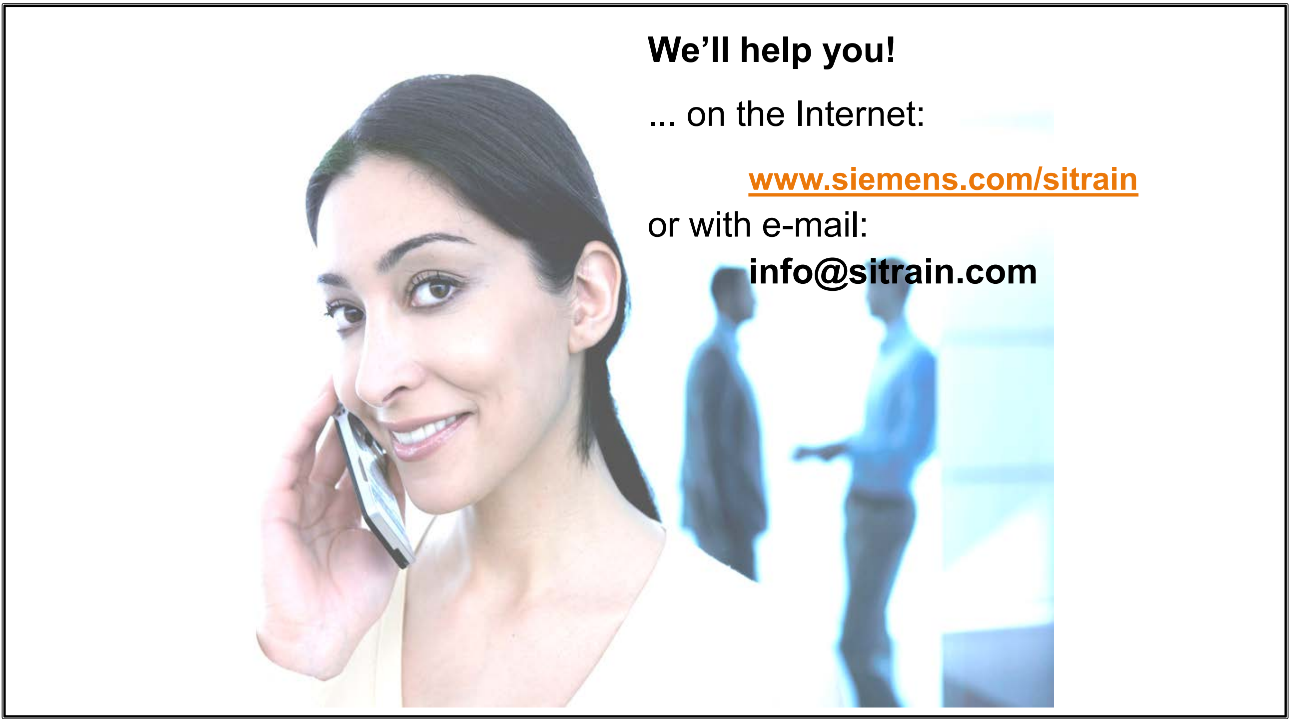
Contents

12

12. Training and Support



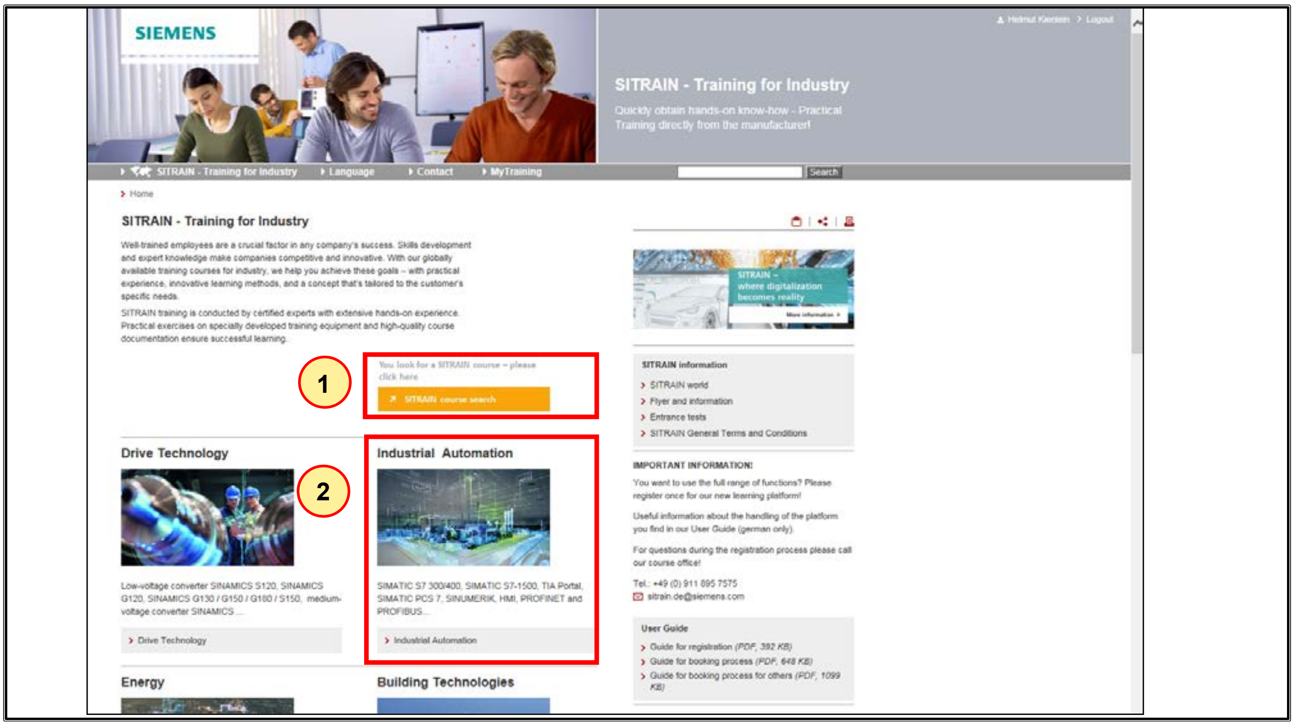
12.1. Any Questions on our Training Courses Offered??



General Information

We'll be glad to help you regarding any questions on our training courses offered.

12.2. www.siemens.com/sitrain



The complete range of courses offered can be accessed via the following links:

www.siemens.de/sitrain or

www.siemens.com/sitrain

Course Search

1 The course search permits the user to find the required courses by applying different search filters such as keyword, target group, etc. The filters can also be combined.

Course Catalog

The course catalog permits you to find the required course via learning paths or via the Siemens Mall structure.

Top Links

Various courses, e.g. SIMATIC S7-1500 solution line, etc., can be reached directly via the top links.

2

> Home > Industrial Automation > Automation Systems > SIMATIC Industrial Automation Systems

SIMATIC Industrial Automation Systems

Consistent and efficient

A centerpiece of our comprehensive range of products and services for industrial automation is SIMATIC, a unique, consistent system of first-class products for every field of application, in all industries. Regardless of whether it's manufacturing and process automation or solutions for infrastructure tasks: with SIMATIC we make an important contribution toward improving your productivity.

SITRAIN has a portfolio of training courses that are perfectly matched to your requirements and your plant's lifecycle.

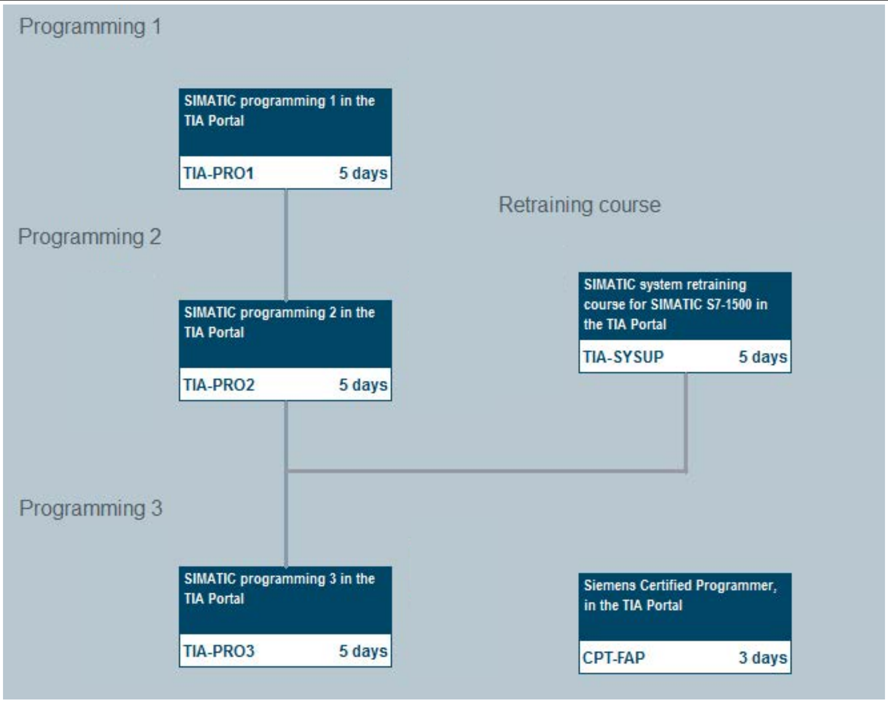
SIMATIC S7 TIA Portal

- On the path to the digital enterprise - discover your potential with training courses for SIMATIC S7-1500 training in the TIA Portal
- SIMATIC TIA Übersicht
- SIMATIC S7 Programming in the TIA Portal
- SIMATIC S7 Service Training in the TIA Portal
- SIMATIC Safety Integrated in the TIA Portal
- SIMATIC S7 Engineering Tools in the TIA Portal
- SIMATIC Technology im TIA Portal
- SIMATIC S7-1200

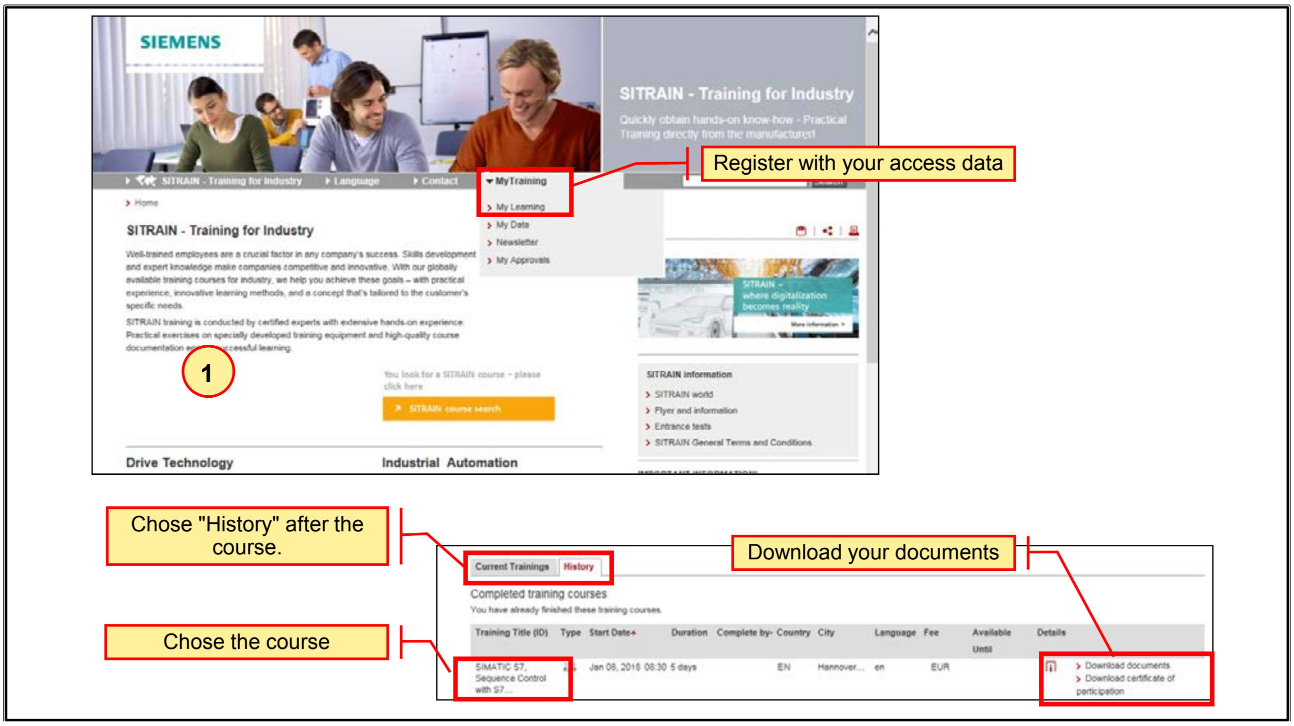
SIMATIC S7-300/-400 with STEP 7 V5.x

- SIMATIC S7 Trainings based on SIMATIC S7-300/-400 with STEP 7 V5.x
- SIMATIC S7 Programming based on STEP 7 V5.x
- SIMATIC S7 Service Training based on STEP 7 V5.x
- SIMATIC Safety Integrated based on STEP 7 V5.x
- SIMATIC S7 Engineering Tools based on STEP 7 V5.x
- SIMATIC Technology based on STEP 7 V5.x

12.3. Learning path: SIMATIC S7 Prgramming in the TIA Portal



12.4. Download the training documents



If you want to download the training documents, proceed as follows:

- Visit our new SITRAIN homepage at http://www.siemens.de/sitrain
- Register with your access data under the menu option **MyTraining**.
- Select **MyLearning** on the right-hand side of the submenu.
- Select your course and download your documents with a click on ”Download documents”.

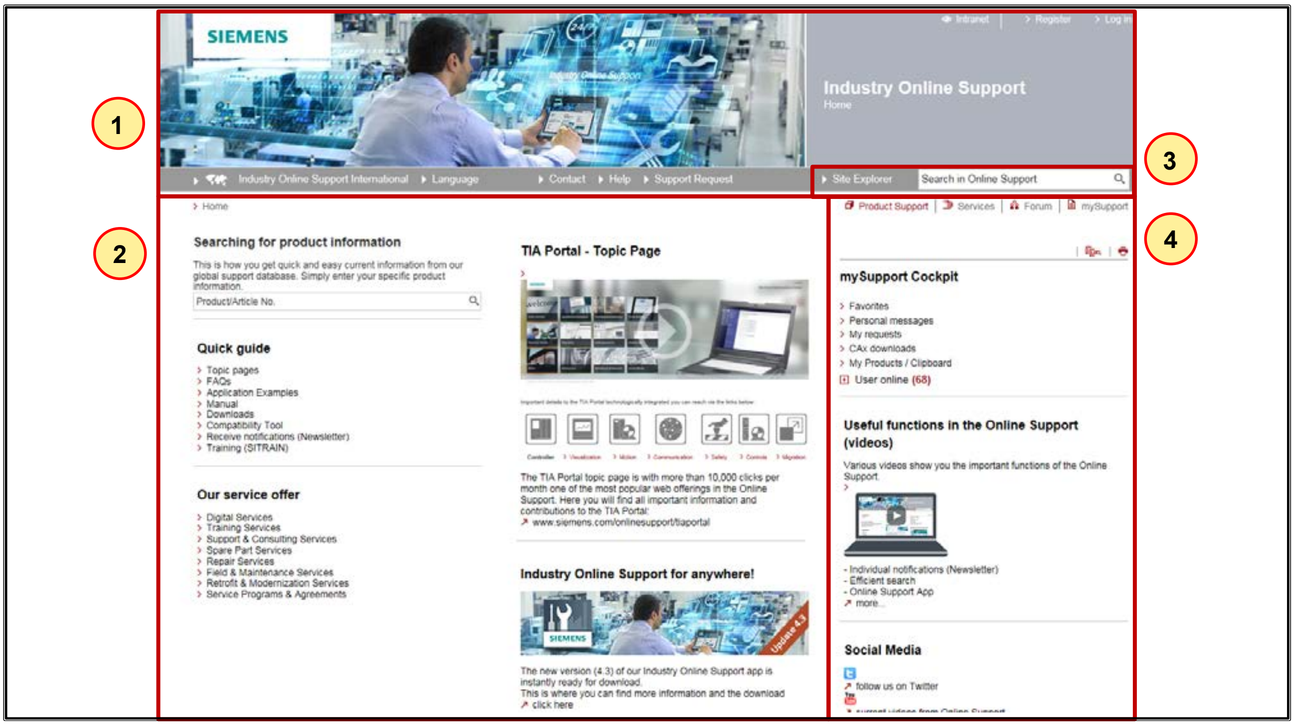
Documents ✕

Name	Size
> SIMATIC S7 Sequence Control with …	18,47 MB

Hint:

Please note that the training documents may be used for personal purposes exclusively. You agree that you will not copy the training documents or make them accessible to third parties and that you will be liable for any damage resulting thereof.

12.5. The Industry Online Support – the most important innovations



The most important functions are always in the same place on all the pages:

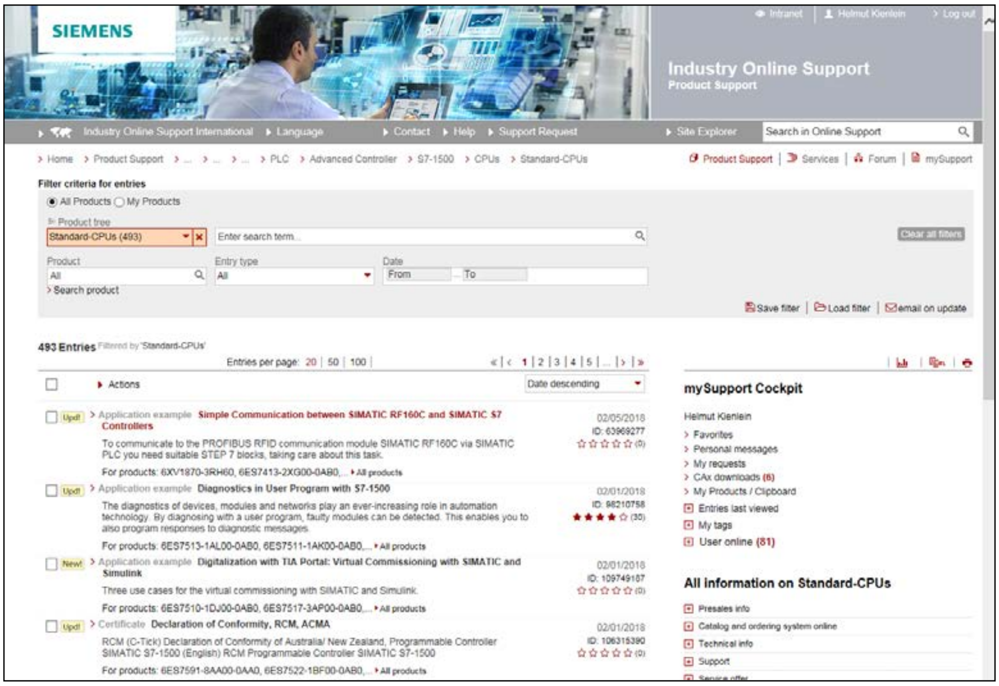
1 The menu bar links to the main areas of the site. You can subscribe and register at any time to benefit from the features the personalized mySupport option offers.

2 Links to our service offerings are in the center. On the start page, you will find up-to-date information and links, which quickly brings you to your destination in other areas of Online Support.

3 Links from the menu bar are repeated at the top of the page: Product Support, Services, Forum and mySupport.

4 On every page, you will find your personal mySupport cockpit. There, for example, you can see when the status of your support inquiry changes.

12.6. The Principle of Navigation



Here, you will find information about all the current and discontinued products, such as:

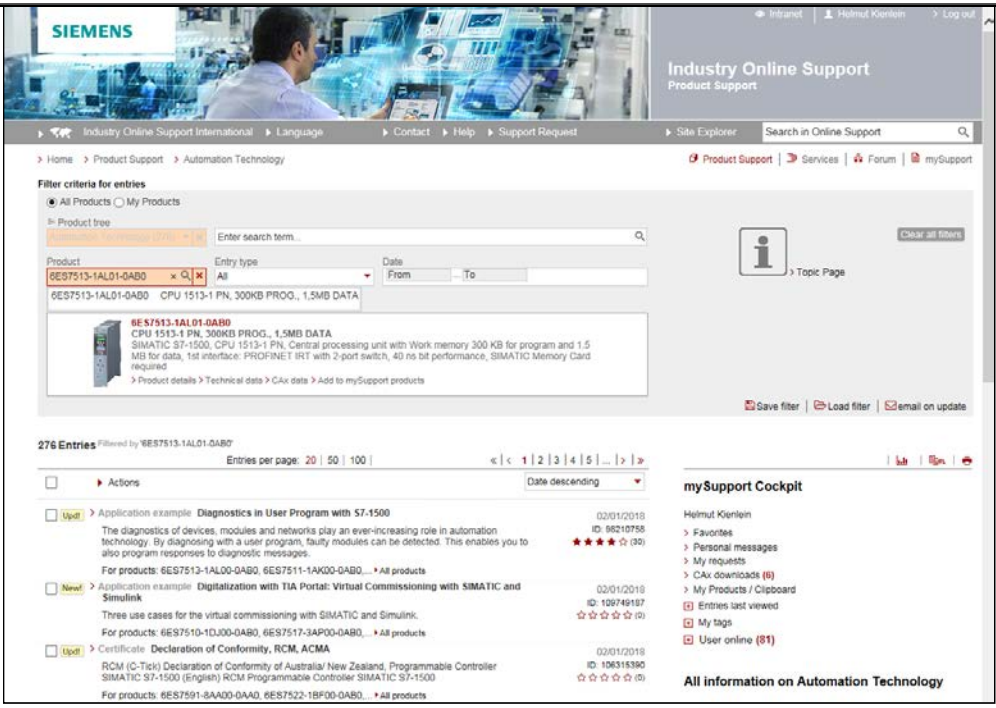
- Frequently Asked Questions (FAQ)
- Manuals and Operating Instructions
- Downloads
- Product Notes (product announcements, discontinuation, etc.)
- Certificates
- Characteristics
- Application Examples

You will not only be able to access these articles though the product tree, but also through a central filter bar. The integration of various search filters will give you access to relevant information after only a few clicks. The product tree has been moved to an equivalent filter. This has the effect that several filter steps can be combined clearly and comprehensibly.

Based on the preview numbers you can see the expected set of results before using a filter. This makes finding relevant information considerably easier and more efficient.

For example, you can customize your search by combining the product tree, a search keyword and a document type in your search.
There will be no hidden search parameters; all the settings and results will be clearly displayed.

12.7. Complete product information



A powerful function of the Industry Online Support is the direct access to complete product information. You can use it if you are looking for a quick and easy access to all the technical information about a Siemens Industry product. For example, for comparing products, if you are expanding your system or replacing individual components, this is how to do it:

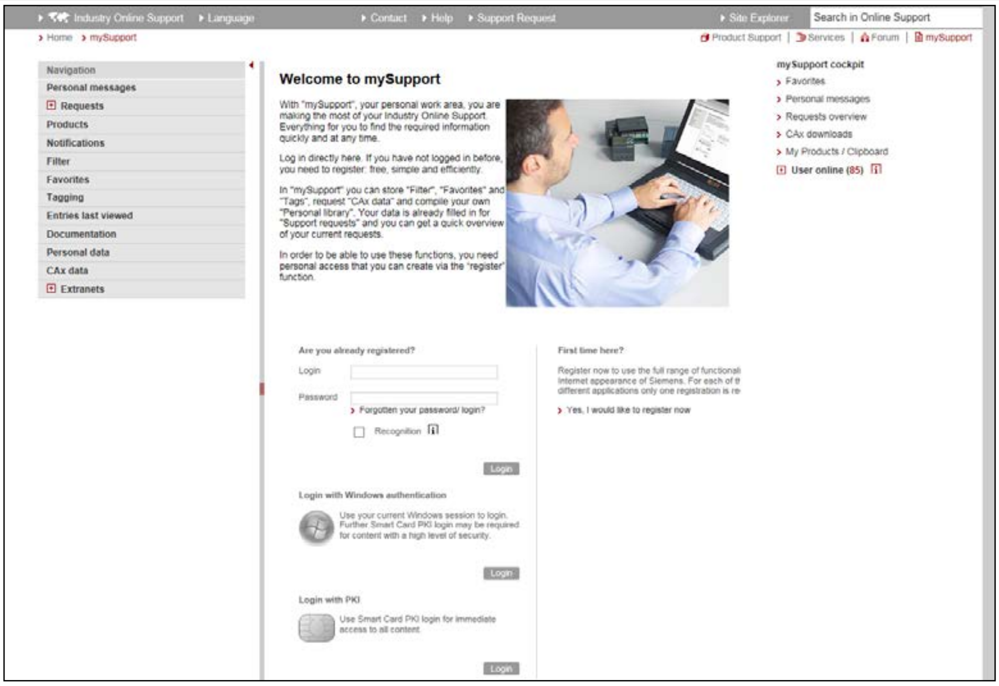
In the Product Support area, there is the central navigation bar.

To select a product, simply select the filter “Product.” Enter an order number or a product name here. You will be supported by a dynamic display of suitable products (list of suggestions).

One more click and the details of the selected product will be displayed – always up to date:

- Product life cycle, consisting of milestones with dates (e.g. delivery release, discontinuation of the product, …). You will find out whether the selected product is a current product or whether the product is already in the discontinuation phase.
- Successor products for discontinued products and new developments will be suggested. If there is a successor product, you will get a direct link to the product information of this product.
- Technical data – clear, compact and complete. You get all the available technical data concerning the selected product here – dimensions, operating voltage or the number of inputs/outputs, etc.

12.8. mySupport – Overview



mySupport

The mySupport area will always remain your personal workplace; with this feature you can make the best of your Industry Online Support experience.

The most important thing, if you're already working with mySupport, you can take all your previous personal data and information you've filed away with you to the Industry Online Support.

In this area, you can compile the information that is important for your daily work – we provide you with the suitable tools. Create your own folder structures and file information such as bookmarks. There are numerous options, whether you want to file items by project or by products.

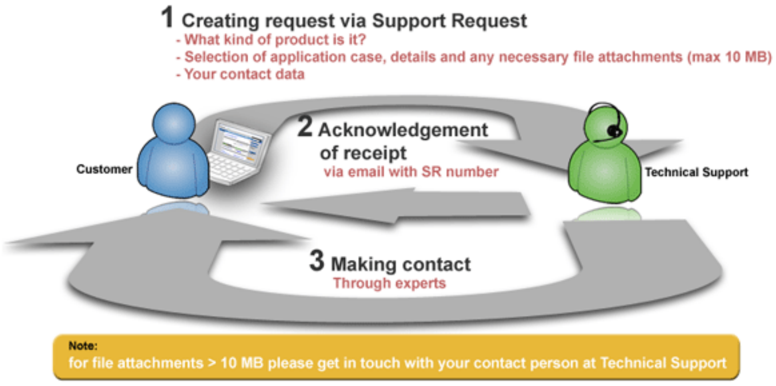
Moreover, you can now add notes, comments and tags (keywords). The system automatically creates a "Tag Cloud" based on your entries so you can access information quickly and easily by means of your own terms. The operation is consistent throughout mySupport so that you will easily find your way around. "Drag &drop" is also possible.

As soon as you are logged on, the mySupport cockpit is always at your side. It will immediately show you when the status of a support request changes, or when you receive new personal messages. You also have direct access to your personal keywords in the tag cloud, to the entries last visited, and you can see which user is online.

Here, just a few highlights:

- The previous MyDocumentationManager is now completely integrated into mySupport under the name of "mySupport-Documentation." The function category "Documentation" contains all the functions of the MyDocumentationManager and provides a few innovations, too.
- The Service & Support Newsletter has been completely revamped. An individual messaging system will more than replace it.

12.9. Support Request



Support Request

To create a Support Request, different options are available to you in Online Support:

- You will find the "Support Request" option in the menu on all Online Support pages.
- Alternatively, you can create a new request in mySupport in the "Requests" category.
- Or directly click on the following link:

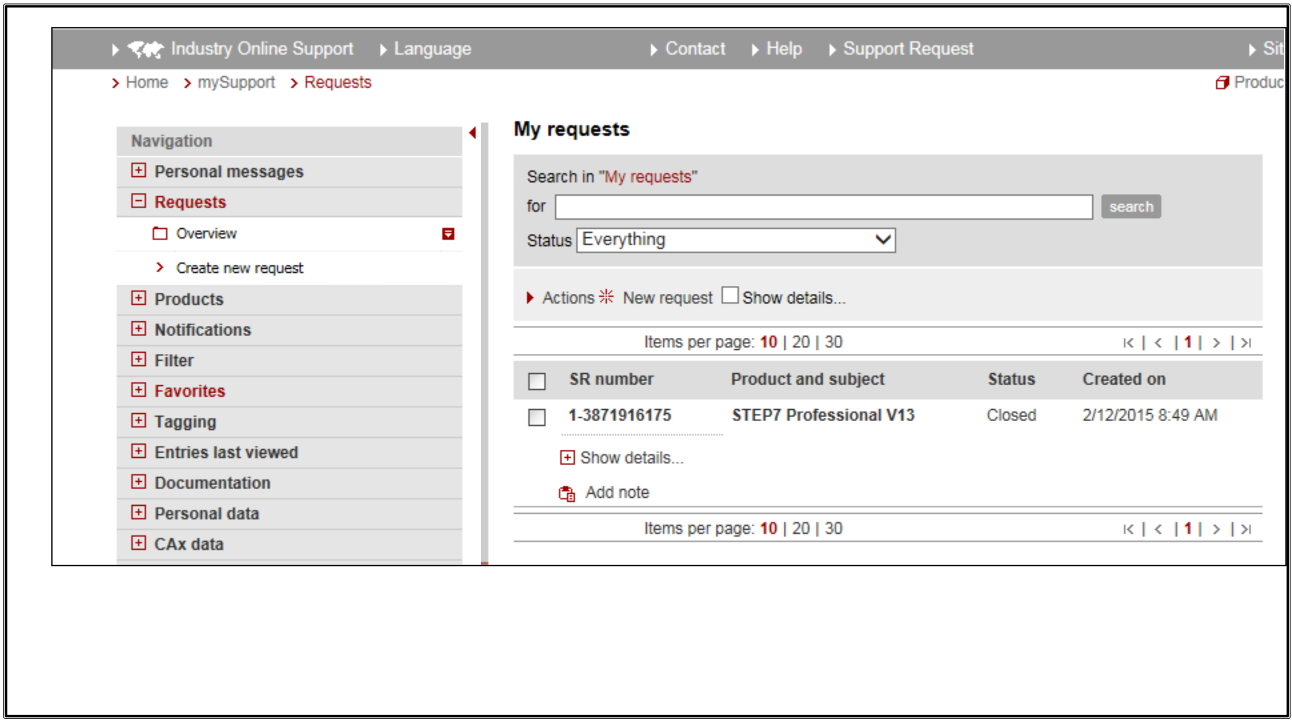
http://www.siemens.com/automation/support-request

Tips for creating a request:

- Select your product and use case as accurately as possible; try to avoid selecting "Other". By doing so, you ensure optimum support by our experts and appropriate suggested solutions.
- Did other users have a similar problem? This step already offers frequent problems and solutions. Take a look – it will be worth your while!
- Describe your problem with as much detail as possible. Pictures or explanatory attachments allow our experts to consider your problem from all sides and develop solutions. You can upload multiple attachments up to 10 MB per file.
- Before each sending, verify your personal contact information and the data you have entered. The final step additionally offers the option to print the summary.

As a logged in user, you can track the status of your requests online. To do so, navigate to "My requests" in the "Requests" category in mySupport.

12.10. Support Request



12.11. Industry Online Support – wherever you go

- Mobile access to more than 300,000 entries on all Siemens Industry products
- Reduced to the essential functions
- Application case: initial diagnosis of problem or in case of failures directly at the system or machine

Quick and easy ccess to technical information, anytime.
Scanning function, search and Support Request – everything at your fingertips at any time.

The app supports you, for example, in the following fields:

- Problem solving during the implementation of a project
- Troubleshooting of failures
- Expanding or restructuring your system

It also provides you with access to the Technical Forum and to further entries created for you by our experts:

- FAQs
- Application examples
- Manuals
- Certificates
- Product notes and many others

The main functions at a glance:

- Scan your product codes / EAN codes for a direct display of all technical and graphic data (e.g. CAx data) about your Siemens Industry product.
- Send your product information or entries per e-mail in order to process the information directly at the workstation.
- Send your requests to Technical Support at your convenience. Detail information can easily be added using the scan or photo function.
- Use the offline cache function to save your favorites to your device. In this way you can call these entries, products and conferences even without network coverage.
- Transfer PDF documents to an external library.
- The contents and surfaces are available in six languages (German, English, French, Italian, Spanish and Chinese) - including a temporary switching to English.

12.11.1. Scanning product/EAN code

- After scanning a code, the product view will open in most cases.
- Specialized search options are available for configurable products.
- Depending on the product, the result can also be displayed as a list of products, in which
- the user can select the appropriate product.

12.11.2. Scan functionality

Data matrix codes

on Siemens products
as per standard SN60450

QR code

e.g.: in advertisements
relating to Siemens content

EAN13 bar code

on Siemens products

Code39 bar code

(very hard to recognize / scan) on Siemens products as per standard SN60450

The scan functionality in the Online Support app supports the following types of code:

Data matrix code

QR code

EAN13 bar code

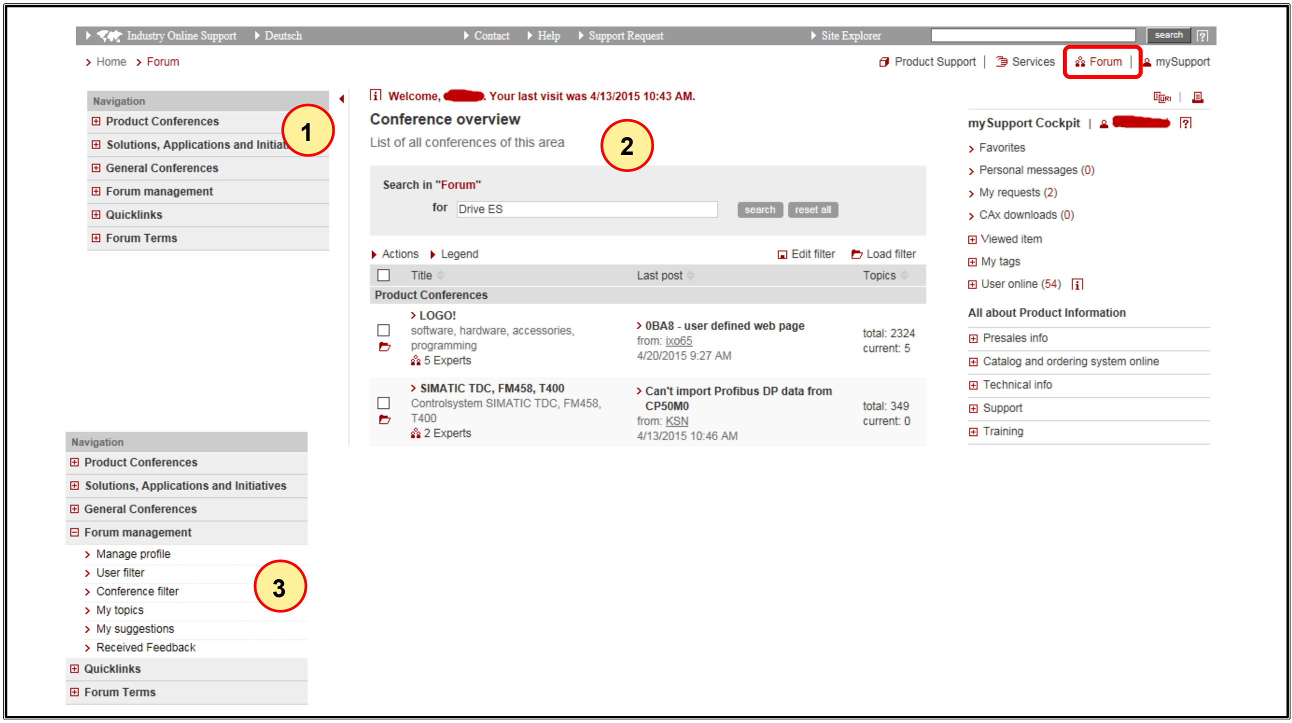
Code39 bar code

When one of these codes is recognized, the respective product view is called up in the app.

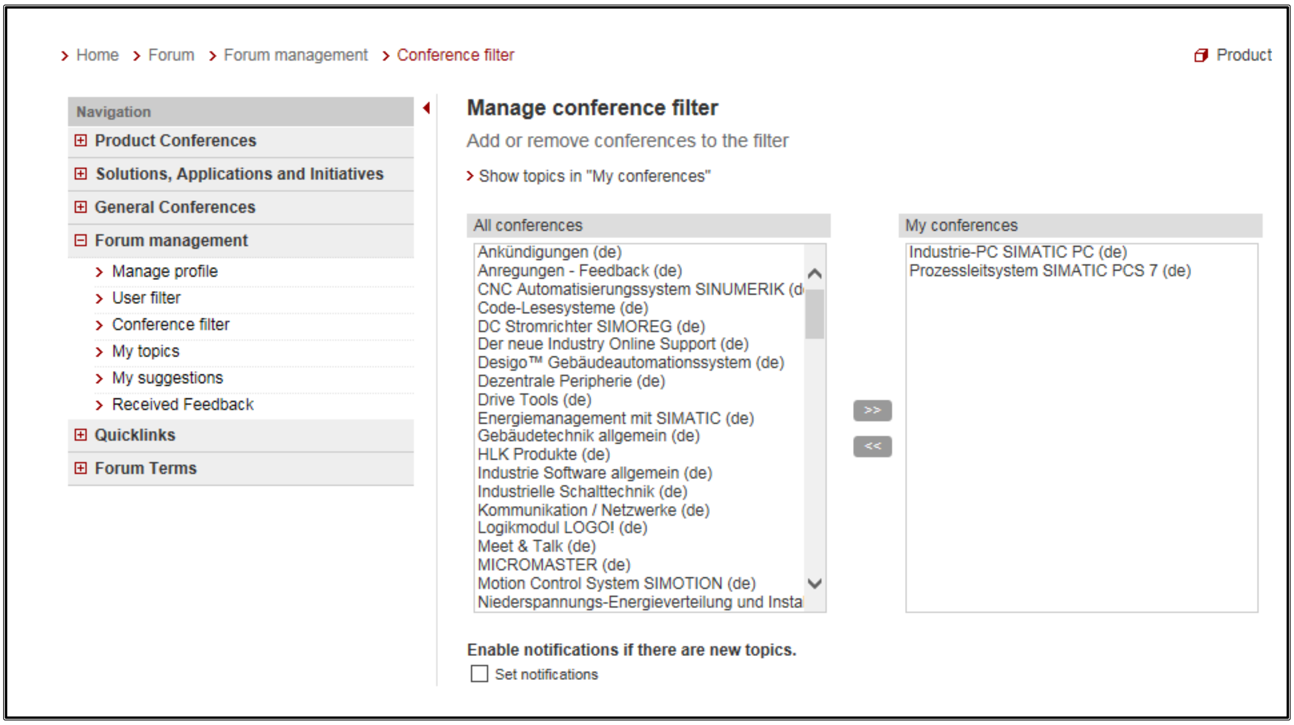
Exception:
The QR codes contain URLs – these are directly called up and displayed in the app by the integrated browser (but only, if "siemens" is contained in the URL).

12.12. Forum - the communication platform for Siemens Industry products

12.12.1. Conferences and Forum management



1	On the left side, you will find the so-called conference tree. It allows you to navigate through the individual discussion areas.
2	The conference overview is the central discussion area of the Technical Forum. This is where the community meets to discuss technical questions about Siemens Industry products.
3	In forum management, you will find your personal control center for the Technical Forum. It allows you to manage your specific profile data and filters.



Conference filter

Add conferences to your personal filter of preferred conferences.

This allows you to enable a notification that informs you when new topics are started in these conferences.

In Quicklinks, the Technical Forum additionally offers an overview page that contains all topics of your preferred conferences.

Managing profile

Profile management provides interesting information and functions:

- You get an overview of your activities in the Technical Forum.
- You can view your rank, any special permissions and your ranking progress.
- You can store a signature and a personal description for your profile in the forum.
- You have direct access to the quick links to get an overview of all topics you have contributed to.

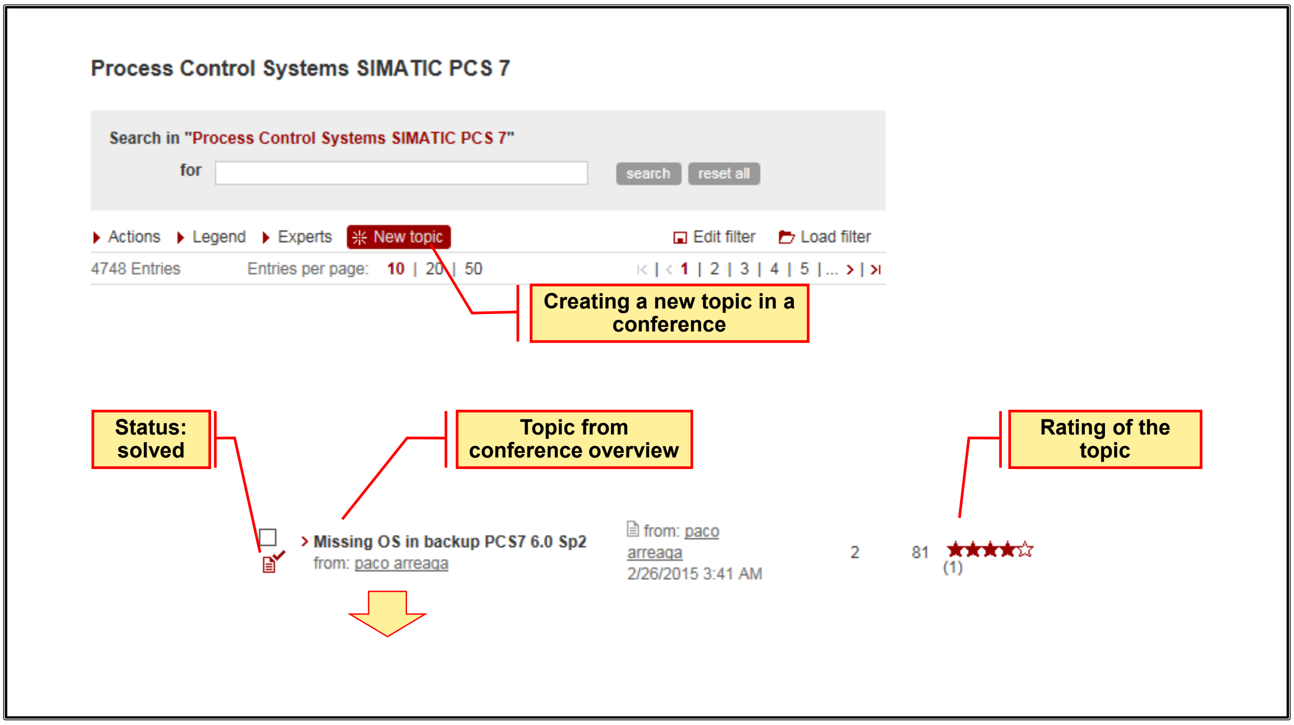
User filter

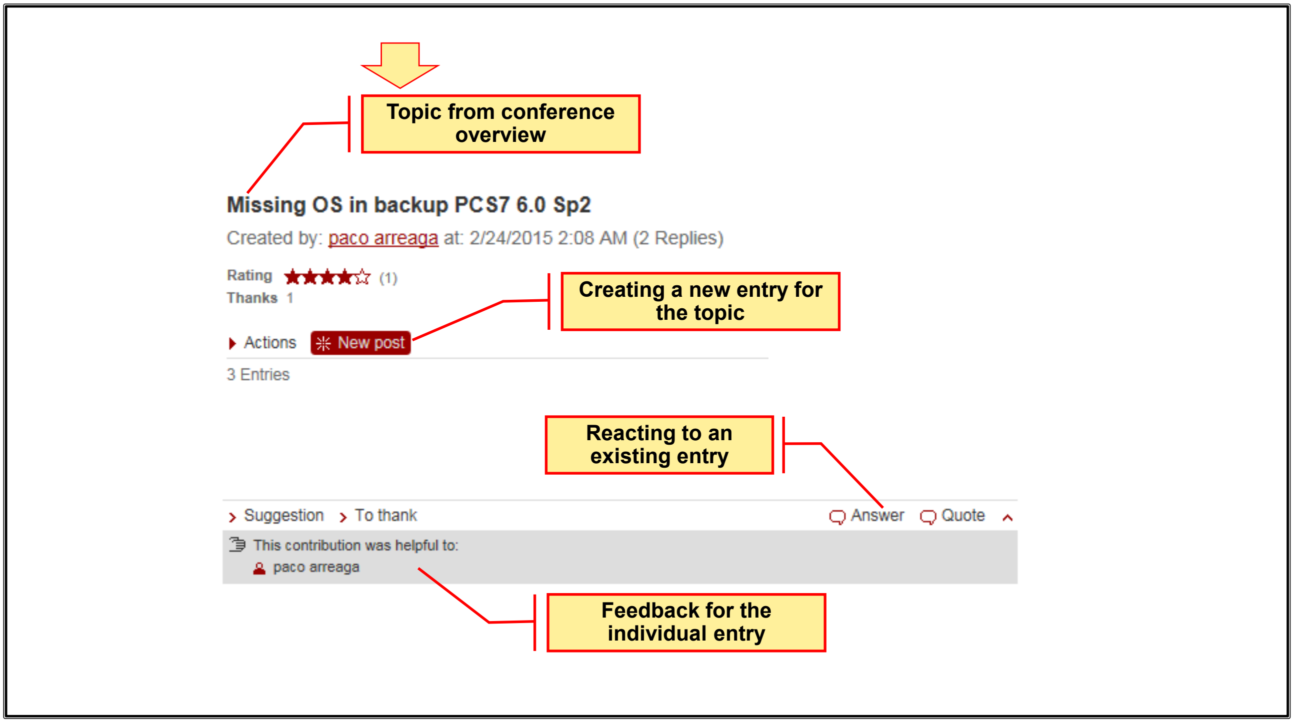
Have you found a user in the Technical Forum who posts entries that are particularly interesting? Then add this user to your list of "preferred users".

This allows you to enable a notification that informs you when the user has posted a new entry.

In Quicklinks, the Technical Forum additionally offers an overview page that contains all topics of your preferred users.

12.12.2. Interactions in the Forum





Creating a new entry

Do you want to create or format a new entry? The entry editor provides all the necessary functions.

- You can upload and publish in the forum a file with "Add attachment".
- You would like to check before the publication how your entry will actually look? A preview is available for this purpose.
- You would like to look at the topic again to which you create an entry? Please, you used the link over the input area (right mouse button > open in a new tab or window)

Posting / replying to an entry

Do you want to participate in an existing discussion with your own entry? Click on "Reply" and post your personal entry to support other users in answering the question.

- Use the "Reply" link to go to the entry editor and create a reply without quoting the entry.
- If you want to quote the entry, possibly only excerpts of it, use the "Quote" link. The content of the quoted entry is then displayed accordingly in the entry editor.

Rating an entry / saying thank you

Do you find an entry particularly interesting? Use the available functions and rate the entry or say thank you to provide personal feedback. Ratings and thank yours are the rewards our community members get for the support they provide. When you rate an author or entry, this will be added to the already existing ratings. The average value of all ratings is displayed.

Aside from feedback to the author of the entry, you also draw other readers' attention to particularly valuable entries and helpful authors.

12.13. Task and Checkpoint

Task: Software compatibility

Goal

Find out which current version of virus scanners is compatible with your engineering software.

Use all information sources available:

- Readme files in the installation folder
- The compatibility tool of the Industry Online Support
- Entries in the Product support
- Entries in the Forum
- Create a Support Request.

Checkpoint

Let's think about this:

- **Name some reasons for registration in MySupport.**
- **What do you think is the best way to have always the latest version of the required manuals for your job with you?**