SIEMENS

SIMATIC

Process Control System PCS 7 Compendium Part B - Process Safety (V9.1)

Operating Manual

Valid for PCS 7 V9.1
SIMATIC S7 F Systems V6.4
SIMATIC S7 Safety Matrix V6.3 Upd2

10/2022
A5E42576080-AB

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E42576080-AA
Ⓟ 04/2022 Subject to change

Table of contents

1 Security information

Security information

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

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

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

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

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

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

Preface

2

Subject of the manual

As a distinctly open system, SIMATIC PCS 7 can be flexibly adapted to a wide range of customer needs. The system software provides the project engineer with a great deal of freedom in terms of project configuration, as well as in the design of the program and visualization.

Experience has shown that subsequent modernization or plant expansion work is made much easier if the project is configured "in conformance with PCS 7" as far as possible right from the start. This means users must adhere to certain basic rules to ensure that the provided system functions will offer optimum usability in the future.

This manual serves as a compendium in addition to the product documentation for SIMATIC PCS 7. The basic tasks for creating and configuring the project are described in the form of instructions with numerous illustrations.

The compendium is divided into the following parts:

- Configuration guidelines including checklist
- Process safety including two checklists
- Technical functions with SFC types
- Operation and maintenance including checklist
- Hardware installation including checklist
- Industrial Security

Subject of Part B - Process safety

This compendium directly reflects the recommended method for configuration and corresponds to the procedure described in the documentation for S7 F/FH Systems, whereby numerous practical experiences were evaluated. The description relates to working with the project and the parameter settings of the components it contains but not the application itself. Observe the warnings in the manuals of the respective components.

Compendium Part B is dedicated to the implementation of the fail-safe part of an S7 program.

It examines the following F-software components:

- SIMATIC S7 F Systems
- SIMATIC S7 Safety Matrix

Checklists

You can download the checklist for the SIMATIC PCS 7 Compendium Part B as a zip file via the "Appendix" button in the Industry Online Support Portal.

Validity

This documentation is valid for the software packages:

- SIMATIC PCS 7 V9.1
- SIMATIC S7 F Systems V6.4
- SIMATIC S7 Safety Matrix V6.3 Upd2

Conventions

The following terms are used in this documentation...

- The terms "safety engineering" and "fail-safe engineering" are used synonymously in this manual. The same applies to the terms "fail-safe" and "F-".
- "S7 F Systems" refers to the optional package "SIMATIC S7 F Systems" for the F-system "SIMATIC S7 F/FH Systems".
- "Safety Matrix" refers to the option "SIMATIC S7 Safety Matrix".
- The term "safety program" refers to the fail-safe part of the user program and is used synonymously with "fail-safe user program", "F-program", etc. For purposes of contrast, the non-safety-related user program is referred to as the "standard user program".
- "F-CPU" denotes a CPU with fail-safe capability. An F-CPU with fail-safe capability is a central processing unit that is approved for use in S7 F/FH Systems.

SIMATIC PCS 7 in Industry Online Support

An overview of the most important technical information and solutions for SIMATIC PCS 7 is available at http://www.siemens.com/industry/onlinesupport/pcs7.

SIMATIC PCS 7 documentation

Full PCS 7 documentation is available to you free of charge and in multiple languages in PDF format at www.siemens.com/pcs7-documentation.

What's new?

3

The contents of the compendium have been updated to reflect the new functionalities and operator input options of SIMATIC PCS 7 V9.1.

Changes and extensions were made in the following sections in particular:

- Cyclic interrupts
- Setting system parameters for F-signal modules
- Monitoring times and system response times

Note

Observe the compatibility statements in the compatibility tool:
http://www.siemens.com/kompatool

See also

SIMATIC S7 F/FH Systems – Configuring and Programming
(https://support.industry.siemens.com/cs/ww/en/view/109802562)

4 Installing the fail-safe system

4.1 Software components

This documentation is based on PCS 7 V9.1 and the following additional software components:

- SIMATIC S7 F Systems V6.4
  - S7 F Systems HMI V6.4
  - S7 F Systems Lib V1_3 SP4
  - S7 F Device Integration Pack V6.4
  - S7 F Configuration Pack V5.5 SP13
- SIMATIC Safety Matrix V6.3 Upd2
  - Safety Matrix Engineering Tool V6.3 Upd2
  - Safety Matrix Viewer V6.3 Upd2
  - Safety Matrix AS-OS Engineering V6.3 Upd2

A "S7 F-Systems RT License" is also required for operating a safety-related automation system.

All SIMATIC software must be closed during the installation process.

Note

You can find more information in the following manuals:

- SIMATIC S7 F/FH Systems – Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/109802562)
- SIMATIC Safety Matrix (https://support.industry.siemens.com/cs/ww/en/view/109766685)
- Information on the separately available versions of the S7 F Device Integration Pack (https://support.industry.siemens.com/cs/ww/en/view/109782016)

4.2 Installation on the PCS 7 engineering station (ES)

4.2.1 Installing SIMATIC S7 F Systems

Procedure

1. Run SETUP.EXE to start the installation and follow the instructions in the setup program.
2. Select the "Engineering AS OS" package for installation on the ES. The following components are selected for installation in the next window:
   - S7 F Systems V6.4
   - S7 F Systems HMI V6.4
   - S7 F Systems Lib V1_3 SP4
   - S7 F ConfigurationPack V5.5 SP13
   - S7 F Device Integration Pack V6.4
3. Carry out the installation.

Note

With an update installation, check whether the new version of S7 F-Systems Lib is required or the old version is to be retained. As of S7 F Systems V6.2, only S7 F Systems Lib as of V1_3 is supported.

When employing PCS 7, check whether PCS 7 supports the F-modules used.

4.2.2 Installing SIMATIC Safety Matrix

Procedure

Safety Matrix Engineering requires an installation of S7 F Systems. Check if a corresponding version is installed.

1. Start the installation of the Safety Matrix using SETUP.EXE.
2. Follow the instructions of the setup wizard and select the "Engineering AS OS" package. The following components are selected for installation in the next window:
   - Safety Matrix Engineering Tool V6.3 Upd2
   - Safety Matrix Viewer V6.3 Upd2
   - Safety Matrix AS-OS Engineering V6.3 Upd2
3. Carry out the installation.

4.3 Installation on the PCS 7 operator station (OS)

The next section outlines the installation steps for an OS client. Please follow these if you are using an OS single station or an OS server for operation.

4.4 OS client installation

4.4.1 Installing SIMATIC S7 F Systems

Procedure

When using Secure Write Command ++ (SWC_QOS, SWC_MOS or SWC_CHG), start the installation using SETUP.EXE and activate the "Runtime" package. The following components are selected for installation in the next dialog:

- S7 F Systems HMI V6.4

4.4.2 Installing SIMATIC Safety Matrix

Procedure

Start the installation using SETUP.EXE. Follow the instructions of the setup wizard and select the "Runtime" package. The following components are selected for installation in the next dialog:

- Safety Matrix Viewer V6.3 Upd2

5 Advanced PCS 7 ES settings

5.1 Access protection

An S7 F/FH system being operated as a safety system is protected by two passwords:

- The CPU password is configured in the hardware configuration and is intended to protect the CPU against accidental downloading or the wrong program being downloaded.
- Another password is configured in the "Edit Safety Program" dialog box, It protects the fail-safe user program and the parameters of the signal modules and, where necessary, the parameters of the CPU (option in the "Protection" register of the CPU properties).

5.1.1 General measures

You can restrict access to the ES by implementing access protection for authorized persons: To do this you can, for example, install the ES in an operating area that can only be accessed by these persons.

You can use the options offered by the operating system by protecting the ES with a password and setting a screen saver that is activated automatically.

To protect the safety program, you can implement organizational measures to ensure that:

- The passwords for the CPU and safety program can only be accessed by authorized persons.
- The timer is reset for the security password (menu "Options > Edit safety program > Password > Cancel" or close all applications and the SIMATIC Manager).
- Authorized persons expressly reset access authorization for the F-CPU before exiting the ES (by selecting "CPU > Access authorization > Cancel" or closing all applications in the SIMATIC Manager).

5.1.2 Access protection with SIMATIC Logon

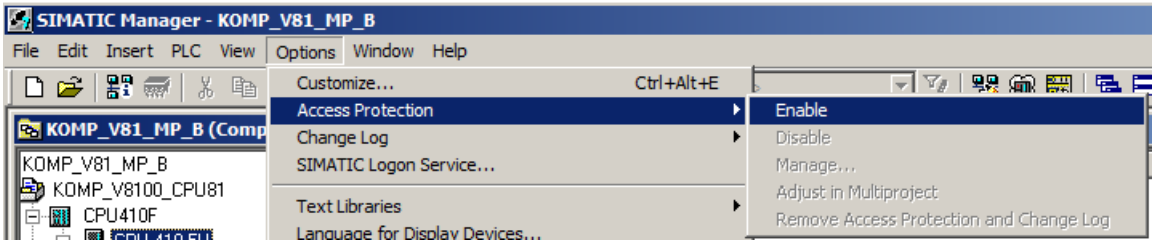
As of PCS 7 V7.0, it is possible to set up access protection for individual subprojects with SIMATIC Logon. With a station-selective multiproject structure, this means that it is possible to assign access rights to protect AS projects with F program.

Requirement

The SIMATIC Logon Service V1.3 SP1 or higher is installed.

Procedure

1. Activate access protection in the SIMATIC Manager with the selected project node via the "Options > Access Protection" menu.



   The project format is changed the first time access protection is activated. A message appears indicating that the modified project can no longer be edited with older versions of STEP 7 (< 5.4).

2. This is followed by logon to the SIMATIC Logon Service.

   The Windows user activating access protection is entered automatically as the first project administrator. The project password is set at this time.

   Note

   When a multiproject is opened without prior authentication, the projects with activated access protection are displayed grayed-out.

Note

As of S7 F Systems V6.2, certain events from S7 F/FH Systems are logged when using SIMATIC Logon as of V1.3 and STEP 7 as of V5.5.4 Upd9 (corresponds to PCS 7 V8.1):

- Safety mode has been enabled/disabled.
- The password for the safety program has been changed.
- Access permission for the safety program has been granted/revoked.

6 Configuring S7F/FH hardware

The following CPU types have been released for using S7 F-systems in conjunction with PCS 7:

- CPU 410H
- CPU 410E
- CPU 412H
- CPU 414H
- CPU 416H
- CPU 417H

In the SIMATIC PCS 7 catalog, safety-related automation systems can be configured and ordered as bundles with a single or redundancy station in various designs.

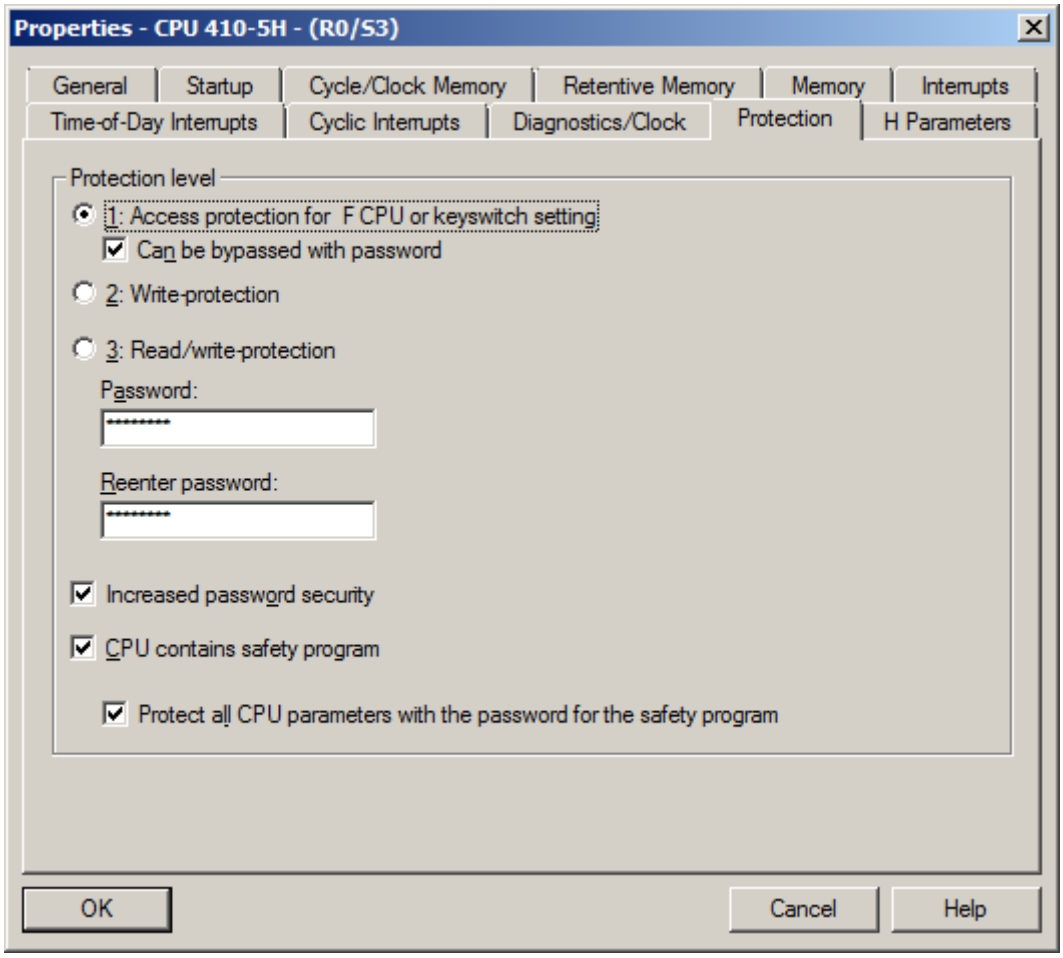
6.1 Adapting CPU parameters (single F-system)

6.1.1 Password and access protection

In order to activate the safety functions contained in the H-CPU's operating system, you need to enter a password. A prompt appears accordingly on CPU download.

The "CPU contains safety program" option also needs to be activated.

There is the option of protecting the CPU parameters with the password for the safety program.



As of PCS 7 V8.1, you can encrypt the CPU password assigned by the hardware configuration in the project data management. The increased password security is only relevant for the engineering system. If the check box is selected, the password entered in the data

management is stored encrypted. This setting increases the password security. The function of the password remains the same.

NOTICE
Using the "Increased password security" functionality Projects in which the "Increased password security" option is activated may only continue to be used in STEP 7 V5.5 SP4 or higher, because this functionality is not backwards compatible!

Note

At least protection level 1 and "Can be bypassed by password" must be configured.

In addition, the fail-safe program is assigned a password that is created the first time the safety-related software or hardware is used. This password must not be the same as the CPU password.

6.1.2 Access protection with SFC 109

There is an additional mode for SFC 109 as of firmware V6.0 of the H-CPU. With MODE = 12, protection level 3 can be set without password authorization.

Calling of SFC 109 with MODE=0

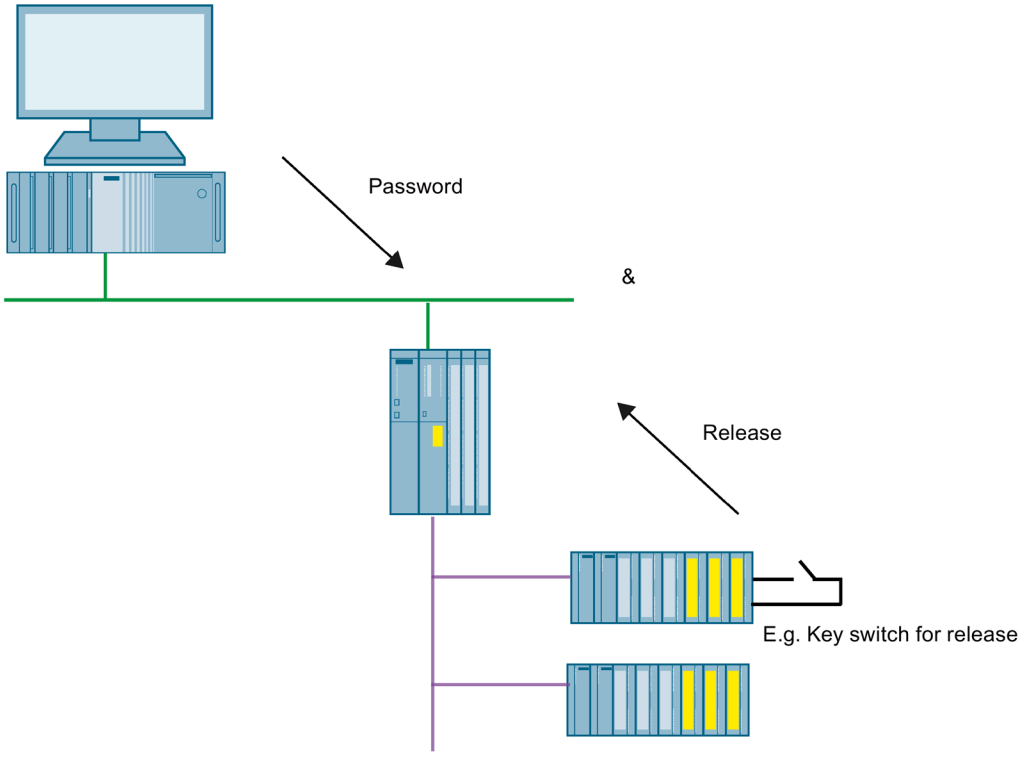
Setting the protection level: Any applicable block that is present on password authorization is lifted through this call.

Calling of SFC 109 with MODE=1

Setting of protection level 2 with password authorization: This means that you can lift the write protection set with SFC 109 when knowing the valid password. Any applicable block that is present on password authorization is lifted through this call.

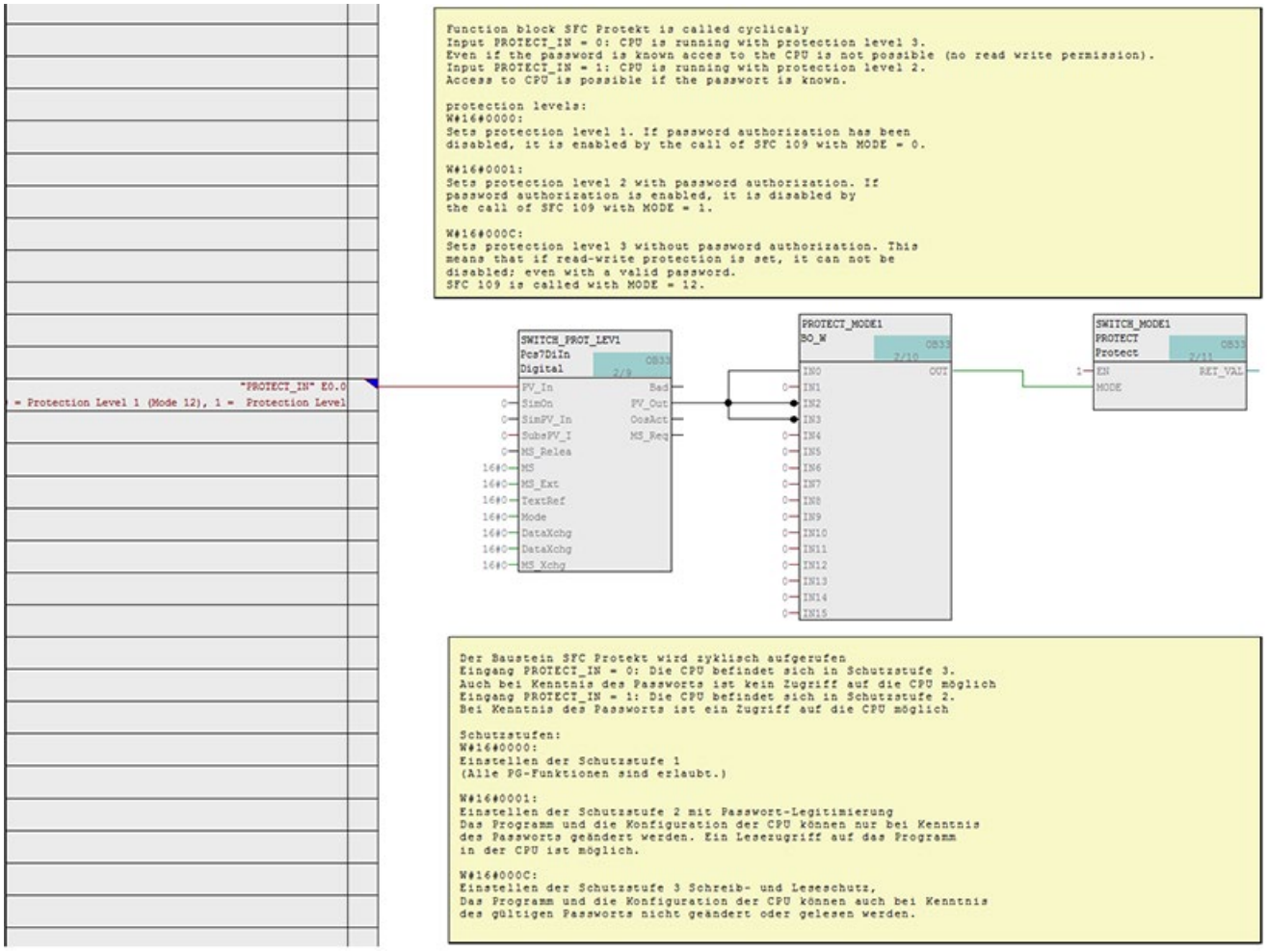
Calling of SFC 109 with MODE=12

Setting of protection level 3 without password authorization: This means that you cannot lift the read and write protection set with SFC 109 even when knowing the valid password. If, at the time of the call up of SFC 109 with MODE=12, an authorized connection is present, the calling of SFC 109 for this connection remains without effect.



Example

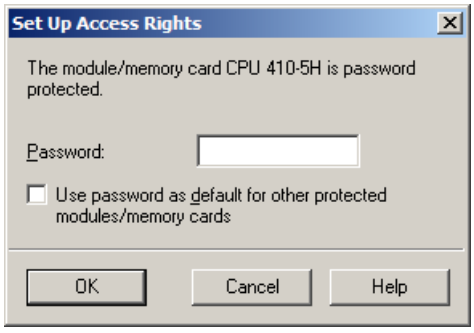
The following example shows how you can switch between protection level "2" (MODE = 1) and "3" (MODE = 12) of the CPU with a digital input signal (e.g. from a key switch) with SFC 109. When the system, or the safety program, starts up, protection level "3" is activated with a signal "0" at the input. With a signal "1", this is reduced to protection level "2". At this protection level, the CPU can be accessed and changes loaded into the CPU if the password is known.



Note

The figure is available in its original size as appendix to the manual in the ZIP download of the checklists.

When the password prompt appears, disable the "Use password as default for other protected modules/memory cards" function, so that the password is not used by the system for other functions and is prompted again when required.

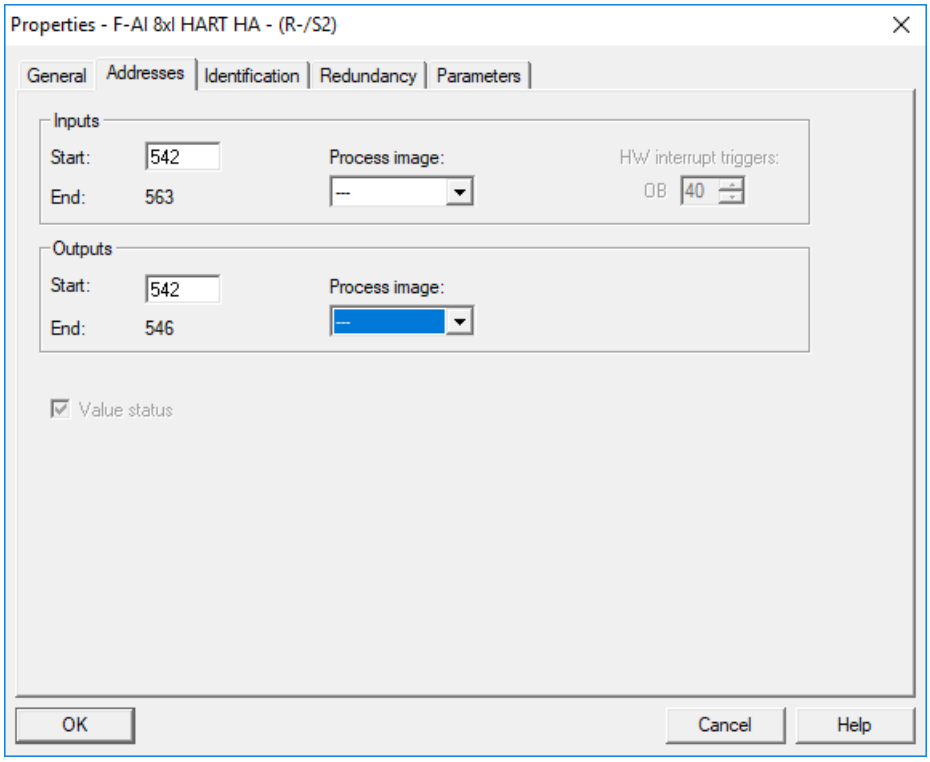


6.1.3 Cyclic interrupts

Parameter assignment

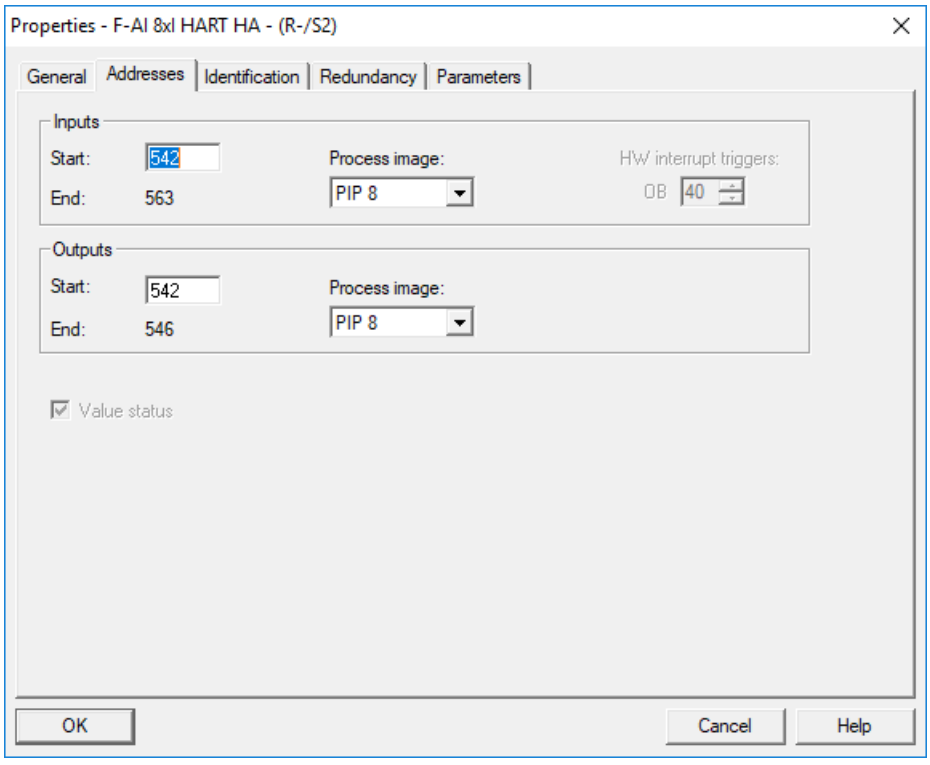
The configuration of process image partitions is generally not required for F-program parts, because access to the F-signal modules in S7 F/FH systems occurs via F-module drivers instead of the process image.

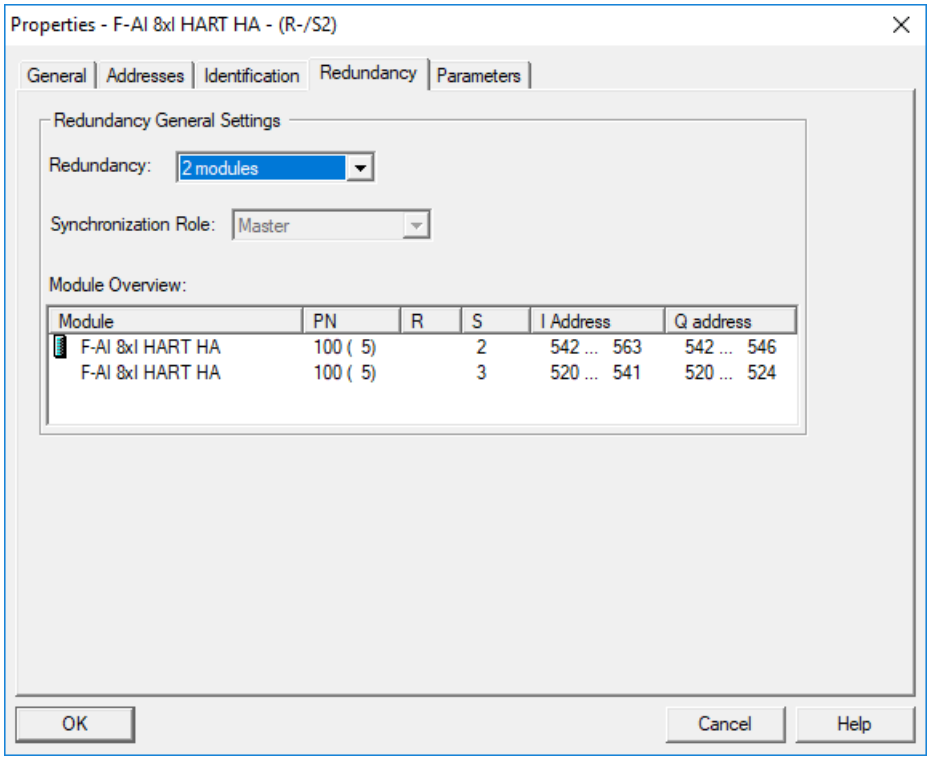
It is therefore recommended to select "---" for the F-signal modules as the process image in the module properties. This avoids an additional update of a process image for the F-signal modules and reduces CPU usage.



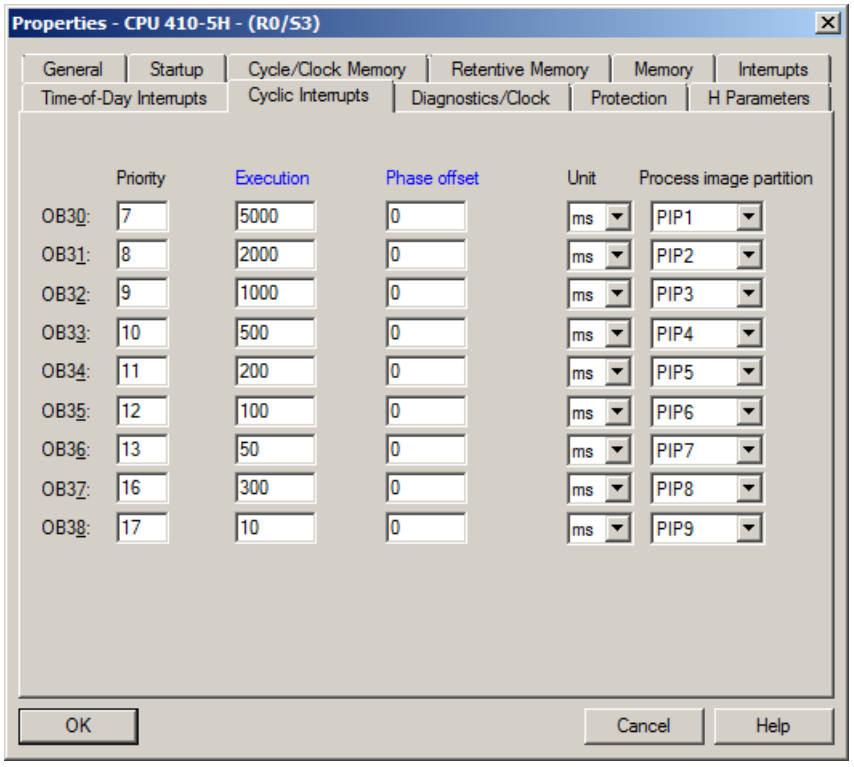
An exception applies to the use of the F-signal modules of the ET 200SP HA when using module redundancy. For this application, a process image must be set up in order to fully support the diagnostic functionality within the framework of PCS 7 Asset Management.

Example ET 200SP HA F-AI8 HART, Properties of the module in the hardware configuration





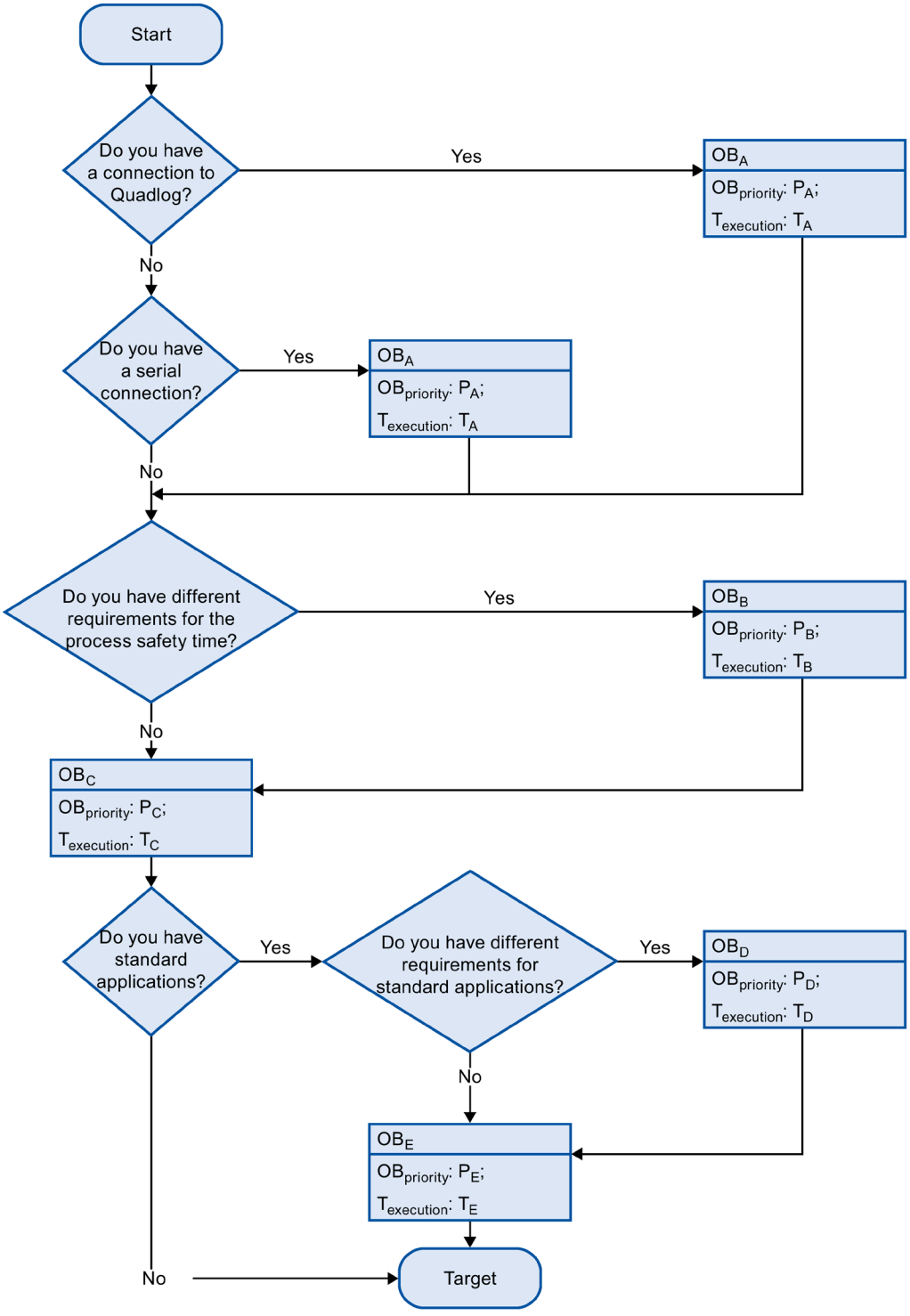
When a process image is assigned to an F-signal module, it must match the process image of the cyclic interrupt in which the F-module driver is processed.



Note

No reduction ratio or phase offset may be configured for cyclic interrupt OBs with F-program.

The flow diagram below demonstrates one method you can use for structuring your program according to process requirements, using the cyclic interrupt OBs.



The user program is divided to cyclic interrupt OBs according to the requirements:

- OB_A
  - Very fast applications
  - For example connections, such as Quadlog or Modbus
- OB_B
  - Fast F applications
  - For example pressure protection functions
- OB_C
  - (Slow) F-applications
  - For example slow temperature protection functions
- OB_D
  - Fast standard applications
  - For example fast control functions
- OB_E
  - Slow standard applications
  - For example temperature measurements, visualization functions, enable functions

The following rules apply:

- OB_A to OB_E:
  - One of the cyclic interrupt OBs from OB30 to OB38
  - Only certain cyclic interrupt OBs are available, depending on the CPU type.
- $T_{execution}$: $T_A < T_B < T_C < T_D < T_E$
  ($T_{execution}$ = The execution time of the cyclic interrupt OBs in ms configured in the CPU properties)
- $OB_{priority}$: $P_A > P_B > P_C > P_D > P_E$
  ($OB_{priority}$ = The priority of the cyclic interrupt OBs configured in the CPU properties. Possible values are 7 to 18.)

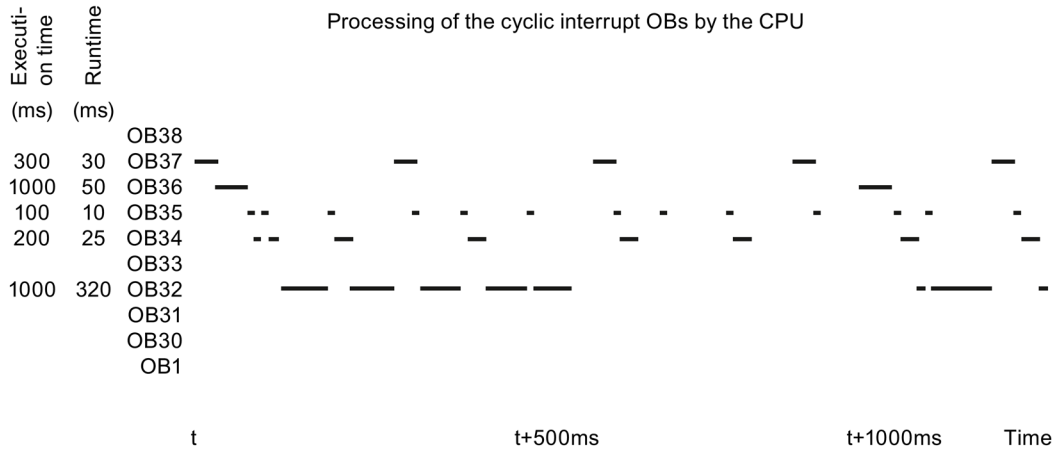
Example 1: Reconfiguration (no Quadlog connection, no serial communication)

OB	Prio	Call interval	Purpose	Comment
OB 38	15	10 ms	Empty	
OB 37	17	300 ms	Fast F-application	
OB 36	16	1000 ms	F application	
OB 35	12	100 ms	Fast standard application	Ex.: Control
OB 34	11	200 ms	Standard application	Ex.: Pressure measurement
OB 33	10	500 ms	Empty	
OB 32	9	1000 ms	Slow standard application	Ex.: Temperature measurement, visualization function, enable function
OB 31	8	2000 ms	Empty	
OB 30	7	5000 ms	Empty	

Note

If you are using high-precision time stamping, the setting for OB 40 should be changed from Prio16 to Prio18.

The following figure shows how the individual cyclic interrupt OBs from Example 1 are processed over a period of 1280 ms, starting from the point in time (t) at which the CPU begins program processing. In this example, the CPU utilization is at approximately 65%.



Example 2: Reconfiguration/migration, for which the hardware present must be connected via serial communication (Modbus)

OB	Prio	Call interval	Purpose	Comment
OB 38	18	50 ms	Serial communication	Ex.: Modbus
OB 37	17	300 ms	Fast F-application	
OB 36	16	1000 ms	F application	
OB 35	12	100 ms	Fast standard application	Ex.: Control
OB 34	11	200 ms	Standard application	Ex.: Pressure measurement
OB 33	10	500 ms		
OB 32	9	1000 ms	Slow standard application	Ex.: Temperature measurement, visualization function, enable function
OB 31	8	2000 ms	Empty	
OB 30	7	5000 ms	Empty	

Note

If you are using high-precision time stamping, the setting for OB 40 should be changed from Prio16 to Prio19.

Example 3: Reconfiguration/migration, for which the Quadlog hardware present must be connected via DP/IO bus link

OB	Prio	Call interval	Purpose	Comment
OB 38	17	10 ms	Quadlog connection	
OB 37	16	300 ms	F application	
OB 36	13	50 ms	Empty	
OB 35	12	100 ms	Empty	
OB 34	11	200 ms	Empty	
OB 33	10	500 ms	Empty	
OB 32	9	1000 ms	Slow standard application	Ex.: Temperature measurement, visualization function, enable function
OB 31	8	2000 ms	Empty	
OB 30	7	5000 ms	Empty	

Note

If you are using high-precision time stamping, the setting for OB40 should be changed from Prio16 to Prio18.

CPU utilization

The cycle utilization of the system should never be above 75%, regardless of whether it involves a standard AS or an H system.

Note

To help you determine the processing times of the individual cyclic interrupt OBs, please refer to the FAQ "How can you calculate the cycle load of the automation system (AS) online?" (https://support.industry.siemens.com/cs/ww/en/view/22000962)

As of PCS 7 V7.0 and an S7-400H CPU as of FW V4.5, the run times of the cyclic interrupt OBs and the total load of the AS can be read at the CPU_RT block.

As of PCS 7 V7.0 with PCS 7 Library V7.0, the block CPU_RT will be installed in each CPU. This block prevents a CPU STOP as a result of cycle overload. thanks to a two-stage "load-shedding" process:

- In the first stage of load shedding, all cyclic interrupt OBs that have not been disabled for the function by the project engineer are not processed for one cycle.
- In the second stage, none of the cyclic interrupt OBs are processed for one cycle (even the ones that were excluded previously). If this does not have a steadying effect, whenever cyclic interrupt OBs are processed their processing will be suspended again for one cycle.

Note

In order to prevent F-cycle-time monitoring in the CPU and the F-monitoring time on the F-signal modules from being triggered, and the system response time from being extended, you must disable the cyclic interrupt OBs with the F-program during the stage 1 of stop prevention.

Alternatively, you can disable stop prevention altogether by setting the parameter for input Max_RTRG of block CPU_RT to 0. You can find this block in the @CPU_RT chart.

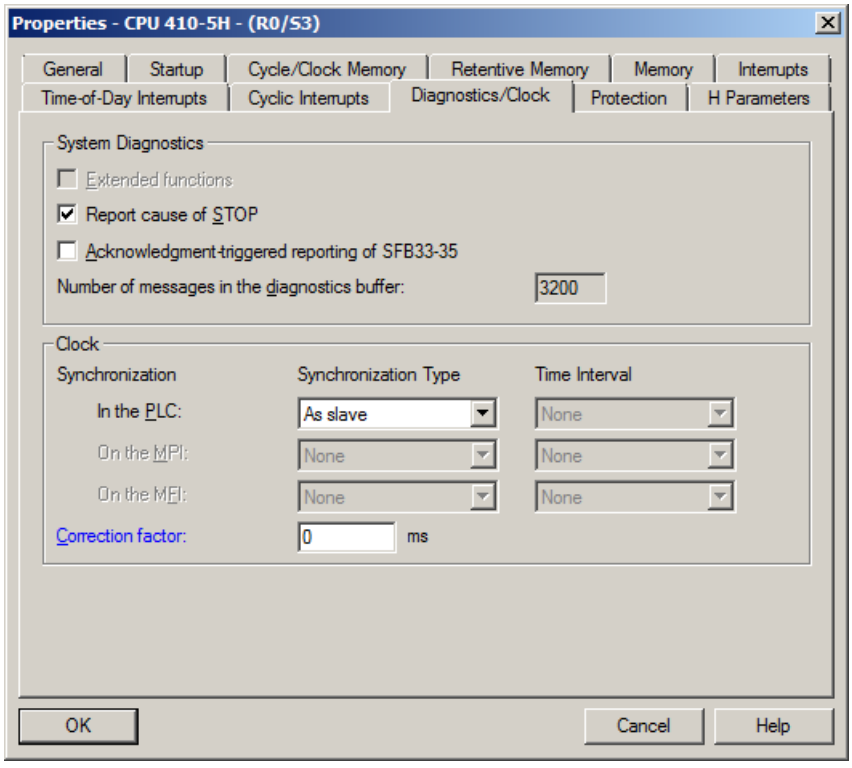
For more information on the subject of CPU stop prevention, please refer to the help section for the CPU_RT block.

6.1.4 Diagnostics/Clock

For process data to be compatible for evaluation, all components of the process control system must work with the same time of day so that messages – regardless of the time zone in which they are generated – can be assigned correctly in terms of temporal sequence. For this purpose, the function of the time master is usually assigned to an OS server or an external clock (Bürk Mobatime). All other operator stations and automation systems on the plant bus then have the time from this time master and, therefore, identical time.

You can find additional information about configuring the time synchronization in the manual "SIMATIC Process Control System PCS 7 Time Synchronization" (https://support.industry.siemens.com/cs/ww/en/view/109794383).

Check that the correction factor is set to 0 ms under "Time" on the "Diagnostics/Clock" tab in a CPU with safety program.



Note

See also Compendium Part A "Configuration of the Hardware > General CPU Settings > Diagnostics/Clock".

6.1.5 H parameters

Self-test (advanced CPU test)

The CPU tests the following during the self-test:

- Processor
- Internal memory
- I/O bus

If the test detects any faults, they are reported and the CPU goes to STOP.

Test cycle time

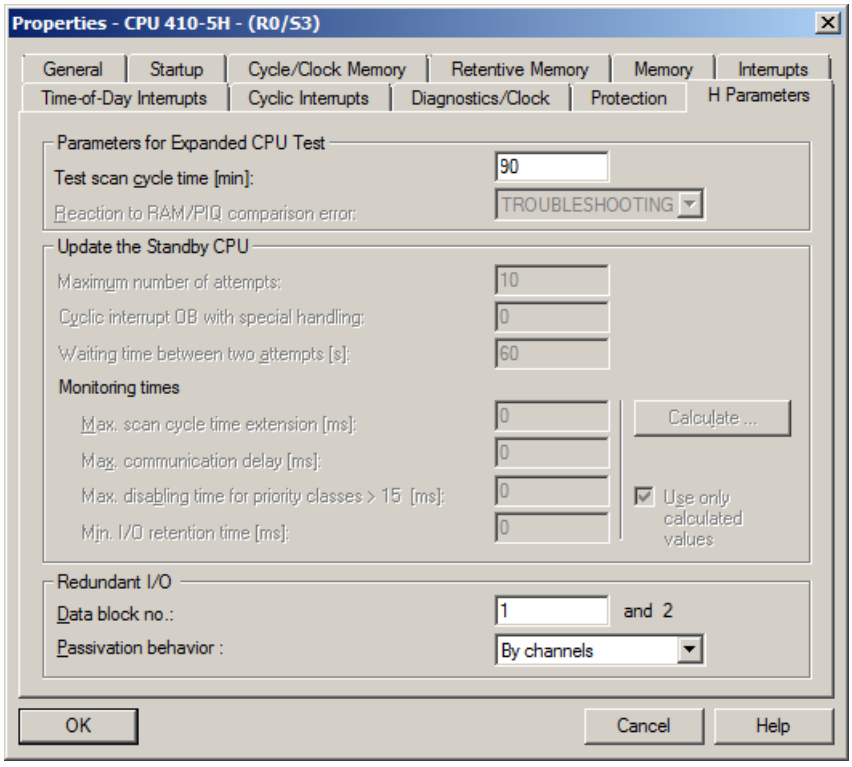
The test cycle time (default setting: 90 minutes) indicates the time taken for a complete background self-test.

Note

For S7 F/FH systems, this parameter can be increased up to a maximum of 12 hours (720 minutes).

In S7 F/FH systems, the test may not be modified by calling SFC 90, "H_CTRL".
Otherwise, the safety program will go to F-STOP after a maximum of 24 hours. Switching test components on or off is prohibited.

In the event of a STOP, the self-test enters the following diagnostics event in the diagnostic buffer of the F CPU: "Safety program: Error detected" (event ID 16#75E1).



Note

If you are using redundant standard signal modules, the system will generate two data blocks in the AS: DB 1, with the number specified, and DB 2, with the number following this.

Make sure that these blocks are not used twice (e.g. in a Modbus connection). If necessary, adjust the DB numbers in the H parameters.

6.2 Adapting CPU parameters (fault-tolerant F system)

All settings made in the single F-system must also be made in the fault-tolerant F-system.

Note

Parameters in blue can be changed during operation on an H system.

The following settings must also be made when using redundant CPUs:

- Reaction to RAM/PIQ comparison error
- Cyclic interrupt OB with special handling
- Monitoring times

6.2.1 Reaction to RAM/PIQ comparison error

Troubleshooting

TROUBLESHOOTING mode is set by default in response to a comparison error (default response). The purpose of troubleshooting is to locate a faulty CPU.

Select how the H system should react to an error generated during the comparison of the RAM areas and the process images of the outputs:

- Troubleshooting:

  TROUBLESHOOTING mode can only be reached from the "Redundant" system state.

If an error occurs in redundant mode and depending on the error, one of the CPUs goes into TROUBLESHOOTING mode and performs a full self-test. The other CPU becomes the master. If a hardware error is detected, the CPU goes to DEFECTIVE mode. If no error is detected, the CPU is coupled again. The H system goes back into the "Redundant" system state. This is followed by an automatic master-standby switchover. This ensures that when the next error is detected in troubleshooting mode, the hardware of the previous master CPU is tested.

Note

The events that trigger TROUBLESHOOTING mode are described in the following manuals:

- "SIMATIC High Availability Systems S7-400H (https://support.industry.siemens.com/cs/ww/en/view/82478488)"
- "SIMATIC PCS 7 Process Control System CPU 410 Process Automation V8 (https://support.industry.siemens.com/cs/ww/en/view/109801828)"

- H system STOP:
  The entire H system is set to the STOP system mode.
- Standby CPU STOP:
  The standby CPU is set to the STOP mode. The master CPU remains in RUN (solo system mode).

Note

Processing is also paused briefly in the master CPU for the purpose of updating a CPU that is starting up (see Monitoring times).

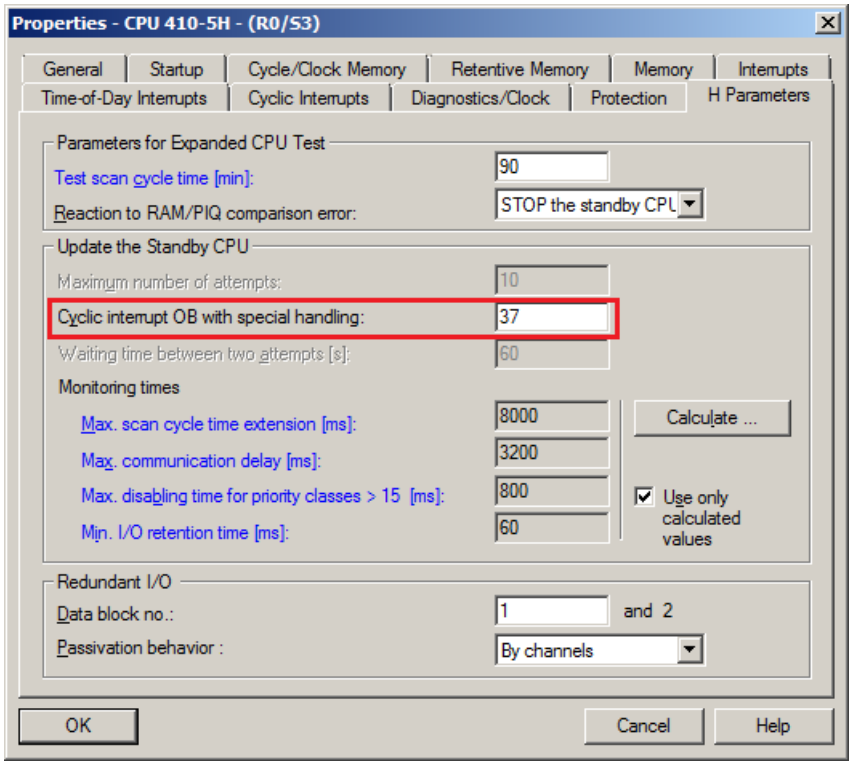
If this is only to occur at certain times defined by the plant operator, "Standby STEO" must be selected as the error reaction. Following this, maintenance personnel must carry out a self-test on both CPUs at an appropriate point in time, by performing a non-buffered CPU startup.

6.2.2 Cyclic interrupt OB with special handling

Priority class

To prevent time monitoring (cyclic interrupt OB or the monitoring time of modules) from being triggered in the event of a CPU that is starting up in the H-system being coupled/updated, you need to set the priority of the cyclic interrupt OBs allocated to the F-program (OB 30 to OB 38) to > 15 on the "Cyclic Interrupts" tab (see Monitoring times).

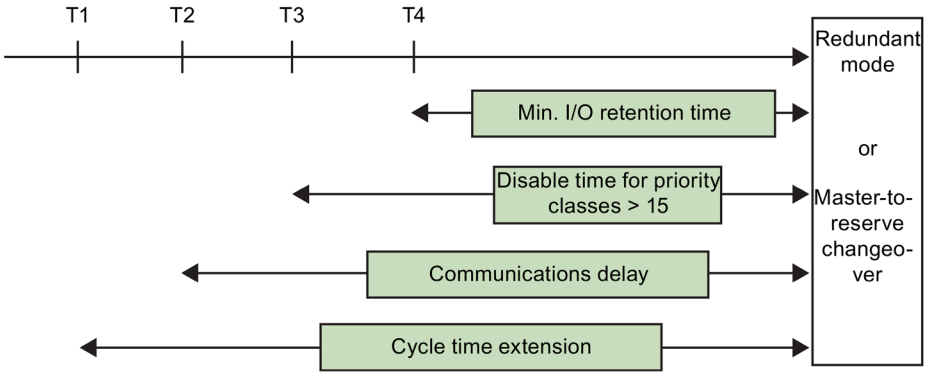
"Cyclic interrupt OB with special handling" is an H parameter containing the number of the cyclic interrupt OB which is called specifically by the operating system when the standby CPU is updated, once all interrupts have been disabled. Here, enter the number of the cyclic interrupt OB with the highest priority, to which F-blocks are assigned in CFC.



6.2.3 Monitoring times

During the update of the standby CPU, it is monitored whether the cycle time extension, the communication delay and the disabling time for priority classes > 15 do not exceed the maximum values you have set. At the same time, it is ensured that the configured minimum I/O retention time is maintained.

The times of relevance to the update process are summarized in the figure below.



T1: End of active OBs up to priority class 15

T2: Stopping of all communication functions

T3: End of cyclic interrupt OB with special handling

T4: End of copying of outputs to standby CPU

If the update fails due to a maximum value being exceeded, the CPU will continue to run in solo mode and try again to update the standby CPU once the specified wait time has elapsed.

Note

You will find more information in the following manuals:

- "SIMATIC High Availability Systems S7-400H (https://support.industry.siemens.com/cs/ww/en/view/82478488)"
- "SIMATIC PCS 7 Process Control System CPU 410 Process Automation (https://support.industry.siemens.com/cs/ww/en/view/109801828)"

If the "Use only calculated values" box is checked (recommended default setting), it will not be possible to enter or modify the monitoring times manually. The best values for the user program can then be determined automatically by clicking the "Calculate..." button.

Note

We recommend only using calculated values.

6.2.4 Calculating monitoring times

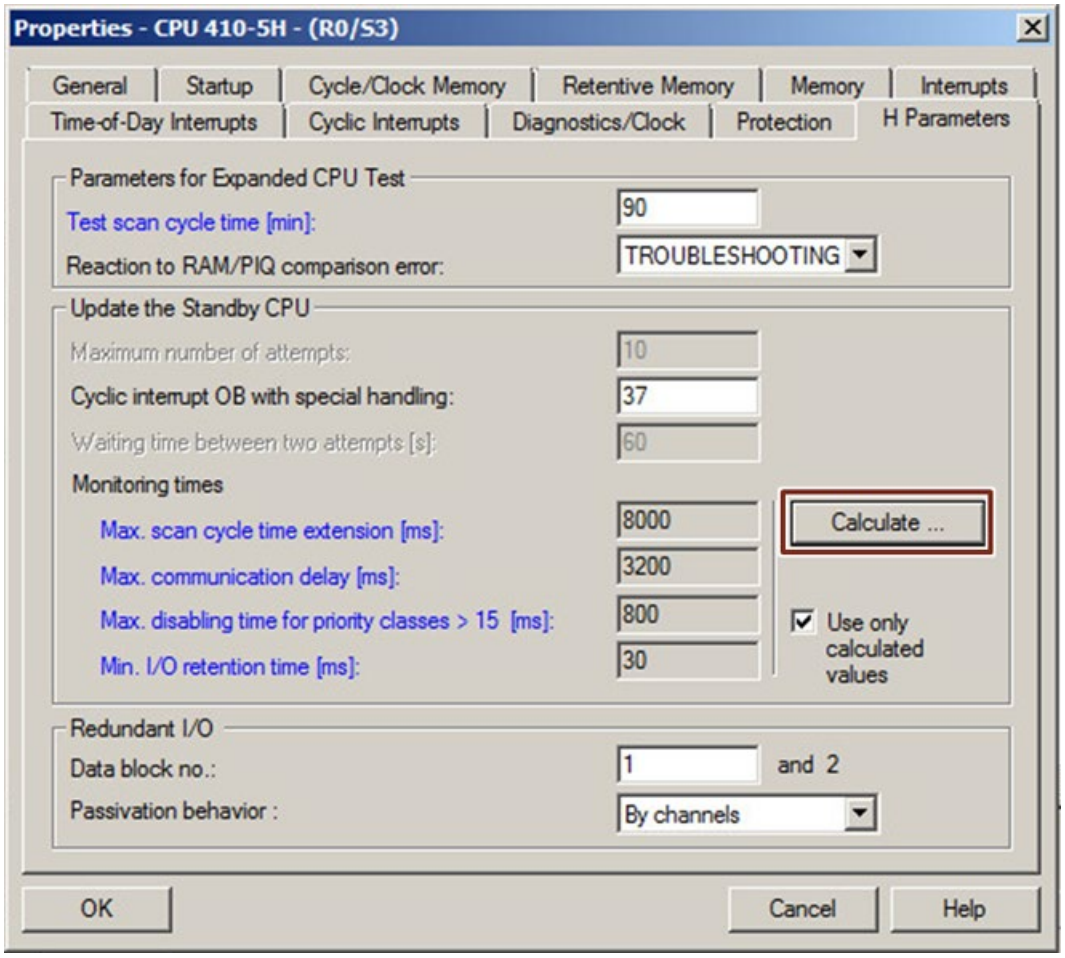
Calculation

You can use this dialog to calculate monitoring times for updating the standby CPU.

You need to enter information about your user program for this purpose:

- Runtime of cyclic interrupt OB with special handling
- Work memory used for all data blocks in the user program

Defaults from the process (monitoring times) and the current configuration (bus parameters, number and type of DP slaves, etc.) are also used in the calculation.



Run time of the cyclic interrupt concerned

If a cyclic interrupt OB with special handling has already been configured, half its execution interval will be entered as the default setting for "Runtime of the watchdog interrupt concerned".

Here, enter the actual runtime of the cyclic interrupt with special handling, plus some reserve time (10 to 20%).

Note

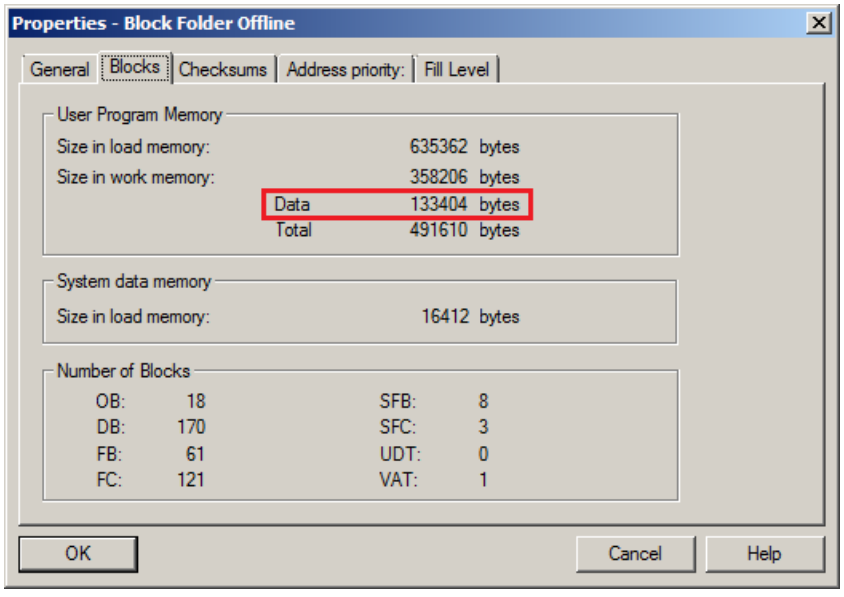
The runtime can be calculated using the TIME_BEG and TIME_END blocks.
You can find information on this in the "How do I set the runtime and time scale of a cyclic interrupt OB?" (https://support.industry.siemens.com/cs/ww/en/view/1023077) FAQ.

As of PCS 7 V7.0 and an S7-400H CPU as of FW V4.5, the run times for the cyclic interrupt OBs may also be read at the CPU_RT block.

Work memory allocation (data memory)

The work memory allocation comprises all data blocks; in other words, it also includes DBs generated dynamically. A value of 1024 KB is entered here by default. This value should be modified to reflect the actual data memory requirements of the user program. We recommend adding an expansion reserve of approximately 10%.

The allocation of work memory for data blocks can be read in SIMATIC Manager by selecting the block container with the menu command "Edit > Object Properties".



Calculation

Once all the parameters have been set, the values are calculated by pressing the "Recalculate" button.

If the F-signal modules are configured in safety mode in HW Config, the "Max. disabling time for priority classes > 15" parameter is calculated using the following formula:

- T_{P15} (DP master system) = T_{PTO} - (2 x T_{TR} + T_{CI} + T_{PROG} + T_{DP_ST} + T_{SLAVE_ST})
  (determined for each DP master system)
- T_{P15_UP} in ms = 0.7 x size of DBs in work memory in bytes/1024 + 75

where:

- T_{PTO} = Shortest F-monitoring time configured on an F-signal module
- T_{TR} = Target rotation time of the PROFIBUS line
- T_{CI} = Call time of the cyclic interrupt OB
- T_{PROG} = Runtime of the cyclic interrupt OB
- T_{DP_ST} = DP switchover time
- T_{SLAVE_ST} = Slave switchover time
- T_{P15_UP} = Time for copying the DBs of the user program (UP)

Calculating the parameters may cause one of the following messages to appear:

- "The F-monitoring times cannot be adhered to due to the configuration specified. Times which can no longer be used were output."

  if:

  "Maximum disabling time for priority classes > 15" < "Minimum I/O retention time" + 50 ms
- "Due to the configuration specified, monitoring times have been calculated to ensure that the F-monitoring time can be adhered to. It cannot be guaranteed that each attempt at coupling and updating will be successful."

  if:

  T_{P15} (DP master system) < T_{P15_UP}

The "Maximum communication delay" and "Maximum scan cycle time extension" are calculated from the "Maximum disabling time for priority classes > 15" by multiplying this setting once by 4 and once by 10.

Note

When determining the shortest F-monitoring time configured on an F-signal module, none of the monitoring times set in PROFIsafe PA devices are taken into account.

Maximum disabling time for priority classes

Check the value for "Maximum disabling time for priority classes > 15".

Note

We recommend doing this again on the plant once commissioning is complete.

Follow the steps outlined below:

- Start up the standby CPU in an H-system.
  Observe the FAQ "What do I have to keep in mind when downloading changes of an H-system with safety program?" (https://support.industry.siemens.com/cs/ww/en/view/89330232).
- The "Maximum disabling time for priority classes > 15" must be greater than the update time that is named in event 16#7303 "Transition to redundant mode" (diagnostics buffer of the master CPU). Make sure you factor reserve time of approximately 20% into your setting.

Note

For more information and remedies, refer to the following manuals:

- "SIMATIC High Availability Systems S7-400H (https://support.industry.siemens.com/cs/ww/en/view/82478488)"
- "SIMATIC PCS 7 Process Control System CPU 410 Process Automation V8 (https://support.industry.siemens.com/cs/ww/en/view/109801828)"

6.3 Communications module parameters/Networks

The settings for communication modules are explained in Compendium Part A.

It may be advisable to operate the F-I/O on a separate DP master system when there are numerous nodes or nodes with low transmission speeds.

PROFINET

PROFINET with PROFINET IO is increasingly used in automation engineering.

PROFINET IO is the open standard defined according to the PROFINET standard for communication between controller and I/O devices based on Switched Ethernet.

The PROFIsafe specification has been expanded for fail-safe communication between controller and PROFINET IOs, and is used in version PROFIsafe V2.x with PROFINET.

You can find additional information about PROFINET IO in the entry "PROFINET in Process Automation with SIMATIC PCS 7" (https://support.industry.siemens.com/cs/ww/en/view/72887082).

Requirements for using PROFINET with S7 F Systems

PROFIsafe version V2, which is required for fail-safe communication via PROFINET, is available in S7 F Systems as of V6.0.

The following components are required to use PROFINET with S7 F Systems:

Software requirements:

- PCS 7 V8.0 SP2 or higher
- S7 F Systems as of V6.1 SP1
- S7 F Systems Lib as of V1_3
- S7 F Configuration Pack V5.5 SP11 or higher

Hardware requirements:

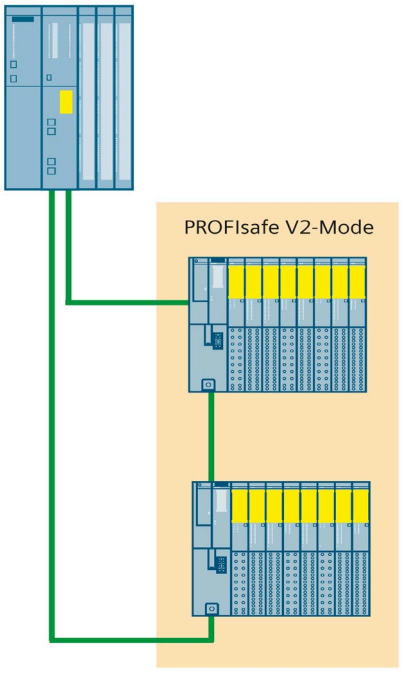
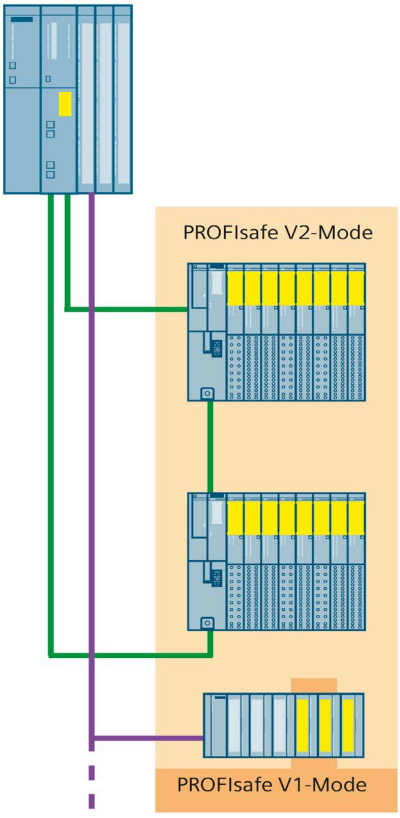
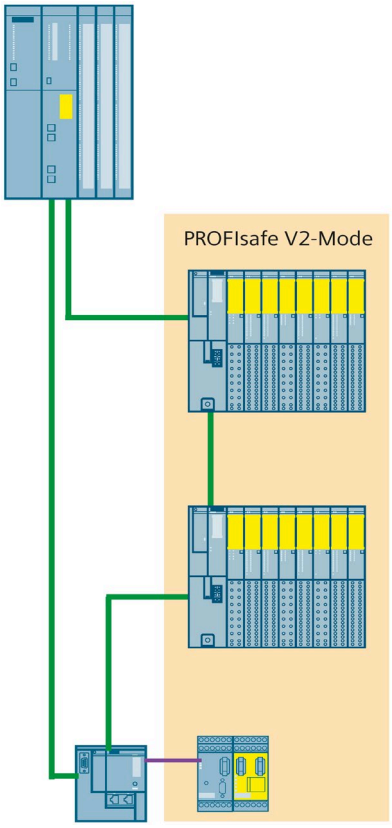
- CPU (CPU 412-5H PN/DP, CPU 414-5H PN/DP, CPU 416-5H PN/DP, CPU 417-5H PN/DP or CPU 410-5H, CPU 410E)
- IO modules ET 200M:
  - SM 326F, DI 24xDC24V (6ES7 326-1BK02-0AB0)
  - SM 326F, DO 10xDC24V/2A, P-switching (6ES7 326-2BF10-0AB0)
  - SM 326F, DO 8xDC24V/2A, P-M-switching (6ES7 326-2BF41-0AB0)
  - SM 336F, AI 6x0/4...20mA HART (6ES7 336-4GE00-0AB0)
- I/O modules ET 200SP HA (S7 F Systems as of V6.3):
  - F-DI 16xDC24V HA (6DL1136-6BA00-0PH1)
  - F-DQ 10xDC24V/2A PP HA (6DL1136-6DA00-0PH1)
- I/O modules ET 200SP HA (S7 F Systems as of V6.4):
  - F-AI 8xI 2/4-wire HART HA (6DL1136-6AA00-0PH1)
    When using F-AI in PCS 7 V9.1, you also need the PCS 7 hardware upgrade package "PCS 7 V9.1 HUP ET 200SP HA F-AI8xI 2/4-wire HART HA" (https://support.industry.siemens.com/cs/ww/en/view/109801821).

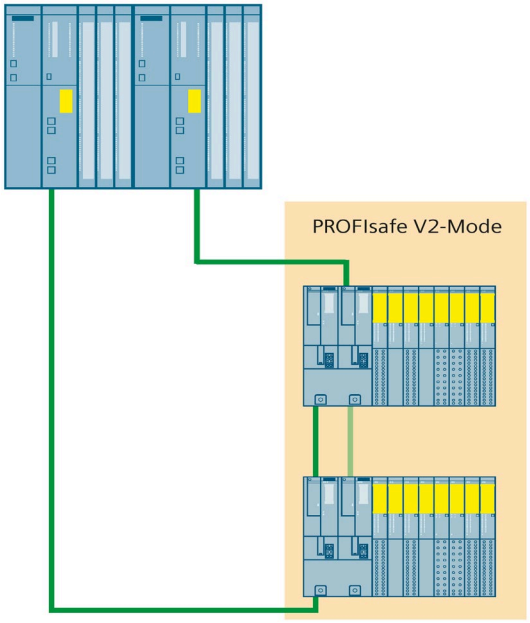
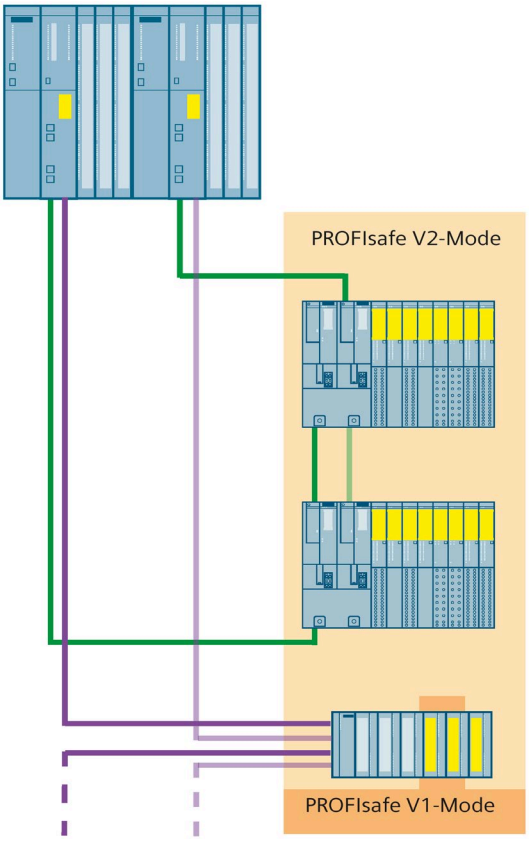
Note

Before you use the fail-safe devices make sure that they support PROFIsafe V2 mode (F_Par_Version = 1) on PROFINET IO as well as in the downstream networks (PROFINET IO or PROFIBUS DP).

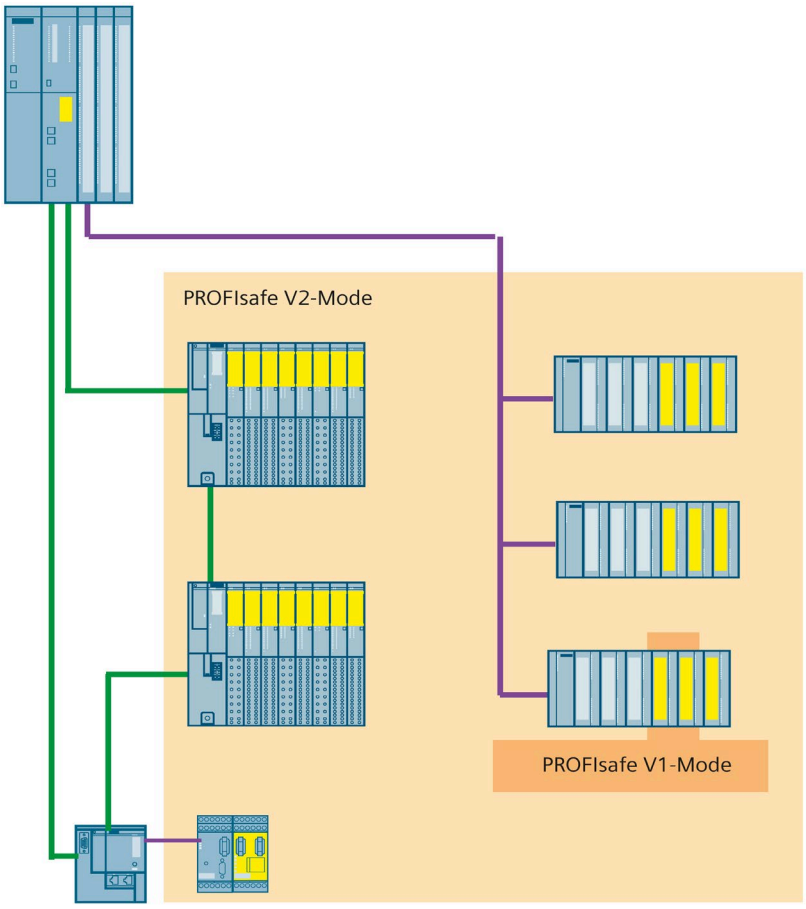
The set PROFIsafe mode of the device is documented in the hardware printout.

Example

Fail-safe signal modules on PROFINET IO	Fail-safe signal modules on PROFINET IO as well as on PROFIBUS DP*	Fail-safe signal modules on PROFINET IO as well as in the downstream PROFIBUS DP* via IE/PB Link
		
	* PROFIsafe V1 mode possible	* PROFIsafe V2 mode required

Fail-safe signal modules on PROFINET IO	**Fail-safe signal modules on PROFINET IO as well as on PROFIBUS DP***
	
	* PROFIsafe V1 mode possible

Fail-safe signal modules on PROFINET IO as well as in the downstream PROFIBUS DP* via IE/PB Link in combination with signal modules on PROFIBUS DP



* PROFIsafe V2 mode required

6.4 Setting system parameters for F-signal modules

Similar to standard modules, F-signal modules are configured in HW Config. This requires the corresponding S7 F Configuration Pack as well as the S7 F Device Integration Pack.

Unused channels can be added during operation, provided that, during first commissioning, they have been activated in HW Config and equipped with resistors in order to suppress channel faults.

Procedure

Once you have added the F-signal modules to the station in HW Config, you can access the "Properties" dialog by selecting the menu command "Edit > Object Properties" or double-clicking the corresponding F-signal module.

6.4.1 Operating mode

Safety mode

For the F-signal modules of the ET 200M, you can use the "Operating mode" parameter to specify whether the modules are to be used in standard mode (use as standard signal modules except SM 326; DO 8 x DC 24V/2A (6ES7326-2BF40-0AB0, 6ES7326-2BF41-0AB0), SM 326 F DO 10xDC24V/2A PP (6ES7326-2BF10-0AB0) and SM 336 F AI6x0/4..20mA HART (6ES7336-4GE00-0AB0)) or safety mode.

F-signal modules of the ET 200SP HA and ET 200iSP can only be used in safety mode.

6.4.2 PROFIsafe addresses

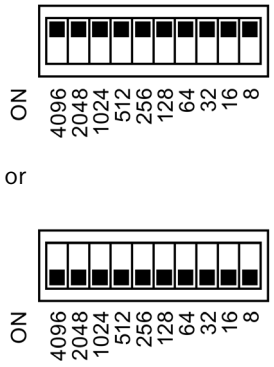
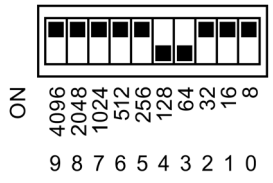
F source and destination addresses

The PROFIsafe addresses (F_SOURCE_ADD, F_DEST_ADD) are used to uniquely identify the source and destination during PROFIsafe communication. The F_DEST_ADD uniquely identifies the PROFIsafe destination (the module). The F_DEST_ADD must, therefore, be unique across both the network and the station. The F_SOURCE_ADD is permanently assigned to the CPU.

To prevent parameter assignment errors, the F_SOURCE_ADD and the F_DEST_ADD are assigned automatically.

Assigning the F-destination address via DIP switch positions

F-signal modules, such as the ET 200M, have DIP switches with which you assign the unique F_DEST_ADD. The DIP switch setting is the binary representation of the F_DEST_ADD. It must be set on the F-signal module DIP switches before you install the F-signal module.

Standard mode	Safety mode
	All possible combinations that do not correspond to standard mode  Module start address 192 corresponds to F_DEST_ADD 24

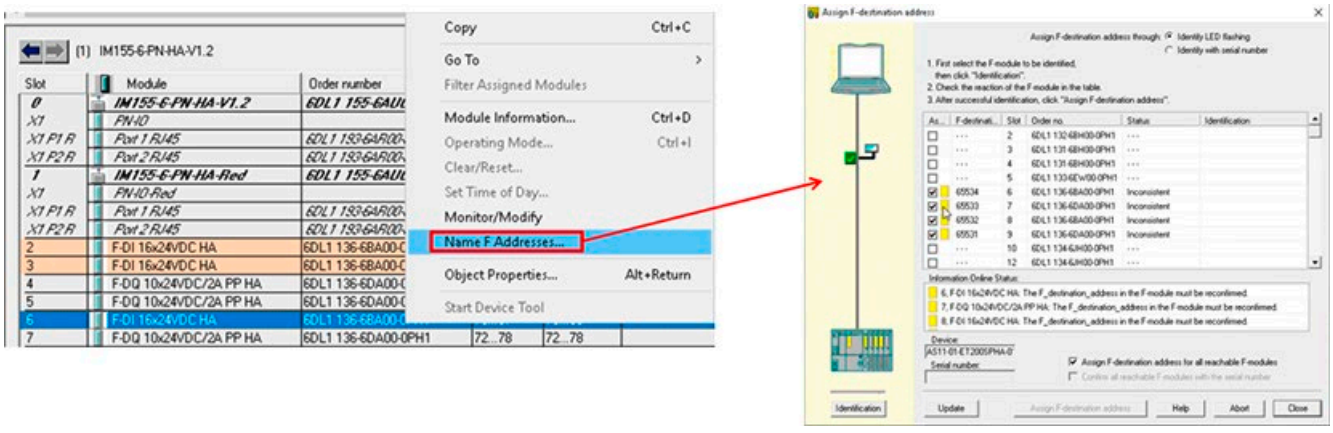
When these modules are in standard mode, F_DEST_ADD is always set to "0" (delivery condition).

In the case of older module versions, the F_DEST_ADD is dependent on the module start address. The following applies: F_DEST_ADD = Module start address/8.

Assigning the F-destination address in the engineering system

F-signal modules, such as the ET 200SP HA, do not have a DIP switch with which you assign the unique F_DEST_ADD. Here, you assign the PROFIsafe address (F_SOURCE_ADD, F_DEST_ADD) directly from the engineering system. The following is a description of the basic procedure:

1. Configure the F_DEST_ADD in HW Config.
2. Switch to online mode and start the tool for assigning the F-destination address.
3. Identify the F-signal modules in the distributed I/O to which you want to assign the configured F_DEST_ADD (together with the F_SOURCE_ADD).
4. Assign the F_DEST_ADD (together with the F_SOURCE_ADD) to the F-signal modules.



Note

You can find additional information on the procedure in the manual "SIMATIC S7 F/FH Systems - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/109802562)".

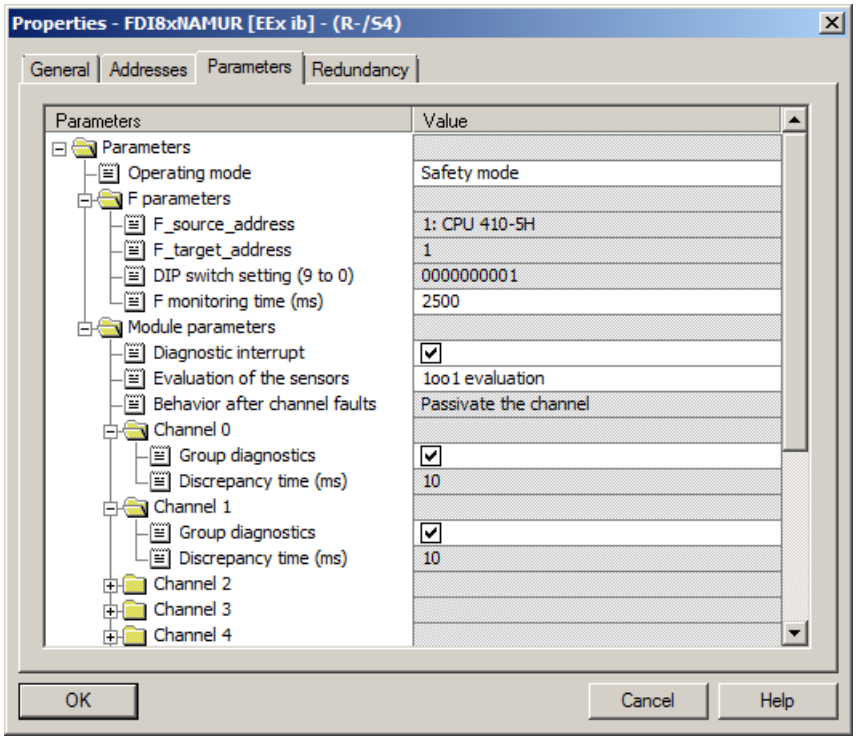
F monitoring time

If you are operating the F-signal module in safety mode, this is where, you set the F-monitoring time for safety-related communication between the F-CPU and F-signal module (PROFIsafe monitoring time).

Note

You can find information on setting the PROFIsafe monitoring time in the "Monitoring and system reaction times (Page 195)" section.

6.4.3 Module parameters - general



Diagnostic interrupt

To enable the PCS 7 driver blocks to report interrupts, the diagnostic interrupt for the F-signal module must always be activated in safety mode.

Various error events, which the fail-safe signal module can define using its diagnostics function, trigger a diagnostics interrupt. The diagnostics events which occur are made available by the F CPU module.

Group diagnostics

If you check this box for a specific channel, a channel-specific event (a wire break, for example) will trigger an error reaction in the safety program (the substitute value is activated on the channel driver and QBAD is set). If "Enable diagnostics interrupt" is selected, a diagnostics interrupt will be triggered in the CPU and a corresponding process control message will be sent on the OS.

The "Group diagnostics" parameter is used to activate and deactivate the transfer of channel-specific diagnostic messages (e.g. wire break, short-circuit) on F-signal modules to the CPU.

For the following F-signal modules of the ET 200M, group diagnostics must also be activated when a channel is activated:

- SM 326; DI 8 x NAMUR (order no. 6ES7326-1RF00-0AB0; 6ES7326-1RF01-0AB0)
- SM 326; DI 24 x DC 24 V (order no. 6ES7326-1BK00-0AB0)
- SM 336; DO 10 x DC 24V/2A (order no. 6ES7326-2BF00-0AB0; 6ES7326-2BF01-0AB0)
- SM 326; AI 6 x 13 Bit (order no. 6ES7336-1HE00-0AB0)

With all other F-signal modules, this takes place automatically when you activate a channel.

To maintain an overview, you should deactivate group diagnostics on input or output channels which are not in use on the F-signal modules or wire the module so that no channel errors occur.

Note

Where fail-safe input and output modules in safety mode are concerned, group diagnostics must be active on all connected channels. Please check that group diagnostics has only been deactivated for input and output channels which are not in use.

6.4.4 Activating channels

With fail-safe signal modules, it is not possible to make and download changes in runtime due to their design.

You can find additional information about changes in HW Config in the section Changes in HW Config (Page 250).

In order to be able to use free channels on F-signal modules for expansion during operation, the channels in the HW Config must be enabled and configured accordingly beforehand. Configure the channels differently in order to be able to connect different sensor types. Due to the diagnostics for the F-signal modules, however, activated channels lead to pending errors, which you can suppress by equipping the channels with equivalent resistors. Channel drivers are not required for these channels. After acknowledgment at an existing F-channel driver, all channels of the affected module are reintegrated.

ET 200SP HA, F-DI 16 x DC 24V HA (6DL1136-6BA00-0PH1)

- Set module parameters
- Determine sensor evaluation
- Determine sensor supply
- If necessary, set discrepancy reaction and discrepancy time
- Activate channel, if needed
- Set channel parameters
- Define potential group
- The following applies for unconnected channels, provided that the sensor supply is provided by the module: Connect the input to the sensor supply via a resistor (e.g. 27 Kilohm).

ET 200SP HA, F-DQ 10 x DC 24V/ 2A PP HA (6DL1136-6DA00-0PH1)

- Set module parameters
- Activate channel, if needed
- Set channel parameters
- Define potential group
- To simulate an actuator, connect the output with a resistor (e.g. 1.8 Kilohm) downstream of the ground connection

ET 200SP HA, F-AI 8xI HART HA (6DL1136-6AA00-0PH1)

- Set module parameters
- Set measurement type
- Set measuring range
- Set channel parameters
- Define potential group
- For unconnected channels, connect the plus input of the channel to the supply voltage via a resistor (e.g. 3.9 Kilohm) and connect the minus input to ground

ET 200M, SM326; F-DI 8 x NAMUR [EEx ib] (6ES7326-1RF00-0AB0 / 6ES7326-1RF01-0AB0)

- Determine operating mode
- Determine operating parameters
- Determine module parameters
- Activate group diagnostics for the channel
- For the suppression of channel errors with unconnected channels, the terminals of the channel can be connected to a resistor (minimum 1 kilohm, optimum 11 kilohms)

ET 200M, SM326; F-DI 24 x DC 24V (6ES7326-1BK00-0AB0 / 6ES7326-1BK01-0AB0 / 6ES7326-1BK02-0AB0)

- Determine operating mode
- Determine module parameters
- Determine sensor supply
- Activate channel
- Determine sensor evaluation
- Determine type of sensor interconnection
- If necessary, set discrepancy reaction and discrepancy time
- Provided that the sensor supply comes from the module:
  Connect input to the sensor supply via a resistor (e.g.: 1 kilohm).

ET 200M, SM326; F-DO 10 x DC 24V/2A (6ES7326-2BF01-0AB0)

- Determine operating mode
- Determine module parameters
- Activate group diagnostics for the channel
- For unconnected channels, to simulate an actuator, connect the output with a resistor (e.g. 2.7 Kilohm) downstream of the ground connection

ET 200M, SM326; F-DO 10 x DC 24V/2A PP (6ES7326-2BF10-0AB0)

- Determine module parameters
- Activate group diagnostics for the channel
- For unconnected channels, to simulate an actuator, connect the output with a resistor (e.g. 2.7 Kilohm) downstream of the ground connection

ET 200M, SM326; F-DO 8 x DC 24V/2A PM (6ES7326-2BF40-0AB0 / 6ES7326-2BF41-0AB0)

- Determine module parameters
- Activate group diagnostics for the channel
- For unconnected channels, to simulate an actuator, connect the output with a resistor (e.g. 2.7 Kilohm) downstream of the ground connection

ET 200M, SM 336; F-AI 6 x 13 Bit (6ES7336-1HE00-0AB0)

- Determine module parameters
- Activate group diagnostics for the channel
- Make channel-specific settings
- For unconnected channels, connect the plus input of the channel to the supply voltage via a resistor (e.g. 3.9 Kilohm) and connect the minus input to ground

ET 200M, SM 336; F-AI 6 x 0/4...20mA HART (6ES7336-4GE00-0AB0)

- Determine module parameters
- Determine type of sensor interconnection
- Make channel-specific settings
- Make HART communication settings
- For unconnected channels, connect the plus input of the channel to the supply voltage via a resistor (e.g. 3.9 Kilohm) and connect the minus input to ground

ET 200iSP, EM; F-DI 8 x NAMUR Ex (6ES7138-7FN00-0AB0)

- Determine module parameters
- Determine sensor supply
- Activate channel
- Determine sensor evaluation
- Determine type of sensor interconnection
- If necessary, set discrepancy reaction and discrepancy time
- The following applies for unconnected channels, provided that the sensor supply is provided by the module: Connect the input to the sensor supply via a resistor (minimum 1 kilohm, optimum 11 kilohms).

ET 200iSP, EM; F-DO 4 x 17.4V/40mA Ex (6ES7138-7FD00-0AB0)

- Determine module parameters
- Activate group diagnostics for the channel
- For unconnected channels, to simulate an actuator, connect the output with a resistor (e.g. 2.7 Kilohm) downstream of the ground connection

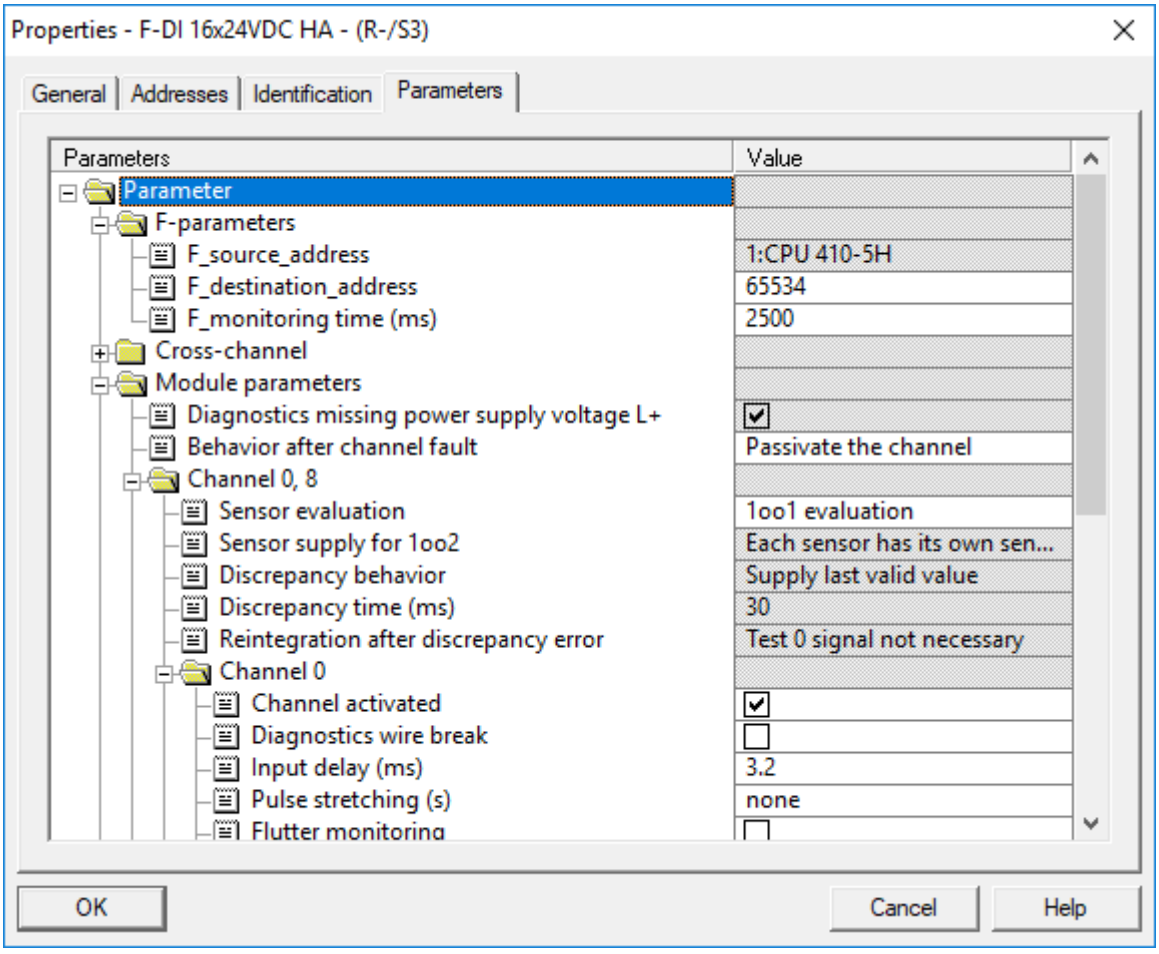
ET 200iSP, EM; F-AI 4 x 0/4...20mA Ex HART (6ES7138-7FA00-0AB0)

- Determine module parameters
- Make channel-specific settings
- Make HART communication settings
- For unconnected channels, connect the plus input of the channel via a resistor (e.g. 3.9 Kilohm) to the minus input of the channel

See also

SIMATIC S7 F/FH Systems – Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/109802562)

6.4.5 Configuration for ET 200SP HA, F-DI 16 x DC 24V HA



Sensor supply

You can set whether the sensor is supplied via the F-signal module using these parameters. Additionally, you can also activate a short-circuit test for the supply through the F-signal group.

Short-circuit test

Here, you activate the short-circuit detection for the channels of the F-module for which an internal sensor supply is set.

The short-circuit test is only possible if an internal sensor supply is set. A short-circuit test is not possible for sensors with power supply, e.g. 3-/4-wire proximity switches.

Short-circuit detection disconnects the sensor supply briefly. The switch-off duration is the same as the configured "Time for short-circuit test (ms)".

If a short-circuit is detected, the F-module triggers a diagnostic interrupt in the F-CPU and the input is passivated.

Sensor evaluation

- 1oo1 evaluation

A sensor connected 1-channel to the F-signal module

- 1oo2 non-equivalent evaluation
- 1oo2 equivalent evaluation

For a process signal one or two sensors are connected to two inputs on an F-signal module. The signal states of inputs (equivalence or non-equivalence) are compared internally.

Discrepancy behavior

For "discrepancy behavior", parameterize the value provided to the safety program in the F CPU during the discrepancy between the two affected input channels – i.e. during running discrepancy time. You configure the discrepancy behavior as follows:

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

Discrepancy time

Where "1oo1 evaluation" is concerned, the value displayed is not relevant.

In most cases, the discrepancy time is started but does not completely elapse because the signal differences even out after a short time.

Select a sufficiently long discrepancy time so that in the error-free case the difference between the two signals always disappears before the discrepancy time expires (when testing for non-equivalence: the equivalence of the two signals).

Reintegration after discrepancy error

You can use this parameter to determine when a discrepancy error is considered lifted and, therefore, when a reintegration of the affected input channels is possible. You can choose between the following parameter options:

- "Test 0 signal required"
- "Test 0 signal not required"

Option "Test 0 signal required":

- If you have configured "Test 0 signal required", a discrepancy error is only considered to be lifted when a 0 signal is again present at both input channels concerned.
- If you use non-equivalent sensors, that is, you have set the "Sensor evaluation" to "1oo2 evaluation, non-equivalent", then the result of the channel pair must be "0" again.

Option "Test 0 signal not required":

- If you have configured "Test 0 signal not required", a discrepancy error is regarded as corrected when a discrepancy is no longer present at both of the affected input channels.

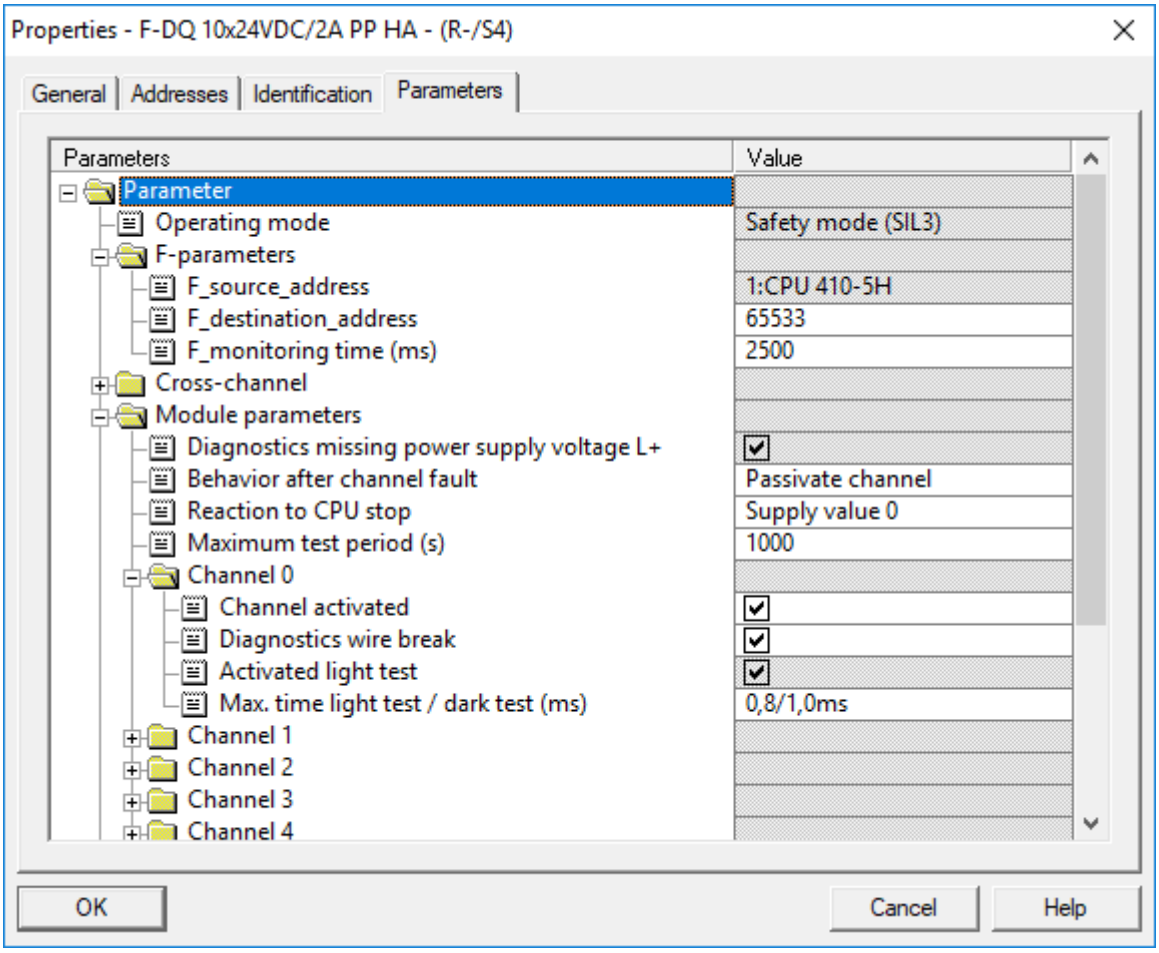
Potential group

Specifies whether the I/O module is located on a terminal block with supply voltage infeed

Note

You can find additional information on configuration in the manual "SIMATIC ET 200SP HA Digital Input Module F-DI 16x24VDC (https://support.industry.siemens.com/cs/ww/en/view/109802477)"

6.4.6 Configuration for ET 200SP HA, F-DQ 10 x DC 24V/ 2A PP HA



Behavior after channel fault

You can use this parameter to specify whether the entire I/O module is passivated after a channel error or if only the faulty channel(s) is/are passivated:

- "Passivate entire module"
- "Passivate channel"

Response to CPU STOP

Defines the behavior of the digital output at CPU STOP or in case of a communication failure between interface module and CPU:

- Supply 0 value
- Supply last valid value

Maximum test time

You can use this parameter to define the time within which the light, dark and switch-on tests (complete bit pattern test) are performed module-wide. After this time elapses the tests are repeated.

- Use "1000 s", for example, to spare your actuators
- Use "100 s" to detect errors faster

Light test activated

The "Light test activated" parameter is only for display. The light test is always active when the channel is activated.

Max. time for light test/dark test

You can use this parameter to set the times for readback during the light test and the dark test.

Note

Effects of "Max. time light test/dark test" on the error response time

Since the error response time is increased by the time "Max. time light test/dark test", we recommend that you set this time as low as possible, but high enough so that the output channel is not passivated.

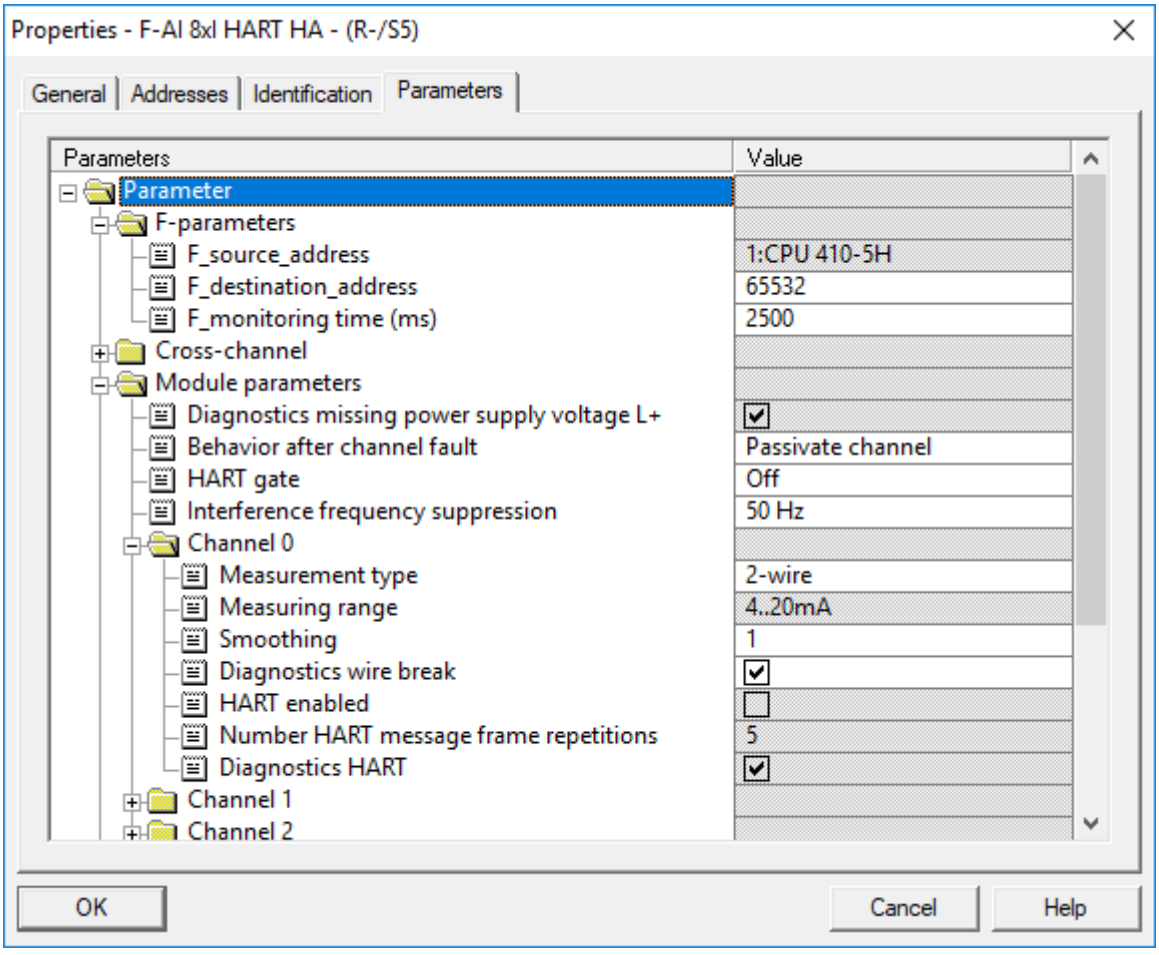
Potential group

Specifies whether the I/O module is located on a terminal block with supply voltage infeed

Note

You can find additional information on configuration in the manual "SIMATIC ET 200SP HA Digital Output Module F-DQ 10x24VDC/2A PP HA (https://support.industry.siemens.com/cs/ww/en/view/109802499)"

6.4.7 Configuration for ET 200SP HA, F-AI 8xI 2-/4-wire HART HA



Measurement type

You can use this parameter to choose between 2-wire and 4-wire transmitters. With a 2-wire transmitter, the sensor supply is internal, with a 4-wire transmitter it is external. To deactivate unused channels, select "deactivated". If you deactivate unused channels, the response time of the F-I/O module is reduced.

Note

Behavior of the internal sensor supply with measurement type "2-wire"

After activation of the internal sensor supply (e.g. during the module startup or after a short-circuit of the sensor supply), the "Wire break" diagnostic and "Low limit violated" are suppressed for three seconds to avoid passivation of the respective channel by the sensor ramp-up. During this time, the module provides the safe process value 0 on all channels.

Measuring range

At an active channel, you can choose between different measuring ranges via the parameter. The I/O module has the following measuring ranges:

- 0 to 20 mA (4-wire)
- 4 to 20 mA (2-wire / 4-wire)

HART operation is only possible with a measuring range of 4 to 20 mA. HART communication is not switched off even at currents below 4 mA.

Filter

Compensates for measured value fluctuations. Individual measured values are smoothed using filtering. Smoothing is achieved by the F-I/O module forming the moving average of a number of digitized analog values specified with the "Smoothing" parameter.

Note

Smoothing is reset after startup, short-circuit, wire break or another channel error. If smoothing is configured with 16 conversion cycles and all channels are active, for example, it takes up to 2400 ms with a set interference frequency suppression of 50 Hz until the process value is reported. Until the first valid process value, the I/O module reports the value 0 and QI = 0 for the channel.

Diagnostics wire break

Enable wire break detection. The module can only detect a wire break when the parameter is enabled. Here, you enable wire break detection for a configured measuring range of 4 to 20 mA. If you do not need a channel, disable it. Then there is no wire break detection.

HART gate

You can use this parameter to enable the HART communication for the I/O module. The "HART gate" parameter acts as a module-wide, fail-safe "main switch". The following parameter assignments are possible:

- "On": HART communication is enabled
- "Off": HART communication is disabled

HART enabled

You can use this parameter to enable HART communication for the relevant channel. Can only be configured if "HART gate" is enabled and the measuring range "4 to 20 mA" is set. The parameter is not safety-related, that is, no fail-safe switch-off of the HART communication is possible with this parameter.

Number of HART telegram repetitions

Specifies the number of HART telegram repetitions. If the I/O module receives no response or an incorrect response to a HART telegram sent to the field device, the telegram is repeated accordingly, that is, it is sent to the field device again. The parameter is only relevant if the "HART enabled" parameter is activated.

HART diagnostics

Enabling the diagnostics for the HART telegram-specific supervisions and the status information supplied by the connected field device in the HART telegram. The parameter is only relevant if the "HART enabled" parameter is activated. HART diagnostics are reported as maintenance events.

Behavior after channel fault

You can use this parameter to specify whether the entire F-module is passivated after channel errors have occurred, or only the faulty channels are passivated:

- "Passivate entire module"
- "Passivate channel"

Interference frequency suppression

Suppresses the interference caused by the frequency of the AC network used. The following parameter assignments are possible:

- 50 Hz (integration time 20 ms)
- 60 Hz (integration time 16.6 ms)

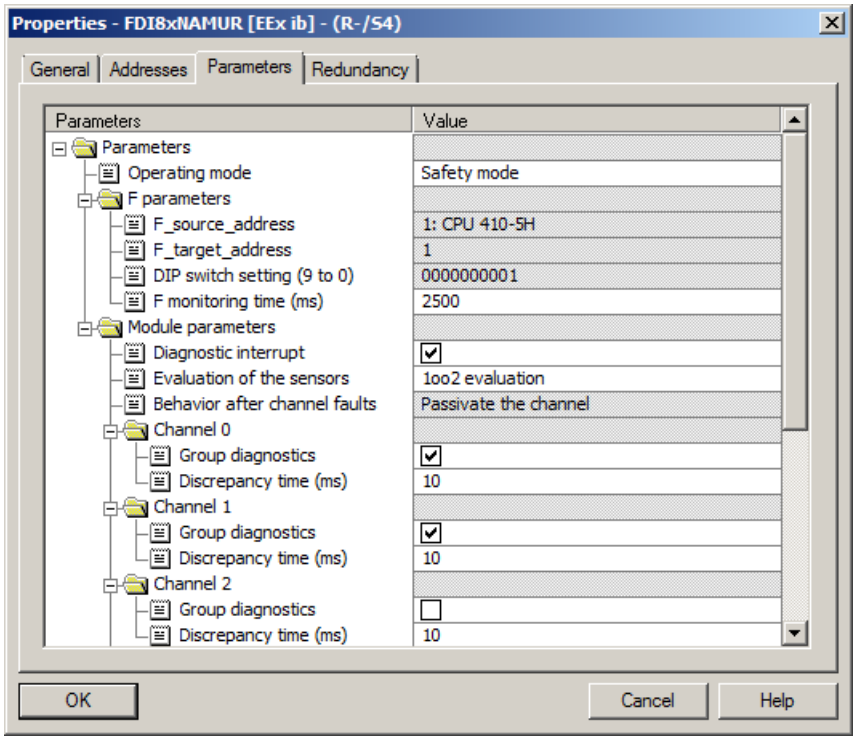
Potential group

Specifies whether the I/O module is located on a terminal block with supply voltage infeed

Note

You can find additional information on configuration in the manual "SIMATIC ET 200SP HA Analog Input Module F-AI 8xI 2-/4-wire HART HA (https://support.industry.siemens.com/cs/ww/en/view/109802504)"

6.4.8 Configuration for ET 200M, SM326; DI 8 x NAMUR



Sensor evaluation

- 1oo1 evaluation

  A sensor connected 1-channel to the F-signal module

- 1oo2 evaluation

  For a process signal one or two sensors are connected to two opposite inputs on a F-signal module. The signal states of inputs (equivalence or non-equivalence) are compared internally.

The following safety classes can be achieved:

- 1-channel – SIL 2; in the case of multiple channels SIL 3 can be achieved via evaluation in the CPU.
- 2-channel - SIL 3 (evaluation on module)

Group diagnostics

Group diagnostics must be activated for all used channels.

Discrepancy time

Where "1oo1 evaluation" is concerned, the value displayed is not relevant.

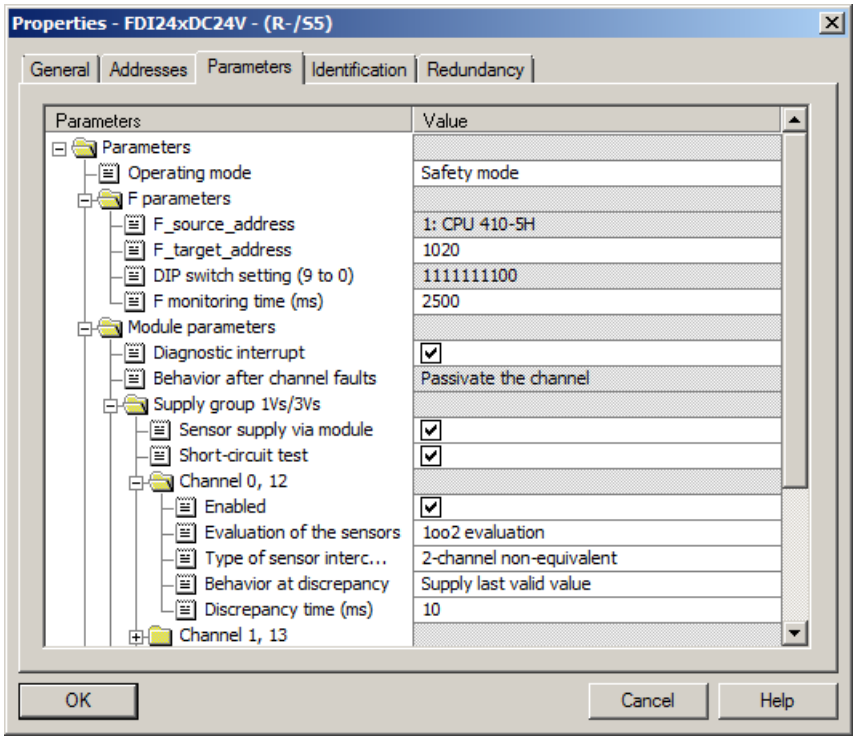
The discrepancy analysis is used for fail-safe inputs in order to detect errors from the temporal characteristic of two signals with identical functionality.

The discrepancy analysis is started if different levels are determined for two associated input signals. A test is run to see whether the difference disappears once a configurable period of time known as the discrepancy time has elapsed. If not, there is a discrepancy error. Monitoring of the discrepancy time extends the system response time. Therefore, select the lowest possible number of channels with discrepancy evaluation.

Note

You can find additional information on configuration in the manual "SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-safe Signal Modules (https://support.industry.siemens.com/cs/ww/en/view/19026151)"

6.4.9 Configuration for ET 200M, SM326; DI 24 x DC 24V



Sensor supply via module

You can set whether the sensor is supplied via the F-signal module using these parameters. Additionally, you can also activate a short-circuit test for the supply through the F-signal group.

Short-circuit test

You can use this parameter to activate short-circuit detection for the F-signal module.

The short-circuit test can only be activated for sensors that are supplied by the F-signal module.

Short-circuit detection disconnects the sensor supply briefly and tests the input signal. In so doing, a cross circuit is detected between the channels and an "L+" fault at the active inputs. Whenever a short-circuit is detected, the F-signal module will trigger a diagnostic interrupt on the CPU and send a corresponding process control message to the OS.

Sensor evaluation

- 1oo1 evaluation
  A sensor connected 1-channel to the F-signal module.
- 1oo2 evaluation
  For a process signal one or two sensors are connected to two opposite inputs of an F-signal module. The signal states of inputs (equivalence or non-equivalence) are compared internally.

The following safety classes can be achieved:

- 1-channel – SIL 2; in the case of multiple channels SIL 3 can be achieved via evaluation in the CPU.
- 2-channel - SIL 3 (evaluation on module)

Type of sensor interconnection

If "1oo2 sensor evaluation" is selected, you can select the type of sensor interconnection for each input channel (exception: SM 326; DI 8 x NAMUR, for which this parameter does not exist. For this module, only 2-channel equivalent sensor interconnection can generally be selected where "1oo2 evaluation" is concerned.):

- "2-channel equivalent"
  A two-channel sensor or two single-channel sensors (2-channel connection) is/are connected to two opposite input channels
- "2-channel non-equivalent"
  One non-equivalent sensor or two single-channel, non-equivalent sensors (2-channel connection) is/are connected to two opposite input channels
- "1-channel"
  A sensor (1-channel) is connected to two opposite inputs.

Note

If you are using the "2-channel non-equivalent" or "1-channel" type of sensor interconnection, and the internal sensor supply and the short-circuit test are configured, the Vss supply voltage from the left-hand side of the F-signal module must be used.

Discrepancy behavior

For "discrepancy behavior", parameterize the value provided to the safety program in the F CPU during the discrepancy between the two affected input channels – i.e. during running discrepancy time. You parameterize the discrepancy behavior as follows.

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

Discrepancy time

Where "1oo1 evaluation" is concerned, the value displayed is not relevant.

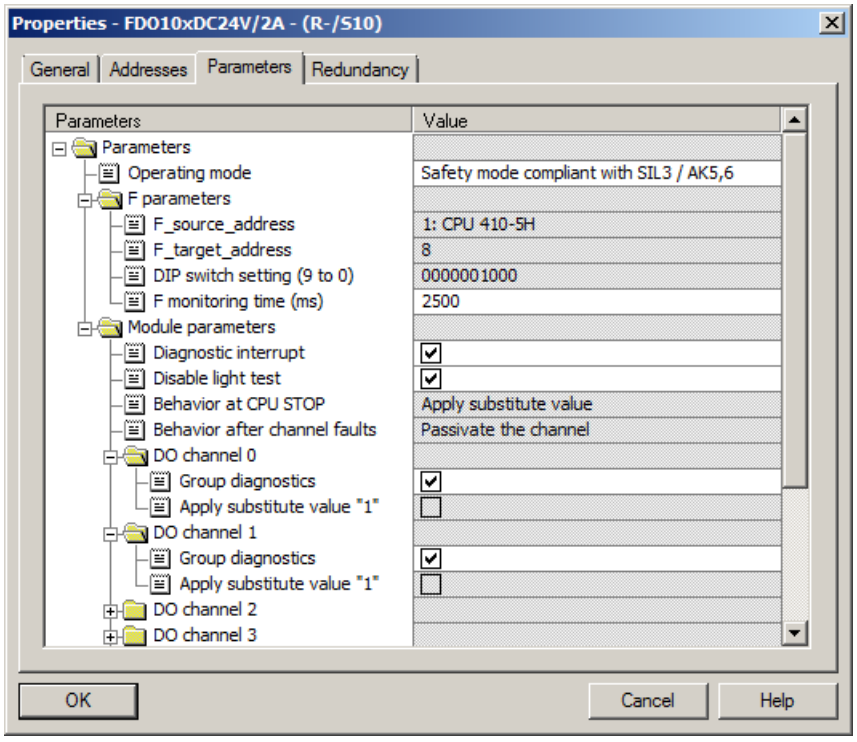
The discrepancy analysis for equivalence/non-equivalence is used for fail-safe inputs in order to detect errors from the temporal characteristic of two signals with identical functionality.

The discrepancy analysis is started whenever different levels (when testing for non-equivalence: the same level) are detected on two associated input signals. A test is run to see whether, once a configurable period of time known as the discrepancy time has elapsed, the difference (when testing for non-equivalence: the match) disappears. If not, there is a discrepancy error. The discrepancy time extends the system response time. Therefore, select as low a discrepancy arrangement of the sensor as possible in the process.

Note

You can find additional information on configuration in the manual "SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-safe Signal Modules (https://support.industry.siemens.com/cs/ww/en/view/19026151)"

6.4.10 Configuration for ET 200M, SM326; DO 10 x DC 24V/2A



On fail-safe output modules, the required safety class is achieved by injecting test signals.

Deactivating the light test

For the purpose of the test, 1-signals are connected to the output while the output is inactive (output signal "0"). This setting activates the output briefly (< 1 ms) (= "light period").

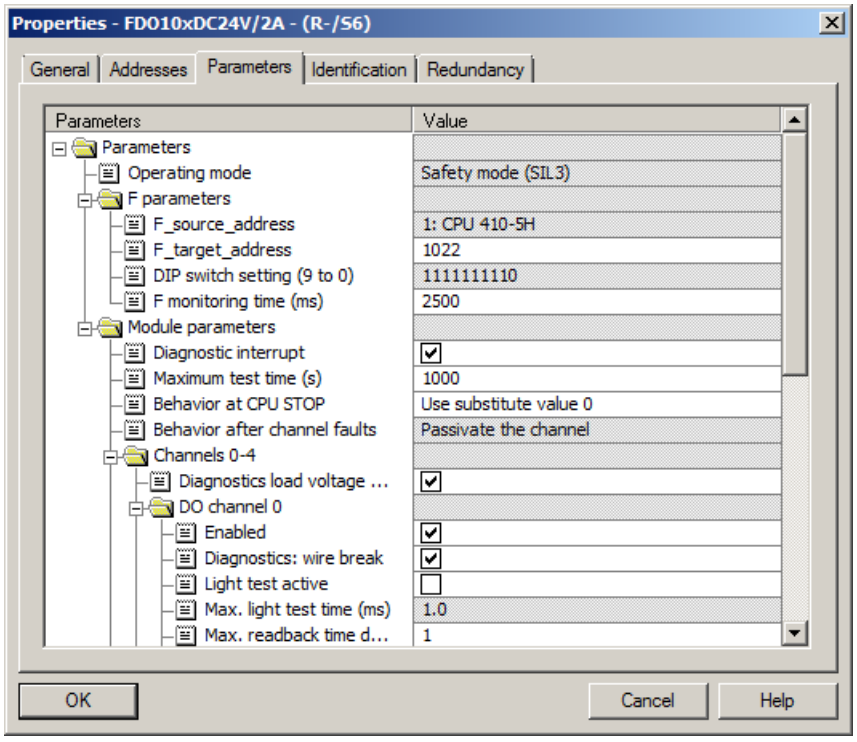
The dark test, which the module performs cyclically, is sufficient for SIL 2. This involves connecting 0 signals to the output while it is active. The output is deactivated briefly (< 1 ms) ("dark period") in order to detect short circuits. In order to detect cross circuits between outputs, during the dark test various bit patterns are issued one after the other to a group of outputs (first the left half of the module, then the right half).

For SIL 3, the light test also needs to be performed or the output switched at least once a day.

Note

You can find additional information on configuration in the manual "SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-safe Signal Modules (https://support.industry.siemens.com/cs/ww/en/view/19026151)"

6.4.11 Configuration for ET 200M, SM326; F-DO 10 x DC 24V/2A PP



Maximum test time

With the parameter "maximum test time(s)", you determine the time within which the light and dark tests are to be conducted (in all combinations) for the whole module. After this time elapses the tests are repeated. Enter 100s if an error is to be detected quickly, or 1000s if an actuator needs to be cleared.

Response to CPU STOP

If "Keep last valid value" is set for this parameter, the last valid process value 0 or 1 is kept in events such as an abortion of PROFIsafe communication or STOP of the F CPU.

Load voltage failure diagnostics

This parameter activates the diagnostic message for a load voltage failure to 2L+ and 3L+.

Light test activated

The module conducts complete bit pattern tests within the configured maximum test time. If the output is active in the "good condition", a dark test is always conducted. If the output is not active in the "good condition", activate the light test with this parameter. If the signal changes daily or more often, SIL3/Kat.4/PLe can be achieved even without a light test. If this is not reached with a "0" signal, the light test must be activated which then fulfills this condition.

Maximum light test time

With the parameter "maximum test time(s)", you determine the time within which the light and dark tests are to be conducted (in all combinations) for the whole module. After this time elapses the tests are repeated.

Light periods arise during the complete bit pattern test. In this process, a test signal is connected to the output from the fail-safe output module while the output is inactive ("0" output signal). This then activates the output briefly (= "light period"). A sufficiently inactive actuator does not respond to this and remains deactivated.

Each output channel has its own configurable maximum light test time.

The maximum light test time should be set sufficiently high if the affected channel switches high capacitive loads. If the maximum light test time is set too low for a controlled capacitive load, the output channel is passivated because charging does not occur within the configured time.

In the event of faulty readback signals, the light test signal is available for the parameterized maximum light test time at the output before the error "Short circuit to M" leads to the passivation of the output channel.

Set maximum light test time:

1. If an output channel is continuously being passivated with an intact F SM, this can be in contact with a capacitive component of the controlled load that is too large.
   In such an instance, configure the maximum light test time to the maximum value of 5 ms.
   If passivation of the channel continues to occur, either an external fault is present or the connected capacity lies outside of the permitted range.
2. Since the fault reaction time is extended by the configured maximum light test time, the light test time should be set as low as possible by trial and error (however, high enough to avoid passivating the output channel).
3. If you have set a maximum light test time in a way that results in the output channel being passivated sporadically, set the next higher value of the maximum light time.

Maximum dark test readback time

Dark times occur during the complete bit pattern test. In this process, a test signal is connected to the output from the fail-safe output module while the output is active ("1" output signal). This deactivates the output briefly (= "dark period"). A sufficiently inactive actuator does not respond to this and remains activated. Each output channel has its own configurable maximum readback time for the dark test.

The maximum readback time should be set sufficiently high if the affected channel switches high capacitive loads. If the maximum readback time is set too low for a connected capacitive load, the output channel is passivated, since discharge does not occur within the configured time.

Configure these parameters so that the module reads back correctly and your actuator still does not react to the switch-off pulse.

Set readback times:

1. If an output channel is continuously being passivated with an intact F-SM, this can be in contact with a capacitive component of the controlled load that is too large.
   In such an instance, configure the readback time to the maximum value of 400 ms. If passivation of the channel continues to occur, either an external fault is present or the connected capacity lies outside of the permitted range.
2. Since the fault response time is extended by the readback time, the readback time should be set as short as possible when testing (but long enough so the output channel is not passivated).
3. If you have set a readback time in a way that results in the output channel being sporadically passivated, set the next higher value for the maximum readback time dark test. Dark periods arise during deactivation tests and the complete bit pattern test. In this process, a test signal is connected to the output from the fail-safe output module while the output is active ("1" output signal).

Redundant interconnection

With this parameter you set whether this channel is operated redundantly.

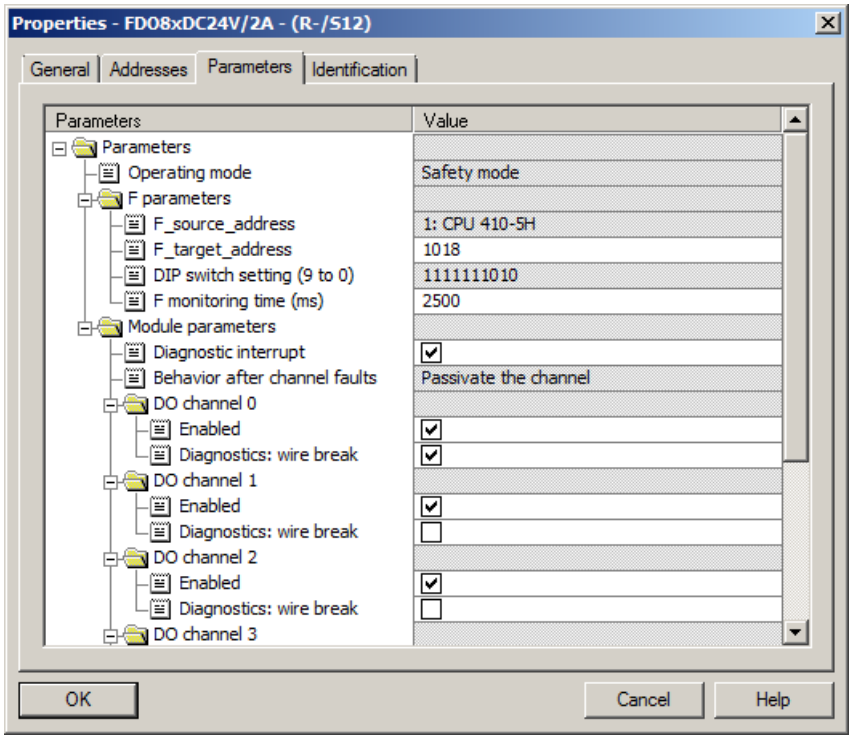
Note

If you do not activate this channel with a redundant interconnection the "Short circuit of output to L+ or output driver defect" diagnosis is reported.

Note

You can find additional information on configuration in the manual "SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-safe Signal Modules (https://support.industry.siemens.com/cs/ww/en/view/19026151)"

6.4.12 Configuration for ET 200M, SM326; F-DO 8 x DC24 V/2A PM



The module can only be used in safety mode, not redundantly. For the purpose of switching an actuator, each module is provided with one switch in the plus line (P switch) and one in the minus line (M switch). An actuator must be connected between the P and M switches to enable the module to be used for safety applications up to SIL 3.

Diagnostic interrupt

The diagnostic interrupt for the F-signal module must always be activated in safety mode.

Enabled

Activates channel processing

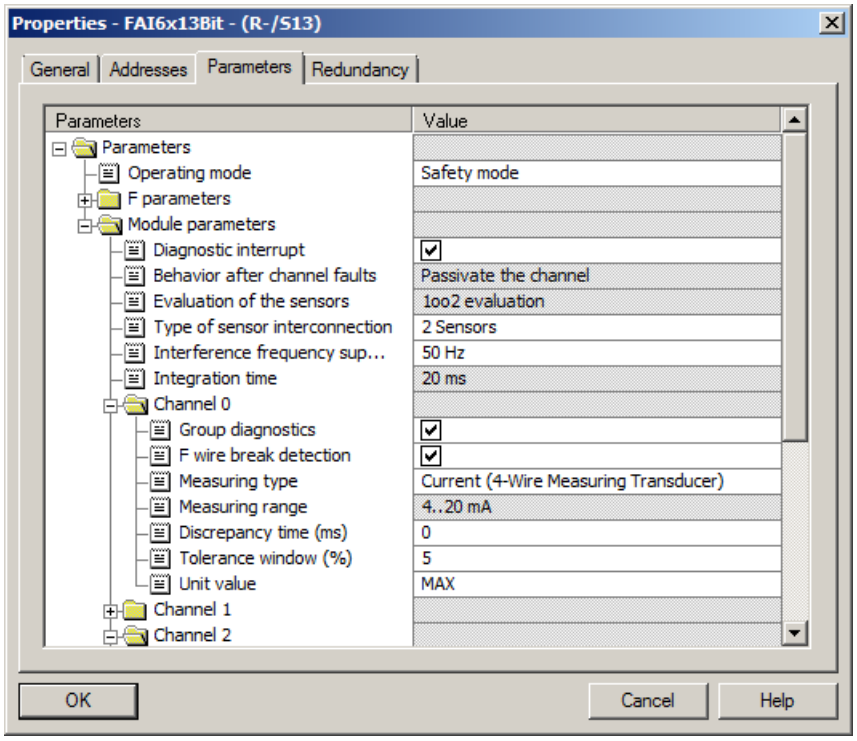
Diagnostics: Wire break

Activates wire-break monitoring on the channel

Note

You can find additional information on configuration in the manual "SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-safe Signal Modules (https://support.industry.siemens.com/cs/ww/en/view/19026151)"

6.4.13 Configuration for ET 200M, SM336; AI 6 x 13Bit

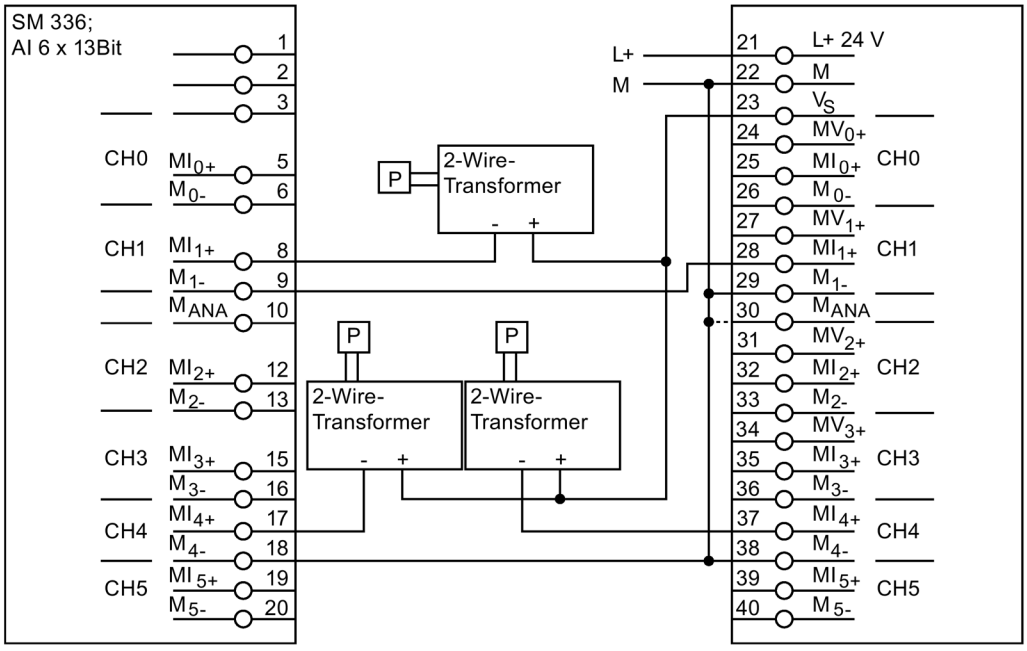


Sensor evaluation (analog inputs)

- 1oo2 evaluation

  1 sensor connected 1-channel redundantly (evaluation on module). The module has six SIL 3 capable channels.

Safety class SIL3 can be achieved here:



Type of sensor interconnection (analog inputs)

When safety mode is activated 1 or 2 sensors can be configured per input channel. Discrepancy handling can be set accordingly.

Interference frequency suppression

Setting interference frequency suppression for the line frequency The corresponding integration time of the analog digital converter is displayed.

If you change this setting, the increment for the F-monitoring time and for the discrepancy times will also change automatically. The values set there will be adjusted to the next lowest value.

F wire-break detection

You can set whether a wire-break check is to be performed for each individual channel (< 3.6 mA; otherwise, detected at 1.18 mA underflow).

If wire break is detected, a diagnostics interrupt will be triggered in the CPU and a corresponding process control message will be sent on the OS.

F-short-circuit detection

If a short-circuit is detected, a diagnostics interrupt will be triggered in the CPU and a corresponding process control message will be sent on the OS.

Advanced short-circuit diagnostics can be triggered when required by means of additional limit-value monitoring.

Measurement type

The measurement type depends on the operating mode selected.

The operating mode can be selected for each channel. In safety mode the following measurement types are available:

- "2DMU" or "4DMU" for current measurements. (4 to 20mA)
- "Deactivated": The channel is not processed by the module.

Measuring range

The selection options in the measuring range field vary depending on the selected mode (safety mode activated or deactivated) as well as the measurement type. If a channel is deactivated, it will not be possible to select a measuring range.

Note

If you are using Marshalled Termination Assemblies (MTAs), you should select 4DMU for the configuration, since the supply is provided via the MTAs.

Note

In safety mode, only the 4 to 20 mA measuring range is permitted. In this measuring range, a current of < 3.6 mA will produce a wire-break signal. If you have to process signals that are lower due to the sensor (e.g. gas sensor), you can deactivate this F-wire break detection. In this case, a current of < 1.18 mA will produce an underflow message.

Discrepancy handling (analog inputs)

In the processing industry, no evaluation is generally performed between 2 signals on the module. 1oo1 is set for sensor evaluation. This makes all the signals available in the user program, where they can be linked in 1oo2 or 2oo3, depending on what is required. If 1oo2 evaluation is to be implemented on the module, you can find the parameter description for discrepancy handling in the online help.

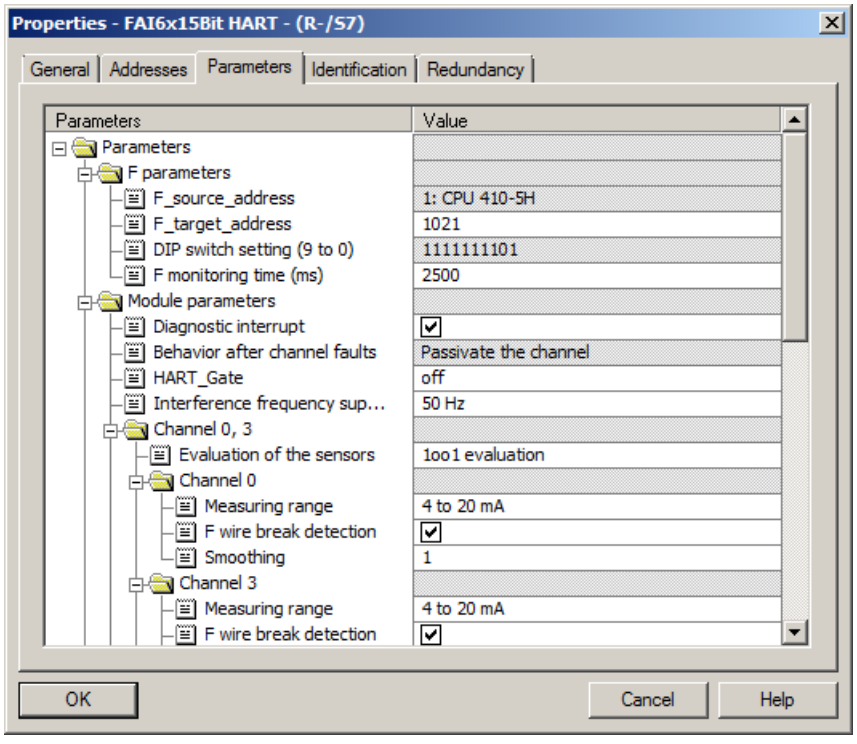
Note

You can find details on possible wiring variants in the application example "Wiring and Voting Architectures for ET 200M F-AI (https://support.industry.siemens.com/cs/ww/en/view/24690377)".

Note

You can find additional information on configuration in the manual "SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-safe Signal Modules (https://support.industry.siemens.com/cs/ww/en/view/19026151)"

6.4.14 Configuration for ET 200M, SM336; F-AI 6 x 0/4...20mA HART



Diagnostic interrupt

The diagnostic interrupt for the F-signal module must always be activated in safety mode.

HART gate

This enables HART communication with the transducers to be controlled. ON/OFF switches HART communication on or off for the entire module, in a safety-related manner. If "Can be switched" is set here, HART communication may be enabled or disabled on the F-channel driver.

Interference frequency suppression

Setting interference frequency suppression for the line frequency The corresponding integration time of the analog digital converter is displayed.

If you change this setting, the increment for the F-monitoring time and for the discrepancy times will also change automatically. The values set there will be adjusted to the next lowest value.

Sensor evaluation

- 1oo1 evaluation: Each channel is considered individually and the input value forwarded to the CPU.
- 1oo2 evaluation: 2 channels are combined in all cases (0/3, 1/4, and 2/5). A discrepancy analysis is performed on the module and the configured input value is forwarded to the CPU. With this setting, the parameters for the discrepancy analysis can be configured.

Measuring range

The measuring ranges 0 to 20 mA and 4 to 20 mA are available for selection. With 0 to 20 mA, HART communication is not possible.

F wire-break detection

In the 4 to 20 mA measuring range and with wire-break detection activated, a message is issued when a current of < 3.6 mA is present. If wire-break detection is deactivated, an underflow message is issued if a current of < 0.4444 mA is present (as with the 0 to 20 mA measuring range).

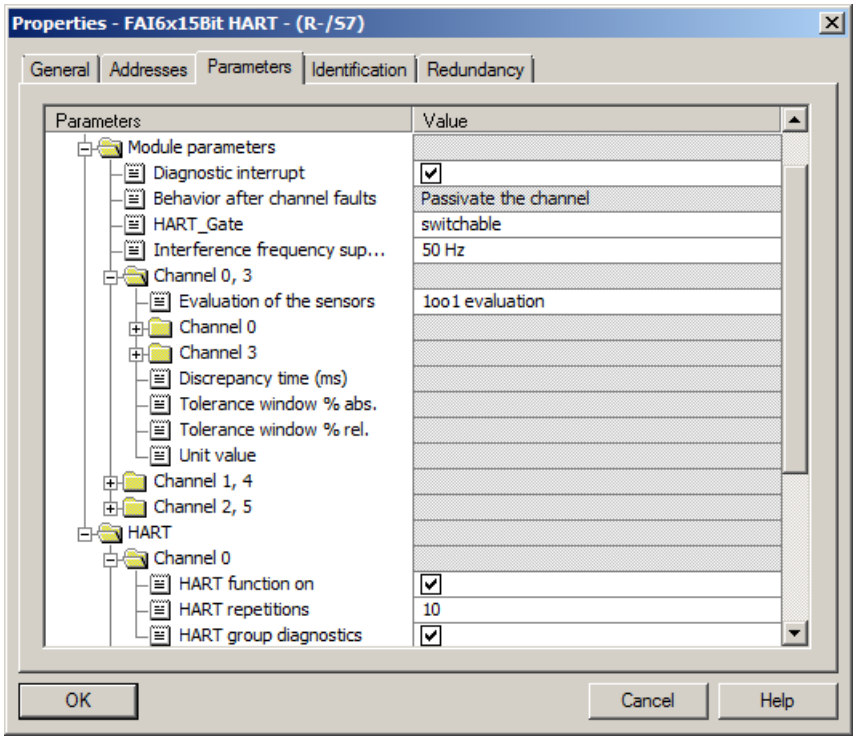
Filter

The module filters the input signal throughout the specified number of acquisition cycles.

Please note that input signal filtering will lengthen the system's reaction time.

Discrepancy handling (analog inputs)

In the processing industry, no evaluation is generally performed between 2 signals on the module. 1oo1 is set for sensor evaluation. This makes all the signals available in the user program, where they can be linked in 1oo2 or 2oo3, depending on what is required. If 1oo2 evaluation is to be implemented on the module, you can find the parameter description for discrepancy handling in the online help.



HART

Here, you can switch off HART communication on specific channels in a non-safety-related manner, as well as enable HART diagnostics options and determine how often the module will attempt to establish HART communication with the transducer before a message is issued.

In the case of HART devices for which parameter assignment cannot be interlocked, HART communication must be switched off.

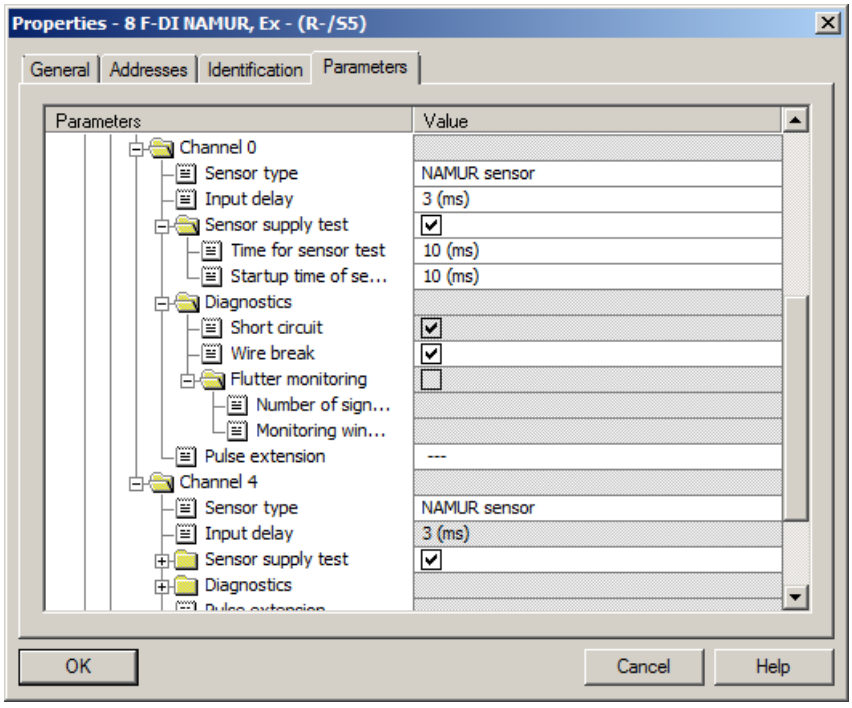
Note

You can find additional information on configuration in the manual "SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-safe Signal Modules (https://support.industry.siemens.com/cs/ww/en/view/19026151)".

See also

Software components (Page 12)

6.4.15 Configuration for ET 200iSP, EM 8 F-DI NAMUR Ex

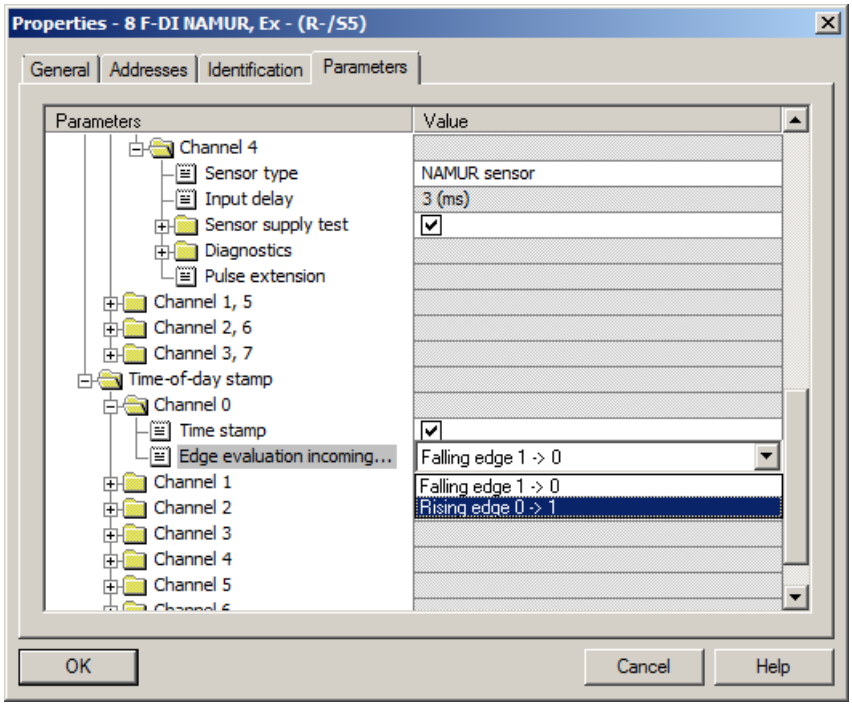


Reintegration following a discrepancy error

You use this parameter to determine when a discrepancy error is considered lifted and, therefore, when a reintegration of the affected input channels is possible. You can choose between the following parameter options:

- "Test 0 signal required"
  If you have configured "Test 0 signal required", a discrepancy error is only considered lifted once a 0 signal is present at both input channels concerned.
  If you employ non-equivalent sensors – i.e. "sensor evaluation" is configured to "1oo2 non-equivalent evaluation" – then a 0 signal must be present at the lower value channel of the pair.

- "Test 0 signal not required"
  If you have configured "Test 0 signal not required", a discrepancy error is considered lifted if no discrepancy is present any more at both input channels.



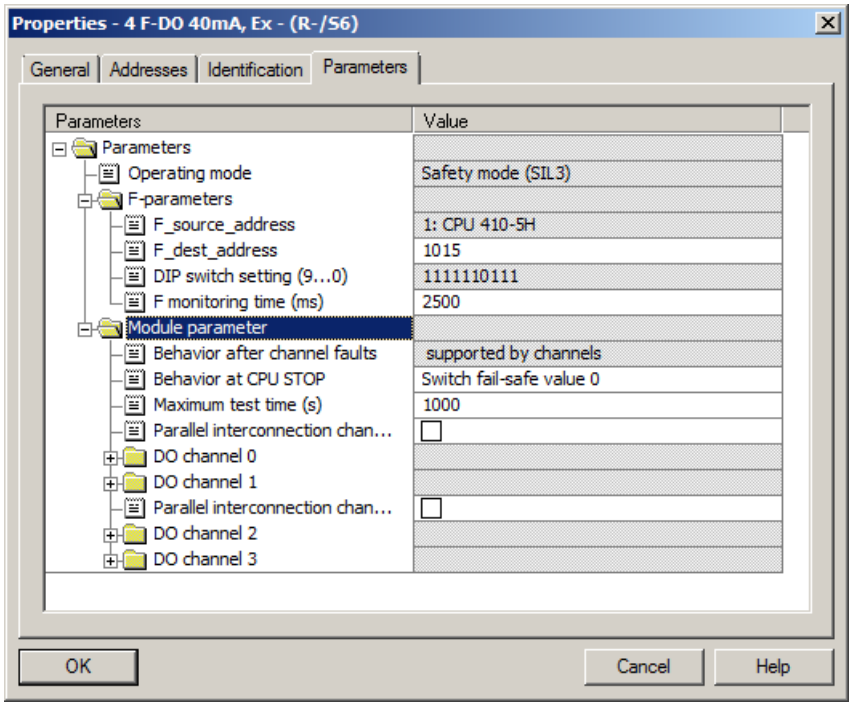
Time stamp

Changes to input signals are provided with a time stamp (date and time) during time stamping and reported as a coming event.

Note

You can find additional information on configuration in the manual "SIMATIC Distributed I/O Distributed I/O device ET 200iSP – Fail-safe Modules (https://support.industry.siemens.com/cs/ww/en/view/47357221)".

6.4.16 Configuration for ET 200iSP, EM 4 F-DO Ex 17.4V/40mA



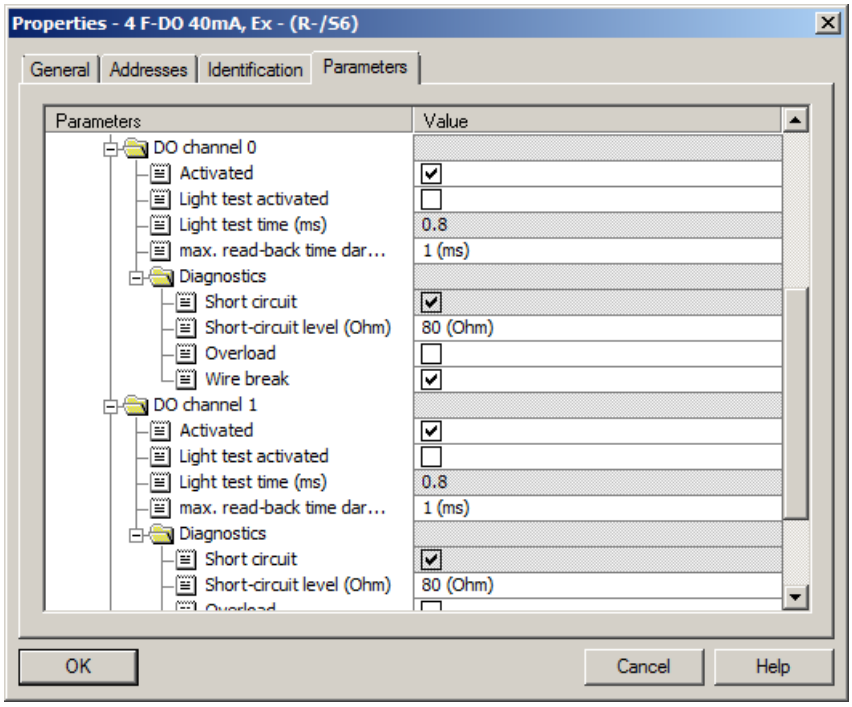
"Maximum test time" parameter

With the parameter "maximum test time(s)", you determine the time within which the light and dark tests are to be conducted (in all combinations) for the whole module. After this time elapses the tests are repeated.

Parallel interconnection

To improve performance you can connect two digital outputs of the module for an actuator in parallel (channel coupling). This increase in performance is only permitted on the same module and between the following channels:

- Channel 0 and channel 1: Connection between terminal 3 and 7
- Channel 2 and channel 3: Connection between terminal 11 and 15



Maximum dark test readback time

Dark periods arise during deactivation tests and the complete bit pattern test. In this process, a test signal is connected to the output from the fail-safe output module while the output is active ("1" output signal).

This deactivates the output briefly (= "dark period"). A sufficiently inactive actuator does not respond to this and remains activated. Each output channel has its own configurable maximum readback time for the dark test. Configure these parameters so that the module reads back correctly and your actuator still does not react to the switch-off pulse.

Short-circuit level

The "short-circuit level" parameter determines the value of the load which, if undershot, leads to the module diagnosing a short circuit and switching off the channel.

This means that in the range between employing the current limiting (the inflection point on the output curve) and the reaching of the short-circuit level, no diagnostics are transmitted. The channel remains switched on until the load undershoots the short-circuit level.

Overload

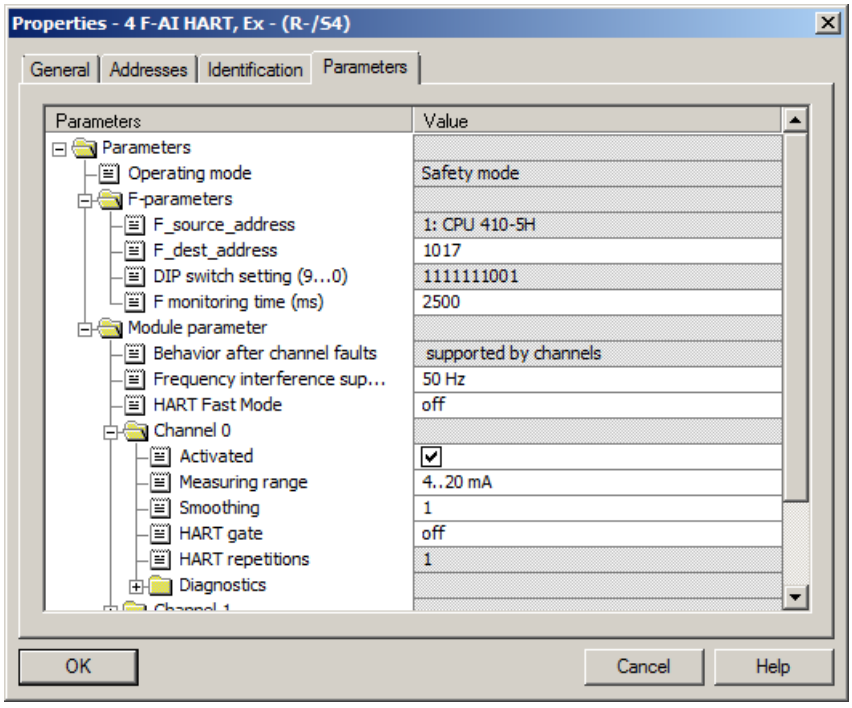
If you use the parameter "overload" in addition to the parameter "short-circuit level", the following will result:

- In the range between employing the current limiting (the inflection point on the output curve) up to the reaching of the short-circuit level, an "overload" diagnostic is transmitted and an entry in the diagnostics buffer is made, without the module switching off the channel.
- The "short-circuit level" parameter in turn determines the value of the load which, if undershot, leads to the module diagnosing a short circuit and switching off the channel.

Note

You can find additional information on configuration in the manual "SIMATIC Distributed I/O Distributed I/O device ET 200iSP – Fail-safe Modules (https://support.industry.siemens.com/cs/ww/en/view/47357221)".

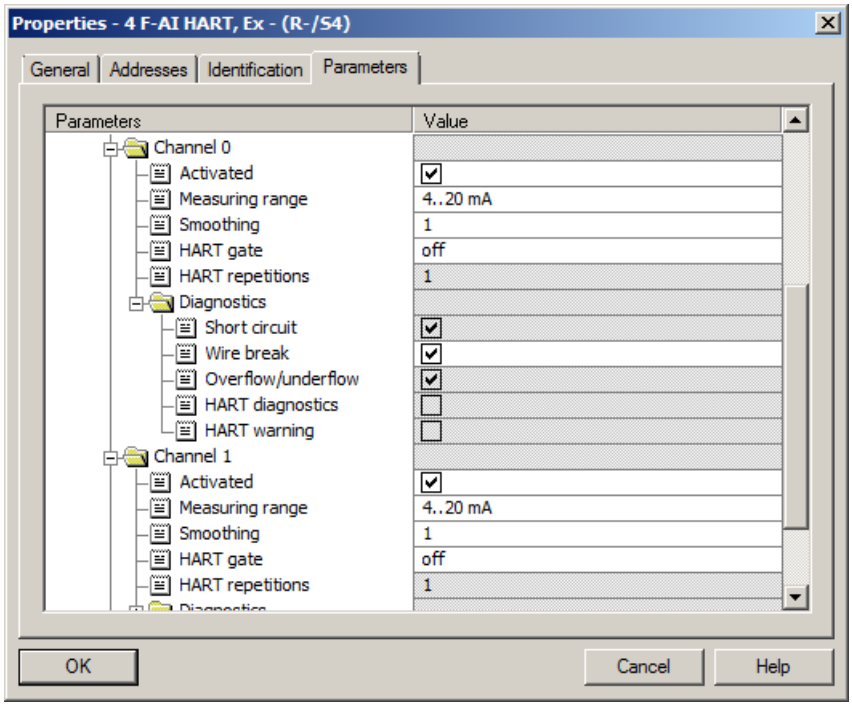
6.4.17 Configuration for ET 200iSP, EM 4 F-AI Ex HART



HART Fast Mode

The electronic module is HART Fast Mode-capable and supports the processing of HART commands as an SHC (Successive HART Command) sequence. If a HART command is detected by the electronic module with a set SHC bit for a channel, the complete HART command processing is reserved for approx. 2 seconds on the electronic module for this channel. For all other channels of the electronic module, no HART command processing occurs during this time.

For each additional HART command with a set SHC bit, the electronic module reserves the HART command processing for this channel again for a further 2 s. If a HART command is recognized for this channel without a set SHC bit, or if no further command for this channel arrives within 2 seconds after the previous HART command, the electronic module returns to "normal" HART command processing. Result: All HART channels are re-processed.



HART diagnostics

If you enable these parameters, a diagnostics interrupt is triggered during subsequent HART diagnostics.

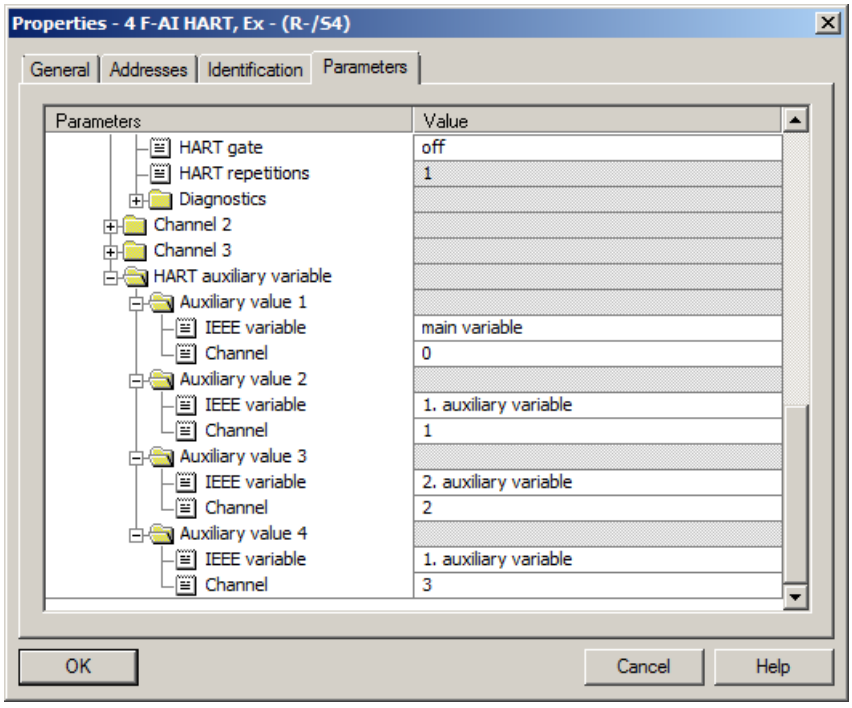
- HART analog output current specified
- HART analog output current saturated
- HART communication error
- HART primary variable outside limits
- HART secondary variable outside limits
- HART error function HART device

HART warning

If you enable these parameters, a diagnostics interrupt is then triggered during subsequent HART diagnostics:

- HART further status available
- HART configuration changed

HART secondary variables



The configured HART secondary variables of the 4 F-AI HART module (6ES7 138-7FA00-0AB0) are not supported by the PCS7 channel driver blocks.

You can find more information in the manual "SIMATIC Distributed I/O Distributed I/O device ET 200iSP – Fail-safe module" (https://support.industry.siemens.com/cs/ww/en/view/47357221).

6.5 Configuring redundant F-signal modules

For redundant, fail-safe digital input modules, the F channel driver F_CH_DI can run a discrepancy analysis to increase availability when S7 F Systems Lib V1_3 is being used. You need to set the "Discrepancy time" parameter in the hardware configuration for this purpose. Set a discrepancy time of "0" to deactivate the discrepancy analysis.

The F-channel driver F_CH_DI provides the result of the discrepancy analysis at output DISCF or DISCF_R. The signals must either be further processed in the logic or signaled with a signal module.

F_CH_AI does not perform a discrepancy analysis prior to S7 F Systems Lib 1_3 SP1 Upd1.

As of S7 F Systems Lib V1_3 SP2, F_CH_AI can also perform a discrepancy analysis. The function must be enabled at the DISC_ON input and discrepancy time (DISC_TIM) and deviation (DELTA) must be configured at the corresponding inputs. As with F_CH_DI, the discrepancy error output (DISCF) must be connected to a message block to signal the error.

6.5.1 IO redundancy of ET 200SP HA

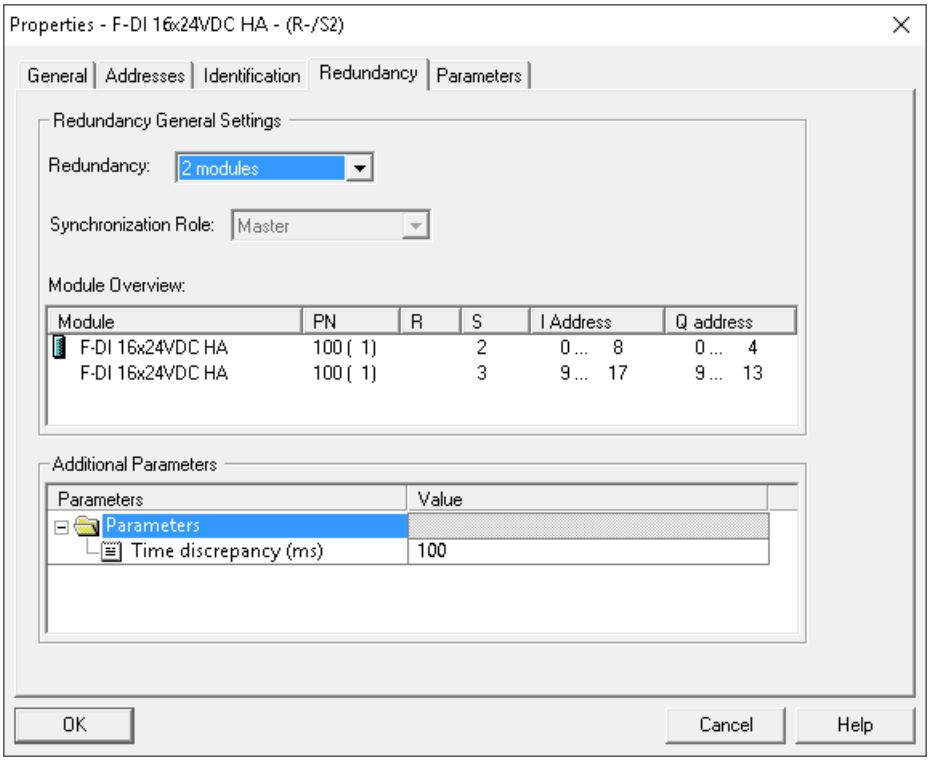
You can use the F-signal modules of the ET 200SP HA redundantly. For IO redundancy, two input/output modules (module pair) of the same type are plugged into a special terminal block next to one another. This terminal block connects the respective process signals of both modules to a common process terminal.

With F-signal modules configured with redundancy, please note the following:

- Both F-signal modules have the same article number, the same firmware version and a compatible hardware version.
- Both F-signal modules of the same type must be placed directly next to each other on a terminal block for IO redundancy of the ET 200SP HA. This terminal block connects the respective process signals of the two modules to a common process terminal. The F-signal module on the left must be plugged into a slot with an even slot number; this is then the master. The F-signal module of the same type placed to the right of it is always the slave. The assignment of the synchronization role cannot be changed.
- If the F-signal modules of the ET 200SP HA are used redundantly, a process image partition must be set for these modules to fully support the diagnostic functionality within the scope of PCS 7 Asset Management. It is not permitted to install the process image partition of the F-module and the call of the F-driver module in different cyclic interrupt OBs.

Procedure

1. In HW Config, you configure the two F-signal modules in the ET 200SP HA station.
2. For one of the two redundant F-signal modules, select the "2 modules" operating mode in the "Redundancy" tab. For the F-signal module placed on the left with the even slot number, the "Master" setting is then automatically displayed in the "Synchronization role" selection field. "Slave" is displayed for the F-signal module placed on the right.
3. Set further parameters as necessary. For redundant F-signal modules, changes can only be made at the master, except for the "F_DEST_ADD". The changes are automatically adopted by the slave.
4. Check the default discrepancy time for redundant, fail-safe digital input modules.



5. Create a symbol for the lower I/O address and interconnect the channel driver with this address.

6.5.2 IO redundancy of ET 200M

With redundantly deployed fail-safe signal input modules of the ET 200M, there are two application cases.

- One sensor: The sensor is wired to both redundant F-signal modules.
- Two sensors: One sensor is wired to each of the redundant F-signal modules (module and sensor are redundant).

If you have wired one sensor to both F-signal modules, Zener diodes are required so that the electrical circuit is not interrupted when a redundant module is pulled. If you require a discrepancy analysis for the purpose of monitoring Zener diodes, select the same procedure as for two sensors. As an alternative, an MTA which already contains the Zener diodes can be used. Also refer to the section "Marshalled Termination Assemblies (MTA) for ET 200M (Page 99)".

If you are using two sensors, then both signals should also be available in the user program. In this case, it is not possible to use the redundancy function of the F-AI module. Read both signals in and use block F_1oo2AI for signal selection and discrepancy analysis purposes.

Note

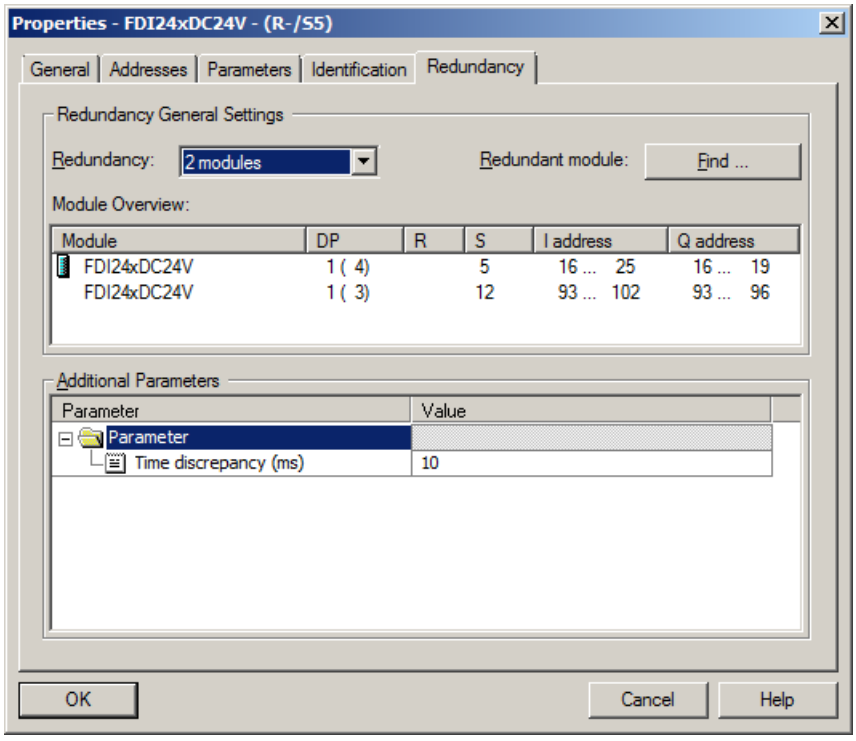
You can find additional information on the configuration of redundant F-signal modules in the manual "SIMATIC S7 F/FH Systems - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/109802562)".

You can use the fail-safe signal modules S7-300 (F-signal modules) – with the exception of the F-DO 8 x DC 24V/2A PM – redundantly in one ET 200M or in several different ET 200Ms. With F-signal modules configured with redundancy, please note the following:

- The two F-signal modules are of the same FW and HW product versions.
- "Safety mode" is set for both F-signal modules.

Procedure

1. In HW Config, configure both F-signal modules in the ET 200M stations.
2. Configure the first F-signal module:
   Activate "Safety mode" in the "Parameters" tab.
3. Configure the second F-signal module:
   Activate "Safety mode" in the "Parameters" tab.
4. For the second F-signal module, select "2 modules" mode in the "Redundancy" tab.
5. In the "Find redundant module" dialog for the F-signal module, select the redundant F-signal module.
6. Set further parameters as necessary. The settings are automatically adopted for the redundant F-signal module. As soon as two F-signal modules are redundant, changes to the parameter settings for one of them will automatically be applied for the other.
7. Check the default discrepancy time for redundant, fail-safe digital input modules.



8. Create a symbol for the lower I/O address and interconnect the channel driver with this address.

If you are operating a HART device on a channel of a redundant module, you also need to follow the steps outlined below:

1. Configure a "HART field device" in both modules on the corresponding channel.
2. In the properties, select "On" or "Can be switched" under the HART_gate parameter and activate the HART function of the relevant channel with the field device.
3. Double-click the HART field device of the module with the lower I/O address and configure the field device in PDM.
4. When you save your settings in PDM, they will all be applied to both modules.

Note

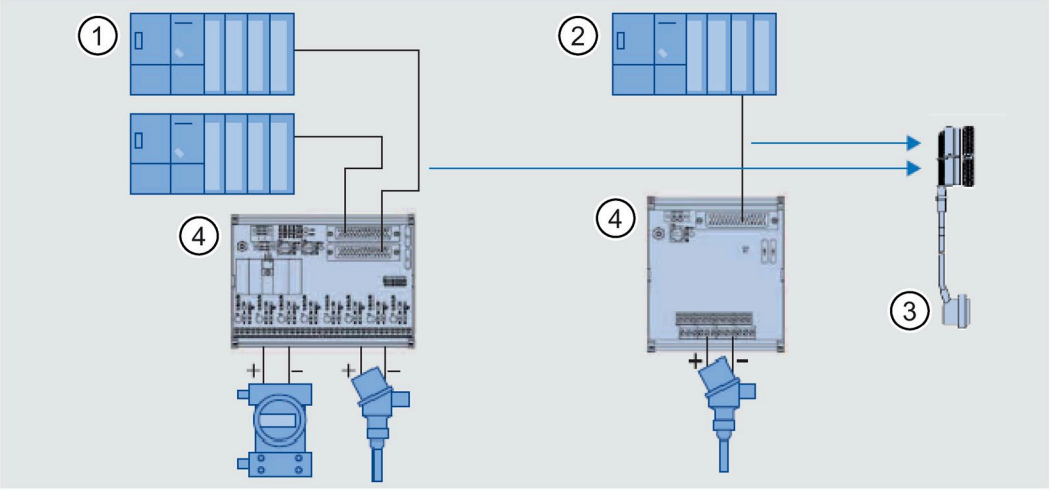
You can find additional information on configuring redundant I/O modules in the "SIMATIC Process Control System PCS 7 Compendium Part A - Configuration Guidelines".

6.6 Marshalled Termination Assemblies (MTA) for ET 200M

The MTA Terminal Modules enable you to connect field devices, sensors, and actuators quickly and easily to the F signal modules of the ET 200M distributed I/O. MTAs are available for standard and F signal modules.

Pre-assembled cables are used to wire the MTAs to the singular or redundant ET 200M modules. MTAs can be used to significantly reduce the time and money spent on cabling and commissioning; they also help to avoid wiring errors.

The figure below shows how an MTA is incorporated into the automation system. Integration can be singular and redundant.



①	ET 200M, redundant
②	ET 200M singular
③	Prefabricated cable with front connector
④	MTA

Note

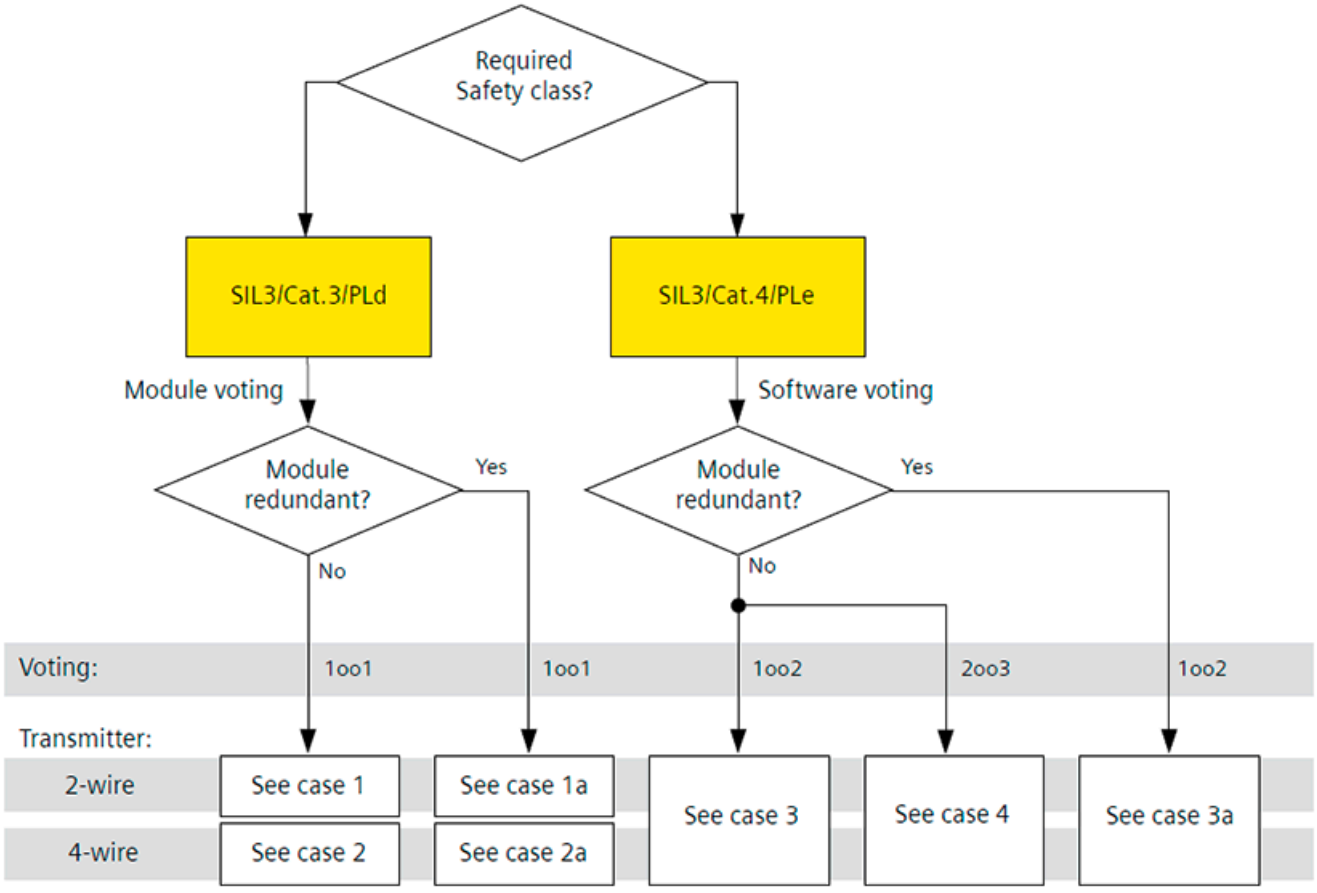
You can find additional information in the manual "ET 200M Marshalled Termination Assemblies Remote I/O Modules (https://support.industry.siemens.com/cs/ww/en/view/22091986)".

6.7 Use cases of I/O Module of ET 200SP HA

The achievable safety class of the F-I/O depends on different conditions. The following sections provide an overview of the I/O modules of the ET 200SP HA. You can find detailed information in the respective manuals.

6.7.1 Use cases of Analog Input Module F-AI 8xI 2-/4-wire HART HA

The following figure will help you select the application according to the requirements for fault tolerance.



Conditions for achieving SIL/Cat./PL

The table below lists the conditions which must be met for achieving at least the corresponding safety requirements.

Application	Sensor evaluation	Sensor supply	Achievable SIL/Cat./PL
1	1oo1	Internal, because 2-wire transmitter	3 / 3 / d
1 a	1oo1	Internal, because 2-wire transmitter	
2	1oo1	External, because 4-wire transmitter	
2 a	1oo1	External, because 4-wire transmitter	
3	1oo2 (not on the module, only in the F-program)	• Internal, if 2-wire transmitter • External, if 4-wire transmitter	3 / 4 / e
3 a	1oo2 (not on the module, only in the F-program)	• Internal, if 2-wire transmitter • External, if 4-wire transmitter	
4	1oo3 (not on the module, only in the F-program)	• Internal, if 2-wire transmitter • External, if 4-wire transmitter	

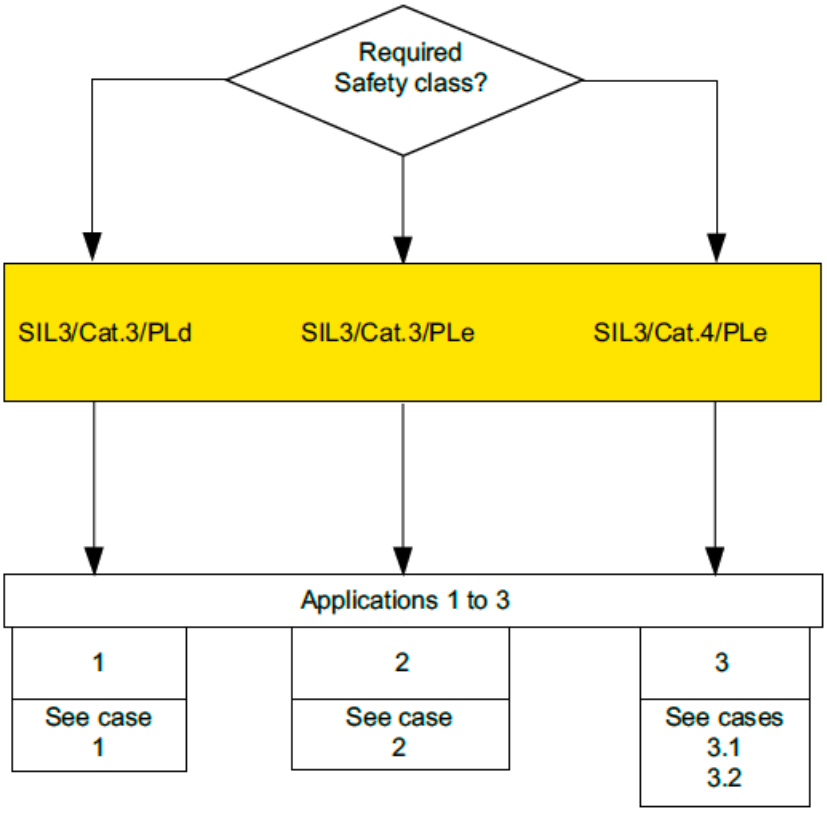
Note that to achieve SIL 3 in the single-channel configuration (application cases 1, 1a, 2, 2a), a sensor must be used that is itself SIL 3 capable. If the sensor quality is not as high as required by the required safety class, the sensor must be deployed redundantly with a 2-channel connection and voting.

Note

Note the additional information on use cases in the following document: "SIMATIC ET 200SP HA Analog Input Module F-AI 8xI 2-/4-wire HART HA (https://support.industry.siemens.com/cs/de/en/view/109802504)"

6.7.2 Use cases of Digital Input Module F-DI 16x24VDC HA

The diagram below supports you in selecting the application that suits your fail-safe requirements.



Conditions for achieving SIL/Cat./PL

The table below lists the conditions which must be met for achieving at least the corresponding safety requirements.

Application	Sensor evaluation	Sensor supply	Achievable SIL/Cat./PL
1	1oo1	Internal or external	3 / 3 / d
2	1oo2 equivalent	• Internal, without short-circuit test • External	3 / 3 / e
3.1	1oo2 equivalent	Internal, with short-circuit test	3 / 4 / e
3.2	1oo2 non-equivalent	External/internal, with short-circuit test	

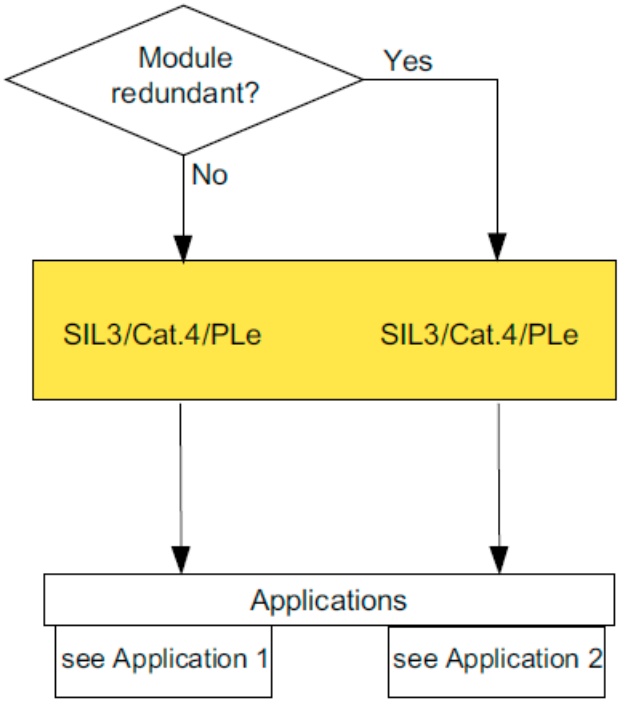
Note that to achieve SIL 3 in the single-channel configuration (application case 1), a sensor must be used that is itself SIL 3 capable. If the sensor quality is not as high as required by the required safety class, the sensor must be deployed redundantly with a 2-channel connection and voting.

Note

Note the additional information on use cases in the following document: SIMATIC ET 200SP HA Digital Input Module F-DI 16x24VDC
(https://support.industry.siemens.com/cs/de/en/view/109802477)

6.7.3 Use cases of Digital Output Module F-DQ 10x24VDC/2A PP HA

The following figure provides an overview of the application cases for a redundant or non-redundant I/O module.



The achievable safety class depends on the routing of the ground cable.

Interconnection	**Achievable safety class**	
	Single ground cable	**Double ground cable**
Connection of the load to the terminal M_n of the terminal block	SIL3/Cat.4/PLe	Not required
Connection of the load to the ground of the power supply unit	SIL3/Cat.3/PLd	SIL3/Cat.4/PLe

Note

Note the additional information on use cases in the following document: "SIMATIC ET 200SP HA Digital Output Module F-DQ 10x24VDC/2A PP HA (https://support.industry.siemens.com/cs/de/en/view/109802499)"

6.8 Wiring & Voting Architectures for ET 200M

Note

You can find details on possible types of interconnection in the following documents:

- Wiring and Voting Architectures for ET 200M F-AI (https://support.industry.siemens.com/cs/ww/en/view/24690377)
- Wiring and Voting Architectures for ET 200M F-DI and F-DO (https://support.industry.siemens.com/cs/ww/en/view/37236961)

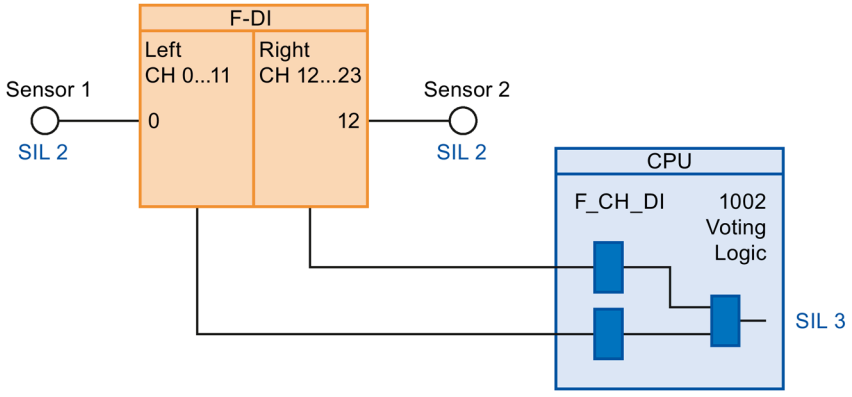
The 1oo2 evaluation of fail-safe input signals can be performed in the F-signal module as well as in the user program.

A 2oo3 evaluation of three fail-safe signals can be implemented in the CFC with a function block or in the Safety Matrix.

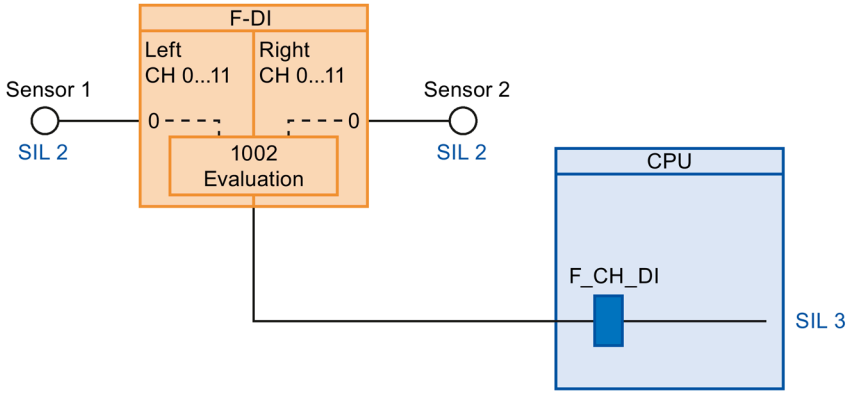
6.8.1 Evaluation on the module or in the CPU

The following examples show different evaluation variants.

SIL 3 by evaluation in the F-user program



SIL 3 by evaluation in module



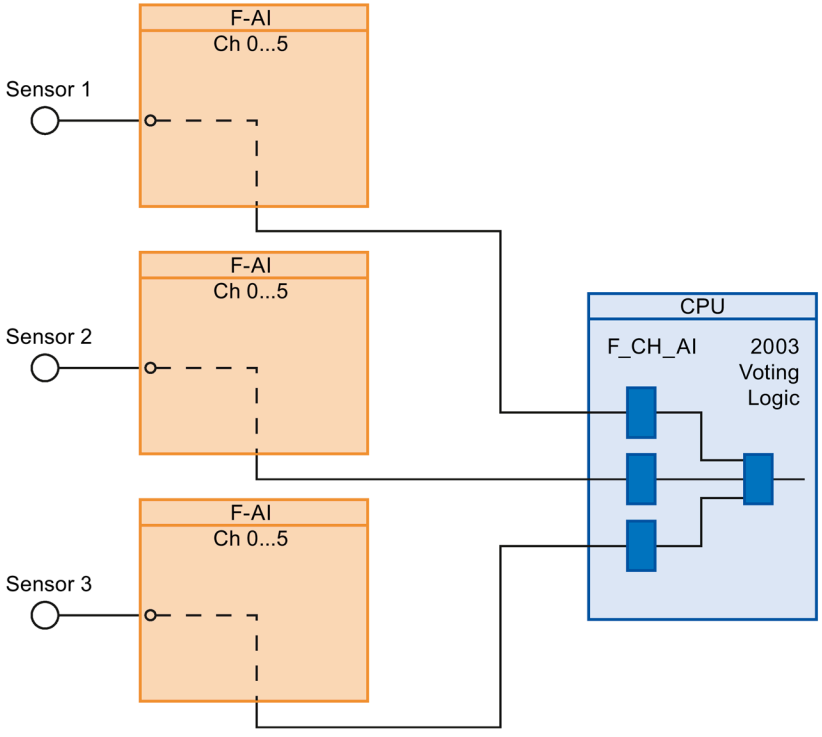
Note

Suitable sensors are required to achieve a specific SIL with this wiring.

6.8.2 2oo3 evaluation with F-AI

2-out-of-3 selection uses three sensors and, for example, three F-AI modules.

In the example, each sensor is wired to channel 0 of an F-AI module. The individual signals are then evaluated in the user program. SIL 3 can be achieved with a 2-channel configuration.

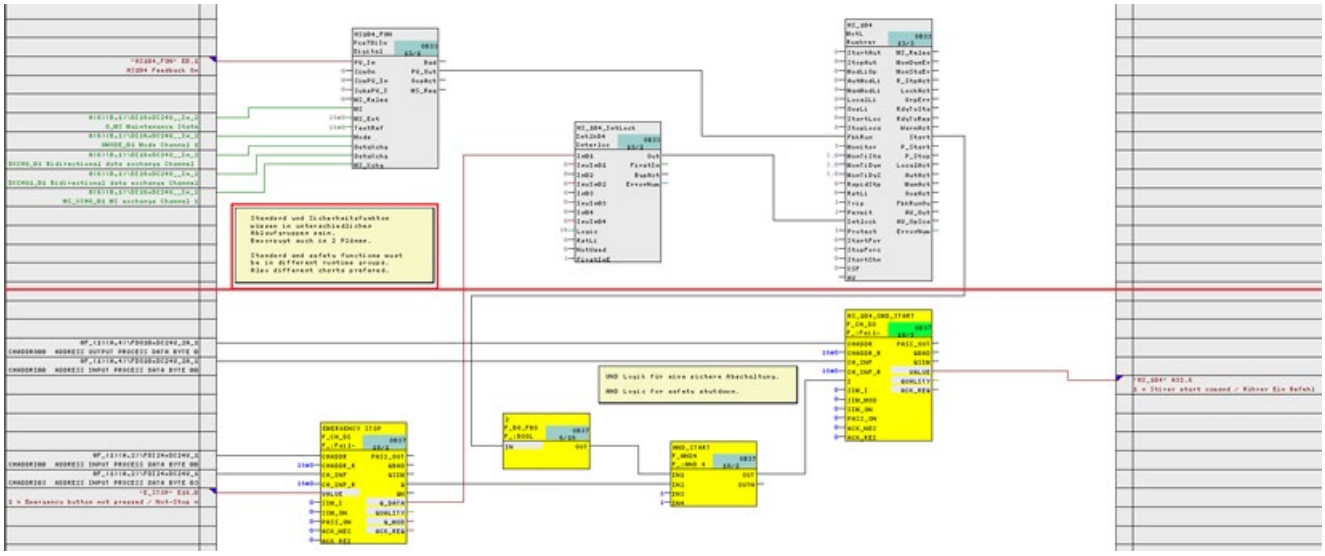


7 Configuring the safety program

7.1 Introduction

Fail-safe user program

Use the F-blocks supplied in a library with the S7 F-Systems optional package to create a fail-safe user program (F program or safety program) with the CFC editor.



Note

The figure is available in its original size as appendix to the manual in the ZIP download of the checklists.

As well as functions for programming safety functions, the F-blocks contain functions for detecting and reacting to errors. In other words, they ensure that failures and errors are detected and that an appropriate reaction is triggered to maintain the F-system in or switch it to a safe state. The safe state in a fail-safe function is generally "0"; i.e. a "0" signal at an input or output leads to disconnection.

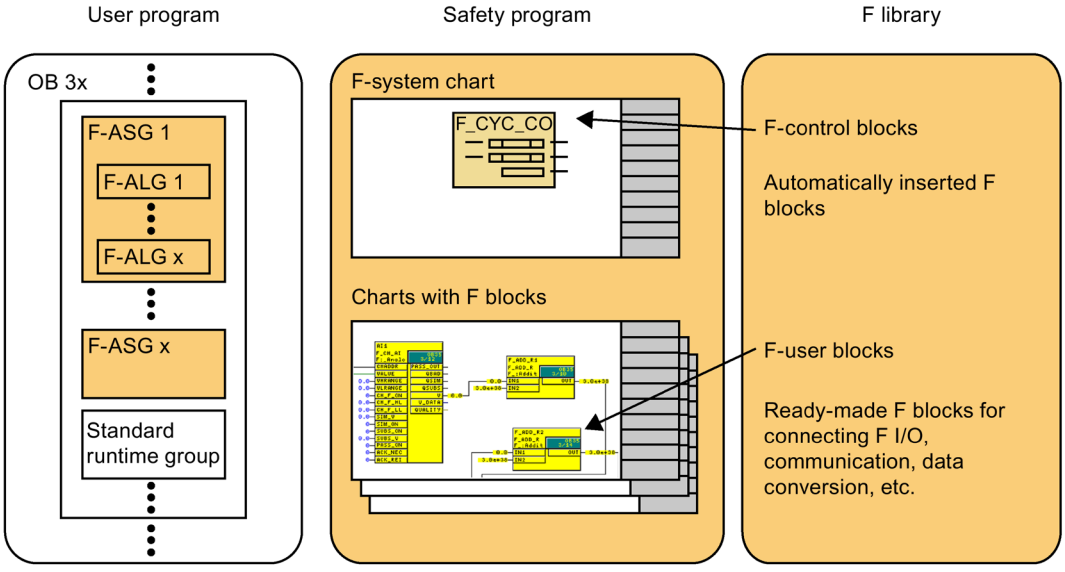
The user program in the CPU can be created from F-and non-F blocks. The F-program is configured in separate runtime groups.

Data transfer between the standard program and the F-program is handled using conversion blocks. Please note that safety functions must be implemented with F-blocks consistently from the input driver to the output driver. Standard signals may only change the state of a safe output if the safety function is in a healthy state.

During compilation, specific functions for detecting and reacting to errors are automatically added to the F-program. The S7 F-System optional package also features functions for comparing F-programs and providing support for the acceptance and approval procedure for F-programs, such as functions for generating a signature via the F-program which can be used to detect changes to functions and parameters. This signature is saved during the plant acceptance procedure.

Program structure of the safety program

The figure below shows a diagram illustrating the structure of a safety program comprising CFC charts with F-blocks which are assigned to F-runtime groups.



Some of the properties possessed by the various components are:

- The safety program contains F-runtime groups and the charts assigned to them. The charts contain F-blocks with their parameter settings and interconnection.
- The F-runtime groups are added to one or more cyclic interrupt OBs.
- F-runtime groups can be combined in F-shutdown groups (F-SG).
- The cyclic interrupt OB can also contain standard runtime groups.
- The F-blocks in the S7 F-Systems F-library appear in yellow on the CFC chart in order to highlight the fact that there is a safety program involved.
- The CFC charts and F-runtime groups with F-blocks appear in yellow and are marked "F" in order to distinguish them from charts and runtime groups associated with the standard user program.

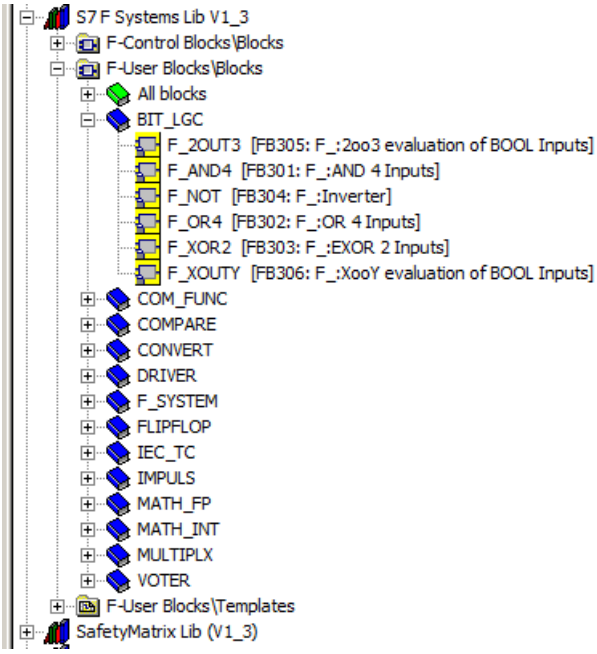
7.2 Creating the safety program

Requirements

- You must have created a project structure in the SIMATIC Manager.
- Prior to programming, you must have configured the hardware components of your project, in particular the F-CPU and the F-signal modules, for safety mode.
- You must have assigned your safety program to an F-capable CPU, for example, a CPU 410-5H.

Library

The F-user blocks must always be used for configuration.



7.2.1 Defining the program structure

In addition to considering the standard scenario, you need to answer the following questions when drafting a safety program:

- Which parts of the user program need to be fail-safe?
- Which response times do you need to achieve?

You will need to split your F-program into various cyclic interrupt OBs (OB 30 to OB 38) in accordance with these requirements.

You will improve performance if you program parts of the program which are not needed for the safety functions in the standard user program.

In terms of dividing your program between the standard user program and the safety program, please remember that the standard user program is easier to change and download to the F-CPU. Changes to the standard user program do not usually need to undergo acceptance and approval.

Rules governing program structure

When drafting a safety program for S7 F/FH Systems, you need to observe the following rules:

- F-runtime groups with F-blocks can only be assigned to cyclic interrupts OB 30 to OB 38.
- A chart can contain both F-blocks and standard blocks; they need to be inserted in separate runtime groups in this case. You are not permitted to use these charts as F-block types.
- In the safety program, access to the F-signal modules is only permitted via the F-channel driver (F_CH_xx).

7.2.2 Creating CFC charts

Inserting CFC charts

Individual CFC charts are added to the chart folder or plant hierarchy (PH) in the same way as for standard user programs:

- In the SIMATIC Manager, in the chart container "Insert new object > CFC".
- Directly in the PH or process object view in the respective hierarchy folder "Insert New Object > CFC".

Inserting F blocks

Blocks are inserted into the chart from the library "S7 F Systems Lib V1_3 > F User Blocks" using drag-and-drop. There is no limit on the number of times a block can be dragged and dropped.

Note

If a block type has been dragged and dropped from the library before, the process can be completed more quickly the next time by using the "CFC block catalog", "Blocks" tab.

7.2.3 Assigning parameters to and interconnecting F-blocks

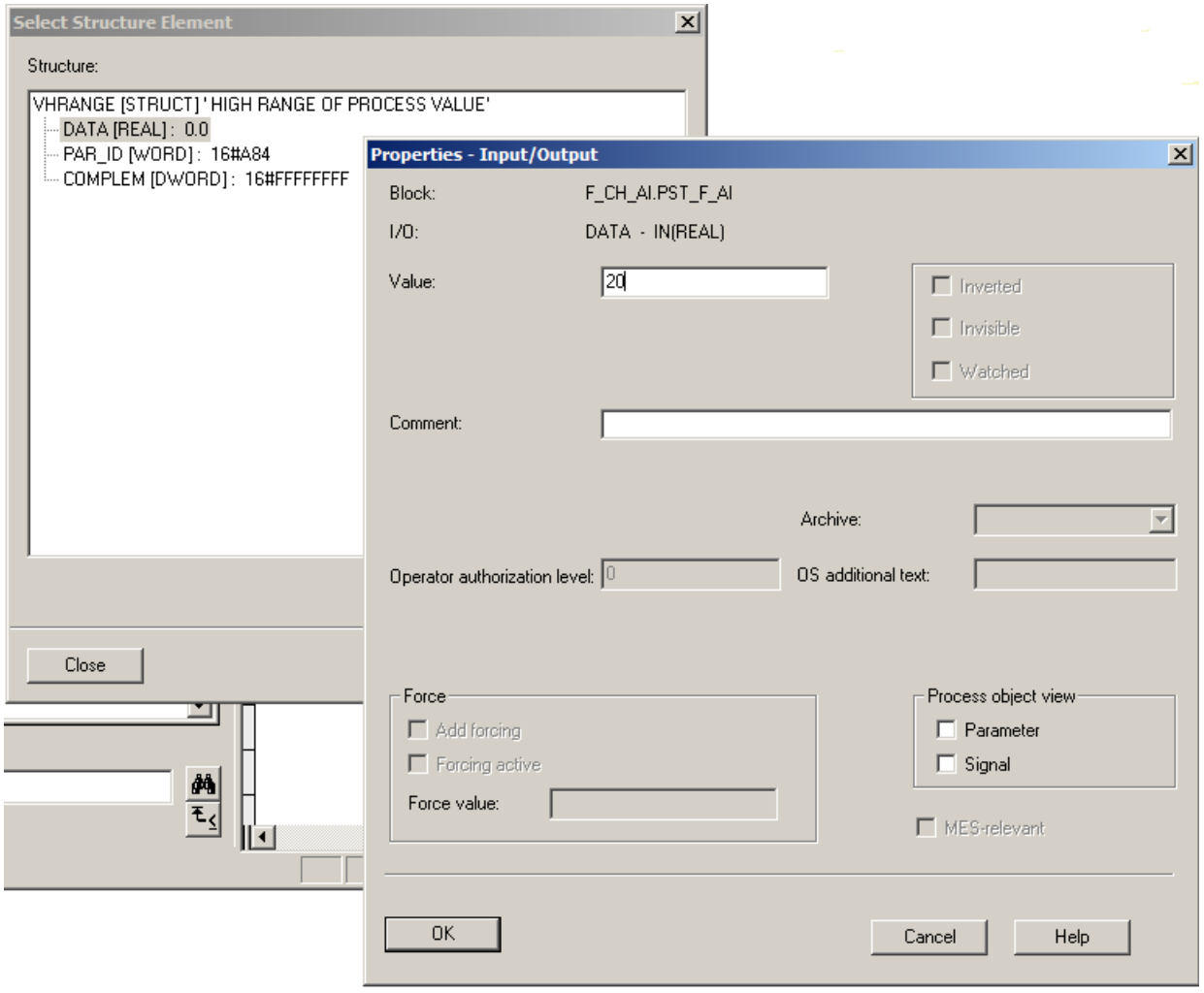
Inputs and outputs of F-blocks are configured and interconnected using the standard CFC procedure.

Note

You are not permitted to interconnect EN/ENO I/Os of F-blocks and F-runtime groups. You may not assign a value of 0 (FALSE) to EN I/Os either.

Special F-data types in a safety data format are used for fail-safe block I/Os. The safety data format enables data and address errors to be detected.

In terms of programming, the F-data types are realized as structures in which always only the "DATA" component is relevant for the user.



Example: Structural element F_Real VHRANGE [STRUCT]"HIGH RANGE OF PROCESS VALUE"

You can change the structure comment to whatever you wish.

If you wish to change the value (default) of a block I/O with an F-data type, you may only change the DATA component.

Changes to the input parameters of F-blocks with F-data types can be made as follows:

- Offline with the assistance of the CFC editor
- Online using CFC test mode with safety mode deactivated
- Offline in the process object view
- Online in the process object view with deactivated safety mode

Note

Values of PAR_ID and COMPLEM must not be changed.

If errors in the safety data format are detected during the execution of the safety program, an F-STOP is triggered.

7.2.4 Run sequence of F-blocks

Defining the run sequence

You define the run sequence in the CFC editor in the same way as for a standard user program. Changing the run sequence also changes the collective signature.

Correct run sequence of F-blocks

The sequence of the F-blocks within the F-shutdown group is relevant. The number of F-runtime groups the F-shutdown group has been split into is of no relevance.

Essentially, the correct run sequence of the various F-block types is as follows:

1. Placed automatically:
   - F module driver for F-signal modules with inputs or with inputs and outputs
   - F-communications blocks and F-system blocks for receiving
   - F blocks for data conversion from standard value to F-structure
   - F modules with OS connection
2. F channel drivers for inputs
3. F blocks for user logic
4. F channel drivers for outputs
5. Placed automatically:
   - F block F_PLK
   - F block F_PSG_M
   - F module driver for F-signal modules with outputs or with inputs and outputs
   - F-communications blocks and F-system blocks for sending
   - F block F_PLK_O
   - F block F_DIAG (S7 F-Systems Lib V1_3 and higher)

The run sequence of the blocks listed under items 1 and 5 is adjusted automatically when the F-program is compiled.

As if S7 F Systems Lib V1_3, separate runtime groups are created for the F blocks listed under points 1 and 5 during the first compilation.

The IPO principle (input, process, output) must always be observed when placing F-channel drivers and F-blocks for user logic. This ensures that all inputs are read first, the relevant processing steps are performed, and all outputs are then written.

Furthermore, F-runtime groups and F-monitoring blocks that are only visible following compilation are also added automatically.

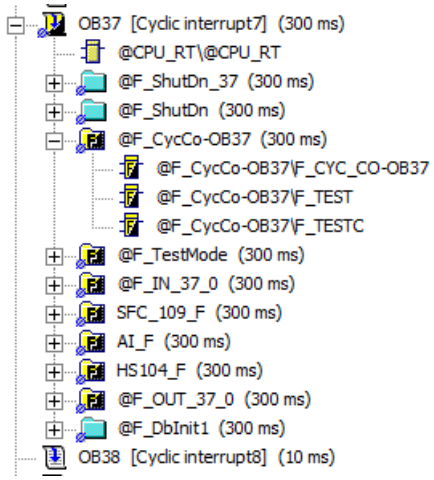
Note

No changes may be made in the automatically added runtime groups with the exception of the scan cycle monitoring on "F_CYC_CO" blocks and the parameter assignment of the "F_SHUTDN" block.

7.2.5 F-runtime groups

During the programming of the safety program, F-blocks cannot be inserted directly into tasks (cyclic interrupt OBs). When a new CFC chart is created in PCS 7, the system will automatically generate a runtime group of the same name, into which the F-blocks placed in the corresponding CFC chart can then be inserted.

An F-runtime group only becomes an F-runtime group (identified by a yellow folder and "F") when F-blocks are called in it.



Runtime groups of an F-program

The F-program is divided into several runtime groups, as shown in the table below.

Note

xx = Number of the cyclic interrupt OB

y = Consecutive numbering if several shutdown groups exist in a single cyclic interrupt OB

Chart	F blocks
@F_ShutDn_xx	Shutdown logic of cyclic interrupt OB The shutdown logic is created with RTGLOGIC and standard logic blocks.
@F_ShutDn	Shutdown block Where an F-program is present in several cyclic interrupt OBs, this runtime group is integrated into the cyclic interrupt OB with the shortest call time. The shutdown logic is created with F_SHUTDN, RTGLOGIC, and standard logic blocks.
@F_CycCo-OBxx	F_CYC_CO, F_TEST and F_TESTC (for tests)
@F_TestMode	F_TESTM for managing safety mode
@F_IN_xx_y	F blocks which supply input values for the F-program (F_QUITES, communication receive blocks, conversion blocks from standard to F-data types, drivers for F-input modules)
	Runtime groups with user logic, in the sequence in which they were created by the user
@F_OUT_xx_y	Blocks which further process output values of F-blocks (communication send blocks, conversion blocks from F-to standard data types, drivers for F-output modules, F_PLK, F_PLK_O, and F_DIAG for program sequence control)
@F_DbInitxx	DB_INIT function block required for the cold restart of an F-runtime group

All required error OBs are added to the block container in the SIMATIC Manager.

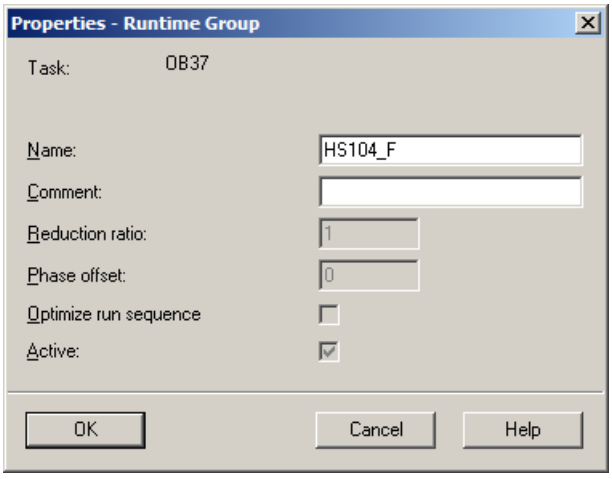
There should only be one @F_IN_xx_y runtime group before the first F-user runtime group and one @F_OUT_xx_y runtime group after the last F-use runtime group. If the safety program consist of several shutdown groups (see section 6.2.6 (Page 120)), there is the @F_IN_xx_y and @F_OUT_xx_y runtime group both before and after the F-user runtime group in the shutdown groups.

Rules for F-runtime groups in the safety program

- We recommend that you proceed as follows in order to make the lengths of the F-cycles as uniform as possible:

  If you mix F-and standard runtime groups in a cyclic interrupt OB, you must execute the F-runtime groups before the standard runtime groups.

- The following defaults are set for properties of an F-runtime group:
  - Reduction ratio = 1
  - Phase offset = 0



- You are not permitted to move automatically generated F-runtime groups (identified by @).

Note

The feature: Optimize Run Sequence in CFC can lead to a change in the collective signature and impair the response times of the safety program, and therefore should not be used in F-runtime groups.

With PCS 7 V7.0 SP1 and higher, it is no longer possible to optimize the run sequence for cyclic interrupt OBs with F-runtime groups.

7.2.6 F-shutdown groups

An F-shutdown group is a self-contained unit in your safety program. It contains user logic which is executed or shut down simultaneously. The F-shutdown group contains one or a number of F-runtime groups which are assigned to a common cyclic interrupt OB. You can choose whether an error during execution of the safety program causes a full shutdown or a partial shutdown of the safety program. With a partial shutdown, only the F-shutdown group in which the error occurred is shut down.

Rules for F-shutdown groups in the safety program

You are not permitted to directly interconnect F-blocks in different F-shutdown groups. Data can only be exchanged between F-shutdown groups using special communication blocks (F_S_xx, F_R_xx for F_BOOL and F_REAL data structures). Therefore, all F-channel drivers in an F-signal module must be in the same F-shutdown group, together with the module driver of the F-signal module.

Defining F-shutdown groups

As soon as you place F-blocks in the CFC editor for the first time, all of the F-runtime groups in a single cyclic interrupt OB will form an F-shutdown group.

You can configure each F-runtime group as the last F-runtime group in an F-shutdown group by placing the F_PSG_M "selection block". The F-system then creates a new F-shutdown group for all subsequent F-runtime groups until another F_PSG_M block is found.

Distribution/Combination by means of manual placing of F_PSG_M

If you add or delete one or a number of F_PSG_M blocks in your project, the order of your F-shutdown groups will change. If you make a change to the layout of your F-shutdown groups, you must make sure that the F-module drivers and all assigned F-channel drivers are integrated in the same F-shutdown group.

You can split one F-shutdown group into two F-shutdown groups.

To do this, in the CFC editor's runtime editor, place the F_PSG_M block in the last F-runtime group which is to be assigned to the first F-shutdown group. All subsequent F-runtime groups will then be assigned to the second F-shutdown group.

The number of F-shutdown groups is limited to 110 in all cyclic interrupt OBs. The system restricts the number of F-runtime groups in an F-shutdown group.

You have the option of combining two F-shutdown groups. To do this, in the runtime editor of the CFC editor, delete the F_PSG_M block between the F-shutdown groups.

If you combine a number of F-shutdown groups which exchange data via F-communication blocks in a single F-shutdown group, you need to remove these F-communications blocks and replace them with direct interconnections.

Programming data exchange between F-shutdown groups

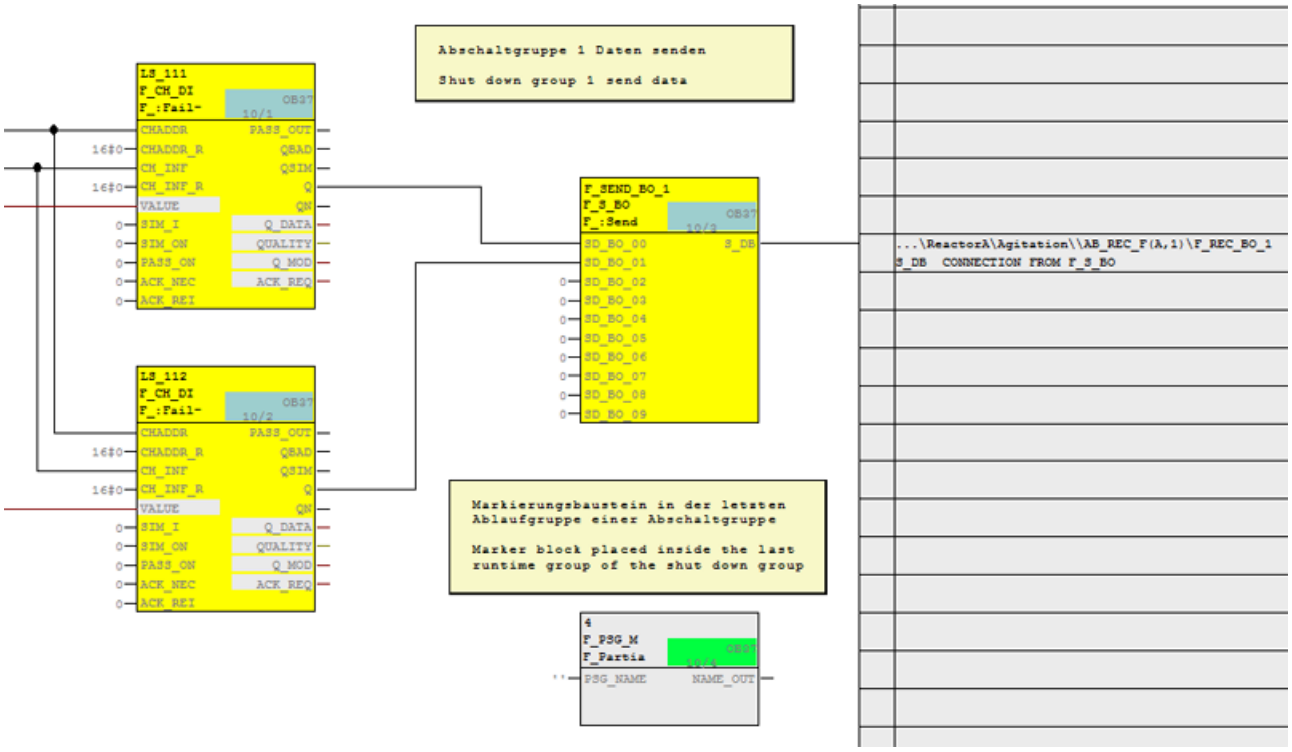
If you wish to exchange data between two F-shutdown groups, you are not permitted to interconnect the inputs and outputs directly. You need to use the following F-system blocks for data exchange between F blocks in different F-shutdown groups:

F block	Description
F_S_R/F_R_R	Safe transfer of 5 data of the F_REAL type
F_S_BO/F_R_BO	Safe transfer of 5 data of the F_BOOL type

Procedure for data exchange

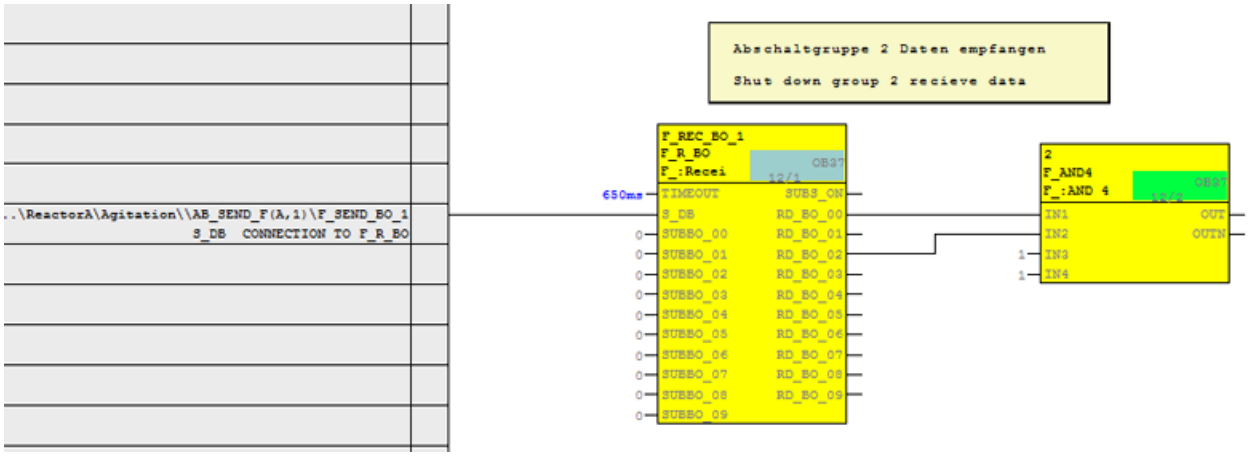
1. In the F-shutdown group from which data is to be transferred, add an F_S_R or F_S_BO type F-block.
2. In the F-shutdown group to which data is to be transferred, add an F_R_R or F_R_BO type F-block.
3. Interconnect the SD_R_xx inputs of the F_S_R or the SD_BO_xx inputs of the F_S_BO with the data to be transferred.
4. Interconnect the RD_R_xx outputs of the F_R_R or the RD_BO_xx outputs of the F_R_BO with the inputs of the F-block for further processing of the data received.
5. Interconnect the S_DB output of the send block with the S_DB input of the associated receive block.
6. Configure the TIMEOUT inputs of the F_R_R and F_R_BO receive blocks with the F-monitoring time calculated.
7. Configure the receive block substitute values for the scenario of a shutdown of the sending shutdown group.

Extract from a chart for shutdown group 1 with send block:



The connection to shutdown group 2 is established by linking output S_DB of block F_S_BO_1 in shutdown group 1 with input S_DB on block F_R_BO_1 in shutdown group 2.

Extract from a chart for shutdown group 2 with receive block:

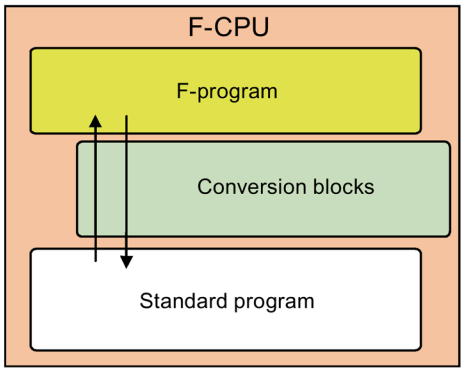


See also

Monitoring times and system response times (Page 195)

7.2.7 Data exchange between the F user program and standard user program

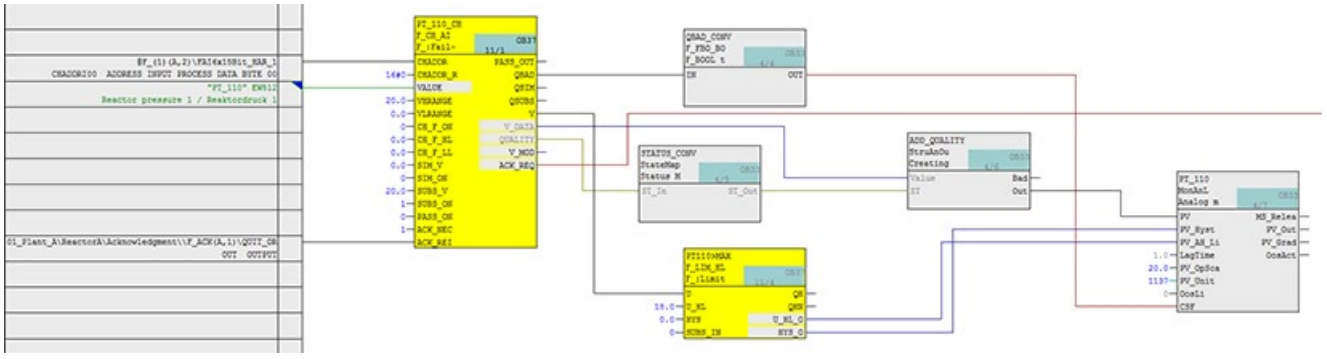
The standard program and the F-program use different data formats. Accordingly, special conversion blocks have to be used for data exchange.



Converting F-data types to standard data types

If you need the standard user program to process data from the F-program further (for monitoring on the PCS 7 OS, for example), a block for F_FDatatype_Datatype data conversion will have to be interconnected in the user program so that the F-data types can be converted into standard data types. This converter blocks must be called in the standard user program (standard runtime group).

Extract from a process tag chart; converting the "QBAD" signal from F_BOOL to BOOL:



Note

The figure is available in its original size as appendix to the manual in the ZIP download of the checklists.

Standard and F-blocks are in different runtime groups.

As shown here, some F-blocks have outputs (depicted in gray), which can be directly interconnected with standard PCS 7 blocks.

PCS 7 blocks such as MonAnL, MonDiL, Event and their associated faceplates and process symbols are used to visualize fail-safe analog values and status messages as well as system states and operating states.

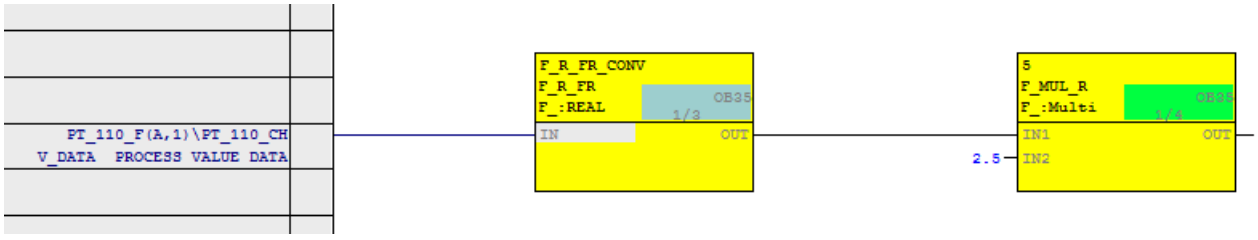
If parameters cannot be directly further interconnected due to the safety data format, the conversion blocks described above can be used.

Converting standard data types into F-data types

If data from the standard user program is to be processed further in the F-program, it will need to be converted.

The blocks for data conversion from standard data types to F-data types (F_datatype_Fdatatype) can only be used in the F-program (F-runtime group).

Extract from an F-chart, conversion from REAL to F_REAL:



Note

The conversion blocks only perform data conversion; in other words, you will need to program additional measures in the F-program for plausibility checking purposes (with F_LIM_R, for example), in order to ensure that only non-hazardous values are possible.

7.2.8 How F-blocks with floating-point operations respond to number range overflows

Within the context of analog value processing, number range overflows/underflows can occur during arithmetic calculations (with division by 0, root from a negative number or number range overflow).

With S7 F Systems Lib V1_3 and higher, the response is as follows in this case:

The results "Overflow (± infinite)", "Denormalized floating-point number" or "Invalid floating-point number (NaN)" are:

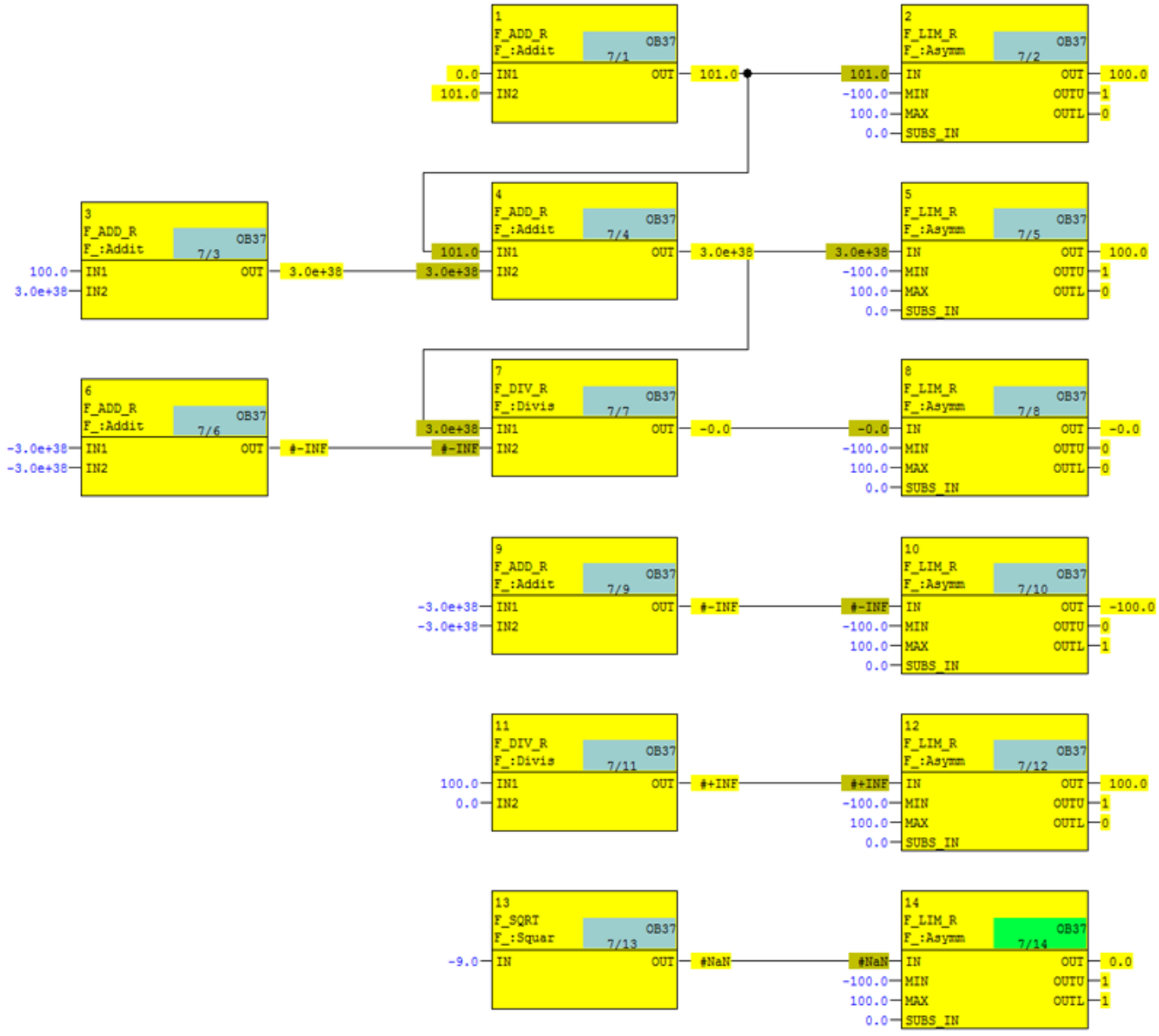
- Either output at the output and can be processed further by subsequent F blocks
- or signaled at special outputs. If necessary, a substitute value is output.

If the floating-point operation produces an invalid floating-point number (NaN) and no invalid floating-point number (NaN) existed as an address prior to this, the following diagnostics event will be entered in the F-CPU's diagnostics buffer:

"Safety program: Invalid REAL number in DB" (event ID 16#75D9)

You can use this entry in the diagnostics buffer to identify the F-block with the invalid floating-point number (NaN).

If you are not able to prevent these events from occurring in your safety program, you will need to decide, on the basis of your application, whether you wish to respond to them in your safety program.



You can use the F_LIM_R F block to check the result of a floating-point operation for overflow (± infinite) and invalid floating-point number (NaN).

- A limit violation is indicated by IN > MAX or "+ infinite". MAX is output at OUT. OUTU is set to 1 and OUTL to 0.
- A limit violation is indicated by IN < MIN or "- infinite". MIN is output at OUT. OUTU is set to 0 and OUTL to 1.
- If IN is between MIN and MAX, the input IN is forwarded to the output OUT. OUTU and OUTL are set to 0.
- If IN is an invalid floating-point number (NaN), the substitute value SUBS_IN is output at OUT. OUTU and OUTL are set to 1.

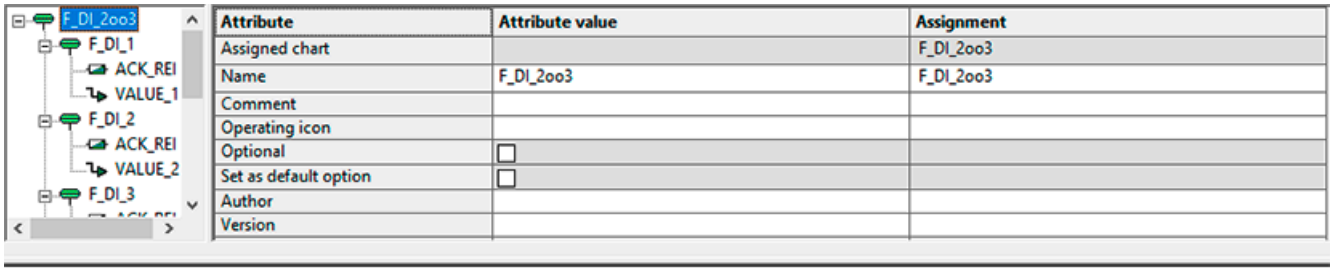
Note

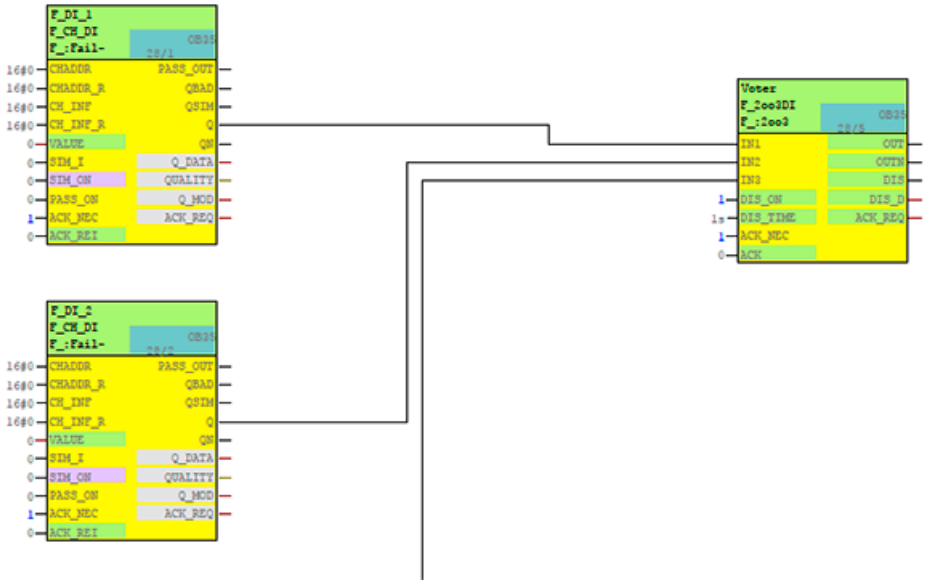
You can find a detailed description of the F-blocks in the help for the blocks, as well as in the "SIMATIC S7 F/FH Systems – Configuring and Programming" (https://support.industry.siemens.com/cs/ww/en/view/109802562) manual.

7.2.9 Control Module Types (CMT) with F-blocks

Control Module Types

Control Module Types (CMT) with F-modules can be used as of S7 F Systems V6.4.





You can find additional information on Control Module Types (CMT) in the documentation for CFC "SIMATIC Process Control System PCS 7; CFC for SIMATIC S7" (https://support.industry.siemens.com/cs/ww/en/view/109782631).

Compared to CMT with standard modules, CMT with F-modules are subject to various restrictions.

You can find detailed information in the programming and operating manual "SIMATIC S7 F/FH Systems - Configuring and Programming" (https://support.industry.siemens.com/cs/ww/en/view/109802562).

Pay particular attention to the warnings described there.

Synchronize

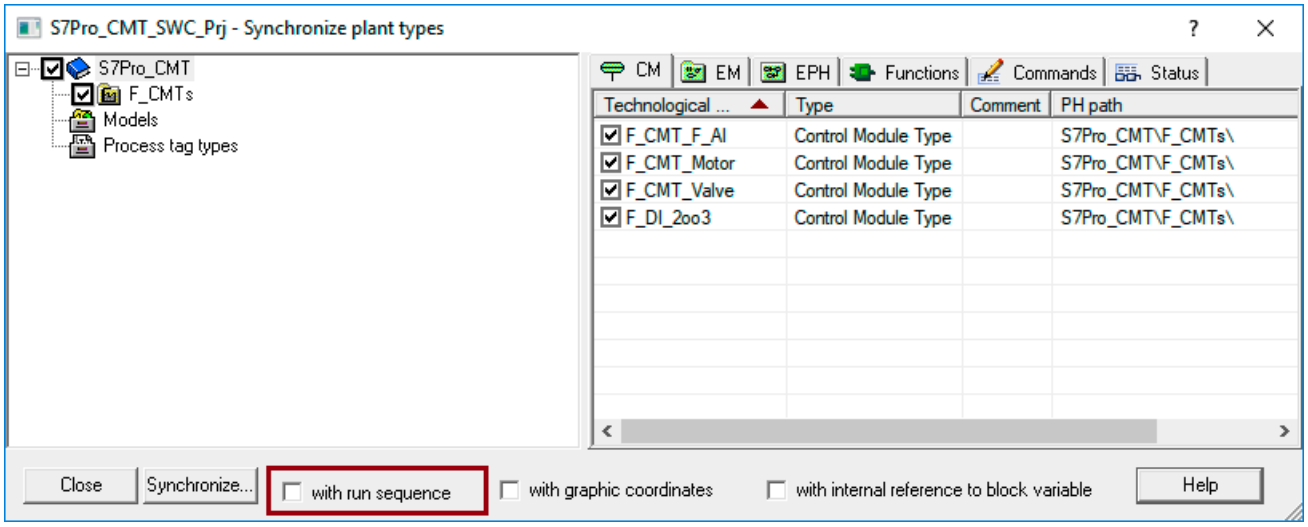
To transfer changes from the Control Module Type to the instance, the control module (CM), the type and instance are synchronized. Create a backup of your multi-project before making changes through the synchronization.

Check the changes in each instance after the synchronization. To do this, use the change tracking functions described in the section "Tracking changes in the safety program (Page 253)".

Only the respective instances (CM) in the safety program are relevant for the acceptance of the safety program.

After synchronization, check the safety program for unintentional changes to the run sequence. This can occur when using automatically placed F-modules. See section "Run sequence of F-blocks (Page 116)".

To prevent changes to the run sequence order by type synchronization, the "with run sequence" option in the "Synchronize technological types" dialog must not be selected.



Note

Follow the instructions in the manuals:

- SIMATIC S7 F/FH Systems – Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/109802562)
- "SIMATIC Process Control System PCS 7 CFC for SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/109782631)"

7.3 Configuring fail-safe AS-AS communication

Like standard communication, safety-related communication between the safety programs of F CPUs via S7 connections is implemented using connection tables in NetPro.

In S7 F/FH systems, safety-related communication via S7 connections is possible between all 41x-xH CPUs.

As of S7 F Systems V6.0 with S7 F Systems Lib V1_3, fail-safe communication to S7 Distributed Safety is also supported with the following F CPUs:

- CPU 416F
- CPU 31xF

Note

Safety-related AS-AS communication is not permitted via public networks.

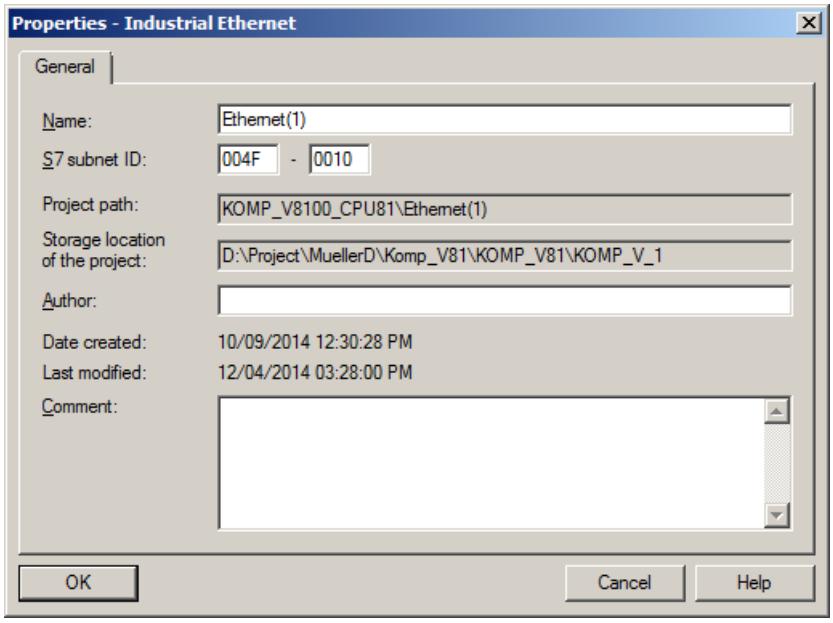
7.3.1 Configuring S7 connections

Configure S7 connections for safety-related AS-AS communication in exactly the same way as for standard communication (you might need also need to set up a fault-tolerant S7 connection).

Note

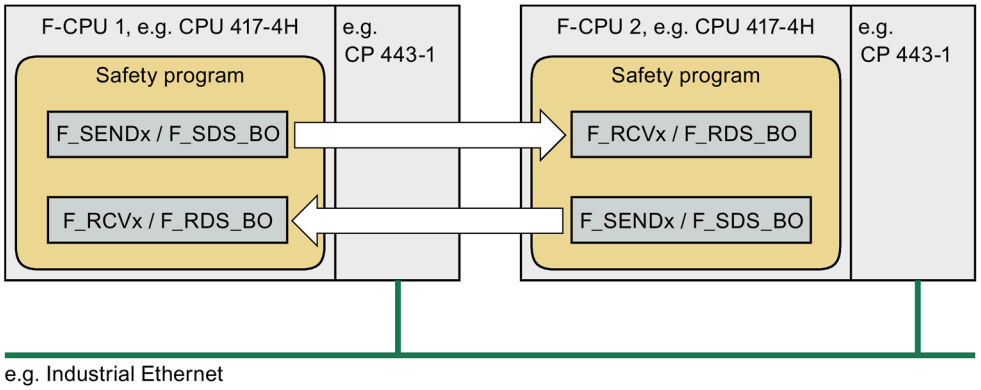
You can find instructions on how to do this in the "SIMATIC Process Control System PCS 7 Compendium Part A - Configuration Guidelines".

During communication between automation systems in various subprojects, please make sure that the S7 subnet ID is the same in each of the respective projects. This ID is involved in the calculation of the CRC sum at the send and receive blocks and must, therefore, be the same in each case.



You can find instructions about how to create a specified communication connection between two multiprojects in the FAQ "How can data be sent with PCS 7 to an H-CPU which was not created in the same multiproject?" (https://support.industry.siemens.com/cs/ww/en/view/43033406).

7.3.2 Configuring F-communications blocks



The following fail-safe blocks are available for communication between safety programs on various CPUs:

Block	Description
F_SENDBO/F_RCVBO	Safe transmission of 20 F_BOOL data type parameters
F_SENDR/F_RCVR:	Safe transmission of 20 F_REAL data type parameters
F_SDS_BO (as of S7 F Systems V6.0)	Fail-safe sending of 32 F_BOOL data type objects to another F-CPU
F_RDS_BO (as of S7 F Systems V6.0)	Fail-safe reception of 32 F_BOOL data type objects from another F-CPU

Requirements

The follow requirements must be fulfilled prior to configuration:

- The S7 connections between the F-CPUs involved must be configured in NetPro.
- Both CPUs must be configured as F-CPUs:
  - The password for the F-CPU must be entered.
  - The "CPU contains safety program" option must be activated.

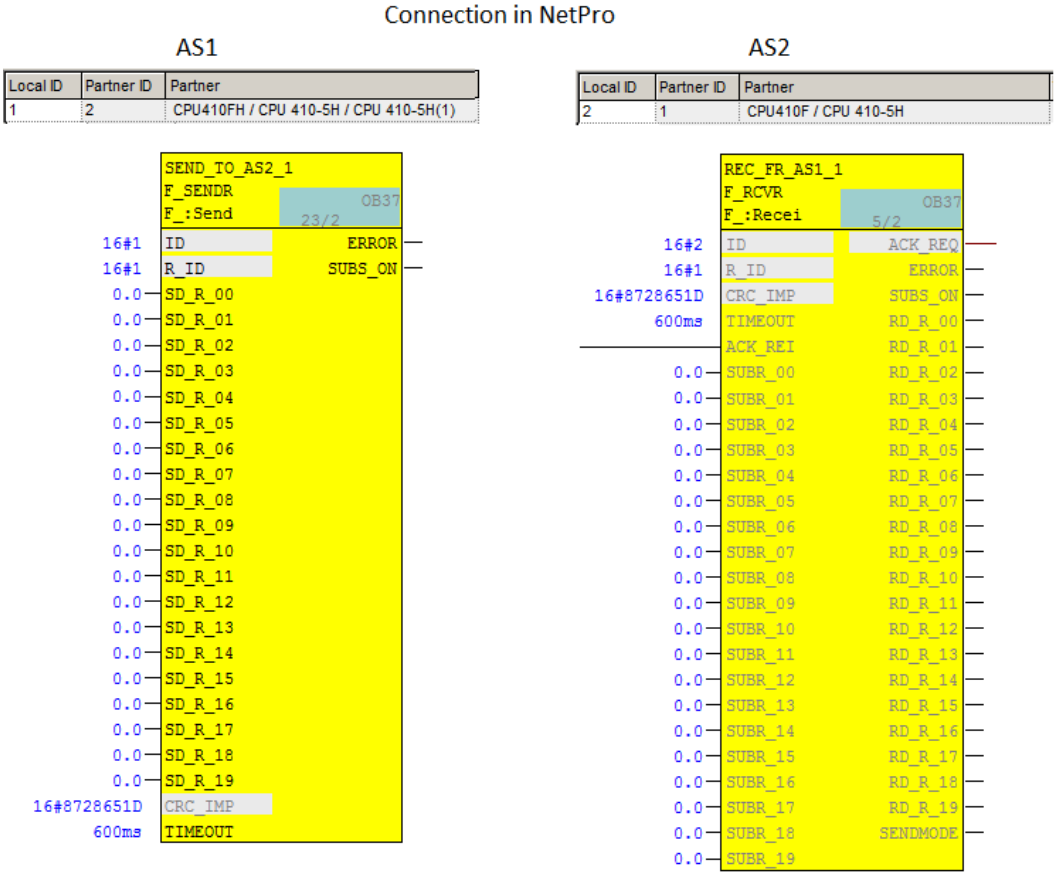
Procedure

Follow the steps outlined below:

1. Add the send block (F_SENDBO/F_SENDR) to the safety program from which data is to be transmitted.
2. Add the receive block (F_RCVBO/F_RCVR) to the safety program to which data is to be transmitted.
3. Assign the relevant IDs of the configured S7 connections to the "ID" inputs.
4. Configure the R_ID inputs. This defines the relationship between a send block and a receive block:

   The associated fail-safe blocks are assigned the same (freely selectable, uneven value for R_ID. Please note that the R_ID+1 value is also assigned automatically.

   Example: Local AS1 is sender, partner AS2 is recipient



Note

If the R_ID is not an uneven number, the following error message will appear when the CFC charts are compiled:

"Module/connection with address/R_ID 16#0002/16#00000004 is used by more than one module. [Assign a module/connection with this address/R_ID to no more than one block and use only uneven R_IDs.]"

5. Interconnect the ACK_REQ outputs of the F_RCVBO, F_RCVR, or F_RDS_BO F-blocks to ascertain whether acknowledgment is required on reintegration following communication error elimination.
6. Interconnect the relevant ACK_REI inputs of the F_RCVBO, F_RCVR, or F_RDS_BO F-blocks with the signal for reintegration.

Note

If the S7 connections between the automation systems have been changed, the safety program will need to be recompiled.

User acknowledgment is always required for reintegration following PROFIsafe communication errors (ACK_REQ output set).

7. Configure the TIMEOUT inputs of the send and receive blocks with the same calculated timeout value.
8. Configure the receive block substitute values for the scenario of a communication fault.

Communication is established internally in both directions (sending and receiving) for the F-communication. Keep in the mind the maximum communication load of the AS.

If the maximum communications load of a system is 100 requests per second, for example, this results in a total of 20 communications requests with 5 F_RECVX and 5 F_SENDX-B blocks. If these are configured in OB 37 (1 s), this corresponds to a communication load of 20%. These blocks, which are integrated into OB 38 (300 ms), correspond to a communication load of 66%.

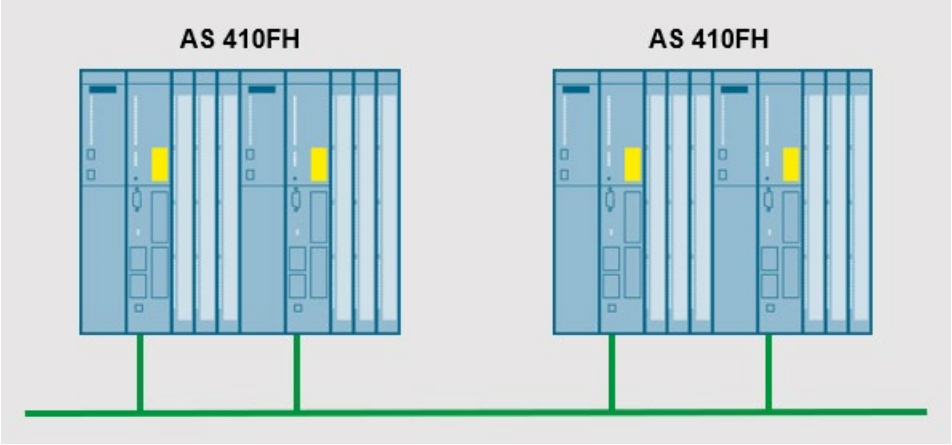
Note

As of S7 F Systems Lib V1.3 SP2, the fail-safe communication blocks have the new input parameter, "COMMVER_USED". You can find additional information about the configuration of the parameter in the FAQ "What should you watch out for when using the fail-safe communication blocks of S7 F Systems Lib V1.3 SP2 and higher". (https://support.industry.siemens.com/cs/ww/en/view/109752514)

7.3.3 Monitoring times

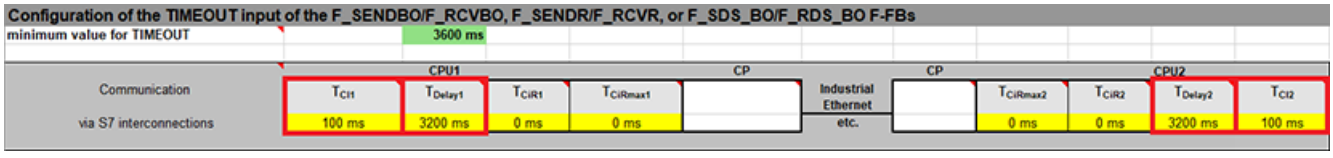
For safety-oriented AS-AS communication, the monitoring times "Send Keepalives for Connections", "Monitoring time of the physical connection" and "F-monitoring time of the communication blocks" must be observed. The steps that are necessary for determining and setting the monitoring times are described below using configuration examples.

F-communication AS 410 high-availability – AS 410 high-availability



Follow the steps outlined below:

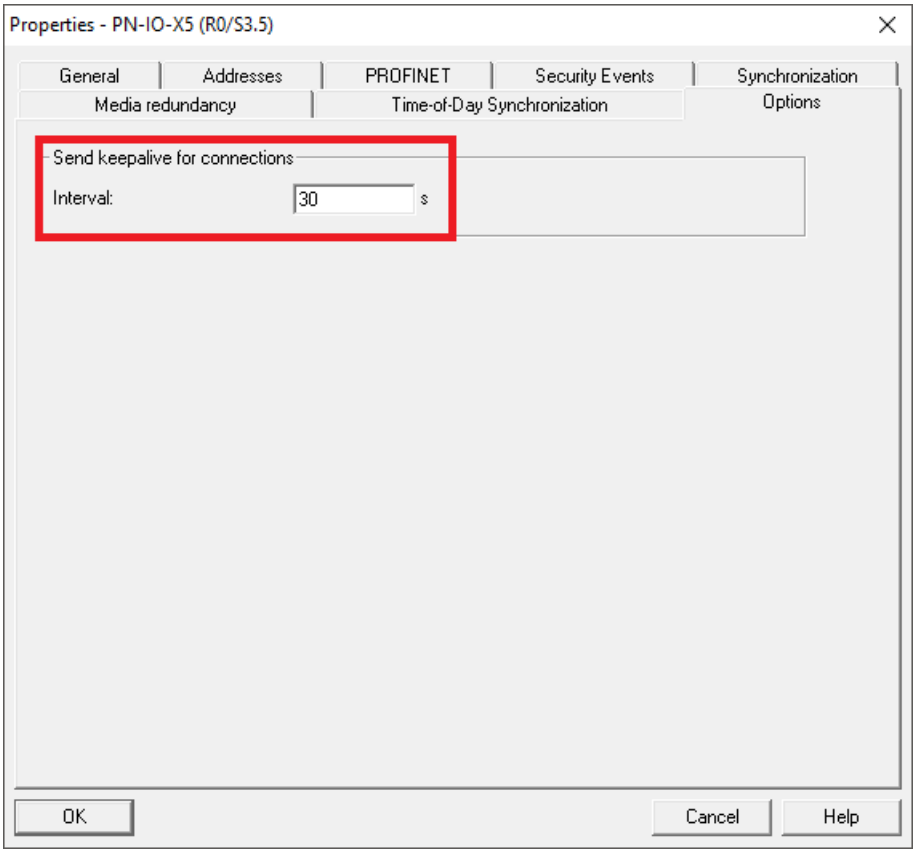
1. Use s7ftime (https://support.industry.siemens.com/cs/ww/en/view/22557362) to calculate the minimum value of the F-monitoring time of the communication blocks as described in the section "Monitoring time of the safety-related communication between F-CPUs (Page 217)".



2. Set the "Send Keepalives for Connections" parameter for both CPUs.

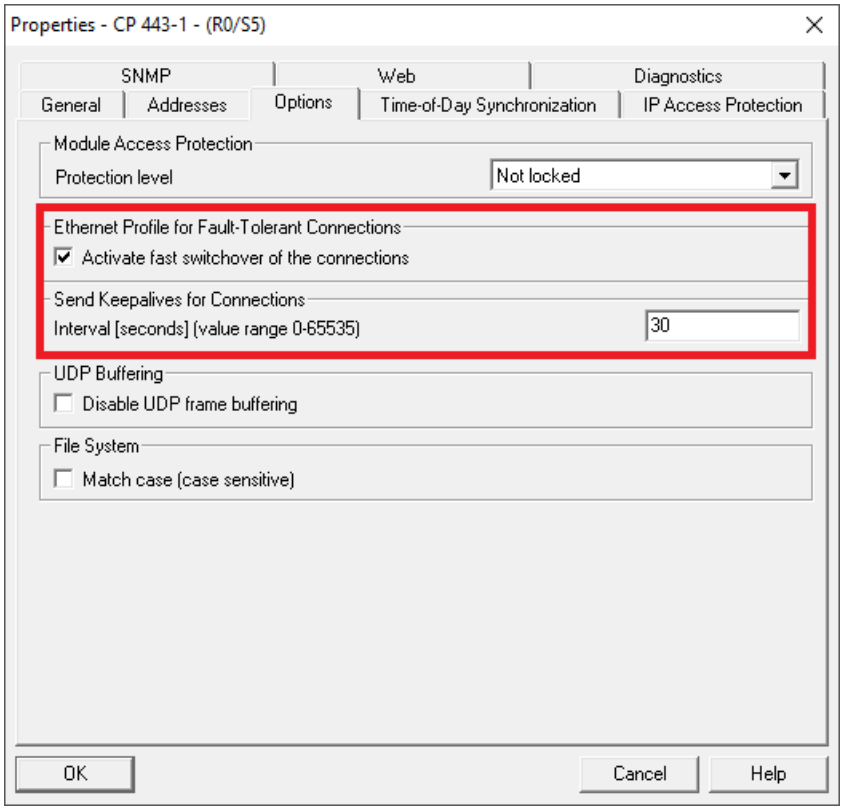
   This is the interval time with which sign-of-life telegrams are sent to the communication partner. Depending on which interface you are using for communication, you set this parameter in the properties of the internal PROFINET interface of the CPU or the CP443-1.

   Internal PROFINET interface of the AS 410



   Leave the interval for "Send Keepalives for Connections" at the default setting of 30 s.

CP 443-1

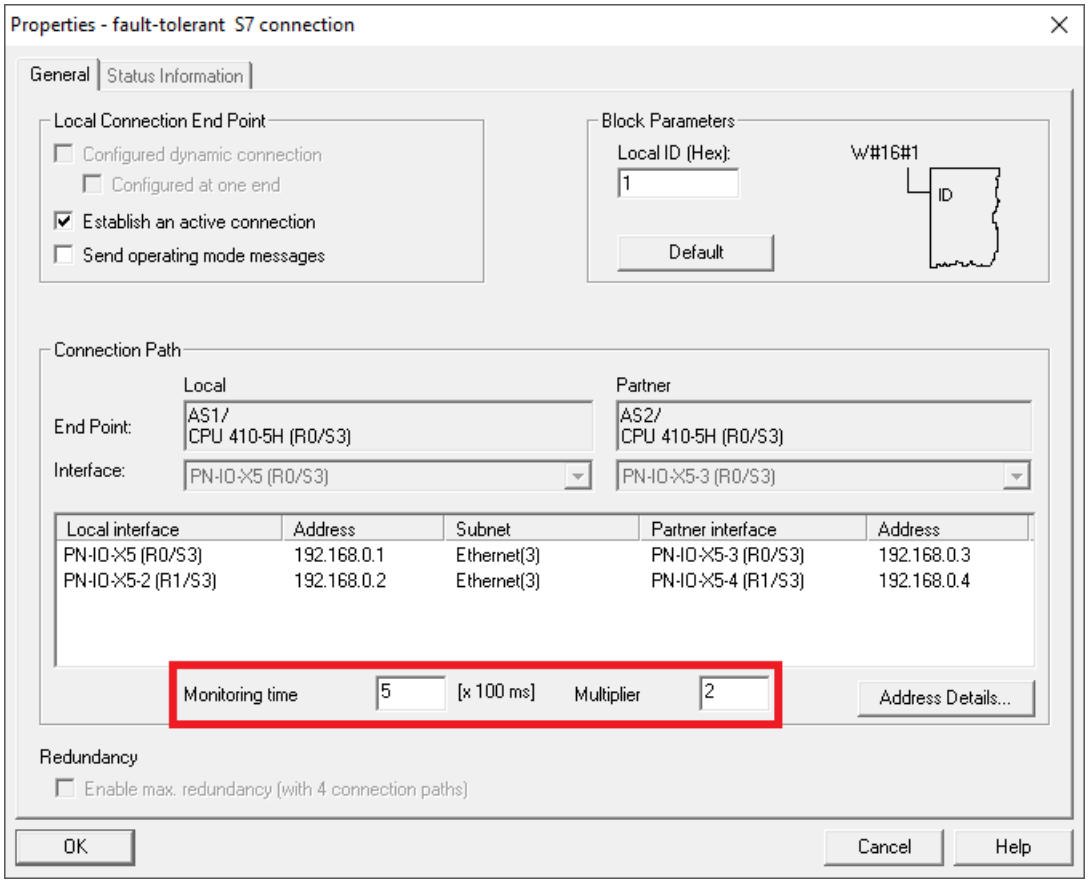


When high-availability S7 connections via a CP 443-1 are used, you enable "Activate fast switchover of the connections" function at "Ethernet Profile for Fault Tolerant Connections". Leave the interval for "Send Keepalives for Connections" at the default setting of 30 s.

3. Set the "Monitoring time of the physical connection".

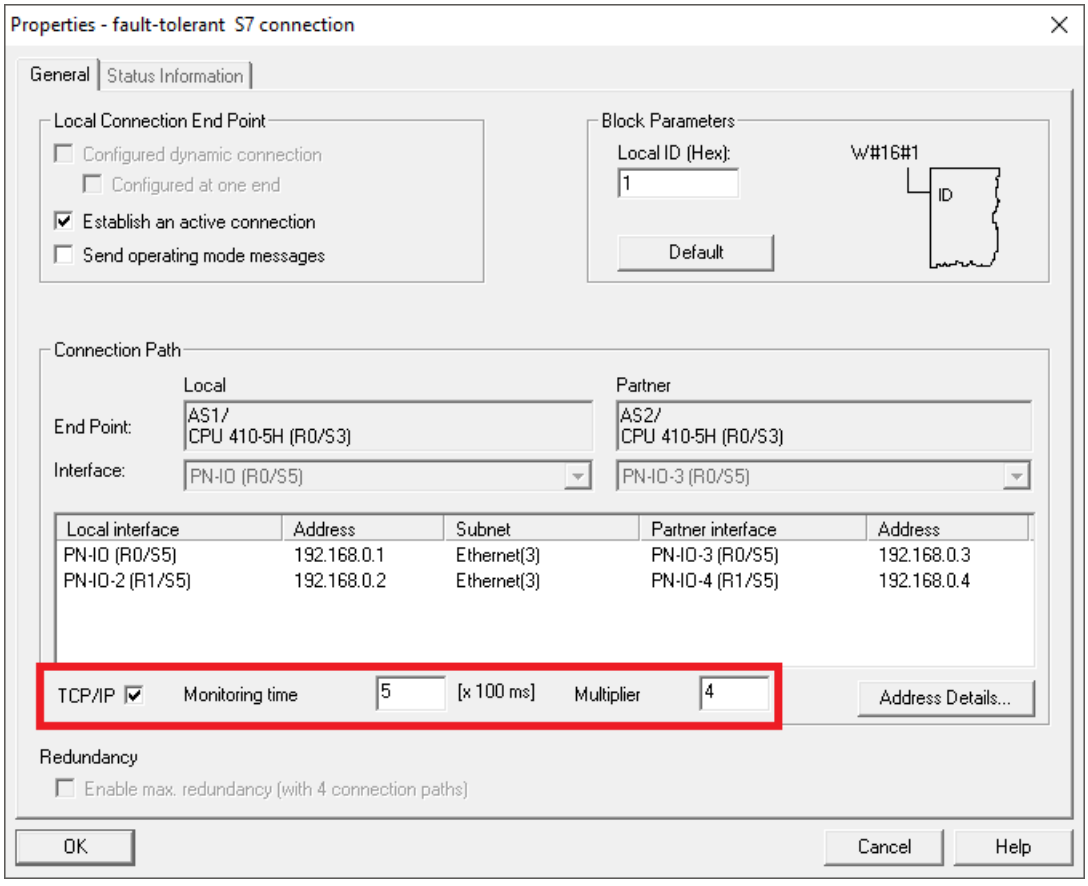
   You can use the parameter to set the monitoring time of the high-availability S7 connection via TCP. A telegram is expected from the communication partner within this time. You can find the parameter in the properties of the high-availability connection in NetPro.

   Internal PROFINET interface of the AS 410



   Set the monitoring time as described in section "SOFTNET-IE/HARDNET-IE S7 REDCONNECT" of the performance data and quantity frameworks of the SIMATIC NET PC software V16 document in the FAQ "What are the quantity frameworks and performance data of each of the SIMATIC NET products? (https://support.industry.siemens.com/cs/ww/en/view/15227599)".

CP 443-1

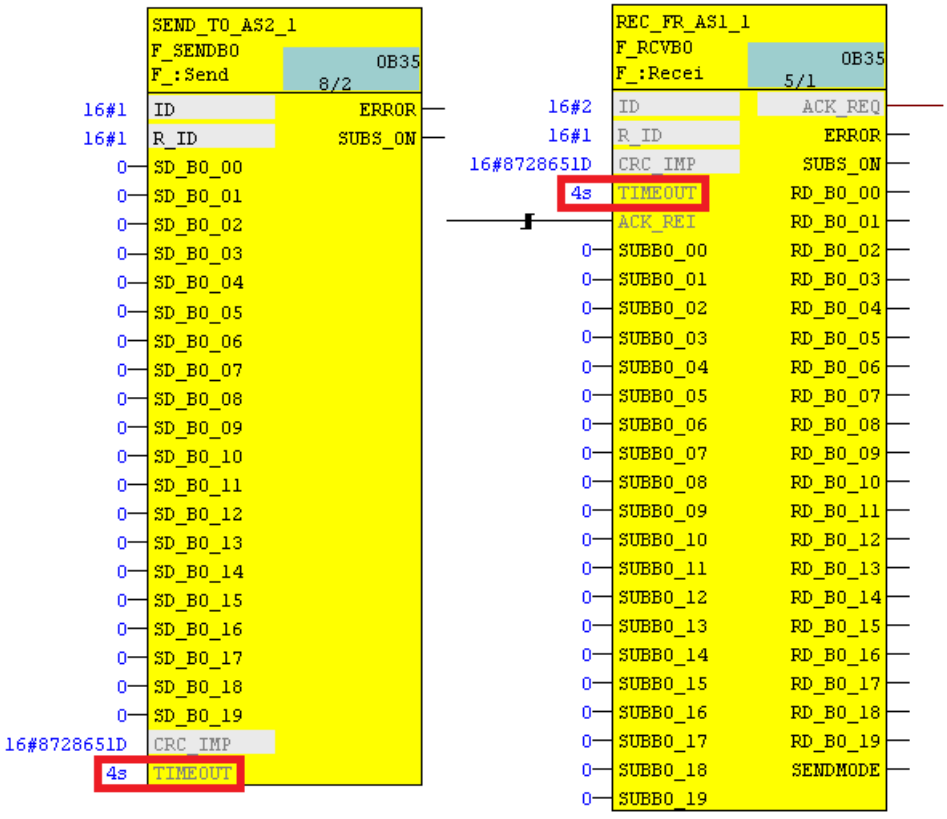


Set the monitoring time to at least 2 s. Background is the time after switching the connection as of which telegrams are once again sent by the CP443-1 (6GK7443-1EX30-0XE0 / 6GK7443-1EX30-0XE1); the time is 1 s.

Note

The monitoring/switchover time for high-availability connections via ISO is approx. 1 s. The value applies to all high-availability connections via ISO regardless of the number of connections.

4. Set the value of the input "TIMEOUT" (F-monitoring time) of the send and receive blocks.



The value of the input "TIMEOUT" (F-monitoring time) of the send and receive blocks F_SENDR and F_RCVR or F_SENDBO and F_RCVBO must be at least twice as high as the monitoring time of the physical connection. From the resulting value and the minimum value initially calculated in s7ftime, you set the greater of the two for the communication blocks.

Example for internal PROFINET interface of the AS 410:

2 x monitoring time of the physical connection = 2 x (5 x 100 ms x 2) = 2 s

Minimum value from s7ftime = 3.6 s

⇒ Set TIMEOUT to at least 3.6 s.

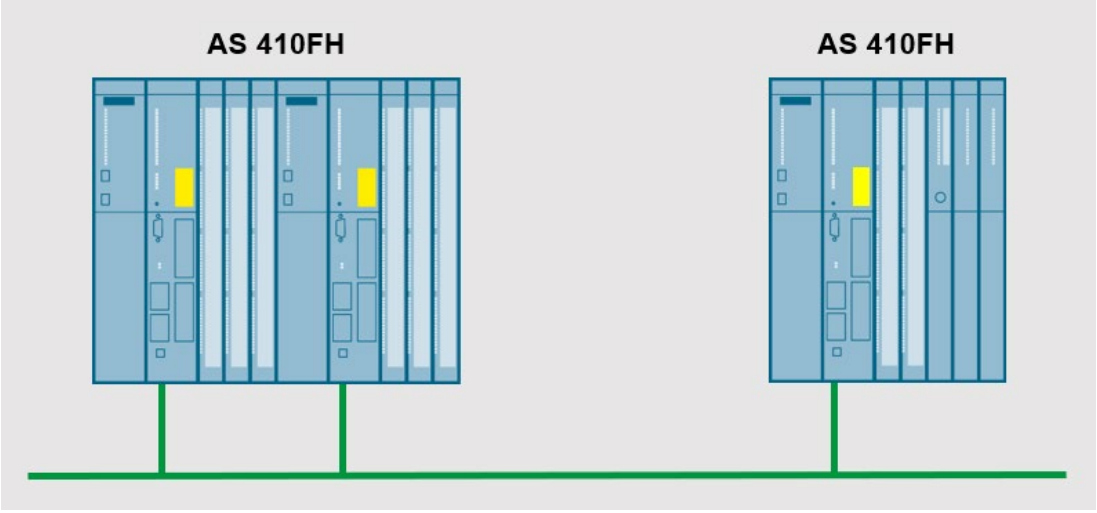
Example for CP 443-1:

2 x monitoring time of the physical connection = 2 x (5 x 100 ms x 4) = 4 s

Minimum value from s7ftime = 3.6 s

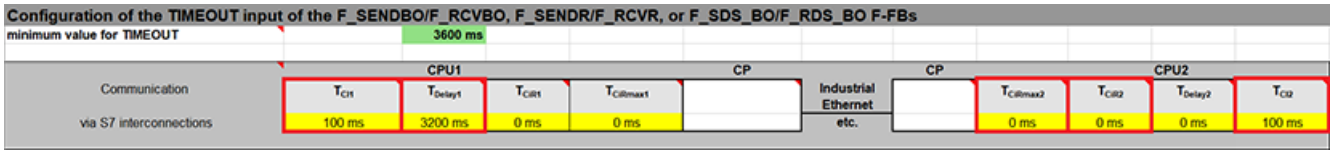
⇒ Set TIMEOUT to at least 4 s.

F-communication AS 410 high-availability – AS 410 single



Follow the steps outlined below:

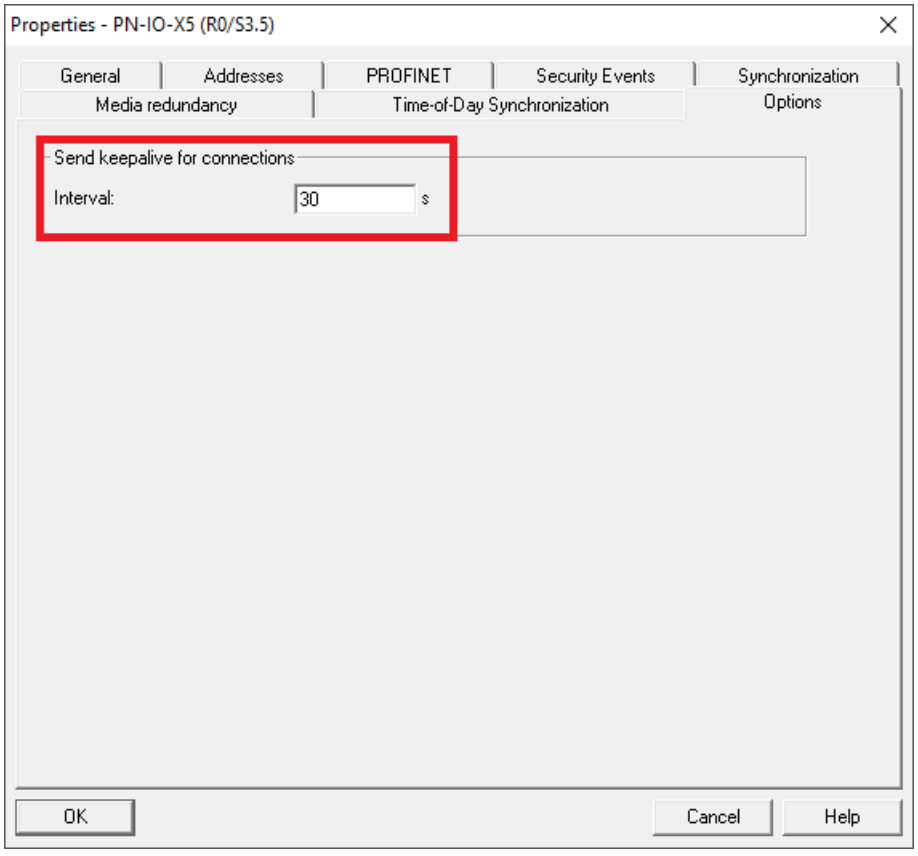
1. Use s7ftime (https://support.industry.siemens.com/cs/ww/en/view/22557362) to calculate the minimum value of the F-monitoring time of the communication blocks as described in the section "Monitoring time of the safety-related communication between F-CPUs (Page 217)".



2. Set the "Send Keepalives for Connections" parameter for both CPUs.

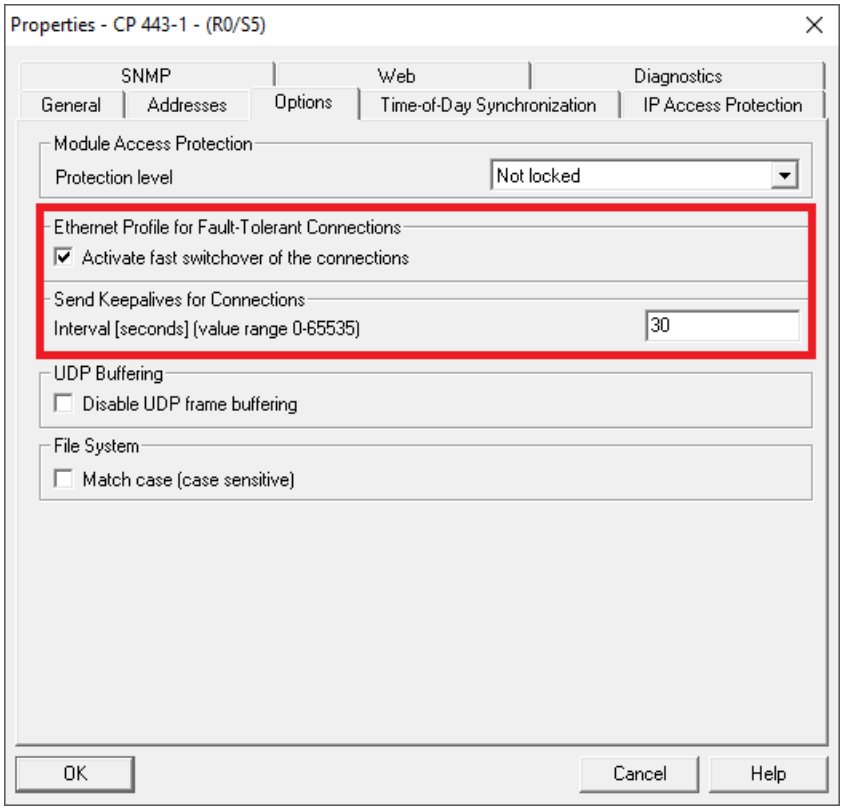
   This is the interval time with which sign-of-life telegrams are sent to the communication partner. Depending on which interface you are using for communication, you set this parameter in the properties of the internal PROFINET interface of the CPU or the CP443-1.

   Internal PROFINET interface of the AS 410 high-availability and single



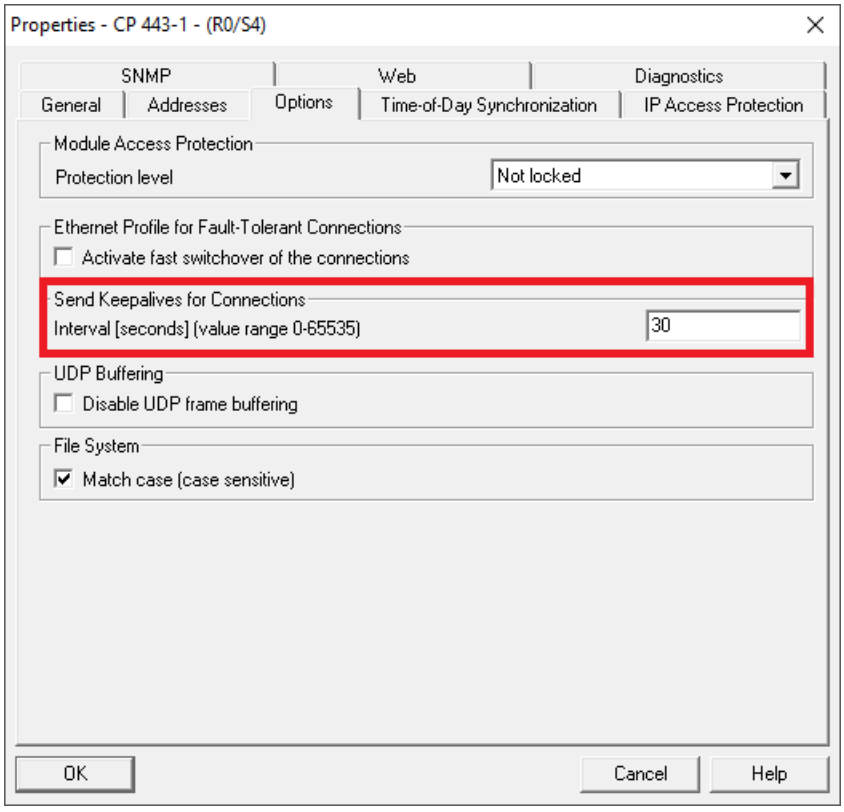
   Leave the interval for "Send Keepalives for Connections" at the default setting of 30 s.

CP 443-1 of the AS 410 high-availability



When high-availability S7 connections via a CP 443-1 are used, you activate "Activate fast switchover of the connections" function at "Ethernet Profile for Fault Tolerant Connections". Leave the interval for "Send Keepalives for Connections" at the default setting of 30 s.

CP 443-1 of the AS 410 single

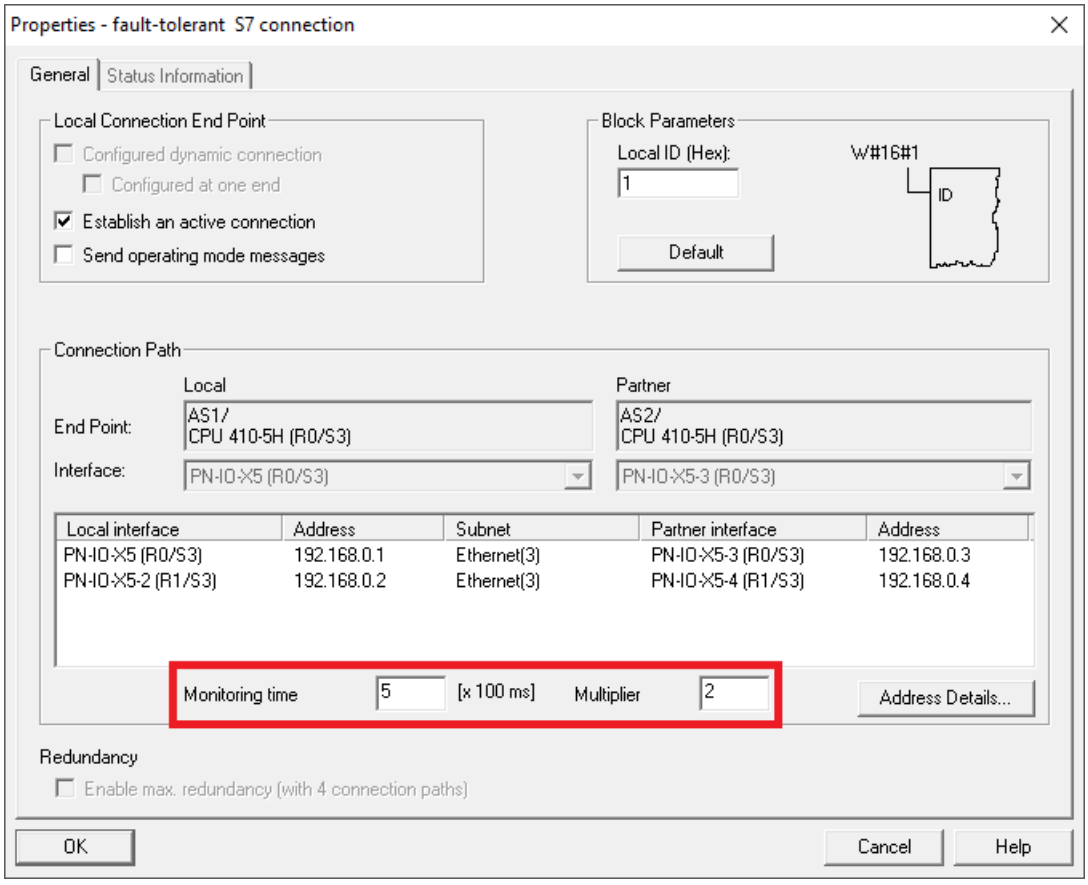


Leave the interval for "Send Keepalives for Connections" at the default setting of 30 s.

3. Set the "Monitoring time of the physical connection".

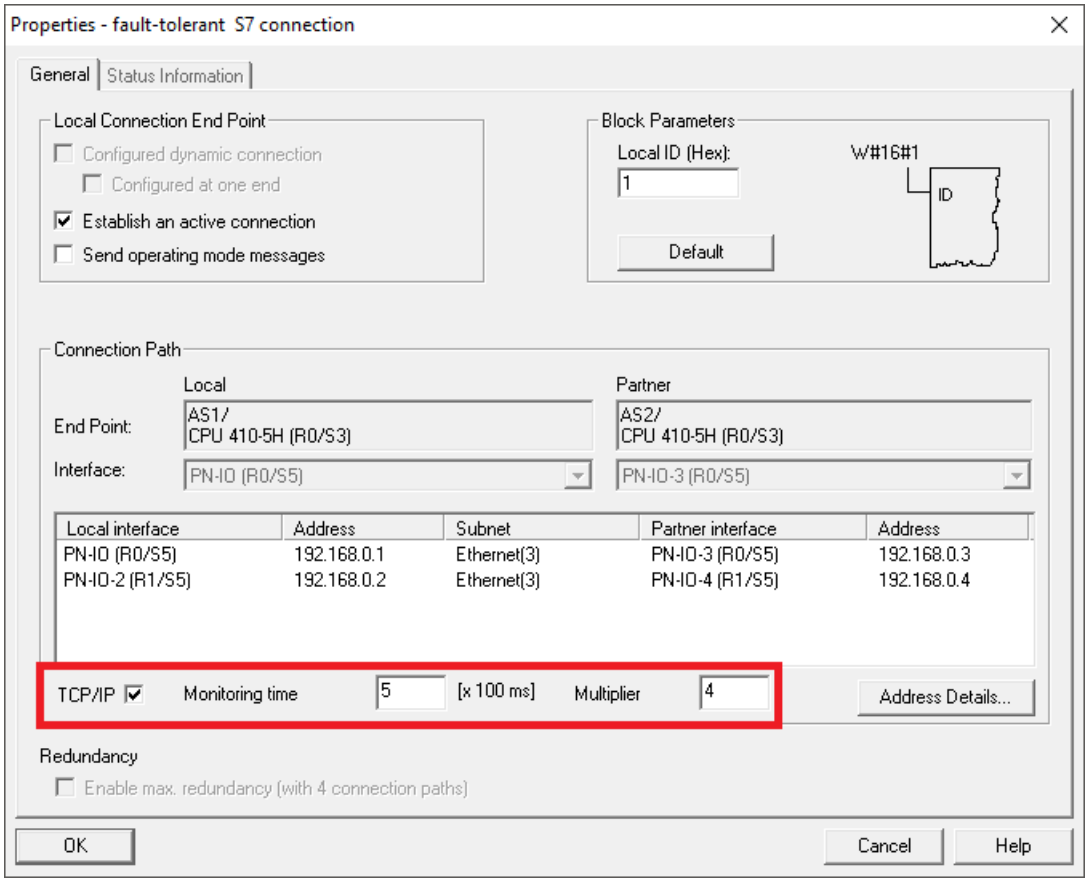
   You can use the parameter to set the monitoring time of the high-availability S7 connection via TCP. A telegram is expected from the communication partner within this time. You can find the parameter in the properties of the high-availability connection in NetPro.

   Internal PROFINET interface of the AS 410



Set the monitoring time as described in section "SOFTNET-IE/HARDNET-IE S7 REDCONNECT" of the performance data and quantity frameworks of the SIMATIC NET PC software V16 document in the FAQ "What are the quantity frameworks and performance data of each of the SIMATIC NET products? (https://support.industry.siemens.com/cs/ww/en/view/15227599)".

CP 443-1

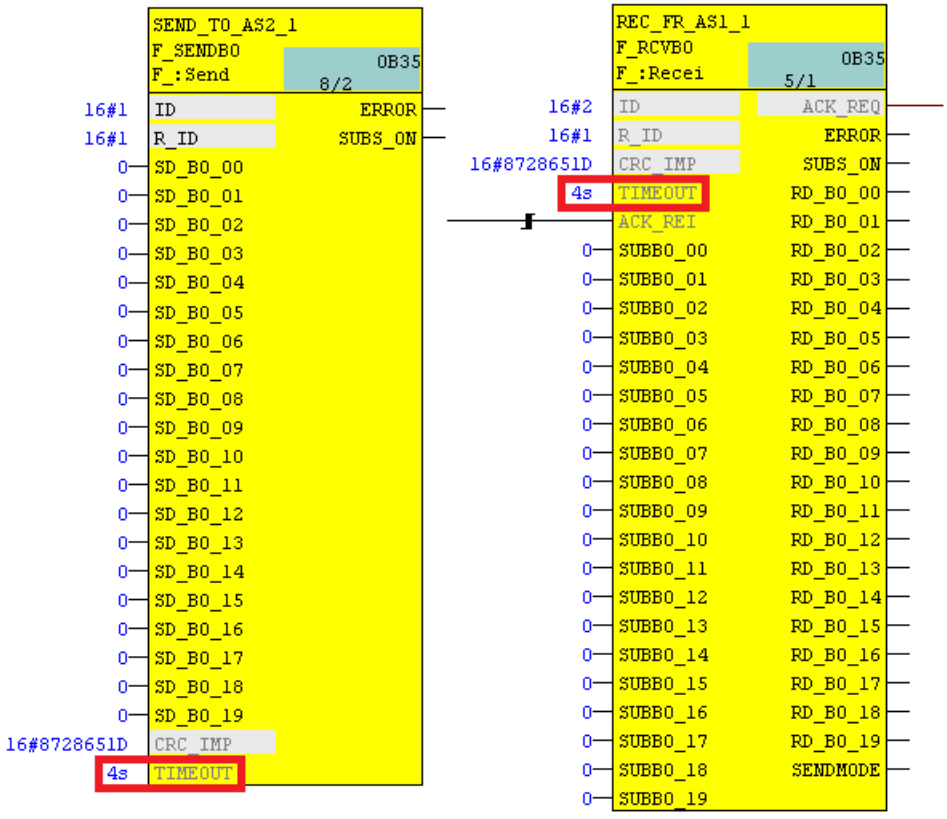


Set the monitoring time to at least 2 s. Background is the time after switching the connection as of which telegrams are once again sent by the CP443-1 (6GK7443-1EX30-0XE0 / 6GK7443-1EX30-0XE1); the time is 1 s.

Note

The monitoring/switchover time for high-availability connections via ISO is approx. 1 s. The value applies to all high-availability connections via ISO regardless of the number of connections.

4. Set the value of the input "TIMEOUT" (F-monitoring time) of the send and receive blocks.



The value of the input "TIMEOUT" (F-monitoring time) of the send and receive blocks F_SENDR and F_RCVR or F_SENDBO and F_RCVBO must be at least twice as high as the monitoring time of the physical connection. From the resulting value and the minimum value initially calculated in s7ftime, you set the greater of the two for the communication blocks.

Example for internal PROFINET interface of the AS 410:

2 x monitoring time of the physical connection = 2 x (5 x 100 ms x 2) = 2 s

Minimum value from s7ftime = 3.6 s

⇒ Set TIMEOUT to at least 3.6 s.

Example for CP 443-1:

2 x monitoring time of the physical connection = 2 x (5 x 100 ms x 4) = 4 s

Minimum value from s7ftime = 3.6 s

⇒ Set TIMEOUT to at least 4 s.

7.4 F-STOP

In the event of an F STOP, either the entire F program (full shutdown) or just the F shutdown group in which the error occurred (partial shutdown) is shut down. All F runtime groups in an F shutdown group are shut down at the same time. The F CPU's standard user program will continue to run in the event of an F STOP.

When F shutdown groups are shut down:

- The outputs of the F signal modules driven by the F shutdown group are passivated.
- As of S7 F Systems Lib V1_3: The F channel drivers of the F shutdown group set the outputs QBAD to "1" and QUALITY to "0".
- Safety-related communication between the F shutdown group and other F CPUs is interrupted.
- Data exchange between the F shutdown group and other F shutdown groups is interrupted.
- Where data exchange between the safety program and the standard user program is concerned, the standard user program is supplied with the last valid values.
- Block F_SHUTDN generates messages which are displayed automatically on the PCS 7 OS. With S7 F Systems Lib V1_3 SP2, the messages have the following message text:
  - Safety program: Partial shutdown
  - Safety program: Complete shutdown
- The corresponding diagnostics events are written to the F CPU's diagnostics buffer.

7.4.1 Complete shutdown

All of the F-CPU's F-shutdown groups are shut down. Shutdown proceeds in the following order:

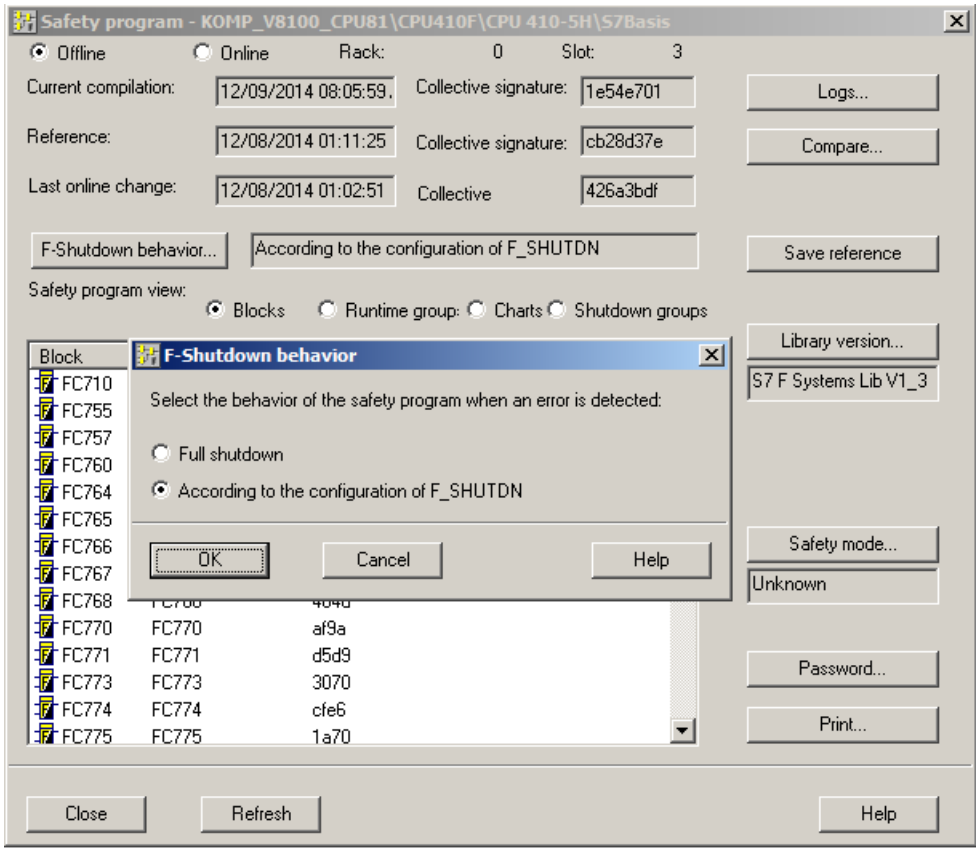
- First, the F-shutdown group in which the error was detected is shut down.
- All other F-shutdown groups are then shut down within double the time period you set as the F monitoring time for the slowest cyclic interrupt OB.

7.4.2 Partial shutdown

Only the F-shutdown group in which the error was detected is shut down.

7.4.3 Parameter assignment for shutdown behavior

From S7 F Systems V6.0 with S7 F Systems Lib V1_3 and higher, the shutdown behavior in the event of an F-STOP is defined in the "Safety Program" dialog using the "Shutdown behavior" button.



You can use the "Shutdown behavior" dialog to select how the safety program should behave when an error is detected (in other words, in the event of an F-STOP):

- "Complete shutdown":

  All F-shutdown groups associated with a safety program are shut down the first time an error is detected in an F-shutdown group.

- "Acc. to parameter assignment at F_SHUTDN":

  Block F_SHUTDN is located in the @F_ShutDn chart. At the SHUTDOWN input, you can choose from:

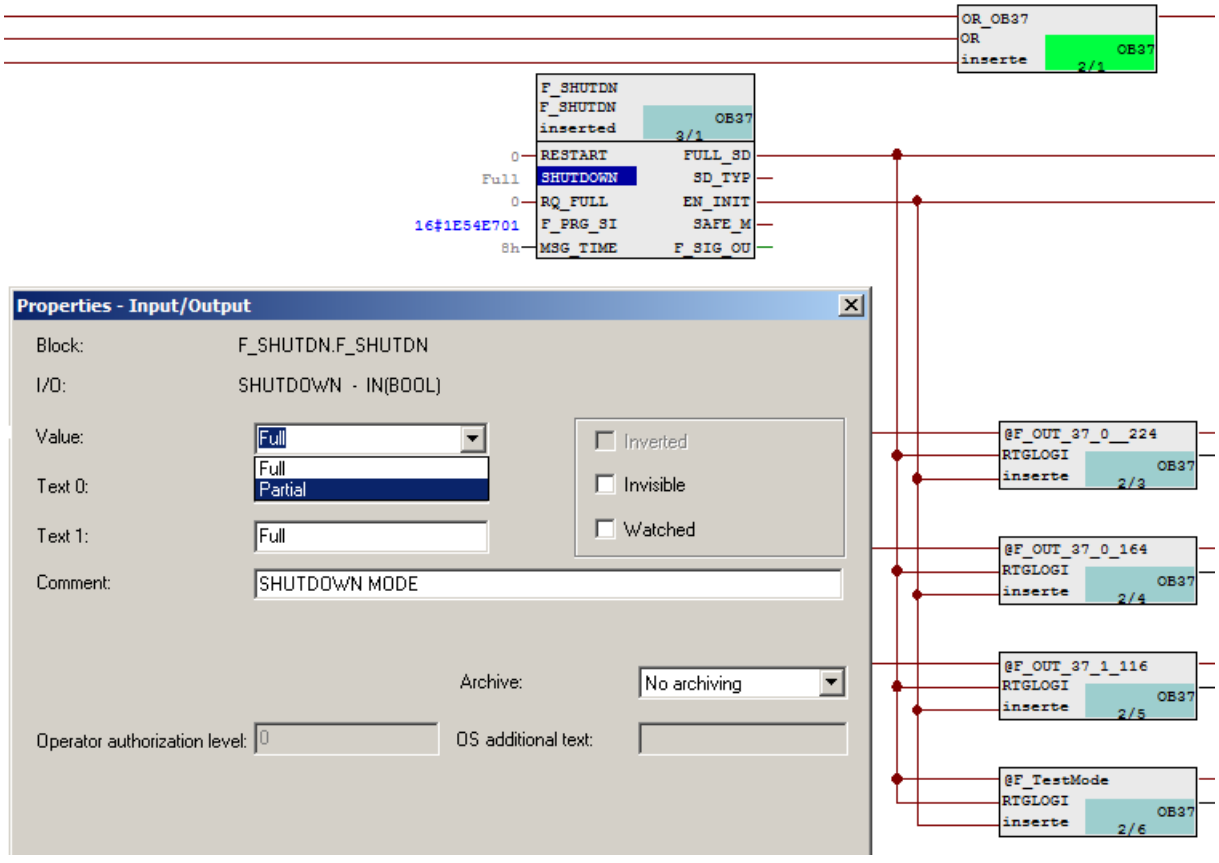
  - "Partial":

    The faulty F-shutdown group(s) is (are) shut down the first time an error is detected in an F-shutdown group (partial shutdown).

    or

  - "Full":

All F shutdown groups associated with a safety program are shut down the first time an error is detected in an F shutdown group.



If you change the shutdown behavior, you must recompile the F program. This applies even if you have changed the shutdown behavior online in CFC.

7.4.4 Causes of errors

Errors that trigger an F-STOP

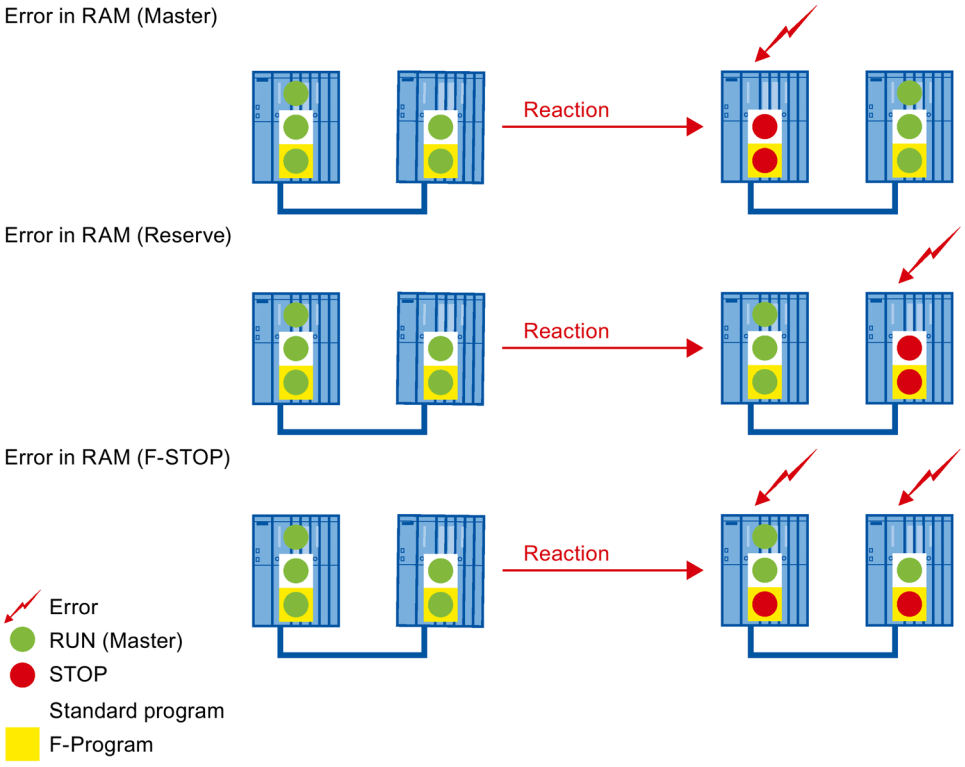
- Distortion of:
  - Data
  - Program sequence
  - Code
- CPU error

Errors that always trigger an F-STOP with full shutdown

Irrespective of the parameter assignment for F-STOP, a full shutdown is always triggered in the event of a cyclic interrupt OB request error (caused by a CPU/OB overload, for example).

7.4.5 Execution of an F-STOP in S7 F/FH systems

F-STOP illustration



Error in master:

Before a safety program in a redundant F CPU goes into F-STOP, it completes the following steps:

- The S7 F/FH system performs a master-to-standby switchover.
- The previous master goes into the configured operating state (default setting: TROUBLESHOOTING).

If no errors are detected, the F CPU reconnects.

Note

Refer to the following manuals for more information:

- "SIMATIC High Availability Systems S7-400H (https://support.industry.siemens.com/cs/ww/en/view/82478488)"
- "SIMATIC PCS 7 Process Control System CPU 410 Process Automation V8 (https://support.industry.siemens.com/cs/ww/en/view/109801828)"

If an error is detected, the previous master goes into FAULT mode (all LEDs on the affected CPU flash).

On redundant F CPUs, errors on one communications partner will not stop program execution.

Error in both F CPUs:

The safety program goes into F-STOP immediately.

7.4.6 Exiting an F-STOP

Run an F-startup as described in the following chapter.

7.5 F startup and (re)start protection

7.5.1 F-startup

S7 F-systems do not make a distinction between a CPU cold restart and a CPU warm restart. An exception are the F-blocks F_MOV_R (from S7 F Systems Lib V1_3), F_SWC_CB and F_SWC_CR (part of the "Secure Write Command++" function).

Both a CPU cold restart and a CPU warm restart will generate an F-startup. With an F-startup, the safety program launches automatically with the initial values.

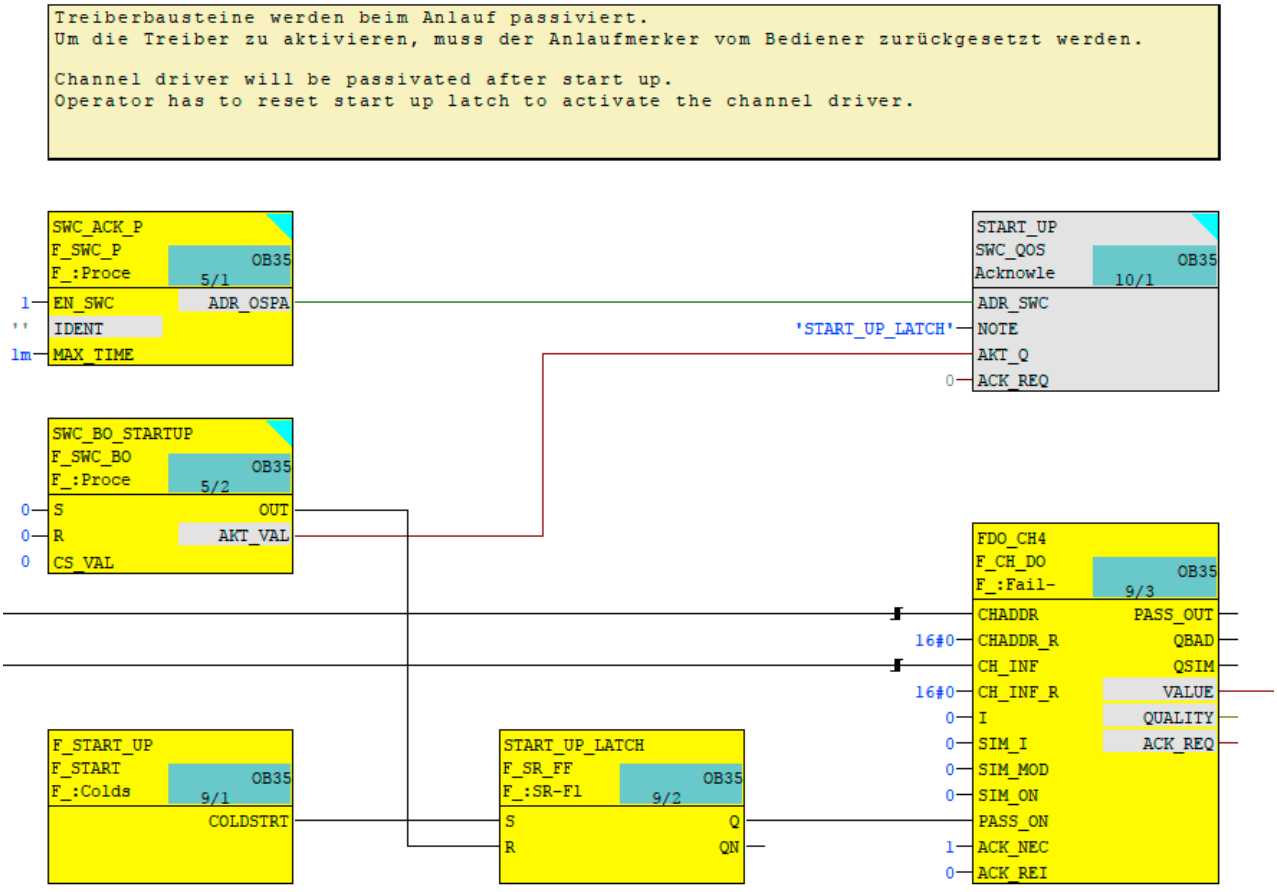
An F-startup is performed:

- After a CPU STOP, when you perform an F-CPU warm restart
- After an F-STOP, when the "F_SHUTDN" F-block detects a positive edge at the RESTART input
  Following a partial shutdown of the safety program, only the F-shutdown groups involved in the F-STOP perform an F-startup. F shutdown groups with errors remain in F-STOP.

7.5.2 (Re)start protection

If the process does not permit the safety program to start up automatically with the initial values, you will need to program a response to F-startup.

The F_START F-block is used to signal an F-startup of the safety program with the initial values. The COLDSTRT output parameter tells you that an F-startup has been triggered.



In this example, a flip-flop is set when the F-program is started up, which passivates the output drivers. Once all the process conditions have been fulfilled, the operator can release the F-output signals by resetting the flip-flop using the F-acknowledgment function.

As of S7 F Systems V6.2 with S7 F Systems Lib V1_3 SP2, you can control the restart of F I/Os via the ES/OS with "Safety Write Command++" ("SWC++") (F_SWC_BO and SWC_QOS). You

can find additional information about using SWC_QOS in the section Fail-safe acknowledgment (SWC_QOS) (Page 178).

Note

Additional options for programming a startup (and restart) protection and "Secure Write Command++" in the manual "SIMATIC Industrial software S7 F/FH Systems - Configuring and Programming" (https://support.industry.siemens.com/cs/ww/en/view/109802562).

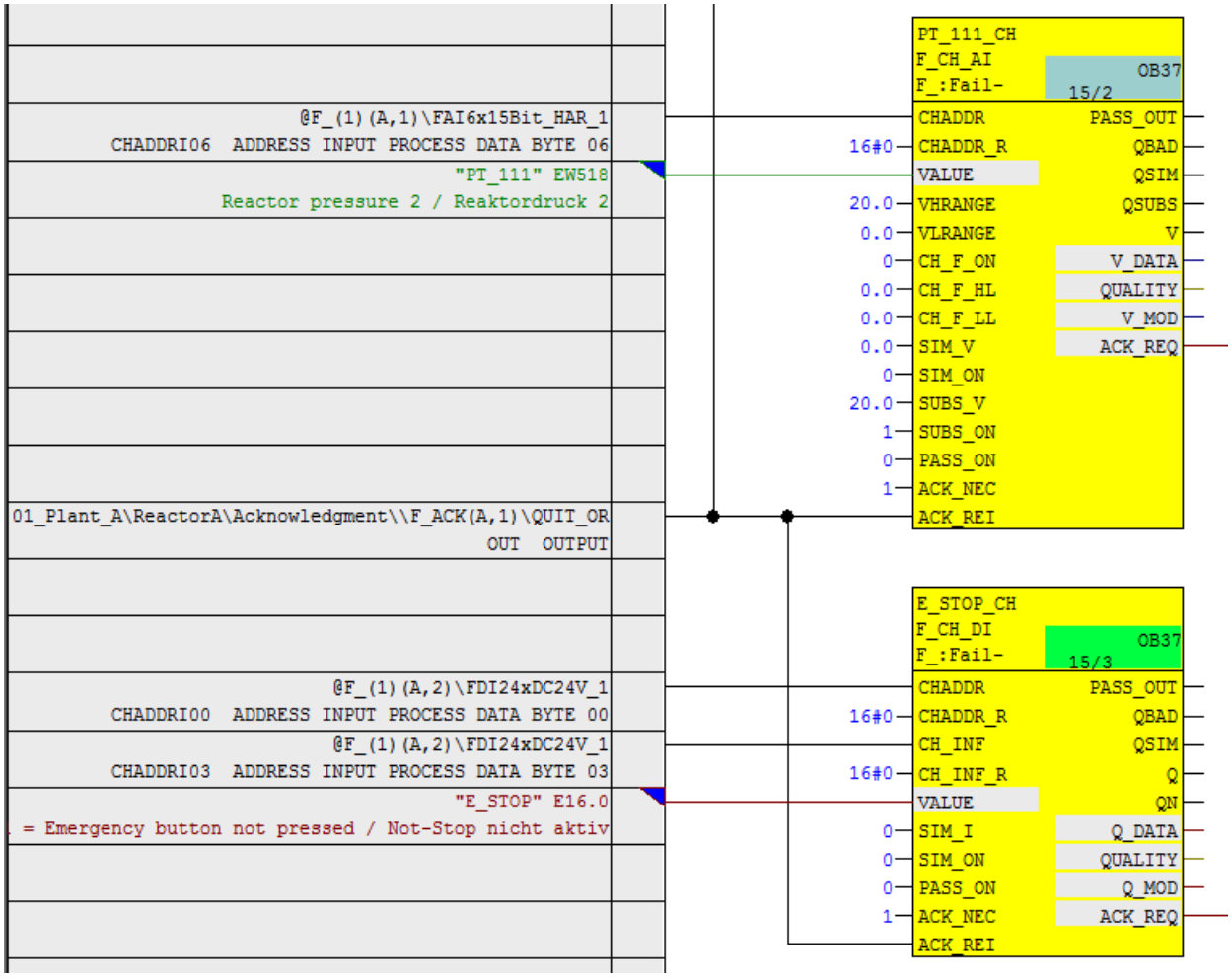
7.6 I/O access via F channel driver blocks

In S7 F systems, F signal modules are accessed via F channel driver blocks and not via the process image. For this purpose, the following driver blocks are used in the program:

- F channel driver (e.g. F_CH_xx) for access to the input/output channels of F signal modules.

  One F-channel driver is required for every input or output channel used. Only one F-channel driver is required for redundant channels.

  In your safety program, F channel drivers provide the interface with a channel of an F signal module and perform signal processing. F channel drivers vary depending on the F-signal modules. They are placed and interconnected in the safety program by the user.



- The CFC compiler creates and interconnects one F-module driver per module for PROFIsafe communication purposes.

Note

When changing the address of an F_CH_AI channel driver block via delta download, read the following FAQ: "What do you have to consider if you want to transfer an address change to an F_CH_AI channel driver module via a delta download?" (https://support.industry.siemens.com/cs/ww/en/view/109756529)

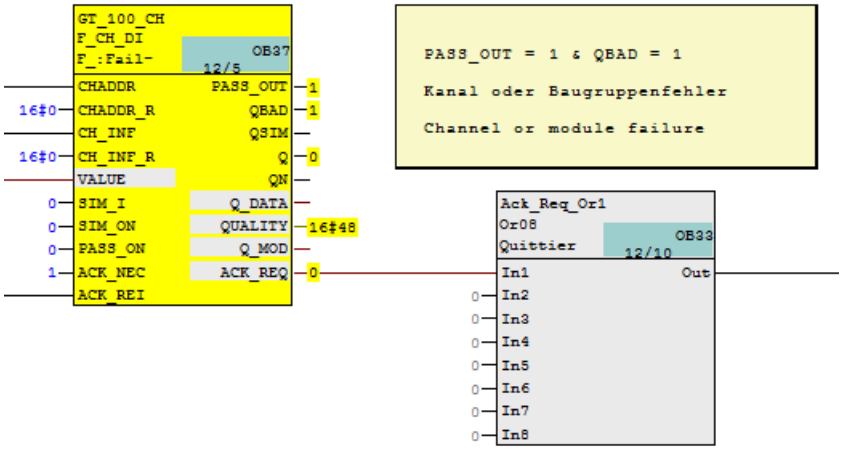
7.7 Passivation and reintegration of input/output channels

7.7.1 Passivation - general

Passivation means that in the event of an error, one or a number of channels on an F signal module are switched to a safe state. In the event of a channel error (a faulty sensor, for example), only the affected channel is passivated.

In the event of a module error (a communication error, for example), all channels on the fail-safe I/O module are passivated.

If an F signal module detects an error, it switches the affected channel or all of its channels to the safe state; in other words, the channels on this module are passivated. The fail-safe F signal module sends a message to the F channel driver and the PCS 7 OS to indicate that it has detected an error.



The PASS_ON input can also be used to activate and deactivate the passivation of a channel in the safety program, e.g. by using a specific condition in the program sequence or restart protection.

When output channels are passivated, the outputs are de-energized (set to a zero-current or zero-voltage state). The F channel driver of a passivated digital output channel issues a substitute value with the quality code (QUALITY) 16#48 and the QBAD output is set to 1.

When input channels are passivated, substitute values are forwarded to the safety program, regardless of the actual process signal.

The F channel driver of a passivated digital input channel outputs substitute value 0 with quality code (QUALITY) 16#48 and the QBAD output is set to 1. In accordance with the parameter assignment at the SUBS_ON input, the F channel driver of an analog input channel will output either a substitute value with quality code (QUALITY) 16#48 or the last valid value with quality code (QUALITY) 16#44. The QBAD output is also set to 1 and, if a substitute value is output, the QSUBS output is set to 1.

See also

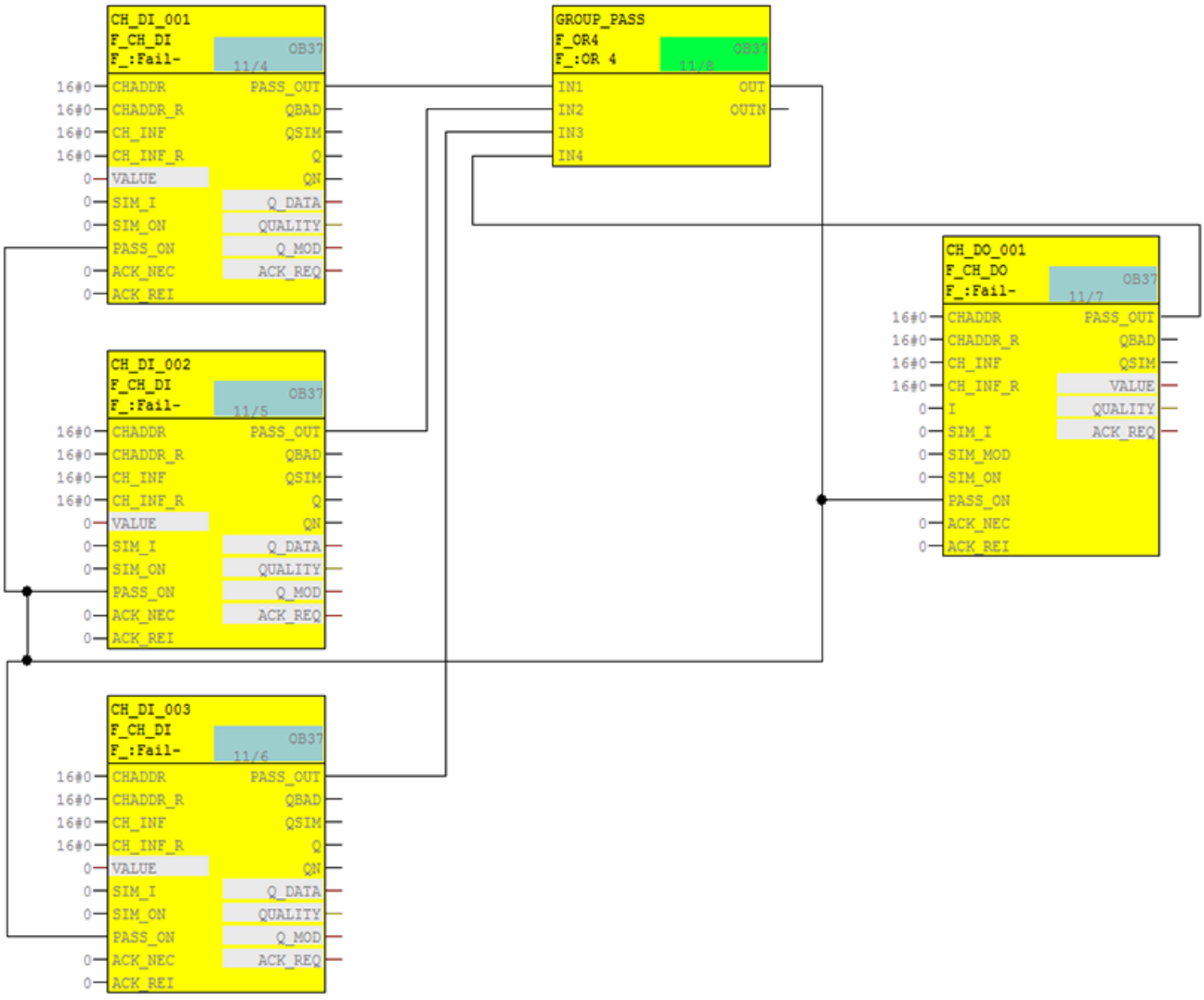
F startup and (re)start protection (Page 156)

7.7.2 Group passivation

If, during passivation of an F-I/O or a channel of an F-I/O, you wish to activate passivation of other F-I/Os, you can use the PASS_OUT output/PASS_ON input to perform group passivation of related F-I/Os.

Group passivation via PASS_OUT/PASS_ON can be used, for example, to force the simultaneous re-integration of all F I/Os after the S7 F system starts.

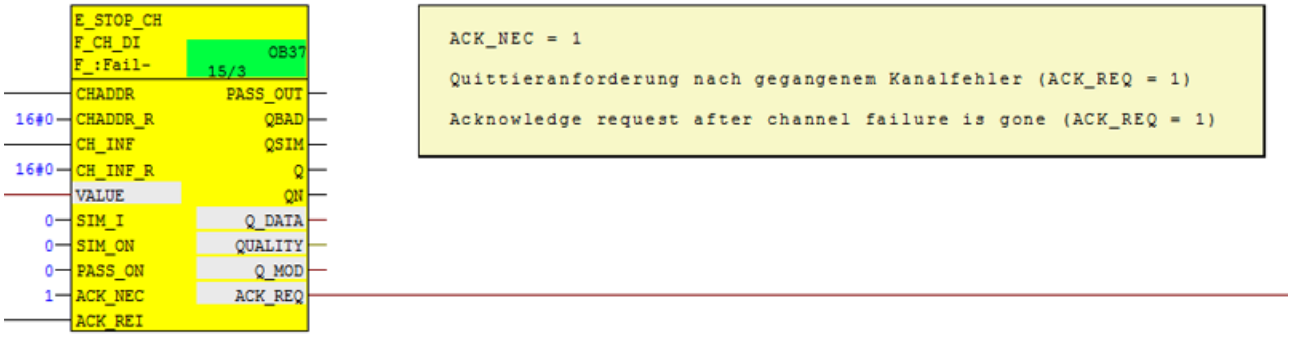
To enable group passivation, you must link all PASS_OUT outputs of the F-channel drivers in this group with F_OR4 F-blocks, and interconnect the OUT output result of F_OR4 with all PASS_ON inputs of the F-channel drivers in this group.



7.7.3 Reintegration following elimination of errors

Reintegration means:

- Valid process values start to be output again at the output channels of the fail-safe output modules.
- The F-channel drivers associated with the fail-safe input modules resume the forwarding of valid process values to the safety program.
- Once a channel error has been eliminated, a channel on a fail-safe module can be reintegrated automatically or following user acknowledgment. You can use the ACK_NEC input of an F-channel driver to specify whether or not user acknowledgment is required:
  - Value 0: Automatic reintegration without user acknowledgment
  - Value 1: Prompt for user acknowledgment for reintegration following error elimination



If passivation was triggered by setting PASS_ON = 1, user acknowledgment will not be required for reintegration.

Note

The ACK_NEC input can only be set to 0 if the process permits automatic reintegration from a safety-related point of view.

7.7.4 Automatic reintegration on channel error

If the ACK_NEC input is not set and once a channel error has been corrected, the affected channel is reintegrated automatically (depassivated) as follows:

- With input modules - immediately
- With output modules - within a matter of minutes (due to required test signal injections, after 2 successful test cycles).

Note

User acknowledgment is always required for reintegration following module errors (ACK_REQ output set), even if ACK_NEC has not been set. An interconnection of the ACK_REI input with an automatically generated signal is not permitted.

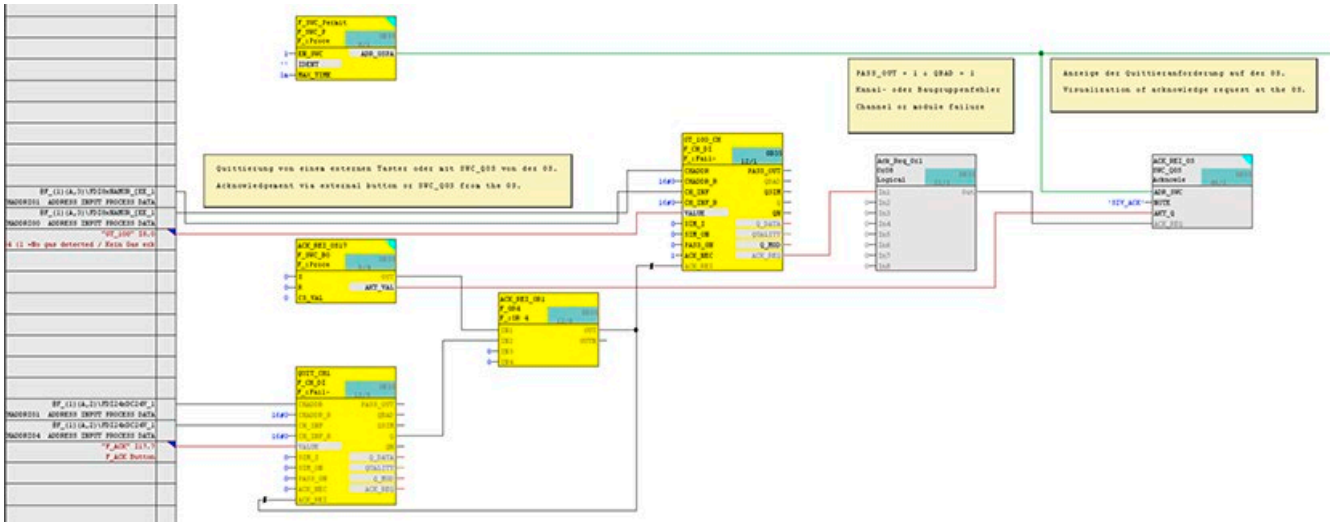
7.7.5 Programming reintegration following module errors or channel errors requiring acknowledgment

A value of 1 at the ACK_REQ output of the F-channel driver indicates that the error has been eliminated and user acknowledgment for reintegration is possible.

When the ACK_NEC input is set, reintegration of the input or output channel is only performed a positive edge at the ACK_REI input of the F-channel driver.

Options for user acknowledgment

- An acknowledgment button is connected to a fail-safe digital input module
- Manual input from an ES or a local operator station via SWC_QOS



Note

The figure is available in its original size as appendix to the manual in the ZIP download of the checklists.

If you use an acknowledgment button for user acknowledgment, in the event of a module error on the F-signal module group to which the acknowledgment button has been connected, you will no longer be able to trigger acknowledgment to reintegrate this F-signal module group. An additional acknowledgment option must be provided for this module group, for example: with a "SWC_QOS" block.

Note

Automatic user acknowledgment is generally not permitted!

Note

You can find additional information about programming fail-safe acknowledgment with "Secure Write Command++" in the manual "SIMATIC Industrial software S7 F/FH Systems - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/109802562)".

7.8 Compiling the F-program

If an S7 program contains charts with F blocks, these will be compiled when the CFC charts are compiled. Measures for eliminating errors will also be expanded and additional safety-relevant checks carried out.

7.8.1 Password protection for safety-related functions and settings

A password protects the fail-safe program and the parameters of the F-modules against unauthorized changes. The password is requested when accessing fail-safe parts of the system, e.g. when editing a fail-safe CFC, when compiling changes in the safety program or when opening the properties of a fail-safe module in the hardware configuration.

As of S7 F Systems V6.2, you can use a more secure password by activating the "Increased password security" option box; this must comply with the "Conditions for a secure password":

- Password length: minimum 8, maximum 32 characters
- At least one capital letter of the Latin alphabet (A - Z); also diacritical characters (umlauts and letters with accents)
- At least one lowercase letter of the Latin alphabet (a- z); also "ß" and diacritical characters (umlauts and letters with accents)
- At least one digit (0-9)
- At least one of the following special characters:
  ~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; ' " < > , . ? /

Note

The use of the "Increased password security" option in the "Create password for safety program" dialog is recommended.

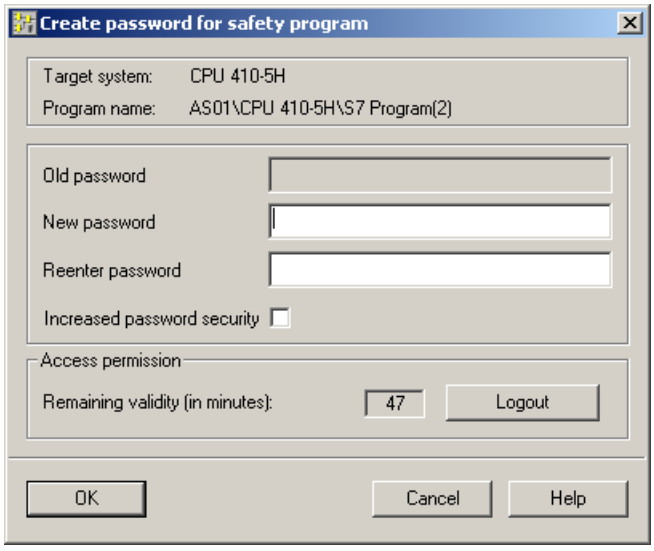
This option is activated by default as of S7 F Systems V6.3. When using Safety Matrix with version V6.2.2 or earlier, the option "Increased password safety" must not be activated.

If the password is entered, it remains valid for one hour. If you have finished your work, reset the password's period of validity.

To do this, in the SIMATIC Manager select the CPU that contains the safety program and use the "Options > Edit Safety Program" menu command to open the relevant dialog.

There you can find the "Password" button that opens the "Create Password for Safety Program" window. The "Clear" button sets the validity period to "0".

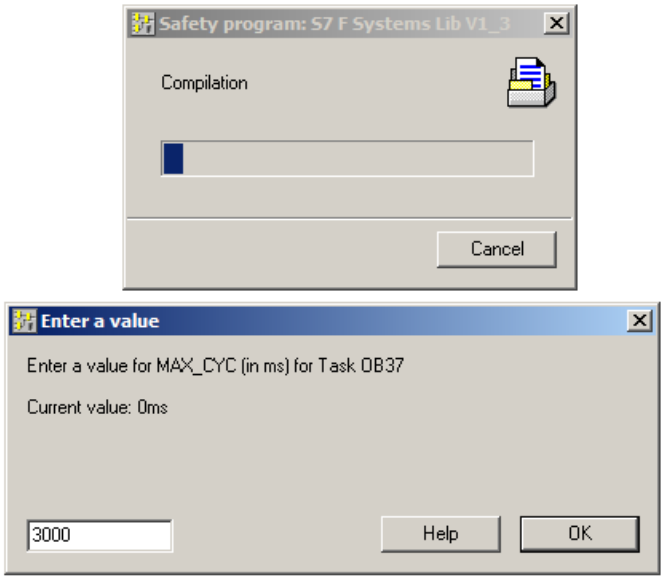
You also have the option of changing the password.



If a standard user program and a fail-safe program are running in one CPU, changes to the standard part can be compiled without the need to enter the F-password. This assumes that no changes have been made to the safety program.

7.8.2 Parameterizing the maximum F cycle monitoring time

The F-CPU runs F-cycle time monitoring for every cyclic interrupt OB containing F-runtime groups. The first time the F-program is compiled, for each cyclic interrupt OB which contains an F-program you will be prompted to enter a value for the maximum cycle time (MAX_CYC) that may elapse between two calls of this cyclic interrupt OB.



The default for the maximum F-cycle time is 3,000 milliseconds.

Check whether this setting is suitable for your process. Change the default if necessary.

Note

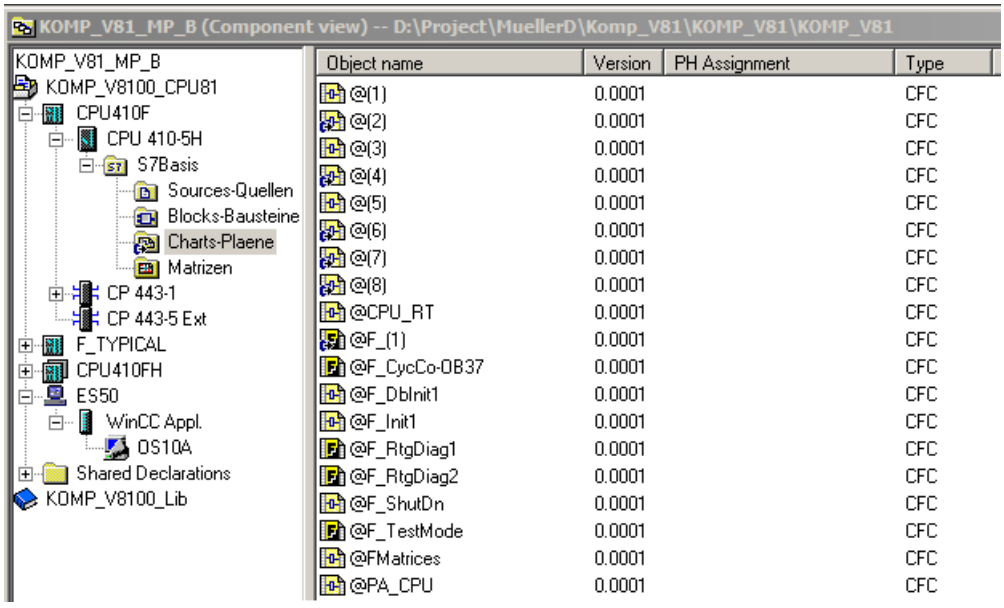
You can change the default value at the MAX_CYC input of the F_CYC_CO block in chart @F_CycCo-OB3x whenever you wish.

You can find information about setting the F-monitoring time and response times in section "Monitoring times and system response times (Page 195)".

7.8.3 Compiling the S7 program

During compilation, the S7 program is automatically expanded to include diagnostics drivers (contained in the @ system charts) and F-specific parts.

F system blocks are stored in @F_xxxx charts.

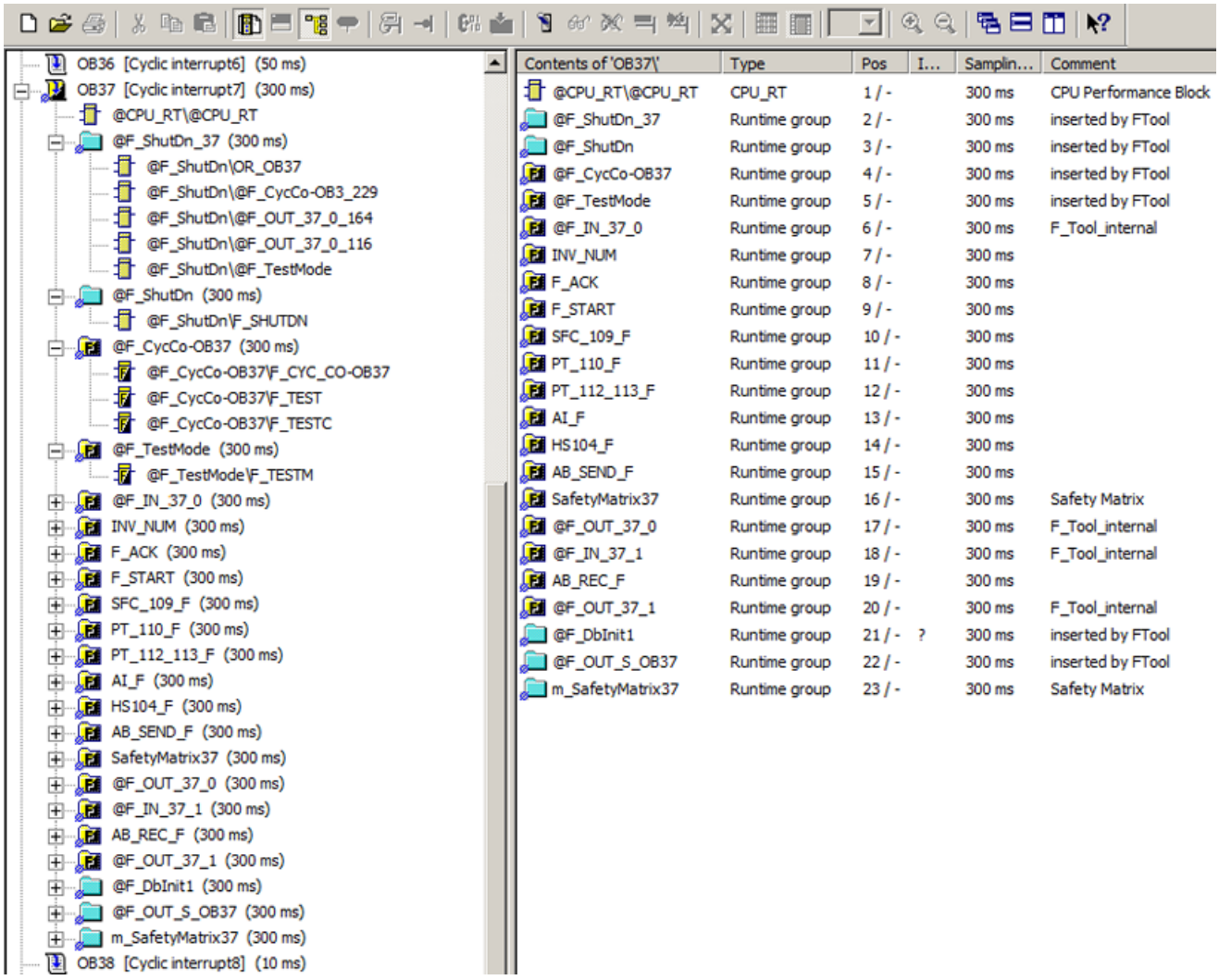


Note

Placements, interconnections, and parameter assignments for F-system blocks completed automatically during the compilation process must not be changed.

You must not change or delete F blocks in the block container.

The CFC compiler also automatically places F system blocks needed for the operation of the safety program in runtime groups. The names of these runtime groups begin with "@F_".



Note

The CFC charts and runtime groups with fail-safe blocks appear in yellow and are marked "F" to distinguish them from standard charts.

7.9 Safety mode and downloading the safety program

Safety mode of the safety program in the F-CPU can be temporarily deactivated and reactivated. This enables you to make changes to the safety program in RUN mode.

7.9.1 Information on safety mode

The safety mode of the safety program in the F-CPU is automatically activated after startup. In safety mode, all functions present in the system for system error detection and for the fail-safe user program are activated. In this state, it is not possible to change the safety program during operation (RUN). To perform online changes of fail-safe parameters from "CFC Online" or to load changes into the fail-safe program, some of the diagnostic functions must be switched off. This is done by disabling safety mode before the changes are performed or loaded online. Before disabling safety mode, it must be ensured that the process is in a non-critical state and is being monitored by an operator during this time (monitored operation). In order to be able to load program changes with disabled safety mode, the parts of the monitoring that would detect changes to the software and trigger an F-STOP are switched off. "Random hardware faults" continue to be detected and the diagnostics for the modules remain active. The safety program continues to be executed, so that a "request" from the field leads to the activation of the safety function. Once the changes have been made, or at the end of the download process, safety mode must be reactivated immediately. Additional required measures may result from the risk analysis.

7.9.2 Deactivating safety mode

Safety mode can be deactivated/activated if a relevant system prompt appears, or from the SIMATIC Manager. To do this, select the CPU that contains the safety program and use the "Options > Edit Safety Program" menu command to open the relevant window.

The field underneath the "Safety Mode..." button shows you whether safety mode is "activated" or "deactivated". If the safety program does not match the safety program in the F-CPU or communication with the F-CPU has failed, "unknown" will appear here.

If there is a connection between the engineering station and the CPU, the current status of the safety program is displayed and can be changed using the "Safety Mode..." button. An additional prompt appears before the status is changed.

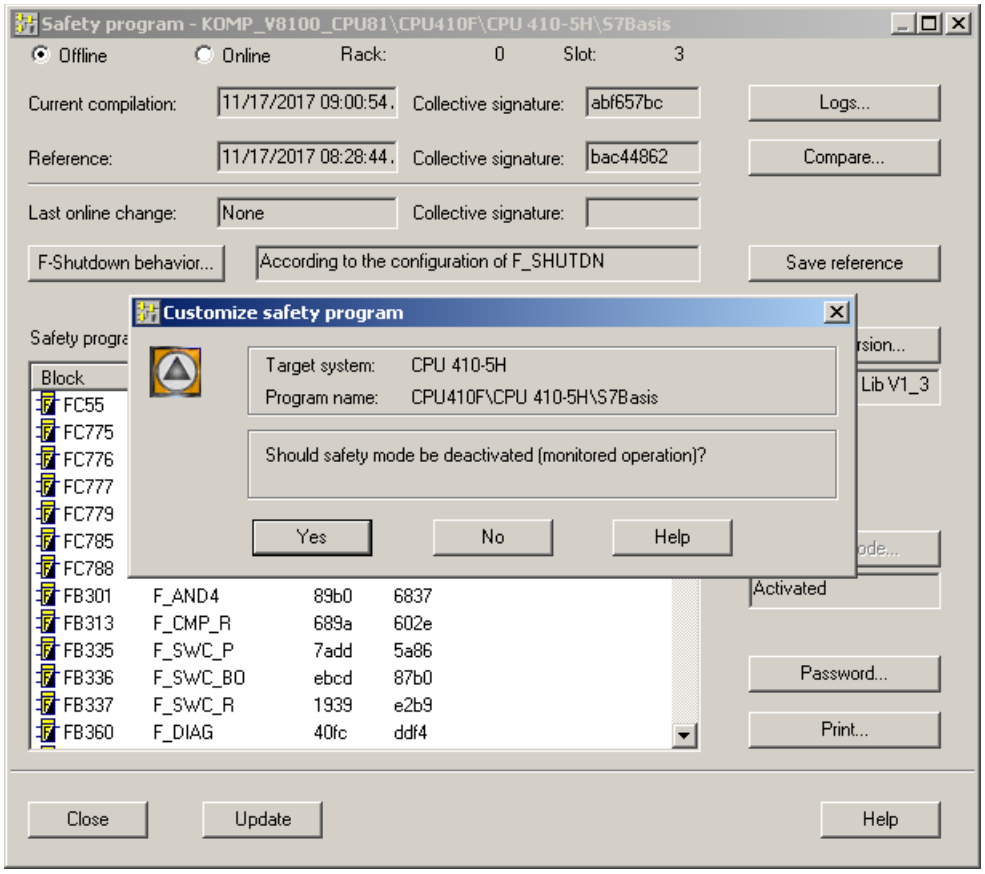
The safety mode status is entered in the CPU diagnostics buffer and reported on the OS, and can be checked in chart @F_Shutdn at the SAFE_M output of the F_SHUTDN block.

Preconditions for deactivating safety mode

- The CPU must be in the RUN state (mode switch in RUN or RUN-P).
- Safety mode must be activated.

Procedure

1. Select the CPU or its S7 program in the SIMATIC Manager.
2. Select the menu command "Options > Edit Safety Program".



3. Click the "Safety mode" button and (if applicable) enter the password for the safety program.
4. Confirm the deactivation of the safety mode.

Note

The F_SHUTDN block generates a message when safety mode is activated/deactivated. The parameter for the message repetition time is assigned at the F_SHUTDN block in chart @F_ShutDn.

Please note the following when deactivating safety mode

Manual intervention in the safety mode of fail-safe systems requires particular care and attention.

- Any changes must be made in accordance with current change management guidelines.
- An influence analysis must be carried out on any changes to be made to the active process.
- If changes are made, the influence on the system behavior must always be analyzed (program run time, etc.) before the program is imported into the running system. Following this, a final function test of all systems affected by the changes (validation) must take place.
- The appropriate procedures for approval must be put in place before safety mode can be deactivated.
  Notification of the plant personnel in charge, deactivation of safety mode, change downloading (delta downloading), and, finally, activation of safety mode must be accompanied by the relevant documentation.
- This documentation will then include the results of the change comparison and its analysis, the log of the relevant function test, and the updated hardware and software documents, together with modified signatures.

Note

Note the section "Tracking changes in the safety program (Page 253)".

While safety mode is deactivated, we highly recommend operating the plant with a high level of supervision by the operating personnel. The measures required for this purpose are derived from the influence analysis. This is urgently recommended due to the concluding safety validation before a program change.
Safety mode should be reactivated as soon as the changes have been performed.

7.9.3 Activating safety mode

Following a download of changes, you will need to reactivate safety mode in order to ensure secure execution of the the safety program.

Procedure

1. Select the CPU or its S7 program in the SIMATIC Manager.
2. Select the menu command "Options > Edit Safety Program".
3. Click the "Safety mode" button.
4. Confirm activation of the safety mode.

Note

If, when safety mode is deactivated, the safety program detects a safety-related error, it will disable the option to activate safety mode. A corresponding message will appear indicating how you can rectify the problem.

7.9.4 Downloading the safety program

After compilation, you can download the program. Depending on whether safety mode is activated or deactivated, you can download program changes as follows:

Download	**AS in STOP** **Single/H-system**	**AS in RUN** **Safety mode active**	**AS in RUN** **Safety mode inactive**
... of the entire program	Possible/Possible	Not possible	Not possible
... of changes in the standard program	Possible/Not possible	Possible	Possible
... of changes in the safety program	Possible/Not possible	Not possible	Possible

Requirements

- The station's hardware configuration data has been downloaded to the CPU.
- The user program has been compiled without errors.
- You have access rights to the CPU.
- There is an online connection between the CPU and your ES.

Rules for downloading

- Prior to loading the safety program, perform a consistency test. The signature in the program information section and in the footer of the safety printout must be the same.
- Empty F-runtime groups may arise when deleting safety functions. Delete these prior to compilation. To do this with PCS 7 V7.0 and higher, perform the following operation in the CFC editor: "Edit > Delete Empty Runtime Groups".
- You can only download the safety program from the CFC editor or the SIMATIC Manager via the chart folder.
- Once you have downloaded an acceptance-tested safety program, you will need to check the collective signature in the same way as during acceptance testing.

Procedure

To download the safety program, select the menu command "CPU > Download > Entire program" in the CFC editor. This will set the F CPU to STOP.

To download changes made to the safety program, select the menu command "CPU > Download > Changes" in the CFC editor. Depending on the CFC editor version you are working with, you may need to deactivate safety mode in the SIMATIC Manager before this process takes place and reactivate it afterwards. Alternatively, a prompt may be issued in CFC offering you the option of deactivating safety mode directly and reactivating it after downloading has taken place.

Note

Before the safety program is downloaded you will be prompted to enter the CPU password if changes are detected in the fail-safe part of the program.

Once you have downloaded the program to the CPU, you will need to compare this program's collective signature with the collective signature in the acceptance-tested printout. With high-availability F-systems, you have to run this comparison for both CPUs.

See also

Tracking changes in the safety program (Page 253)

7.10 Operating and changing safety-related parameters on a PCS 7 OS

Changes to fail-safe parameters of a PCS 7 OS can be made using the following functions:

- Secure Write Command++ (SWC++)
  The "Secure Write Command++" (SWC++) function enables safety-related changes to be made to F parameters in the safety program of an F CPU via an operator station (OS). Various functions are possible with SWC. Each function consists of several blocks in AS and a faceplate in APL style on the OS and:
  - SWC_QOS function for acknowledgment
    The function reports an acknowledgment request as an operator prompt. After successful operation, an acknowledgment pulse is generated.
  - SWC_CHG fnction for changing an F Bool or F Real value
    A corresponding F parameter can be changed in the safety program depending on whether an F_SWC_CB or F_SWC_CR block is used in the function.
  - SWC_MOS Maintenance Override Switch
    This function is suited for maintenance work. It can be used, for example, to switch up to 3 channel drivers from one faceplate into simulation mode and to set a common simulation value. The duration of the simulation can be limited in time and the output value (process value/simulation value) and the value of the module can be displayed by each channel driver for control purposes.
- Safety Matrix
  Additional software for configuring safety functions that supports various operating options such as maintenance, bypass or reset for each cause and effect.

Note

The following functions are recommended for changing fail-safe parameters from a PCS 7 OS:

- Fail-safe acknowledgment (SWC_QOS)
- Change process values (SWC_CHG)
- Maintenance Override Switch (SWC_MOS)

7.10.1 Fail-safe acknowledgment (SWC_QOS)

Introduction

From within the OS, you have the option of re-integrating F I/Os via the "fail-safe acknowledgment" function.

Note

As of S7 F Systems V6.2 with S7 F Systems Lib V1_3 SP2, you can control the re-integration of F I/Os via ES/OS with "SWC++".

The function for "fail-safe acknowledgment" consists of several blocks:

- Three F components, which you integrate into the CFCs of your safety program:
  - F_SWC_P: Central control of operation via the OS
  - F_SWC_BO: Processing of an F_BOOL data type parameter for operation via the OS
  - SWC_QOS: Interface for displaying the "Fail-safe acknowledgment" function on the OS.
- A faceplate that you can integrate into your OS.

Transaction for "Fail-safe acknowledgment"

With "Fail-safe acknowledgment", you can re-integrate F channel drivers into the safety program of an F CPU if you execute a specific operating sequence on the OS within a specified time.

Operator types for "Fail-safe acknowledgment"

A transaction can only be performed by an individual operator who initiates, checks, and confirms the change. However, one transaction can be performed by two operators. The first operator initiates the change (initiator) and the second re-enters, checks, and confirms the value (confirmer).

Operator control permissions are set in the faceplate properties. The connection IDs are generated by the system automatically. In this process, the system uses the "CPU Plant Designation" property or the "IDENT" input of the "F_SWC_P" block. If you assign a plant designation in the general properties of the CPU in HW Config, there is no need to assign a parameter for the "IDENT" input of the "F_SWC_P" block. If you place several F_SWC_P protocol blocks for each shutdown group so that several simultaneous operations are

possible from the OS, then connect the ADR_OSPA output of F_SWC_P to the ADR_SWC input of the "SWC_QOS" faceplate.

Note

As of S7 F Systems V6.2 with S7 F Systems Lib V1_3 SP2, it is possible to place several protocol blocks for each shutdown group and thus enable several simultaneous operations from the OS.

With the "Fail-safe acknowledgment" function, the OS can generated fail-safe pulses in the F program of the automation system. For the F parameters, there is a block ("F_SWC_BO") in the AS at which the assigned signal is available. The fail-safe output of the block is used in the safety program and the standard output for visualization of the current value is interconnected to the "SWC_QOS" block .

Connect the "AKT_VAL" output on the "F_SWC_BO" block to the "AKT_Q" input on the "SWC_QOS" block for "fail-safe acknowledgment" from the OS.

Connect the "OUT" output on the F block "F_SWC_BO" to the inputs ACK_REI of the F blocks which are to be re-integrated from the OS by the "fail-safe acknowledgment".

Connect the "ACK_REQ" output of the fail-safe channel driver devices to the "ACK_REQ" input on the "SWC_QOS" device for the "fail-safe acknowledgment" from the OS.

Note

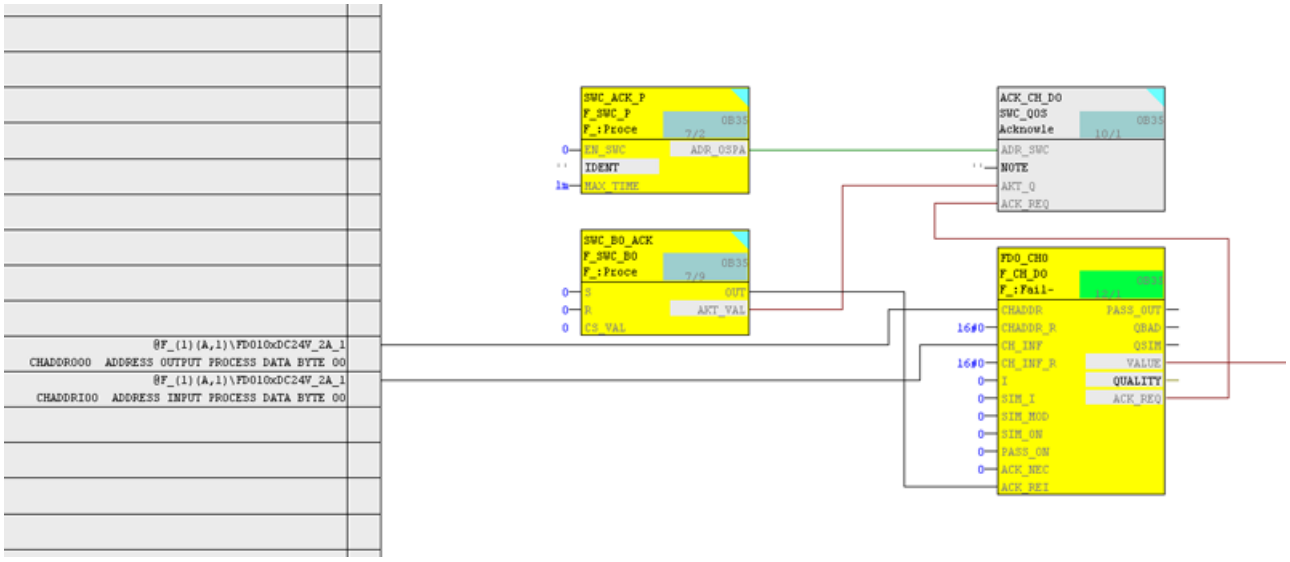
One "SWC_QOS" must be placed for each operator function and inserted into the plant hierarchy...

Function-related names are to be assigned to the "SWC_QOS" blocks. The names are displayed in the faceplate and simplify identifying the function.

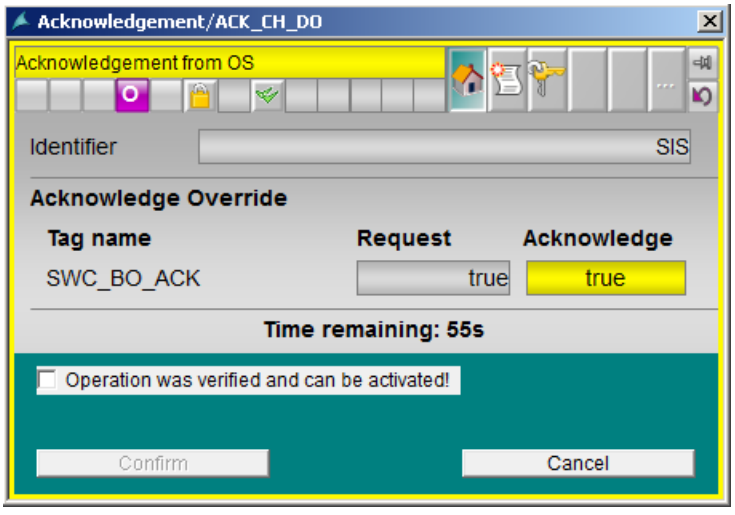
An "F_SWC_P" block is necessary for each shutdown group. It implements a special safety protocol and monitors the required operator sequence from the OS. With the "EN_SWC" input of the block, the operation of all transactions in a shutdown group can be enabled ("1") or disabled ("0"). When the operation is locked, all activated signals are reset. At the "MAX_TIME" input, the maximum time for the sequence of operations is set on the OS. If a plant designation was assigned in the properties of the CPU, the "IDENT" input does not have to be configured.

Example

The following figure shows by way of example how fail-safe acknowledgment of F I/Os can be implemented with the "F_SWC_P", "F_SWC_BO" and "SWC_QOS" blocks:



This implementation in the CFC allows the operator to initiate "fail-safe acknowledgment". The faceplate for re-integration is shown here.



7.10.2 Change process values (SWC_CHG)

Introduction

The "Change process values" function offers you the possibility to change F parameters in the safety program of the OS.

For the "Change process values" function S7 F Systems:

- Four F blocks, which you integrate into the CFC charts in your safety program:
  - F_SWC_P: Central control of operation via the OS
  - F_SWC_CB: Processing of an F_BOOL data type parameter for operation via the OS
  - F_SWC_CR: Processing of an F_REAL data type parameter for operation via the OS
  - SWC_CHG: Interface for displaying the "Process value change" function on the OS.
- Associated faceplates, which you integrate into your OS.

Transaction for "Change process values"

With the "Change process values" function, you can change F parameters in the safety program of an F CPU if you perform a specific operating sequence on the OS within a specified time. The entire change operation is referred to as a "transaction".

Operator types for "Change process values"

A transaction can only be performed by an individual operator who initiates, checks, and confirms the change. However, one transaction can be performed by two operators. The first operator initiates the change (initiator) and the second re-enters, checks, and confirms the value (confirmer).

Operator control permissions are set in the faceplate properties. The connection IDs are generated by the system automatically. In this process, the system uses the "CPU Plant Designation" property or the "IDENT" input of the "F_SWC_P" block. If you assign a plant designation in the general properties of the CPU in HW Config, there is no need to assign a parameter for the "IDENT" input of the "F_SWC_P" block. If you place several F_SWC_P protocol blocks for each shutdown group so that several simultaneous operations are

possible from the OS, then connect the ADR_OSPA output of F_SWC_P to the ADR_SWC input of the corresponding SWC_CHG faceplate.

Note

As of S7 F Systems V6.2 with S7 F Systems Lib V1_3 SP2, it is possible to place several protocol blocks for each shutdown group and thus enable several simultaneous operations from the OS.

With the "Change process values" function, a BOOL value can be switched on/off by the OS or a REAL value can be specified. For each F parameter, there is a block ("F_SWC_CB", "F_SWC_CR") in the AS at which the assigned signal is available. The fail-safe output of the block is used in the safety program and the standard output is connected to the "SWC_CHG" block to visualize the current value.

Connect the "AKT_VAL" output on the "F_SWC_CB" block to the "AKT_V_B" input on the "SWC_CHG" block for changing a BOOL value.

Connect the "AKT_VAL" output on the "F_SWC_CR" block to the "SWC_CHG" block AKT_V_R input for changing a REAL value.

The changed process value is available for further processing in the safety program at the "OUT" output of the "F_SWC_CB" and "F_SWC_CR" F devices.

Note

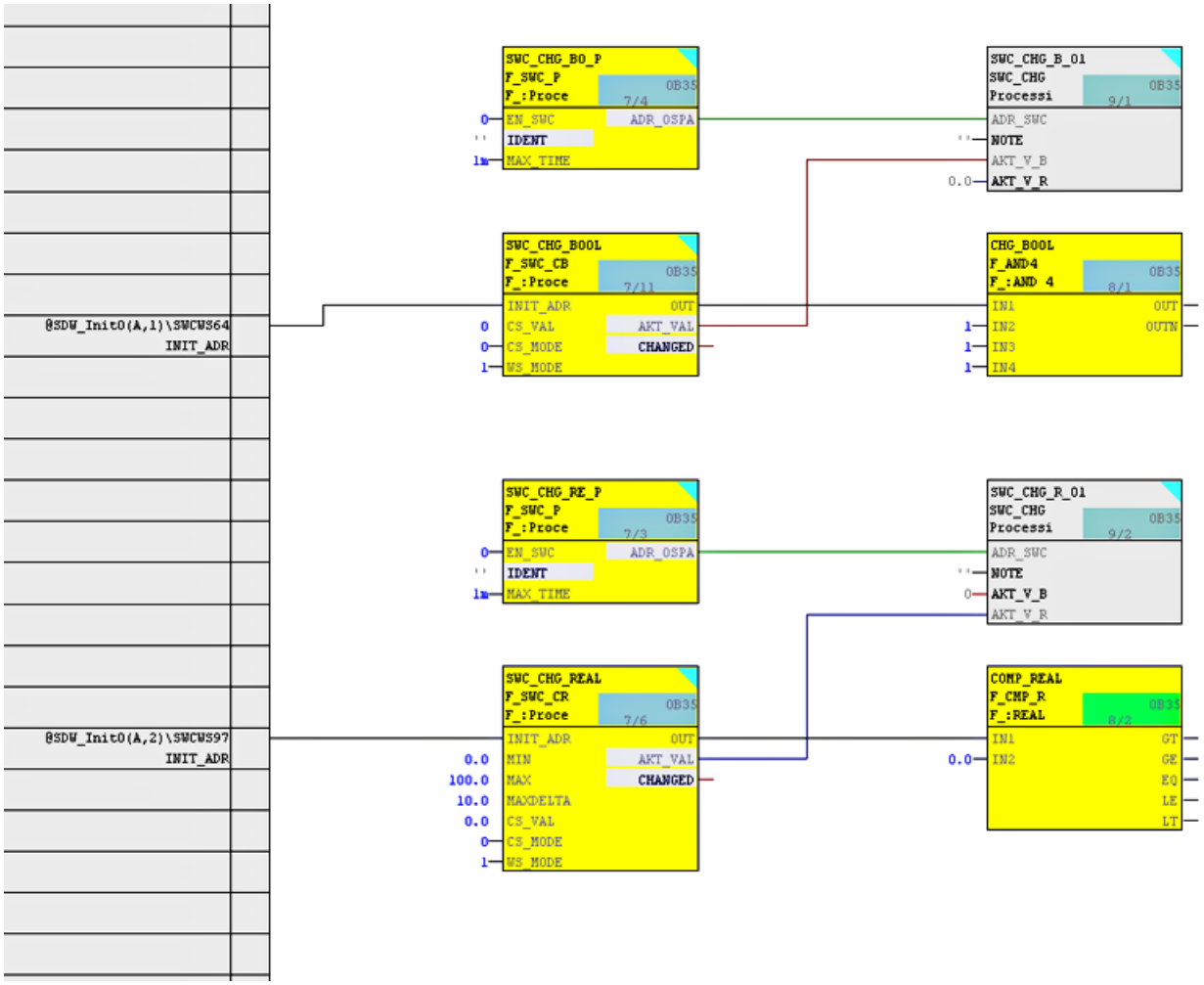
One "SWC_CHG" must be placed for each operator function and inserted into the plant hierarchy.

Function-related names are to be assigned to the "SWC_CHG" blocks. The names are displayed in the faceplate and simplify identifying the function.

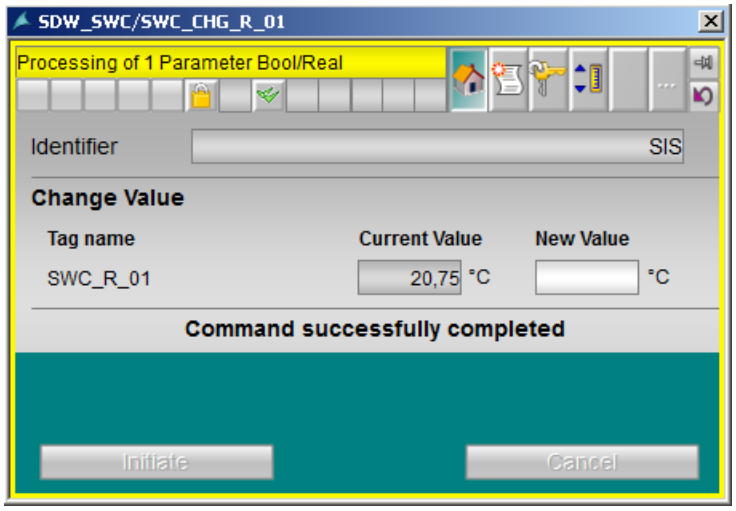
An "F_SWC_P" block is necessary for each shutdown group. It implements a special safety protocol and monitors the required operator sequence from the OS. With the "EN_SWC" input of the block, the operation of all transactions in a shutdown group can be enabled ("1") or disabled ("0"). When the operation is locked, all activated signals are reset. At the "MAX_TIME" input, the maximum time for the sequence of operations is set on the OS. If a plant designation was assigned in the properties of the CPU, the "IDENT" input does not have to be configured.

Example

The following figure shows how an F parameter of type BOOL and REAL can be changed in the AS:



This implementation in the CFC allows the operator to specify the process values. The faceplate for changing a REAL value is shown here.



7.10.3 Maintenance Override Switch (SWC_MOS)

Maintenance Override gives you the option to set bypasses in the safety program from the OS as well as the safety-oriented changing of F-parameters in the safety program of an F-CPU from an OS.

A special safety protocol is used to make changes to F-parameters in safety mode. This meets Safety Integrity Level requirements up to SIL3 in accordance with IEC 61508.

S7 F-systems offers the following for MOS:

- Four F-blocks, which you integrate into the CFC charts in your safety program:
  - F_SWC_P: Central control of operation via the OS
  - F_SWC_BO: Processing of an F_BOOL data type parameter for operation via the OS
  - F_SWC_R: Processing of an F_REAL data type parameter for operation via the OS
  - SWC_MOS: Interface for the display of the MOS function on the OS.
- A template for the temporal limitation of the change (SWC_TR)
- Associated faceplates, which you integrate into your OS.

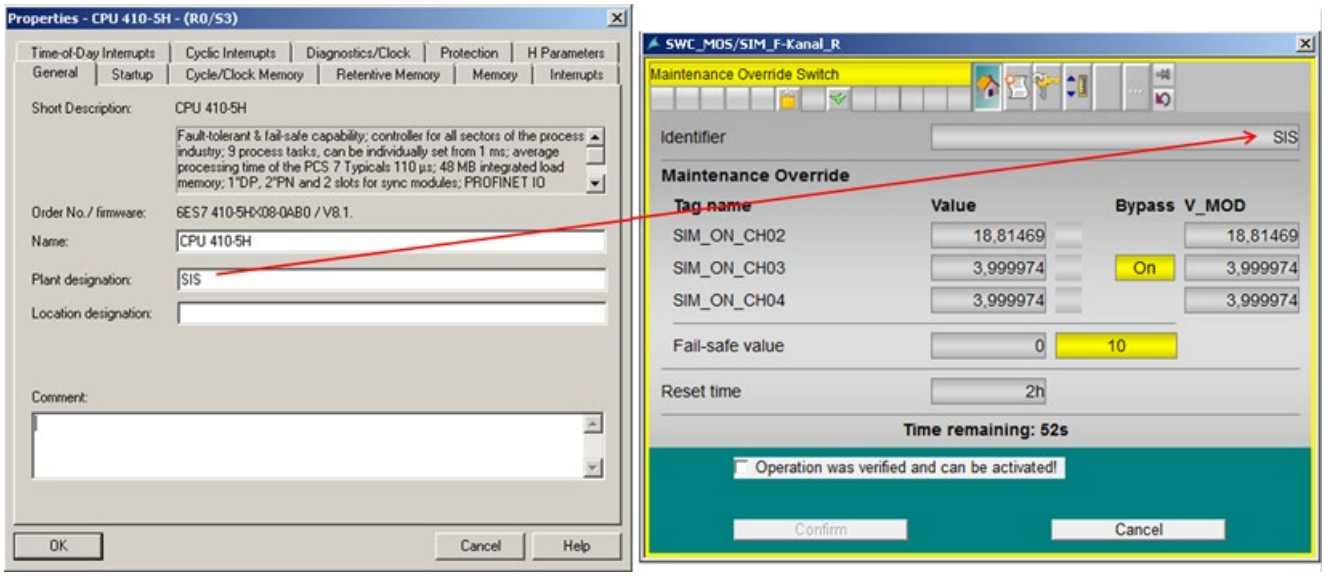
Transaction for MOS

You can use MOS to modify an F-parameter in the safety program of an F-CPU if you perform a specific sequence of operations on the OS within a specified period of time. The entire change operation is known as a "transaction".

Operator types for MOS

A transaction can only be performed by an individual operator who initiates, checks, and confirms the change. However, one transaction can be performed by two operators. The first operator initiates the change (initiator) and the second re-enters, checks, and confirms the value (confirmer).

Operator control permissions are set in the faceplate properties. The connection IDs are generated by the system automatically. In this process, the system uses the "CPU Plant Designation" property or the "IDENT" input of the "F_SWC_P" block. If you assign a plant designation in the general properties of the CPU in HW Config, there is no need to assign a parameter for the "IDENT" input of the "F_SWC_P" block.



Using the MOS function, up to three BOOL values from the OS can be activated or deactivated and a further BOOL or REAL value can be entered. For each value there is a block ("F_SWC_BO", "F_SWC_R") in the AS to which the assigned signal is available. The fail-safe output of the block is used in the safety program and the standard output for visualization of the current value is interconnected to the "SWC_MOS" block . The "F_SWC_BO" blocks have an input for setting and an input for resetting values, whereby the output value can also be controlled by the safety program. For each of these three BOOL values, a further two BOOL or REAL values for the display can be interconnected to the "SWC_MOS2" block (inputs: "VMOD_BxB", "Q_BxB" or "VMOD_BxR", "V_BxR"). Function-related names should be assigned to the "F_SWC_BO" blocks. The names are displayed in the faceplate and simplify identifying the function.

The additional BOOL or REAL value is interconnected to the "AKT_V_B" or "AKT_V_R" input of the "SWC_MOS" block.

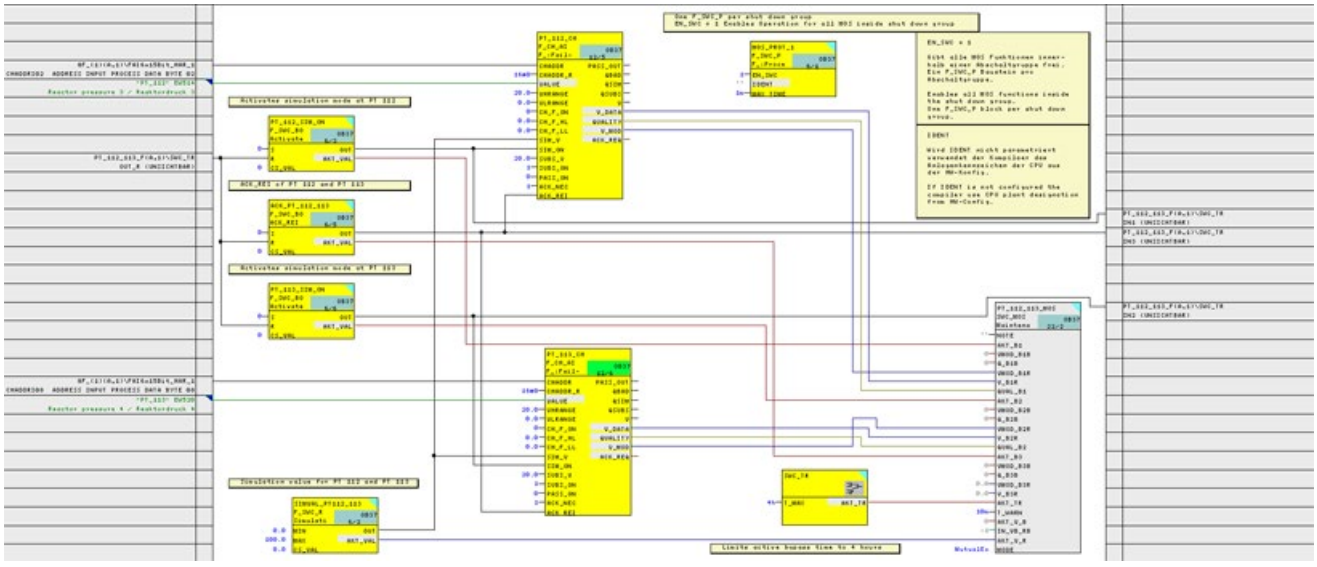
At the "MODE" input of the "SWC_MOS" block, it is determined whether all three BOOL values can be activated at the same time ("Norestrictions"), or if just one ("MutualExclBypass") BOOL value can be activated in each case.

The maximum activation period for the three BOOL values can be limited by using the "SWC_TR" template. After placing the template and connecting the "AKT_TR" output with the "AKT_TR" input of the "SWC_MOS" block, the further connections are established automatically during compilation. The time can be triggered again from the OS before it expires. Through configuring the "T_WARN" input to the "SWC_MOS" block, an alarm is generated prior to the maximum time elapsing.

An "F_SWC_P" block is necessary for each shutdown group. It implements a special safety protocol and monitors the required operator sequence from the OS. With the block's "EN_SWC" input, the operation of all MOS functions in a shutdown group can be enabled ("1") or blocked ("0"). When the operation is locked, all activated signals are reset. At the "MAX_TIME" input, the maximum time for the sequence of operations is set on the OS. If a plant designation was assigned in the properties of the CPU, the "IDENT" input does not have to be configured.

Example

The figure below shows an example of a temporally restricted maintenance function that is, for example, required for a cyclic proof test at a fail-safe analog input and an error acknowledgment:

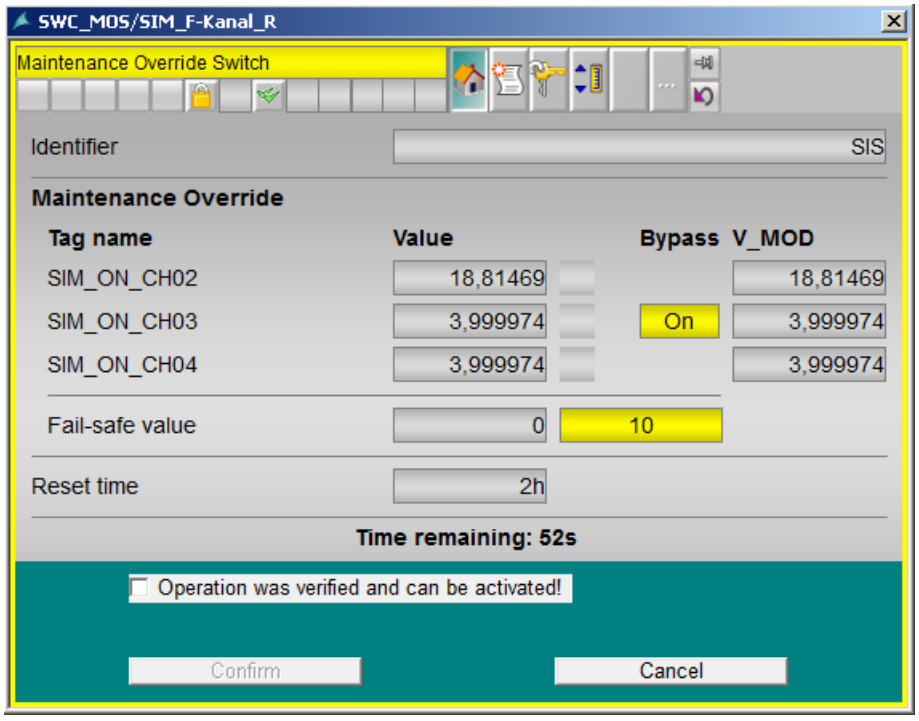


Note

The figure is available in its original size as appendix to the manual in the ZIP download of the checklists.

The CFC chart in this example shows how a REAL value is entered as a simulation value for an "F_CH_AI" block with the MOS function. The first BOOL value is used for the switchover of the "F_CH_AI" block in "Simulation" mode. First enter an appropriate simulation value. With the second BOOL value a fault at the channel driver is acknowledged.

Both BOOL values are reset after 4h.



7.10.4 Migration from a "Safety Data Write"/F_QUITES configuration to the "Secure Write Command" configuration (SWC)

Introduction

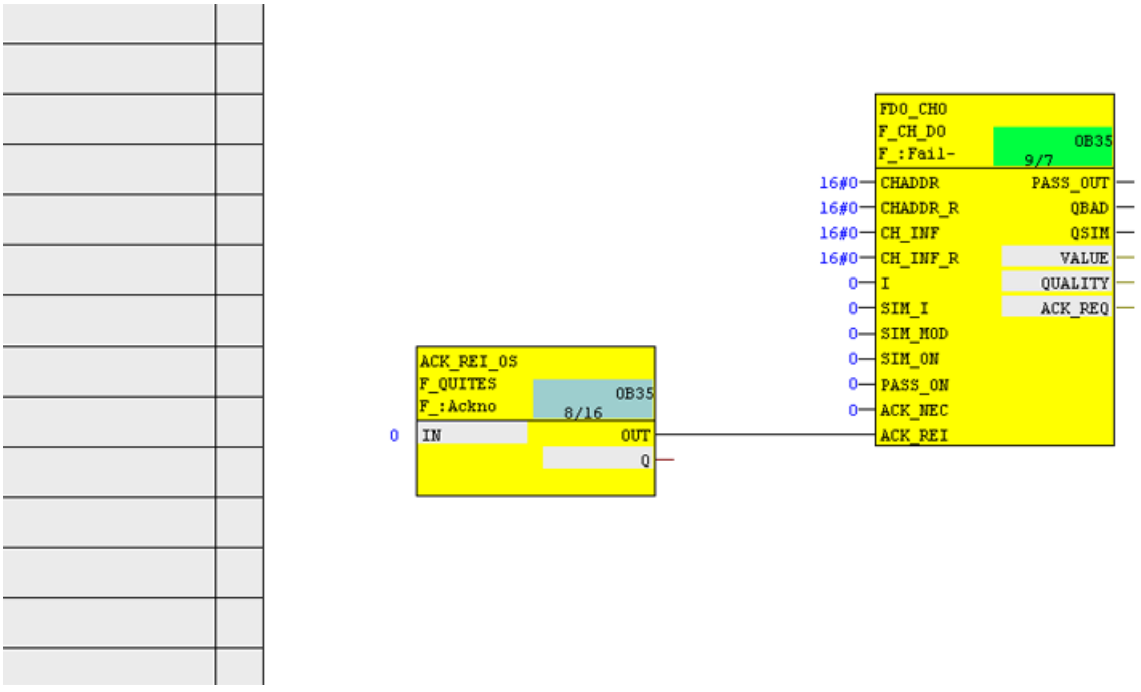
The "S7 F Systems Migration Tool" can be used to migrate existing projects with configurations for "Safety Data Write" (SDW) and fail-safe acknowledgment via the "F_QUITES" block in configurations with "Secure Write Command" (SWC).

- During migration, blocks of types "F_CHG_BO", "F_CHG_R" and "F_QUITES" are automatically replaced by their corresponding SWC solutions.
- The migration affects the signature of the safety program. Therefore, acceptance of changes to the plant is also required.

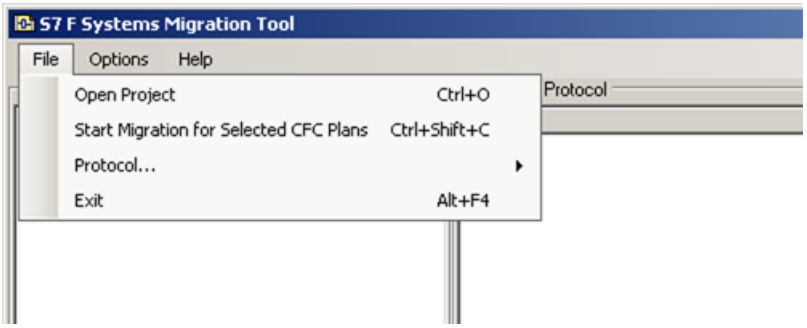
The tool is available as "S7FMigrationTool.exe" in a zip file. You can find the file on the installation CD in the "Options\S7FMigrationTool" directory.

Example for migration of an F_QUITES configuration

The starting point for using the "S7 F Systems Migration Tool" is fail-safe acknowledgment via the "F_QUITES" block.



Close the affected project in the SIMATIC Manager during the migration. Start the file "S7FMigrationTool.exe" and select "File > Open Project" from the menu bar.



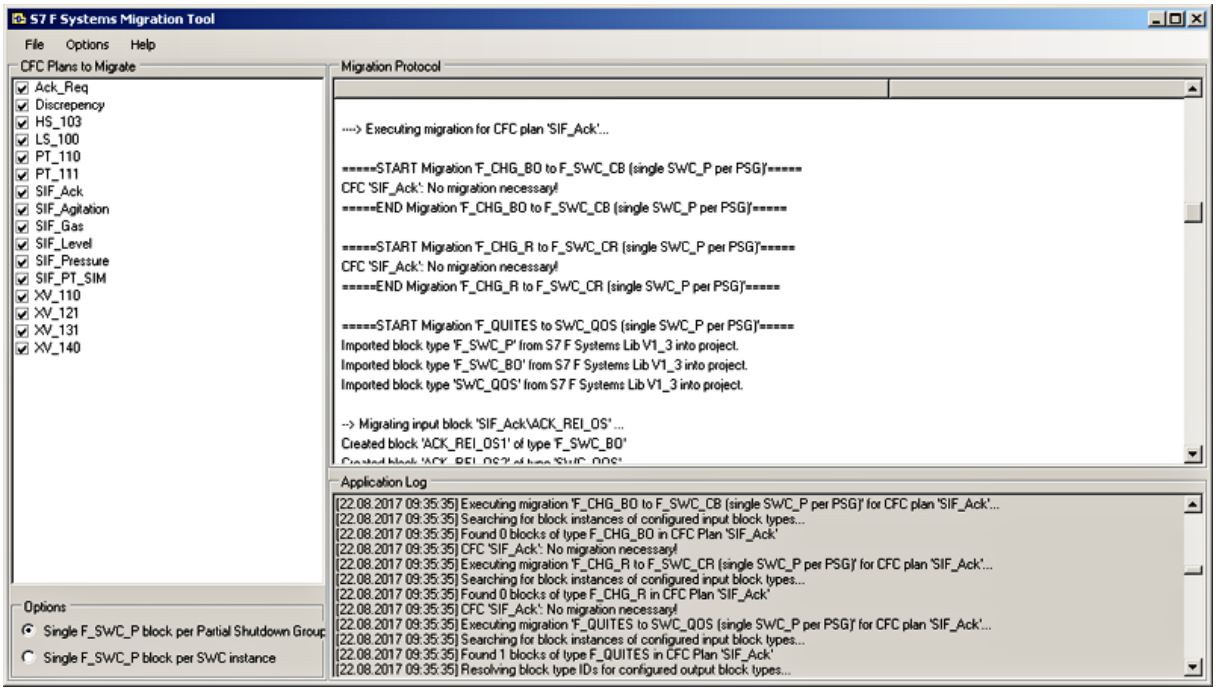
After successful selection, all CFCs found are displayed in the window "CFCs to be migrated". In the list, clear the check boxes for the CFCs that are not to be migrated.

Before you start the migration process via the menu command "File > Migrate selected CFCs", select how a protocol block "F_SWC_P" is to be placed in the "Options" area. If you select the option "One F_SWC_P device per SWC instance", several simultaneous operations are possible from the OS.

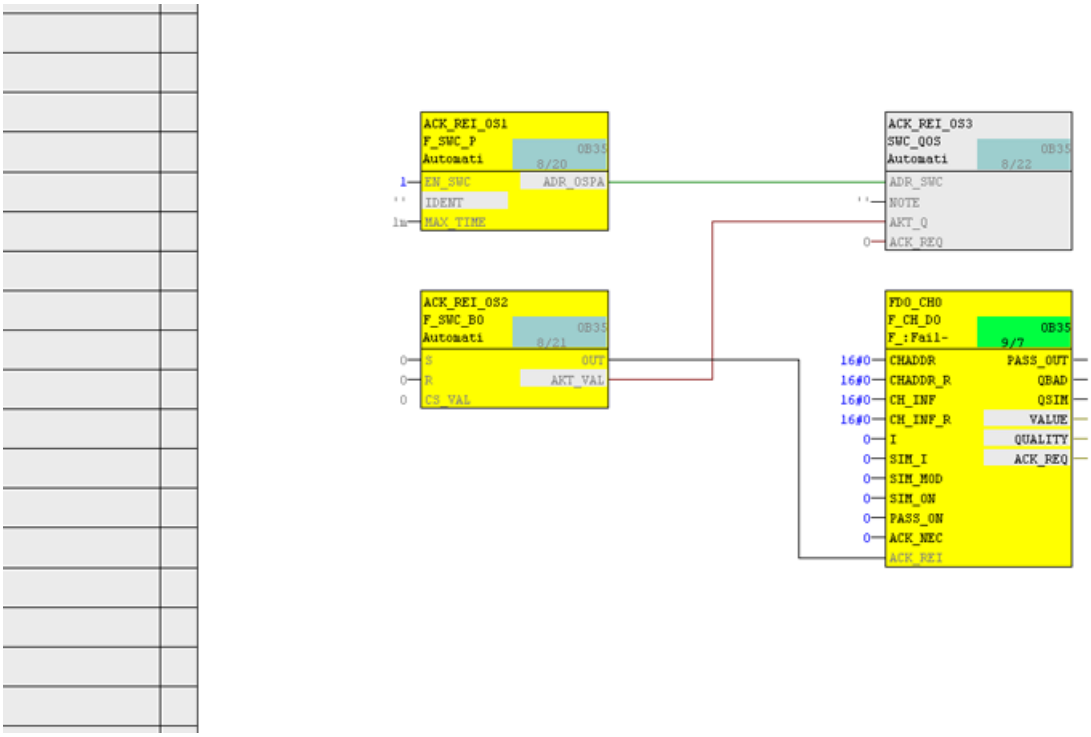
Note

Once the migration is started, the password for the safety program is requested, so that unauthorized persons are not able to change the safety program.

After migration, the corresponding logs are displayed in the "Migration log" and "Application log" windows. If required, you can display the log using the menu command "File > Print migration log".



If the migration was completed, the previously used "F_QUITES" block was replaced by the "F_SWC_P", "F_SWC_BO" and "SWC_QOS" blocks when the option "One F_SWC_P module per SWC instance" was selected beforehand.



Note

If an error occurs during the migration, the respective migration is not performed! The CFC to be migrated is then in the state it was before the migration. This prevents inconsistencies caused by a failed migration.

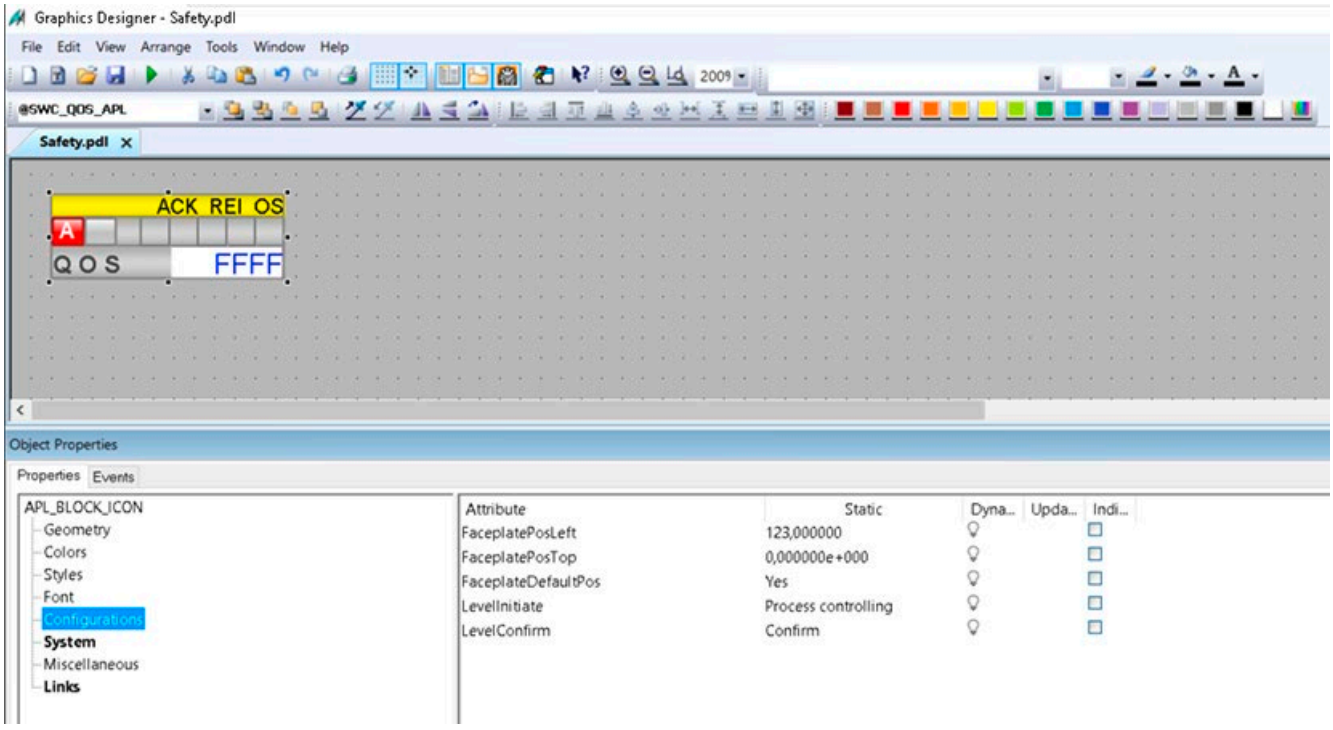
Check and test the safety program after migration. After successful migration, download to the CPU is only possible in STOP mode. Once the CFCs have been migrated, the program must be compiled again. Since the migration affects the signature of the safety program, acceptance of changes to the plant is also required.

7.10.5 Operator authorizations for Secure Write Command

Adapting the operator control permissions using SWC_QOS as an example

The required operator control permissions can be adapted in the properties of the block icon in the Graphics Designer. The procedure for changing the "LevelInitiate" and "LevelConfirm" operator control permissions is described below using SWC_QOS as an example:

1. Double-click the picture file in the plant view of the PCS 7 project.
   WinCC Explorer is started and the picture file is opened in the Graphics Designer.
2. Select the block icon of the SWC_QOS block and open the object properties.
3. In the "Properties" tab, select the "Configurations" entry.
4. Assign the desired permissions to the "LevelInitiate" and "LevelConfirm" attributes. In this example, "LevelConfirm" was changed to "Confirmer" and "LevelInitiate" was left at the default permission.



5. Save and close the picture file.

After the adjustments, the configured authorization levels are required to operate the SWC_QOS faceplate. In this example, an operator with the Process operations authorization level can initiate the transaction, after which an operator with the Confirmer authorization level (e.g. the safety engineer) must confirm the transaction for it to take effect. The Confirmer permission level must be created in the "User Administrator" in WinCC Explorer and assigned to the user.

Note

You can find additional information about the procedure for assigning rights in the "User Administrator" in the manual: "SIMATIC PCS 7 Operator Station" (https://support.industry.siemens.com/cs/ww/en/view/109794374) .

Note

You can find additional information about the Secure Write Command in the manual "SIMATIC Industrial software S7 F/FH Systems - Configuring and Programming" (https://support.industry.siemens.com/cs/ww/en/view/109802562).

Use of an additional enable (for example, key switch)

During an operation, input EN_SWC must be 1 on the F_SWC_P F block.

To ensure that operations can only be performed in certain process states or after enabling, connect the EN_SWC input to the input signal of a key switch or connect it to a logic. If input EN_SWC = 0, all existing bypasses are disabled. However, the configured substitute values are retained.

7.11 Monitoring times and system response times

A fail-safe system must switch the process to a safe state within a defined response time in the event of a system error (e.g. CPU failure, F-signal module failure, communications failure, program execution error).

To achieve this, a variety of monitoring times have been implemented to ensure that the affected functions are brought to a safe state if this time is exceeded.

What is the purpose of monitoring times and system response times?

For the S7-400 F/FH, there are essentially two different types of monitoring/error response:

- If the monitoring times of the fail-safe program are exceeded, the affected F-program switches off and the inputs/outputs of the F-signal modules are passivated.
- If the monitoring time for PROFIsafe communication between the F-CPU and F-signal modules is exceeded, the inputs/outputs of the affected F-signal modules are passivated and the corresponding substitute values are forwarded to the CPU.

When configuring the monitoring times, the safety must be primarily considered but also the availability of the S7 F/FH system and the process.

- Safety:
  The monitoring times must be set sufficiently low to prevent the process safety time from being exceeded.
- Availability:
  The monitoring times must be set sufficiently high to prevent time monitoring from being triggered when no errors are present.

The rule of thumb is that a non-redundant S7 F/FH system supports shorter monitoring times and, therefore, shorter response times in the event of an error. For a redundant system, longer monitoring times have to be configured to allow for switchover of the components (PROFIBUS, interface modules) and the coupling/updating of the H-CPU.

Calculation

An Excel file is used for the monitoring and reaction times calculated below. You can find this file on the Internet by pointing your browser to the following link: (https://support.industry.siemens.com/cs/ww/en/view/22557362)

The Excel file consists of the following sheets:

- Max. runtime F ASG Lib V1_3 SP4
  Here, you can find the run times of the F-blocks from S7 F Systems Lib V1_3 SP4 in the various types of CPU. You can use these to estimate the runtime of your F-program during the configuration stage of your project.
- Max. runtime F ASG Lib V1_3 SP3
  Here, you can find the run times of the F-blocks from S7 F Systems Lib V1_3 SP3 in the various types of CPU. You can use these to estimate the runtime of your F-program during the configuration stage of your project.
- Max. runtime F ASG Lib V1_3 SP2
  Here, you can find the run times of the F-blocks from S7 F Systems Lib V1_3 SP2 in the various types of CPU. You can use these to estimate the runtime of your F-program during the configuration stage of your project.
- Max. runtime F ASG Lib V1_3
  Here, you can find the run times of the F blocks from S7 F Systems Lib V1_3 in the various types of CPU. You can use these to estimate the runtime of your F-program during the configuration stage of your project.
- min. F-specific monitoring times
  This sheet contains formulae for calculating minimum values:
  - MAX_CYC
    Maximum time between 2 calls of the cyclic interrupt OB with F-program
  - PROFIsafe monitoring time
    Maximum time between 2 frames from the master to the F-I/O.
  - TIMEOUT between F-shutdown groups
    Timeout value for fail-safe communication between F-shutdown groups in an F-CPU
  - TIMEOUT between F-CPUs
    Timeout value for fail-safe communication between two F-CPUs

- Max. response times
  You can use this to determine the maximum runtime of a signal from an input to an output in the system, with various types of configuration taken into account.
- Response time wizard
  A wizard for estimating the typical response time.
- Max. runtime SM V6.3
  Here, you find the runtime of the causes, effects and intersections of Safety Matrix V6.3 in the different CPU types. Transfer the result into the table "Max. runtime F-ASG Lib V1.3..." into the field "F-FBs/F-FCs from other F-library" to estimate the runtime of your F-program in the configuration phase.

  Note that blocks outside the Safety Matrix (e.g. channel driver, pre-processing) are not included in the result.

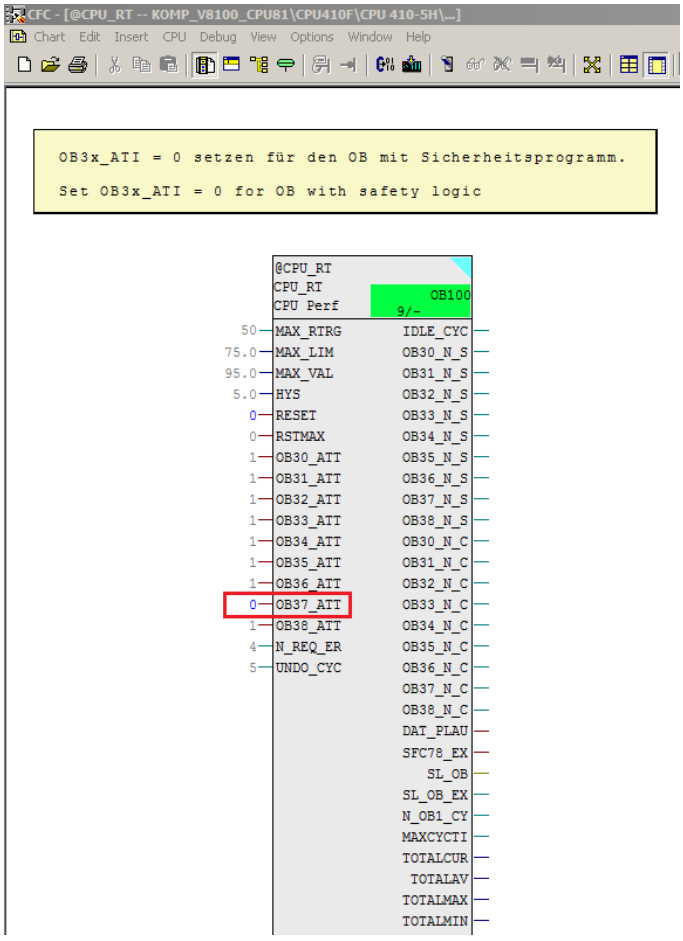
7.11.1 Diagnostic block "CPU_RT"

Diagnostic block "CPU_RT"

In PCS 7 V7.0 and above the "CPU_RT" diagnostic block is inserted with "Generate module drivers" in the @CPU_RT chart. Channel/diagnostic blocks in PCS 7 Library V7.0 and above must be used for this.

The "CPU_RT" diagnostic block implements a new controller and cycle behavior in the overload range. When there is a cycle overload in the CPU, the time intervals between two calls of the interrupt OBs are increased (the number of calls are reduced). In the safety program, this may cause I/O modules to be passivated or an F-STOP to be triggered, depending on the setting of the subsequently calculated monitoring times. To avoid this, the cyclic interrupt OB with security program must be disabled to reduce the calls. To do this, set the OBxx_ATT input (xx = no. of the cyclic interrupt OB with safety program) at the CPU_RT block to "0".

A performance analysis of the AS load is also possible. The performance analysis depends on the CPU firmware (CPU FW V4.5 and above). If the CPU FW supports SFC78, the performance data can be read via "CPU_RT". The performance data is shown in the diagnostic area of PCS 7 Asset Management.

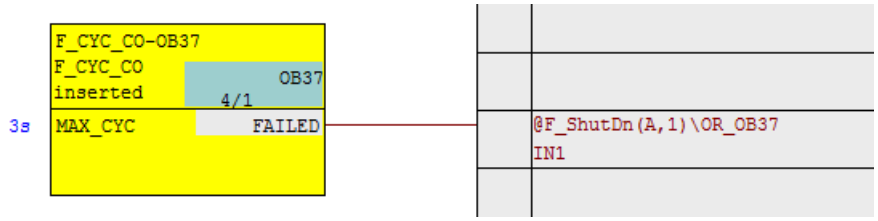


Note

You can find additional information on "CPU_RT" in the section "Family: @System" of the "SIMATIC Process Control System PCS 7 Basic Library" (https://support.industry.siemens.com/cs/ww/en/view/109794382) manual.

7.11.2 Calculating the F-cycle monitoring time (for block F_CYC_CO)

The F-CPU runs execution time monitoring for every cyclic interrupt OB (OB 30 - OB 38) containing F-runtime groups.



Procedure

The first time the F-program is compiled, you will be prompted to enter a value for the maximum cycle time (MAX_CYC) which may elapse between two calls to this cyclic interrupt OB. The default for the maximum F-cycle time is 3000 ms.

Should this default value not be suitable for your process, you can modify it directly at the F_CYC_CO block (located in the automatically generated @F_CycCo-OB3x chart).

You will need the following parameters for an exact calculation of the scan cycle monitoring time for a cyclic interrupt OB:

T_{CI}	Configured execution time of the cyclic interrupt OB in which the F_CYC_CO F-function block is called.
T_{P15}	Configured "max. disabling time for priority classes > 15" Only relevant for redundant systems. Enter a 0 if you are not using an FH system.
Special handling	If the OB is entered as a cyclic interrupt OB with special handling, set "Yes" here.
T_{Prog}	Program runtime of the cyclic interrupt OB
T_{CiR}	CiR synchronization time
T_{CiRmax}	Upper limit of the CiR synchronization time (default setting: 1 s)
T_{CImax}	Shortest possible time for scan cycle monitoring of the cyclic interrupt OB

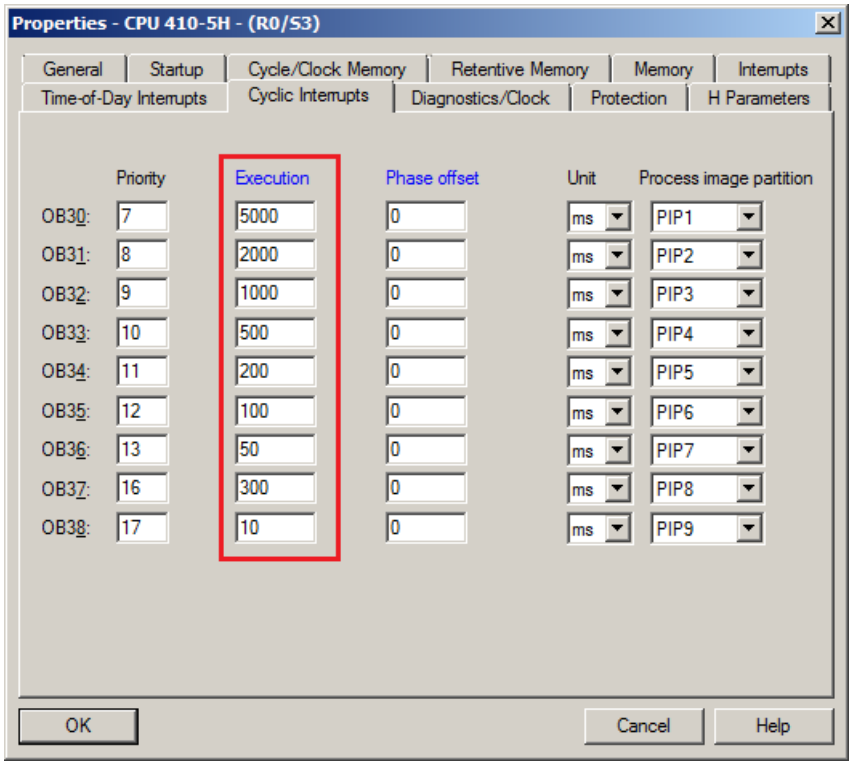
Extract from the Excel file " s7ftime.xlsm":

23	**Configuring the monitoring time of the F-cycle time**		
24	T_{Cl}		100 ms
25	T_{P15}		500 ms
26	Special handling		Yes
27	Runtime of the program execution in the cyclic interrupt OB		30 ms
28	T_{CiR}		0 ms
29	T_{CiRmax}		0 ms
30	**Minimum value for MAX_CYC**	T_{Clmax}	**530 ms**

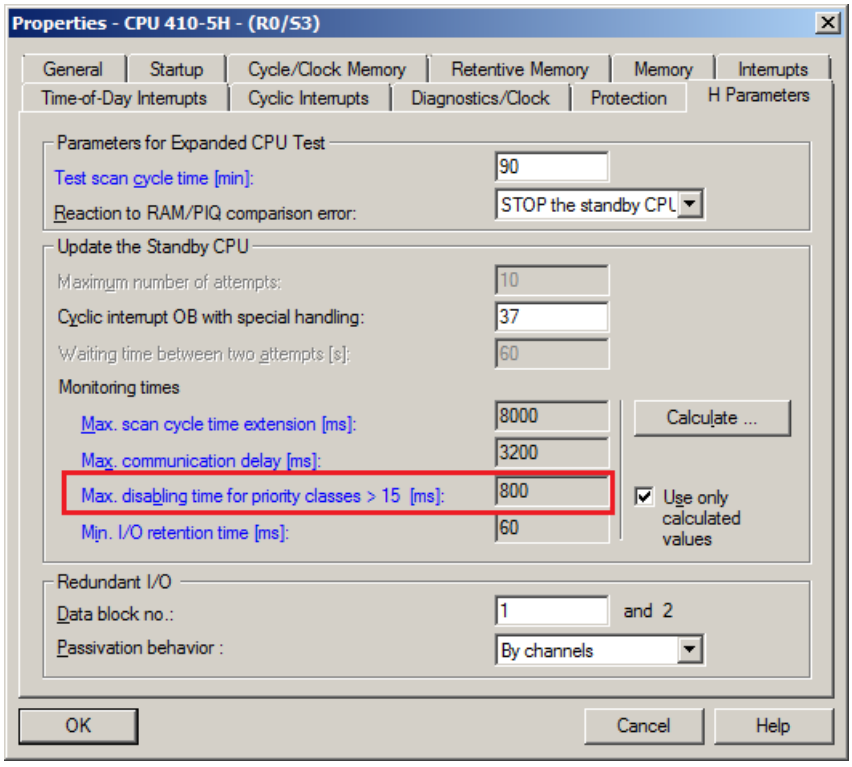
To prevent monitoring from being triggered when no errors are present, MAX_CYC must be set higher than the T_{Clmax} calculated for the corresponding cyclic interrupt OB.

- For non-redundant S7 F/FH systems:
  - The setting for T_{Clmax} must be at least as high as the configured execution time (T_{Cl}) of the cyclic interrupt OB.
- For redundant S7 F/FH systems:
  - A priority > 15 is used in the S7 F/FH-system for cyclic interrupt OBs with a safety program. The maximum disabling time for priority classes > 15 (T_{P15}) must also be taken into account for updating here.

You can find the value for T_{CI} in the "Execution" column of the relevant cyclic interrupt OB, located on the "Cyclic Interrupts" tab in the CPU properties.



Parameter T_{P15} is the same as the "Max. disabling time for priority classes > 15" parameter from the H parameters of the CPU.

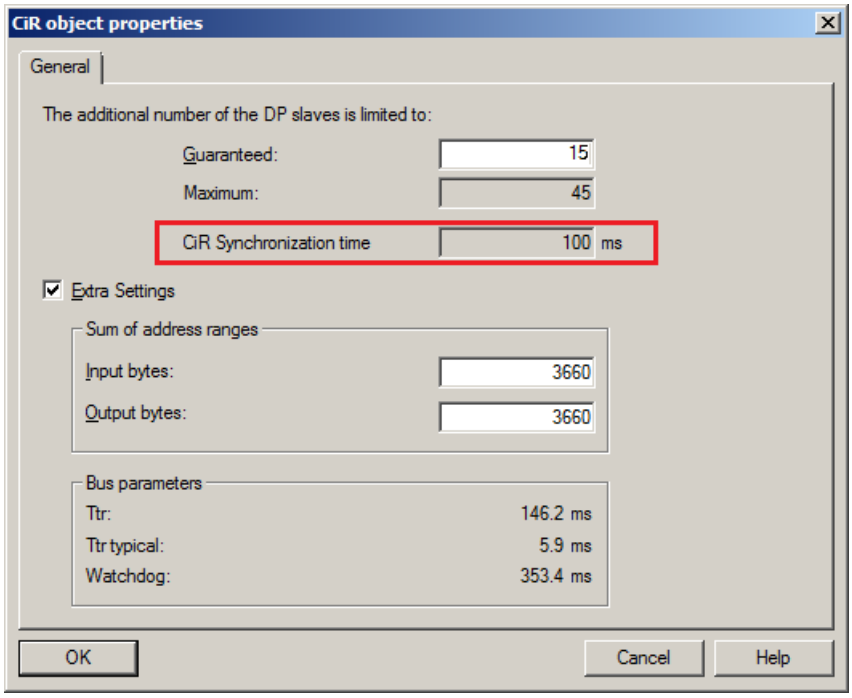


If the cyclic interrupt OB in which the F_CYC_CO block is called has been entered as a "cyclic interrupt OB with special handling", set "Yes" for special handling in the Excel table.

You only have to enter parameters T_{CiR} and T_{CiRmax} if you are not using an H system and have activated the CiR function. If you are not using CiR, enter 0 for both values.

T_{CiRmax} is set to 1 s in the system, but can be changed by calling SFC 104.

Parameter T_{CiR} can be found in the singular system with the CiR function activated, in the "Properties" dialog of the CiR object created.



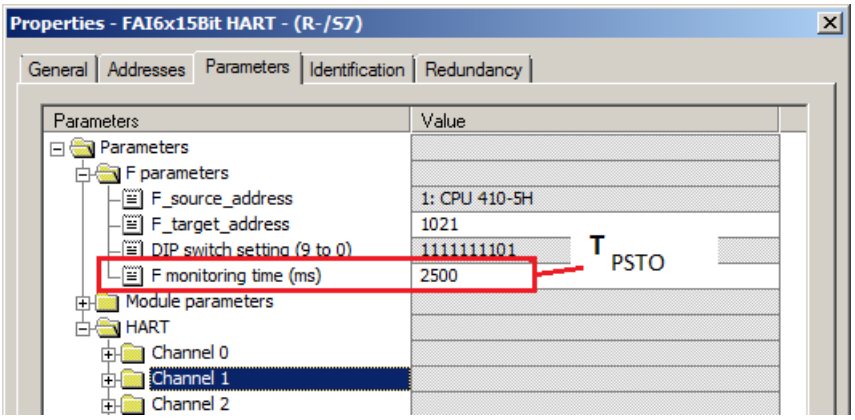
Note

You can find additional information on CiR in the manual "SIMATIC PCS 7 Process Control System CPU 410 Process Automation V8" (https://support.industry.siemens.com/cs/ww/en/view/109801828).

7.11.3 Communication monitoring time for F CPU/F signal modules

Time monitoring of PROFIsafe communication is implemented in the F-signal module groups and in the F-CPU using F-module drivers.

The value is entered while assigning parameters for the F-signal modules in HW Config ("F_monitoring time" parameter) and applied automatically when the F-module drivers are generated.



To prevent either monitoring in the F-module driver or monitoring in the F-signal module from being triggered when no errors are present, the F-monitoring time T_{PSTO} must be set to a sufficiently high value.

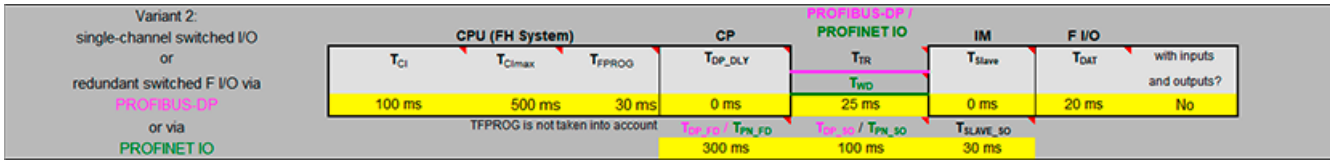
The lowest possible F-monitoring time can be determined with S7tftime.xlsm.

33	**Configuring the PROFIsafe monitoring time**		
34		***Variants 1 to 8:***	**V1: single-channel F I/O via PROFIBUS-DP or via PROFINET IO**
50	**minimum PROFIsafe monitoring time**	T_{PSTO}	**670 ms**

S7ftime.xlsm distinguishes 7 possibilities depending on the hardware configuration:

- Version 1: Single-channel F I/Os via PROFIBUS-DP or PROFINET IO
- Version 2: Single-channel switched F I/Os or redundantly switched F I/Os via PROFIBUS-DP or PROFINET IO
- Variant 3: Single-channel F PA field device via DP/PA coupler
- Variant 4: Single channel F PA device via DP/PA Link
- Variant 5: Single-channel switched F PA device via DP/PA Link
- Variant 6: Single-channel switched F I/O via Y-Link
- Version 7: Single-channel F I/Os via IE/PB link
- Variant 8: Single-channel F PA field device via CFU

The F-monitoring time must be calculated for the relevant variant of each F-signal module type or each device, and the values for the cyclic interrupt OB must be calculated as well. To do this, select the appropriate configuration variant and enter the parameters in the corresponding line.



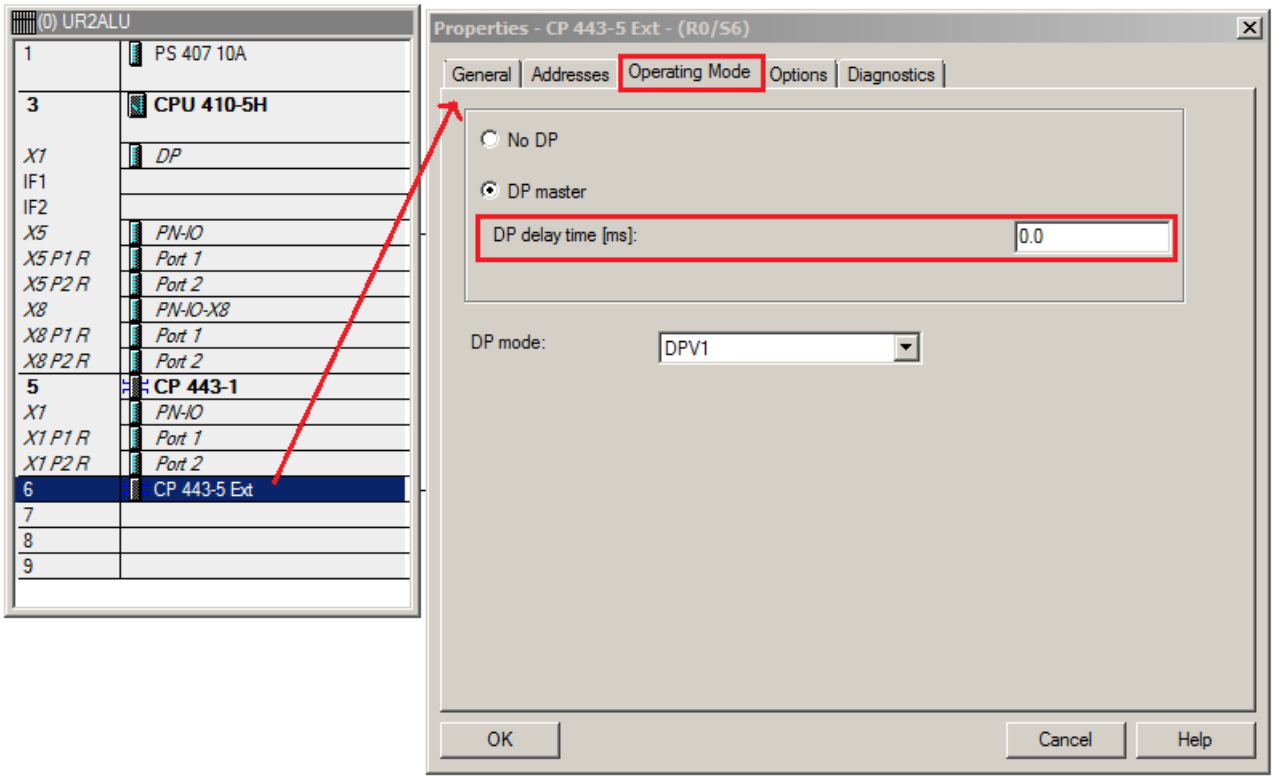
You need the following parameters for the calculation depending on the variant:

T_{CI}	Configured execution time of the cyclic interrupt OB in which the F-module driver is processed
T_{FPROG}	Program runtime of the cyclic interrupt OB in which the F-module driver is processed
T_{CImax}	Time set at the F_CYC_CO block for scan cycle monitoring of the cyclic interrupt OB
T_{DP_DLY}	Additional delay time with external DP interface (via CP 443-5 Extended)
$T_{TR/TR1}$	Maximum target rotation time for the DP master system
T_{TR2}	Maximum target rotation time for the subordinate DP master system on the Y link, or maximum target rotation time for the subordinate PA master system on the DP/PA coupler
$T_{DPPA\_L\_DLY}$	Delay time with a DP/PA link
$T_{Y\_L\_DLY}$	Delay time with a Y link
T_{IEDP_DLY}	Delay time with an IE/PB link
T_{Slave}	Maximum delay time with IM 153-2 / IM 153-4 (typical value for ET 200M = 1 ms)
T_{DAT}	Maximum acknowledgment time of the fail-safe I/O module in safety mode (F-signal module group data sheet)
With inputs and outputs	If you are using F-signal modules with inputs and outputs, set "Yes" here, (e.g. ET 200pro). If you are using an ET 200M, set "No".
T_{DP_FD}	Maximum DP error detection time Only relevant for redundant IM 153-2 (switched I/O). Enter 0 if you are not using a redundant IM.
T_{DP_SO}	Maximum DP switchover time Only relevant for redundant IM 153-2 (switched I/O). Enter 0 if you are not using a redundant IM.

T_{SLAVE_SO}	Max. switchover time of the slaves Only relevant for redundant IM 153-2 (switched I/O). Enter 0 if you are not using a redundant IM.
T_{DP_DLY}	Additional delay time with external DP interface (via CP 443-5 Extended)
T_{CFU_DLY}	Additional delay time due to the CFU - fixed system property of the CFU (100ms)
When PROFINET IO is used, the following PROFINET network parameters are required	
T_{WD}	Watchdog timer of the PROFINET I/O device. You can find these in the "IO Cycle" tab in the properties of the interface of the PROFINET I/O device. The response monitoring time for the I/O device is by default triple the update time from the properties of the PROFINET IO system if this has not been changed by the user.
T_{PN_FD}	Max. PROFINET IO error detection time from the H-parameters tab of the properties of the bus system
T_{PN_SO}	Max. PROFINET IO switchover time from the H-parameters tab of the properties of the bus system

T_{DP_DLY} parameter

You can find the T_{DP_DLY} parameter on the "Operating Mode" tab of the CP 443-5 ext properties in HW Config.

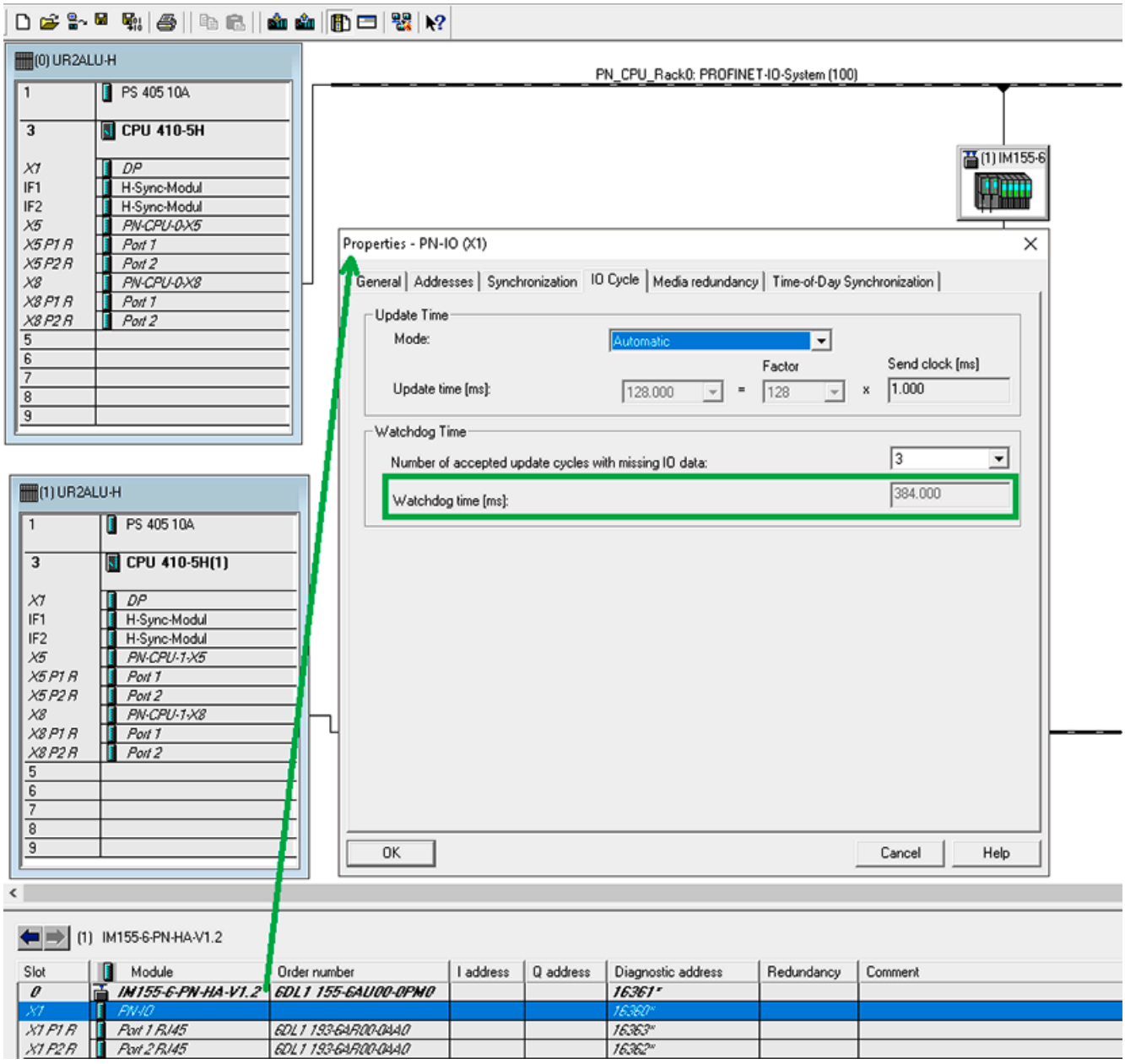


Note

When using an MRP ring, note the setting of the watchdog timer as described in the section "Media redundancy with MRP" of the document "PROFINET in SIMATIC PCS 7 – Guidelines and Blueprints" (https://support.industry.siemens.com/cs/ww/en/view/72887082).

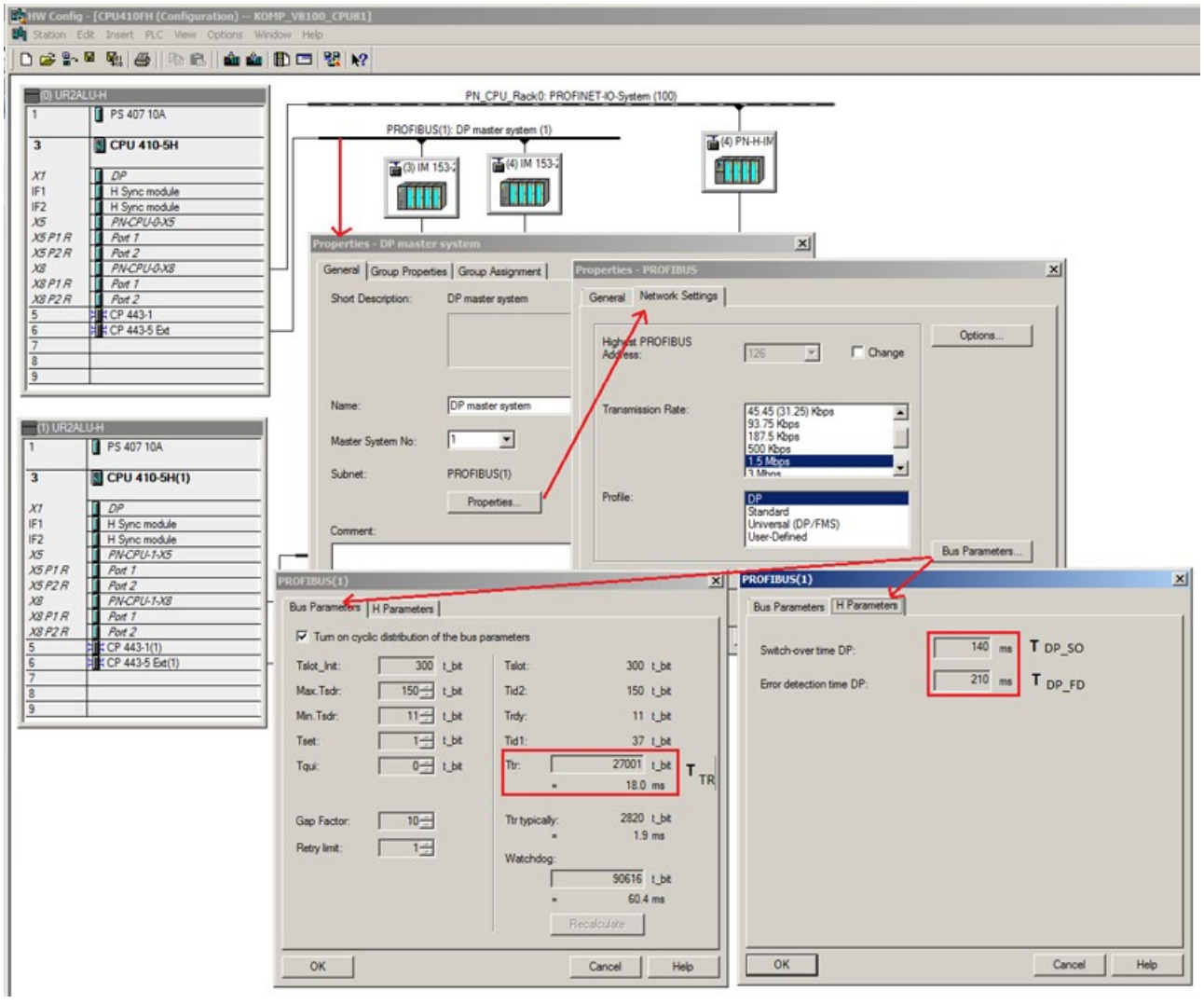
Parameter T_{WD}_

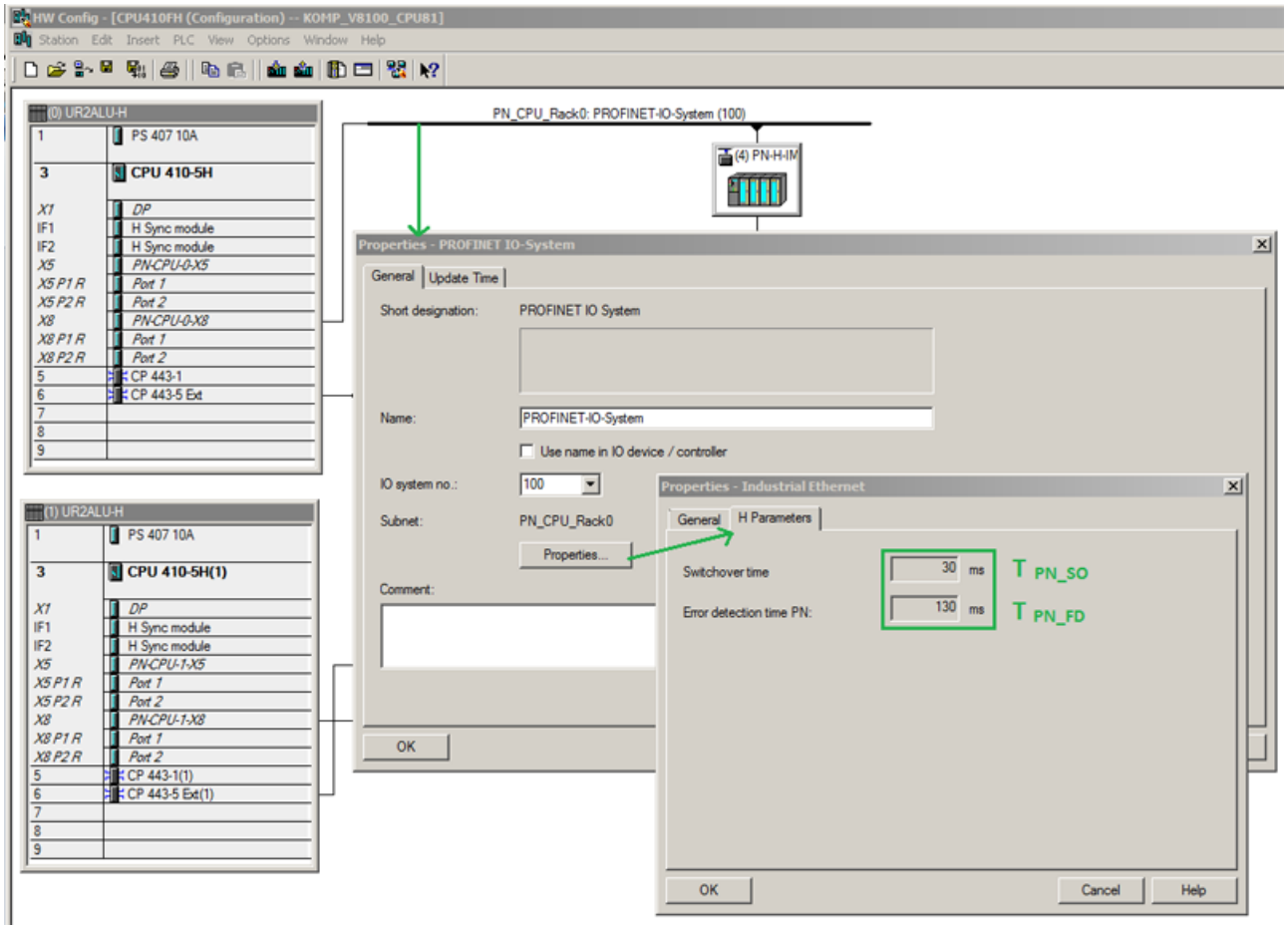
You can find the TWD parameter in the HW Config in the "IO Cycle" tab in the properties of the interface of the PROFINET I/O device.



Parameter $T_{TR/TR1/TR2}$ / T_{DP_FD} / T_{DP_SO}

You can find the parameters in the properties of the PROFIBUS DP or PA master system by double-clicking the bus line. In HW Config, the following screens from which the relevant values can be taken are shown:




HW Config - [CPU410FH (Configuration) -- KOMP_V8100_CPU81]
Station Edit Insert PLC View Options Window Help
(0) UR2ALU-H
1 PS 407 10A
3 CPU 410-5H
X1 DP
IF1 H Sync module
IF2 H Sync module
X5 PN-CPU-0-X5
X5 P1 R Port 1
X5 P2 R Port 2
X8 PN-CPU-0-X8
X8 P1 R Port 1
X8 P2 R Port 2
5 CP 443-1
6 CP 443-5 Ext
7
8
9
(1) UR2ALU-H
1 PS 407 10A
3 CPU 410-5H(1)
X1 DP
IF1 H Sync module
IF2 H Sync module
X5 PN-CPU-1-X5
X5 P1 R Port 1
X5 P2 R Port 2
X8 PN-CPU-1-X8
X8 P1 R Port 1
X8 P2 R Port 2
5 CP 443-1(1)
6 CP 443-5 Ext(1)
7
8
9
PN_CPU_Rack0: PROFINET-IO-System (100)
(4) PN-H-IM
Properties - PROFINET IO-System
General Update Time
Short designation: PROFINET IO System
Name: PROFINET-IO-System
Use name in IO device / controller
IO system no.: 100
Subnet: PN_CPU_Rack0
Properties...
Comment:
OK
Properties - Industrial Ethernet
General H Parameters
Switchover time 30 ms T PN_SO
Error detection time PN: 130 ms T PN_FD
OK Cancel Help

T_{SLAVE_SO} parameter

T_{SLAVE_SO} depends on the IM used.

PROFINET IO system	ET 200SP HA with IM 155	Switchover time	Configuration
T_{SLAVE_SO}	-0PM0	100 ms	Expansion up to 15 modules only from category 0
	-0PM0	200 ms	Full expansion with random modules

The I/O modules of the ET 200SP HA are divided into different categories regarding their user data:

- Category 0: Module versions with a user data length < 32 bytes
- Category > 0: Module versions with a user data length < 32 bytes

DP master system	ET 200M with IM 153	Switchover time	Configuration
T_{SLAVE_SO}	-2AA02	70 ms	Any configuration
	-2AB01	30 ms	...without F, FM, or HART module or similar
	-2Bx00	30 ms	Any configuration
	-2Bxx1	30 ms	Any configuration
	-2Bxx2	30 ms	Any configuration
	-2BA10 / -2BA70	30 ms	Any configuration

DP master system	ET 200iSP with IM 152	Switchover time	Configuration
T_{SLAVE_SO}	-1AA0	50 ms	Any configuration

$T_{DPPA\_L\_DLY}$ parameter

- Additional delay time with a DP/PA coupler in a singular system
- Or additional delay time and switchover time due to a DP/PA link in the redundant system

Precondition	Switchover time
Switchover time with unchanged PA configuration	Typ.: 70 ms + number of PA field devices x 51 ms
	Max.: 820 ms + number of PA field devices x 50 ms
Switchover time when configuration is changed during operation	Typ.: 80 ms + number of PA field devices* x 67 ms
	Max.: 800 ms + number of PA field devices* x 130 ms

* With unchanged PA field device addresses

$T_{Y\_L\_DLY}$ parameter

- Additional delay time with a Y link in the redundant system

Precondition	Switchover time
Delay time with a Y link	5 ms

T_{CFU_DLY} parameter

- Additional delay time by the CFU

Precondition	Switchover time
Delay time by CFU	100 ms

T_{Slave} parameter

Maximum delay time with the IM:

- ET 200SP HA
  The delay time must be calculated for the ET 200SP HA.
  - System connection S1 / S2:
    Response time [ms] = Configured update time + 2 ms
  - System connection R1:
    Response time [ms] = Max. switchover time of the slave
- ET 200M
  A typical value is 1 ms for the ET 200M with IM 153
- ET 200iSP
  The delay time must be calculated for the ET 200iSP. The following equation enables an approximate calculation of the ET 200iSP response time with the IM 152: Response time [ms] = g + 0.065 ms x b
  Explanation of the parameters:
  - g: Base value of the IM 152 depending on the operating mode
  - b: Sum of all input and output bytes of the electronic modules

The following assignment applies to the base value of the IM 152:

Operating mode	**Base value (g)***
No redundancy mode IM 152	1.5 ms
Redundancy mode IM 152	2 ms
* The specified base values are valid only for cyclic data exchange. Acyclic activities (for example, diagnostic interrupts) are not considered.	

Example for determining all input/output bytes with F-modules

The table is only intended as an example and does not include all ET 200iSP modules. You need to add the modules used as required.

Existing standard modules in ET 200iSP must also be taken into account (see the manual "SIMATIC Distributed I/O ET 200iSP" (https://support.industry.siemens.com/cs/ww/en/view/109775437)).

Electronics module	Number of I/O bytes	Number of modules	Total I/O bytes
4 F-AI HART. Ex 6ES7 138-7FA00-0AB0	12/4	1	16
8 F-DI NAMUR, Ex 6ES7 138-7FN00-0AB0	6/4	1	10
4 F-DO 40mA, Ex 6ES7 138-7FD00-0AB0	5/5	1	10
4 AI without HART 6ES7134-7TD00-0AB0	8	1	8
4 AI with HART 6ES7134-7TD00-0AB0	28(max.)	1	28
8 DI NAMUR with digital inputs 6ES7131-7RF00-0AB0	3	-	-
8 DI NAMUR with counter inputs 6ES7131-7RF00-0AB0	7	-	-
		Sum	36

T_{DAT} parameter

You can find the maximum acknowledgment time of the F-signal modules in the corresponding data sheet for the I/O module concerned. The following table shows the max. acknowledgment time of selected F-signal groups:

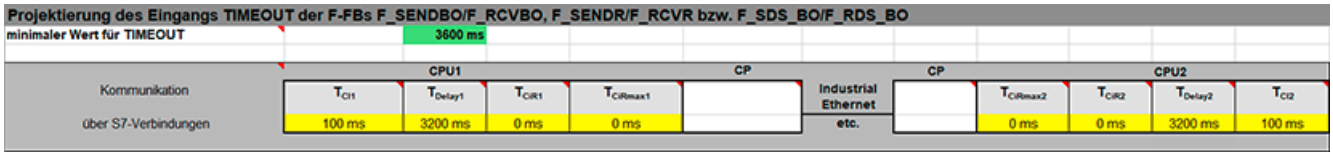
Module	Acknowledgment time in safety mode
ET 200SP HA, F-DI 16 x DC 24V HA 6DL1136-6BA00-0PH1	Max. 12 ms
ET 200SP HA, F-DQ 10 x DC 24V/ 2A PP HA 6DL1136-6DA00-0PH1	Max. 12 ms
ET 200SP HA, F-AI 8xI 2/4-wire HART HA 6DL1136-6AA00-0PH1	Max. 50 ms
ET 200M, SM326; DI x 24 DC 24V 6ES7326-1BK01-0AB0	With sensor evaluation 1oo1: Max. 29 ms
	With sensor evaluation 1oo2: Max. 30 ms
ET 200M, SM326; DI x 24 DC 24V 6ES7326-1BK02-0AB0	With sensor evaluation 1oo1: Max. 29 ms
	With sensor evaluation 1oo2: Max. 29 ms
ET 200M, SM326; DI 8 x NAMUR 6ES7326-1RF00-0AB0 6ES7326-1RF01-0AB0	Max. 68 ms
ET 200M, SM326; DO 10 x DC 24V/2A 6ES7326-2BF01-0AB0	Max. 20 ms
ET 200M, SM326; F-DO 10 x DC 24V/2A PP 6ES7326-2BF10-0AB0	Max. 10 ms
ET 200M, SM326; F-DO 8 x DC 24V/2A PM 6ES7326-2BF40-0AB0	Max. 14 ms
ET 200M, SM326; F-DO 8 x DC 24V/2A PM 6ES7326-2BF41-0AB0	Max. 18 ms
ET 200M, SM336; AI 6 x 13Bit 6ES7336-1HE00-0AB0	Acknowledgment time = Maximum response time = Maximum response time per channel x N + maximum basic response time (N = Number of activated channels) • Response time per activated channel: – At 50 Hz: Max. 50 ms – At 60 Hz: Max. 44 ms • Basic response time: – At 50 Hz: Max. 50 ms – At 60 Hz: Max. 44 ms

Module	Acknowledgment time in safety mode
ET 200M, SM336; F-AI 6 x 0/4 ... 20 mA HART 6ES7336-4GE00-0AB0	100 ms
ET 200iSP, EM 8 F-DI Ex NAMUR 6ES7138-7FN00-0AB0	Max. 26 ms
ET 200iSP, EM 4 F-DO Ex 17.4V/40mA 6ES7138-7FD00-0AB0	Max. 59 ms
ET 200iSP, EM 4 F-AI Ex HART 6ES7138-7FA00-0AB0	• Typ. reaction time (when no errors present) = conversion cycle time × filter • Max. response time (when no errors resent) = 2 × conversion cycle time × filter • Integration time – At 50 Hz 20 ms – At 60 Hz 16.67 ms • Response time per channel – At 50 Hz 23 ms – At 60 Hz 20 ms • Basic response time: 17 ms • Conversion cycle time = basic response time + (n x response time per channel) (n = number of active channels) • Conversion cycle time at 50 Hz, all channels active: 109 ms

7.11.4 Monitoring time for safety-related communication between F-CPUs

Introduction

Time monitoring of fail-safe communication between 2 F-CPUs is implemented in the send and receive blocks F_SENDR and F_RCVR or F_SENDBO and F_RCVBO with the same TIMEOUT monitoring time, which needs to be configured on both the send and receive blocks. The lowest value for the timeout can be determined using S7ftime.xlsm.



You will need the following parameters to calculate the "TIMEOUT" parameter:

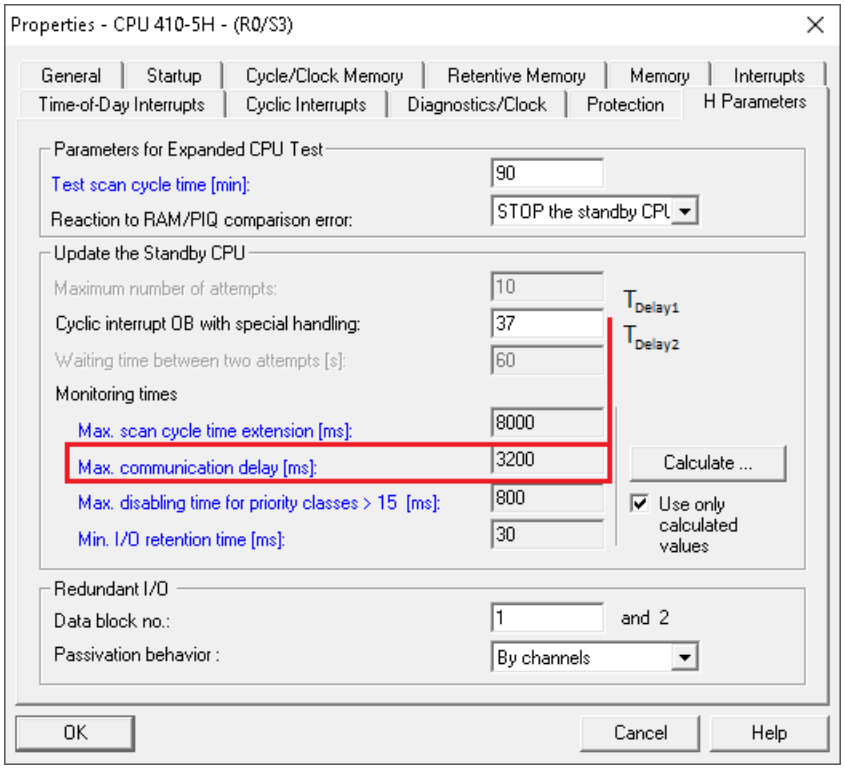
Communication between F-CPUs (TIMEOUT parameter)	
CPU 1, sender	
T_{Ci1}	Configured cycle time of the cyclic interrupt OB in which the send blocks F_SENDBO or F_SENDR are called.
T_{Delay1}	Maximum communication delay when updating the standby in the S7 FH system with call of F_SENDBO or F_SENDR. Only relevant for redundant S7 FH systems. Enter a 0 if you are not using an S7 FH system.
T_{CiR1}	CiR synchronization time Enter 0 if you do not use CiR.
$T_{CiRmax1}$	Upper limit of the CiR synchronization time (default setting: 1s) Enter 0 if you do not use CiR.

CPU 2, recipient	
$T_{CiRmax2}$	Upper limit of the CiR synchronization time (default setting: 1s). Enter 0 if you do not use CiR.
T_{CiR2}	CiR synchronization time Enter 0 if you do not use CiR.
T_{Delay2}	Maximum communication delay when updating the standby in the FH system with call of F_RCVBO or F_RCVR. Only relevant for redundant S7 FH systems, Enter 0 if you are not using an S7 FH-system.
T_{Ci2}	Configured cycle time of the cyclic interrupt OB in which the receive blocks F_RCVBO or F_RCVR are called.

With the exception of the $T_{Delay1/Delay2}$ parameters, all the parameters are described in Section Monitoring times and system response times (Page 195).

$T_{Delay1/Delay2}$ parameters

You can find these parameters in the H parameters within the CPU properties.

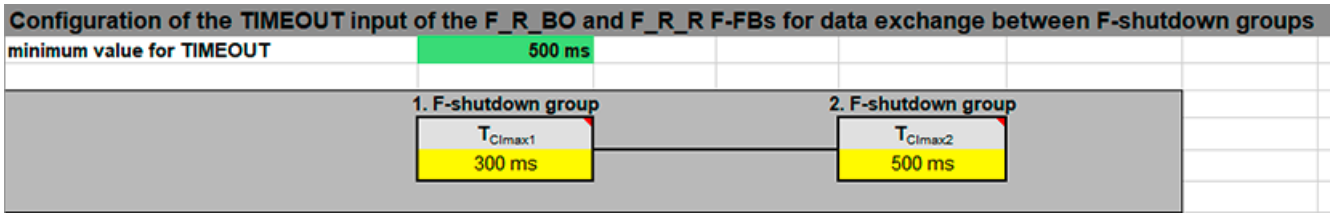


The value should be taken from the transmitting or receiving CPU.

7.11.5 Monitoring communication between F-shutdown groups

Time monitoring is implemented in the F_R_BO or F_R_RF FBs and configured at the "TIMEOUT" input parameter of the receive block.

To prevent time monitoring being triggered when no errors are pending, the TIMEOUT monitoring time must be set to a value which is at least equal to the higher of the two maximum cyclic interrupt cycle times of F_S_R or F_S_BO and F_R_R or F_R_BO. The lowest value for the timeout can be determined using S7ftime.xls.



You will need the following parameters to calculate the "TIMEOUT" parameter:

T_{CImax1}	Maximum cycle time of the cyclic interrupt OB in which the associated send block F_S_BO or F_S_R is called.
T_{CImax2}	Maximum cycle time of the cyclic interrupt OB in which the receive block F_R_BO or F_R_R is called.

The values for T_{CImax1} /T_{CImax2} can be found in chart @F_CycCo-OBxx, at input MAX_CYC of the F_CYC_CO-OBxx F function block (xx = Number of the cyclic interrupt OB with the send/receive block).

7.11.6 Response times of safety functions

Definition of response time

The response time is the time between the detection of an input signal and the changing of a linked output signal.

The actual response time is always between a minimum and a maximum response time. When configuring your plant, you must always assume the maximum response time.

The maximum response time of a safety function must be shorter than the process safety time.

Definition of process safety time

The process safety time is the time within which the process can be left to its own devices without creating a dangerous situation.

Within the process safety time, the S7 F/FH system controlling the process is not under control; in other words, it might malfunction or fail completely. The error tolerance time of a process depends on the type of process and is determined or estimated individually by process engineering.

How to calculate the response time

In S7ftime.xlsm, the path of a signal from the sensor from the system to the actuator is divided into five possible sections:

1. Input:
   Runtime from sensor to user program
2. Processing in the 1st F CPU:
   Cycle time and runtime of F program
3. F CPU-to-F CPU communication:
   Sends the signal to a second F-CPU (optional)
4. Processing in the 2nd F CPU:
   Cycle time and runtime of F program in the second F CPU (optional)
5. Output:
   Runtime from user program to actuator

Different variants may be used in each section. To calculate the maximum reaction time, select the relevant variant from the header line of each section and enter the corresponding values in the variants.

Input/Output

Depending on the hardware configuration of the system, 5 variants are possible here. In terms of the input and output, the variants are exactly the same, with the sole exception that the blocks for the output are in the reverse sequence to those for the input.

You will need the following parameters for the calculation:

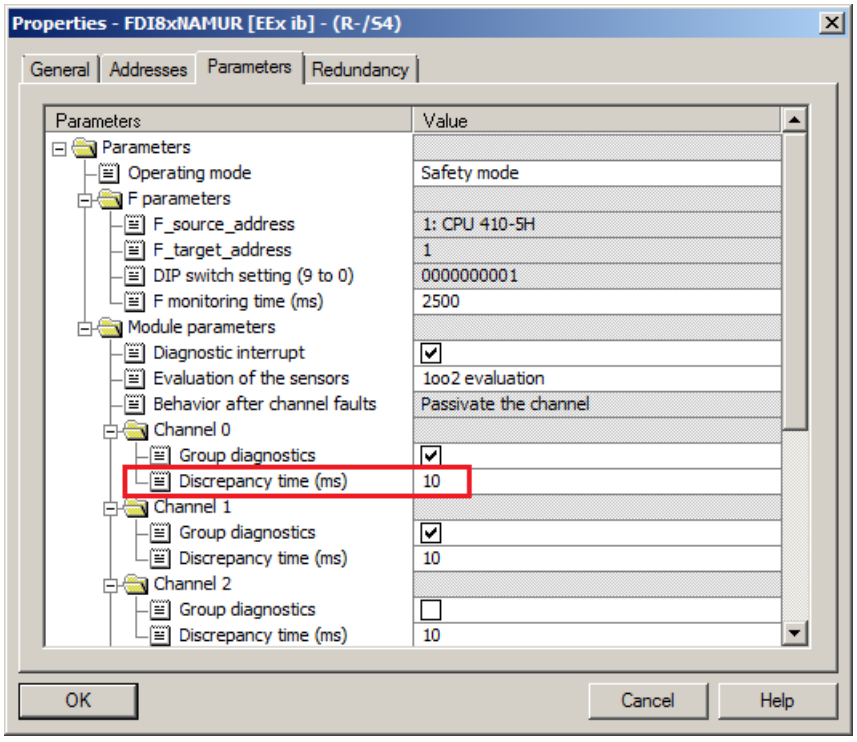
T_{Sensor_DLY}/$T_{Actuator\_DLY}$	Delay time of sensor or actuator
T_{DIS}	Maximum discrepancy time
T_{WCDT}	Worst Case Delay Time Maximum response time when no errors are present
T_{OFDT}	One Fault Delay Time Maximum response time when an error is present
T_{DAT}	Maximum acknowledgment time of the fail-safe I/O module in safety mode (F-signal module group data sheet)
$T_{PSTO, configured}$	Configured PROFIsafe monitoring time
T_{Slave}	Maximum delay time with IM 153-2 (typical value for ET 200M = 1 ms)
$T_{TR/TR1}$	Maximum target rotation time for the DP master system
T_{TR2}	Maximum target rotation time for the subordinate DP master system on the Y link, or maximum target rotation time for the subordinate PA master system on the DP/PA coupler
$T_{DPPA\_L\_DLY}$	Delay time with a DP/PA link
$T_{Y\_L\_DLY}$	Delay time with a Y link
T_{IEDP_DLY}	Delay time with an IE/PB link
T_{DP_DLY}	Additional delay time with external DP interface (via CP 443-5 Extended)
T_{CFU_DLY}	Additional delay time due to the CFU - fixed system property of the CFU (100ms)

T_{Sensor_DLY}/$T_{Actuator\_DLY}$ parameters

The delay times in the table are assumed to be 100 ms in each case; if necessary, the values for these will need to be obtained from the device data sheets.

T_{DIS} parameter

You set the discrepancy time when 1oo2 has been selected in the hardware configuration of the F-signal module.



Enter 0 if:

- No 1oo2 evaluation is performed on the module.
- The value 0 is immediately output in the event of a discrepancy.

TWCDT/TOFDT parameters

Note

Whether errors are present or not, the maximum response times depend on the type of module, and can be obtained from the following manuals:

- SIMATIC ET 200SP HA Digital Input Module F-DI 16x24VDC HA (https://support.industry.siemens.com/cs/ww/en/view/109802477)
- SIMATIC ET 200SP HA Digital Output Module F-DQ 10x24VDC/2A PP HA (https://support.industry.siemens.com/cs/ww/en/view/109802499)
- SIMATIC ET 200SP HA Analog Input Module F-AI 8xI 2-/4-wire HART HA (https://support.industry.siemens.com/cs/ww/en/view/109802504)
- SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-safe Signal Modules (https://support.industry.siemens.com/cs/ww/en/view/19026151)
- Distributed I/O Distributed I/O device ET 200iSP – Fail-safe Module (https://support.industry.siemens.com/cs/ww/en/view/47357221)

F-signal module	T_{WCDT}	T_{OFDT}
ET 200SP HA, F-DI 16 x DC 24V HA 6DL1136-6BA00-0PH1	In the error-free case with 1oo1 evaluation, sensor supply without short-circuit test: <= 2 × T_{cycle} + input delay. In the error-free case with 1oo1 evaluation, sensor supply with short-circuit test: <= 2 × T_{cycle} + input delay + T1 + T2 In the error-free case with 1oo2 evaluation, sensor supply without short-circuit test: <= 2 × T_{cycle} + input delay + discrepancy time*) In the error-free case with 1oo2 evaluation, sensor supply with short-circuit test: <= 2 × T_{cycle} + 2 × input delay + max. (T1p + T2p, T1s + T2s) + discrepancy time*) For external short-circuits: <= 2 × T_{cycle} + 2 × (n × 10 × T_{cycle}) + 2 × total [x=0...15](T1x + T2x) Discrepancy error for 1oo2 evaluation: <= 2 × T_{cycle} + 2 × input delay + discrepancy time + max (T1p + T2p, T1s + T2s). T_{cycle} Max. cycle time = 6 ms T1 Time for short-circuit test T2 Ramp-up time of sensor after short-circuit test T1p Test time for sensor supply of sensor 1 T2p Ramp-up time of sensor after short-circuit test (sensor 1) T1s Test time for sensor supply of sensor 2 T2s Ramp-up time of sensor after short-circuit test (sensor 2) T1x Time for sensor test T2x Ramp-up time of sensor after short-circuit test n number of sensor supplies with activated short-circuit test x sensor supply *) not applicable for discrepancy behavior "Supply 0 value".	
ET 200SP HA, F-DQ 10 x DC 24V/ 2A PP HA 6DL1136-6DA00-0PH1	In the error-free case: <= 2 × T_{cycle} + T2 If a channel error is detected by readback: <= 4 × T_{cycle} + T1 + T2 When a channel error is detected by bit pattern test: <= maximum test time T_{cycle} Max. cycle time = 6 ms T1 Light test time / Readback time T2 Dark test time	

F-signal module	T_{WCDT}	T_{OFDT}
ET 200SP HA, F-AI 8xI 2-/4-wire HART HA 6DL1136-6AA00-0PH1	(2 * N * response time per channel + 3 * basic response time) * smoothing. Response time per channel/channel pair At 50 Hz = 30 ms At 60 Hz = 27 ms Basic response time = 25 ms N number of activated channel pairs	= 2 * N * response time per channel + 3 * basic response time
ET 200M, DI 24 x DC 24 V 6ES7326-1BK02-0AB0	= Max. internal processing time + input delay + short-circuit test time = 23 ms + 3 ms + 6 ms = 32 ms	= 31 ms with 1oo1 evaluation
		= 29 ms with 1oo2 evaluation With parameter assignment: "Supply last valid value", the set discrepancy time has to be added.
ET 200M, DI 8 x NAMUR 6ES7326-1RF00-0AB0 6ES7326-1RF01-0AB0	= Internal processing time + input delay = 55 ms + 3 ms = 58 ms If an error is present, the response time is extended by the configured discrepancy time, if "1oo2 - evaluation" of the sensors has been configured.	
ET 200M, F-DO 8 x DC 24V/2A PM 6ES7326-2BF40-0AB0	= Max. internal processing time =14 ms	
ET 200M, F-DO 8 x DC 24V/2A PM 6ES7326-2BF41-0AB0	= Max. internal processing time =14 ms	
ET 200M, DO 10 x DC 24V/2A 6ES7326-2BF01-0AB0	= Internal processing time =24 ms	
ET 200M, F-DO 10 x DC 24V/2A PP 6ES7326-2BF10-0AB0	Max. response time = 2 × internal processing time + MAX{ Max. dark test readback time, max. light test time } + 10 ms = 2 × 8 ms + MAX{ 1 ms, 0.6 ms } + 10 ms = 27 ms	
ET 200M, AI 6 x 13Bit 6ES7336-1HE00-0AB0	= N × response time per activated channel + basic response time • E.g.: N = 6, interference frequency of 50 Hz = 6 × 50 ms + 50 ms = 350 ms • E.g.: N = 6, interference frequency of 60 Hz = 6 × 44 ms + 44 ms = 308 ms If an error is present, the response time is extended by the configured discrepancy time, if "2 sensors" was configured and the signal does not have a secure failure direction (or the "unit value" was not configured in accordance with this secure failure direction).	

F-signal module	TWCDT	TOFDT
ET 200M, F-AI 6 x 0/4 ... 20 mA HART 6ES7336-4GE00-0AB0	With 1oo1: = 2 × conversion cycle time × filter • E.g.: interference frequency of 50 Hz, filter = 1 conversion cycle, 3 active channel pairs = 2 × (3 x 25 ms + 50 ms) × 1 = 250 ms	= 2 × conversion cycle time e.g.: interference frequency of 50 Hz, 3 active channel pairs = 2 × (3 x 25 ms + 50 ms) = 250 ms
	With 1oo2: = 2 × conversion cycle time × smoothing + 2 × conversion cycle time + discrepancy time • E.g.: Interference frequency 50 Hz, filter = 1 conversion cycle, 3 active channel pairs = 2 × (3 x 25 ms + 50 ms) × 1 + 2 × (3 x 25 ms + 50 ms) + 1000ms = 1500 ms	
	• Conversion cycle time = (Basic response time + N × response time per channel pair) (N = Number of activated channel pairs)	

F-signal module	T_{WCDT}	T_{OFDT}	
ET 200iSP, EM 8 F-DI Ex NAMUR 6ES7138-7FN00-0AB0	Internal processing time		
		Sensor supply test Deactivated	Sensor supply test Activated
	1oo1 evaluation	22 ms	25 ms
	1oo2 evaluation with discrepancy behavior = "Supply 0 value"	22 ms	25 ms
	1oo2 evaluation with discrepancy behavior = "Supply last valid value"	35 ms	48 ms

F-signal module	TWCDT	TOFDT
	• Response time with 1oo1 evaluation (operation with and without errors) Response time = Internal processing time[1] + Input delay + {Time for sensor test + ramp-up time of the sensor after sensor test}2) • Response time at 1oo2 evaluation with discrepancy behavior = "Supply 0 value" (operation with and without errors) Response time = Internal processing time[1] + input delay + MAX { (time for sensor test CHANNEL(n) + ramp-up time of the sensor after sensor testCHANNEL(n))[2], (time for sensor testCHANNEL(n+4) + ramp-up time of the sensor after sensor testCHANNEL(n+4))[2),3)] } • Response time at 1oo2 evaluation with discrepancy behavior = "Supply last valid value" (operation without errors) Response time = Internal processing time[1] + input delay + discrepancy time + (time for sensor test CHANNEL(n) + ramp-up time of the sensor after sensor testCHANNEL(n))[2] + (time for sensor test CHANNEL(n+4) + ramp-up time of the sensor after sensor testCHANNEL(n+4))[2),3)]If the sensor supply test fails, the test is repeated. This repetition only has an effect on the response time for 1oo2 evaluation with discrepancy behavior = "Supply last valid value". • Response time for 1oo2 evaluation with discrepancy behavior = "Supply last valid value" (operation with errors) Response time = Internal processing time[1] + input delay + discrepancy time + 2 x { (time for sensor testCHANNEL(n) + ramp-up time of the sensor after sensor testCHANNEL(n))[2] + (time for sensor testCHANNEL(n+4) + ramp-up time of the sensor after sensor testCHANNEL(n+4))[2),3)]} Explanations: [1] Internal processing time dependent on parameter assignment – see above table "Internal processing time of the EM 8 F-DI Ex NAMUR based on parameter assignment" [2] Response time dependent on the sensor supply test parameter: • Deactivated: For the times within the bracket terms zero values are to be inserted • Activated: For the times within the bracket terms the values from assigned parameters are to be inserted [3] Response time is based on the sensor supply for 1oo2 parameter: • Sensor n and n+4 to Vs n: For the times within the bracket terms zero values are to be inserted • Each sensor to separate Vs: For the times within the bracket terms the values from assigned parameters are to be inserted	

F-signal module	TWCDT	TOFDT
	Example calculation of the response time of EM 8 F-DI Ex NAMUR: • Parameter assignment: – 1oo2 evaluation (equivalent or non-equivalent) – Discrepancy behavior: Supply last valid value – Discrepancy time: 400 ms – Sensor supply for 1oo2: Sensor n and n+4 to Vs n – Input delay: 3 ms – Sensor supply test: Activated – Time for sensor test: 10 ms – Ramp-up time of the sensor after sensor test: 100 ms • Response time = Internal processing time + input delay + discrepancy time + (time for sensor testCHANNEL(n) + ramp-up time of the sensor after sensor testCHANNEL(n)) + (time for sensor testCHANNEL(n+4) + ramp-up time of the sensor after sensor testCHANNEL(n+4)) Result: Response time = 48 ms + 3 ms + 400 ms + (10 ms +100 ms) + (0) = 561 ms • Response time = Internal processing time + input delay + discrepancy time + 2 x { (time for sensor testCHANNEL(n) + ramp-up time of the sensor after sensor testCHANNEL(n)) + (time for sensor testCHANNEL(n+4) + ramp-up time of the sensor after sensor testCHANNEL(n+4)) } Result: Response time = 48 ms + 3 ms + 400 ms + 2x{(10 ms +100 ms) + (0) } = 671 ms	

F-signal module	T_{WCDT}	T_{OFDT}
ET 200iSP, EM 4 F-DO Ex 17.4V/40mA 6ES7138-7FD00-0AB0	Cycle time = 7 ms + configured light test time • Response time = 9 ms + max. {configured light test time; configured max. dark test readback time} Example: • Parameter assignment: – Light test time: 3 ms – Max. dark test readback time: 10 ms • Cycle time: 7 ms + 3 ms = 10 ms • Response time: 9 ms + max. {3, 10} = 9 ms + 10 ms = 19 ms	
ET 200iSP, EM 4 F-AI Ex HART 6ES7138-7FA00-0AB0	Typical response time (when no errors present) = conversion cycle time × filter Maximum response time (when no errors present) = 2 × conversion cycle time × filter Example: • Interference frequency 50 Hz, filter = 1 conversion cycle time, 4 active channels • Maximum response time (when no errors present) = 2 × 109 ms × 1 = 218 ms	Maximum response time (with channel error) = 2 x conversion cycle time Example: • Interference frequency 50 Hz, 4 active channels • Maximum response time (with channel error) = 2 x 109 ms = 218 ms

The discrepancy time is not contained in T_{OFDT}. It should always be entered at parameter T_{DIS}.

Other parameters

The remaining parameters have been discussed in the preceding sections of this section.

Processing in the 1st CPU/Processing in the 2nd CPU

Processing in the 2nd CPU is optional. It involves the same variants as in the 1st CPU.

There are 2 different variants:

- One F-shutdown group is present in the signal flow being examined.
- Two F-shutdown groups are present in the signal flow being examined.

You will need the following parameters for the calculation:

T_{CI}/T_{CI1}/T_{CI2}	Configured cycle time of the cyclic interrupt OB in which the F-function block has been installed in each case
$T_{CImax.proj.}$ / $T_{CImax.proj.1}$ / $T_{CImax.proj.2}$	Time set in chart @F_CycCo-OBxx, at input MAX_CYC of the F_CYC_CO-OBxx F-function block (xx = Number of corresponding cyclic interrupt OB).
T_{FPROG}/T_{FPROG1}/T_{FPROG2}	Program runtime of the corresponding cyclic interrupt OB
TIMEOUT	Time parameterized at the TIMEOUT input of the F_R_BO or F_R_R block

CPU-to-CPU communication (optional)

If your signal is transferred from one CPU to another, select "Yes" in the header. For calculation purposes, you require the time parameterized at the TIMEOUT input of the send and receive blocks for communication.

If CPU-to-CPU communication is not taking place, leave the default setting ("No") unchanged. The next section, "Processing in the 2nd CPU", will not be taken into account during calculation in this case.

Result

S7ftime.xls returns two groups each with 3 times.

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	241 ms
if there is a fault/error	1078 ms
for any runtime of the standard or H-System	3321 ms
max. response time from sensor to actuator	
if there are no faults/errors	441 ms
if there is a fault/error	1278 ms
for any runtime of the standard or H-System	3521 ms

The lower group takes into account the delay times of the sensor and actuator.

Check that the times calculated meet the requirements of your process.

8 Configuration with Safety Matrix

8.1 Creating and configuring a Safety Matrix

Note

For information on creating and configuring a Safety Matrix, refer to the "SIMATIC Safety Matrix" (https://support.industry.siemens.com/cs/ww/en/view/109766685) manual.

Versioning

A Safety Matrix is determined by its version number, file version, and signature. Each time the matrix is saved, the file version changes along with the minor version number depending on the change made. Changing the minor version number also changes the signature. Both values are downloaded to the AS. During online access from the engineering tool or OS, the values are compared and a message is output if any differences are detected. If a matrix with a modified version number and signature is downloaded to the CPU, the OS server and single stations will need to be compiled and downloaded as well.

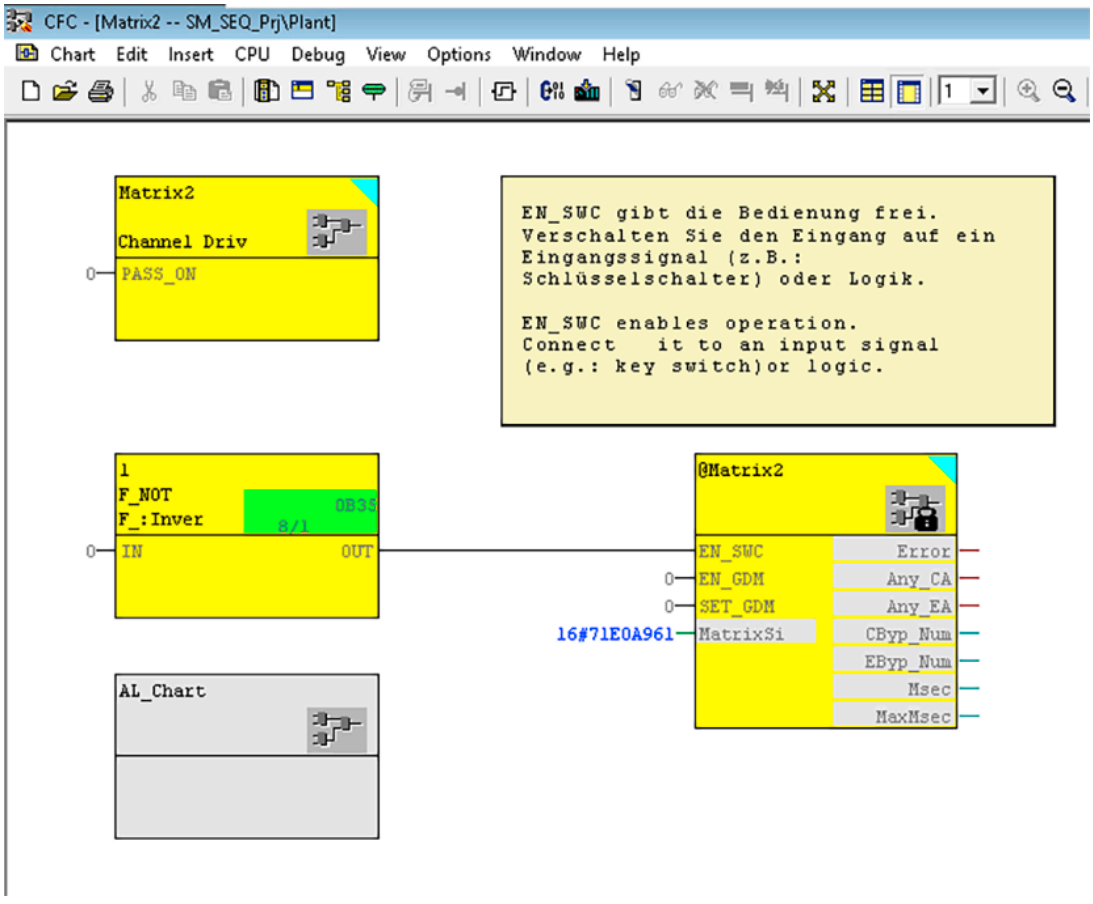
Operator input

The operation of the Safety Matrix must be enabled in the CFC by a "1" signal at the EN_SWC input. This can be done by logic or interconnection to the input channel driver of a key switch. The F-password is also requested in an online mode of the ES. The operator permissions configured in the Safety Matrix Engineering Tool are required for the operation of an OS. If password prompting and operator control permission are adequate for access protection, you can set the EN_SWC input in the Safety Matrix block permanently to "1" with an interconnection to the output of an F_NOT block. This prevents a configured "1" from being overwritten when the Safety Matrix is transferred to the CFC.

All active maintenance functions for Causes/Effects of a Safety Matrix, that is, simulations, soft bypasses and override functions, can be deactivated together via an external signal, for

example, if no visualization is available (or no longer available). To this end, the following inputs are available in the interface of the nested chart of the matrix logic:

- EN_GDM, data type F_BOOL; enable for the group deactivation function.
  The EN_GDM input must be TRUE so that group deactivation can take place via the SET_GDM input. The active status of the input is indicated by a message in Engineering Tool and Viewer.
- SET_GDM, data type F_BOOL; group deactivation function.
  With a rising edge at this input, all active simulations, soft bypasses and override functions for Causes/Effects of a Safety Matrix are deactivated. Group deactivation is done, for example, via a keyswitch.



Warning

Group deactivation of maintenance functions requires additional safety measures:

- Ensure that deactivation can only be performed if this does not affect the plant safety.
- To enable group deactivation, you need to use the EN_GDM input provided, for example, by controlling it with a keyswitch or process-dependent via the safety program.
- Ensure that the enable for group deactivation is only set for the desired period.
- Ensure that the following steps for group deactivation cannot be executed by a single condition.

1. Enable group deactivation (EN_GDM=1)
2. Execution of the group deactivation (SET_GDM=1)
3. Reset of the enable for group deactivation (EN_GDM=0)

- Ensure that only authorized persons can perform group deactivation.

8.2 Documenting a Safety Matrix

Documentation of a Safety Matrix is made via the menu command "Options > Create Report > Configuration". The configuration report contains the complete configuration of the Safety Matrix. This displays all configurations of the matrix in a text file; they can then be printed or saved in this format. The same matrix can be reconfigured on the basis of this text file,

In addition, the Safety Matrix itself can also be printed out with the menu command "File > Print". To ensure that as much information as possible is retained in this printout, activate all options in the "General" tab prior to printing (accessible via "View > Adapt > Layout"); otherwise, fields that are not visible will not be printed.

8.3 Organizing matrices into different shutdown groups

The information below is intended to demonstrate how two matrices located in different shutdown groups but the same OB are installed. This is carried out using S7 F-Systems Lib V1_3.

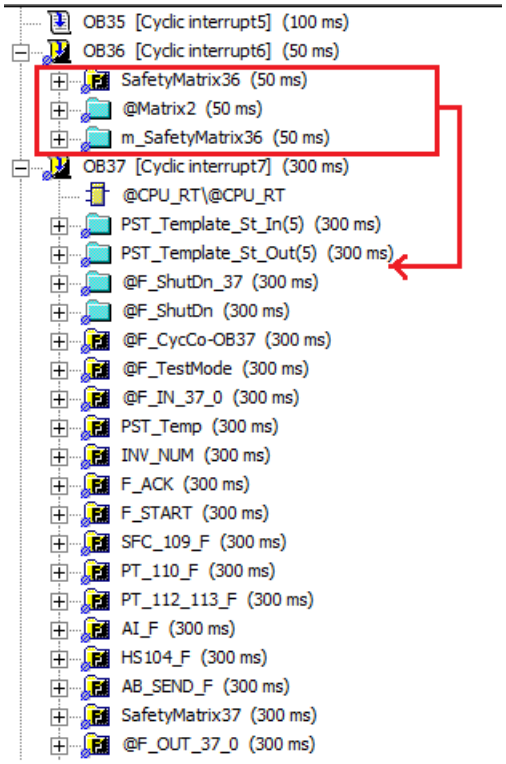
Creating shutdown groups

The F-module driver of an F-signal module may only be assigned to one shutdown group.

Therefore, when creating shutdown groups you must make sure that all signals in an F-signal module are used in the same shutdown group. The use of signals in an F-signal module in different shutdown groups results in errors during compiling due to invalid interconnections.

In the example below, the intention is to have two matrices be executed with a matrix cycle time of 300 ms, but in separate shutdown groups.

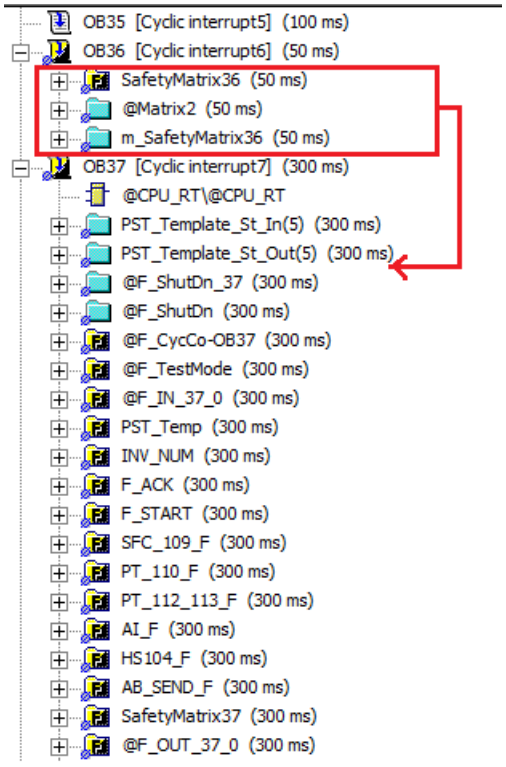
The starting point is the existing program, including the first matrix to have been compiled.



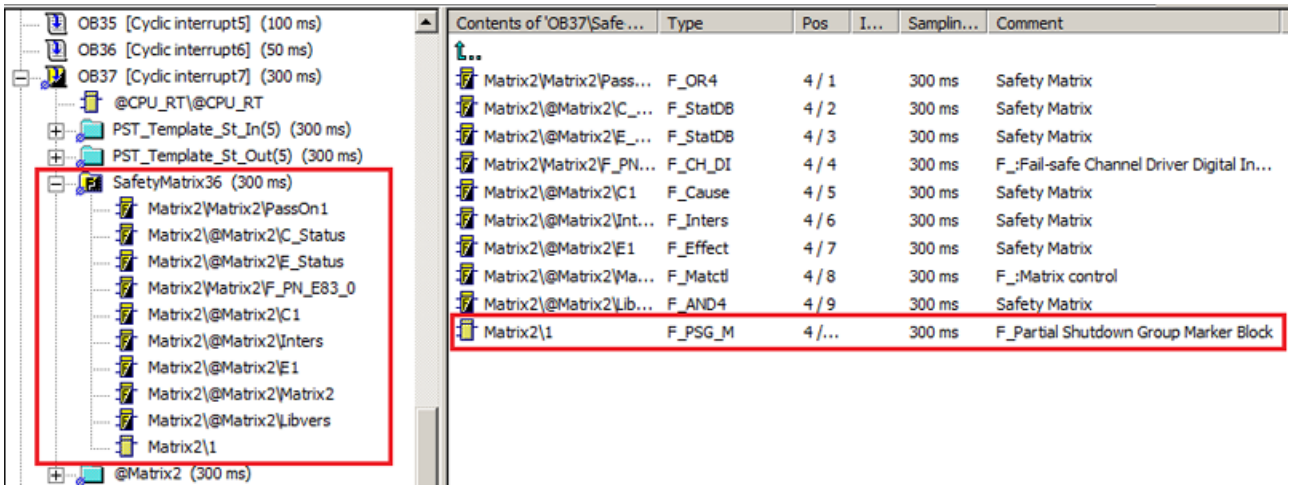
Inserting a new matrix in a new shutdown group.

To insert a new matrix and assign it to a new shutdown group, proceed as outlined below.

1. Create a new matrix and, in the Safety Matrix engineering tool, for the matrix cycle time select a cyclic interrupt OB that is not in use and into which no matrices have yet been inserted.
2. Create your safety function and transfer the matrix. In the cyclic interrupt OB, three runtime groups will be created for this matrix.
3. Move all three runtime groups to the destination cyclic interrupt OB (in this case, cyclic interrupt OB 37) and placing them before the first runtime group of the safety program.



4. Place the F_PSG_M block in the matrix chart to create the required shutdown group. Make sure to insert it at the end of the new matrix runtime group.

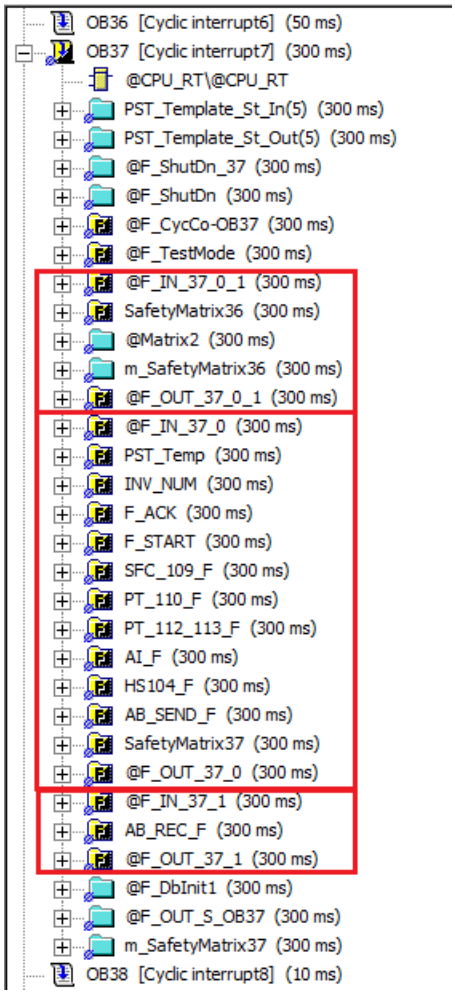


5. In order to transfer any changes that may be made in the Safety Matrix engineering tool to the correct runtime/shutdown group as well, you will then need to set the matrix cycle time to the current value, which in this case is 300 ms (OB 37).

6. Transfer the matrix with the modified cyclic interrupt OB setting to the project. When changes are transferred, the engineering tool will locate the runtime group that has been created and moved, and transfer changes to it as well. The following information appears briefly in the status bar of the Safety Matrix engineering tool:

7. Compile the S7 program.

   The compiler will create the newly generated shutdown group and the additional runtime groups @F_IN_<OBNr>_xx and @F_OUT_<OBNr>_xx.



Note

Please note that if the matrix CFC shutdown groups are subsequently moved or the safety program is subsequently divided into shutdown groups, the amount of additional effort may be considerable in terms of the change configuration work involved. For this reason, you must make sure that division into shutdown groups takes place at the start of configuration and that the F-signal modules are assigned to shutdown groups.

8.4 Exporting/importing matrices

To keep the same selected settings, such as SIF assignments (safety instrumented function groups), in another matrix, it is possible to export the matrix template to a table document. The table document is created in the format "*.ods". It can then be imported into an existing or new/empty Safety Matrix.

The exported Safety Matrix can be opened and adapted for mass data engineering in a spreadsheet program. When exporting, the configuration data of a matrix is stored in several worksheets of the spreadsheet document.

- Matrix properties
- Alarm profiles
- Configuration of Causes
- Overview of intersections
- Configuration of Effects
- Legend

Exporting

1. In the Safety Matrix Engineering Tool, open the matrix whose data you want to export to a table document.
2. Select the menu command File > Export.
3. In the following selection window, select the desired directory and the file name of the table document.
4. Click "Save".

The export of the Safety Matrix data to the table document is started. A message is displayed when the process is complete.

Importing

1. In the Safety Matrix Engineering Tool, open the desired Safety Matrix into which you want to import the data of the table document.
2. Select the menu command File > Import... .
3. In the following selection window, select the directory and the table document to be imported.
4. Click "Open".

When the process is complete, the Safety Matrix is displayed and the Reports window opens with the import log in the "Import/Export" tab. After importing a table document "*.ods", the following values are entered in the "Matrix comparison" section of the import log:

- "Source" = Table document "*.ods".
- "Reference" = Safety Matrix before import. In the dialog shown below, enter a new name for the matrix; this must be different from the one assigned to the template.

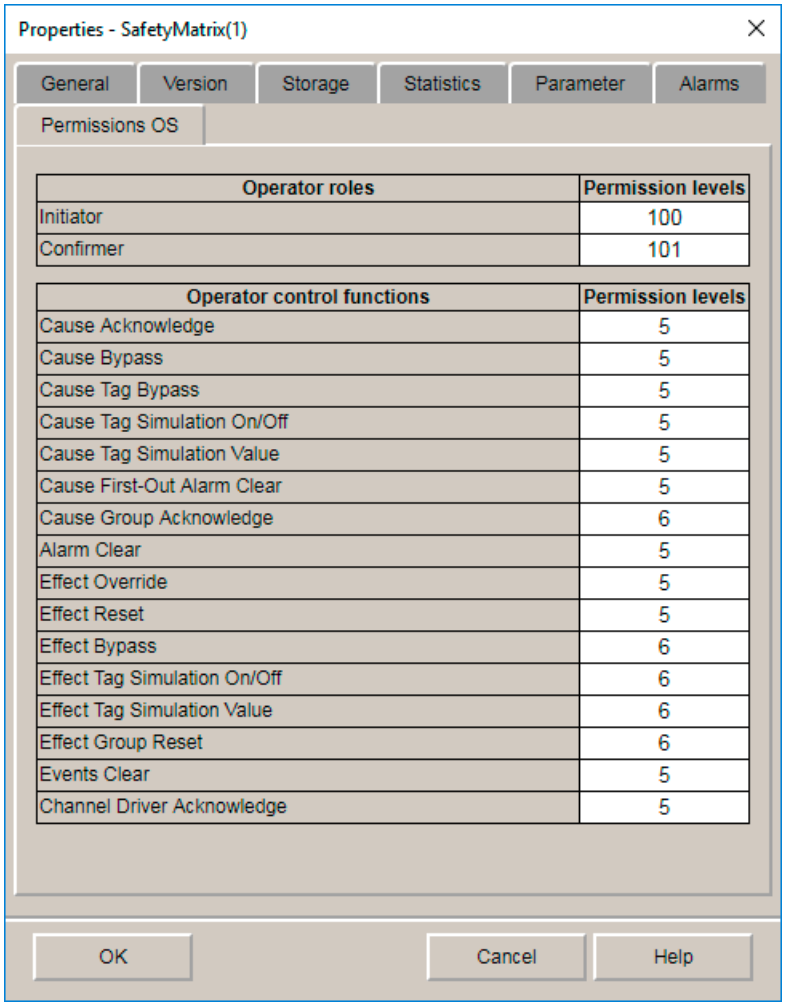
8.5 User authorizations for the Safety Matrix Viewer

In the properties of the Safety Matrix in the Safety Matrix Engineering Tool, you can set up a separate user authorization for each action and assign it to selected users.

In addition to the "Initiator" and/or "Confirmer" authorization, users must have the specified authorization level for the respective operator function to be executed. In the example configuration shown below, there is a "User" who has "Initiator" (authorization level 100) rights. In addition to the "Initiator", it has the "Process control" authorization (authorization level 5) and the "Higher-level process control" (authorization level 6).

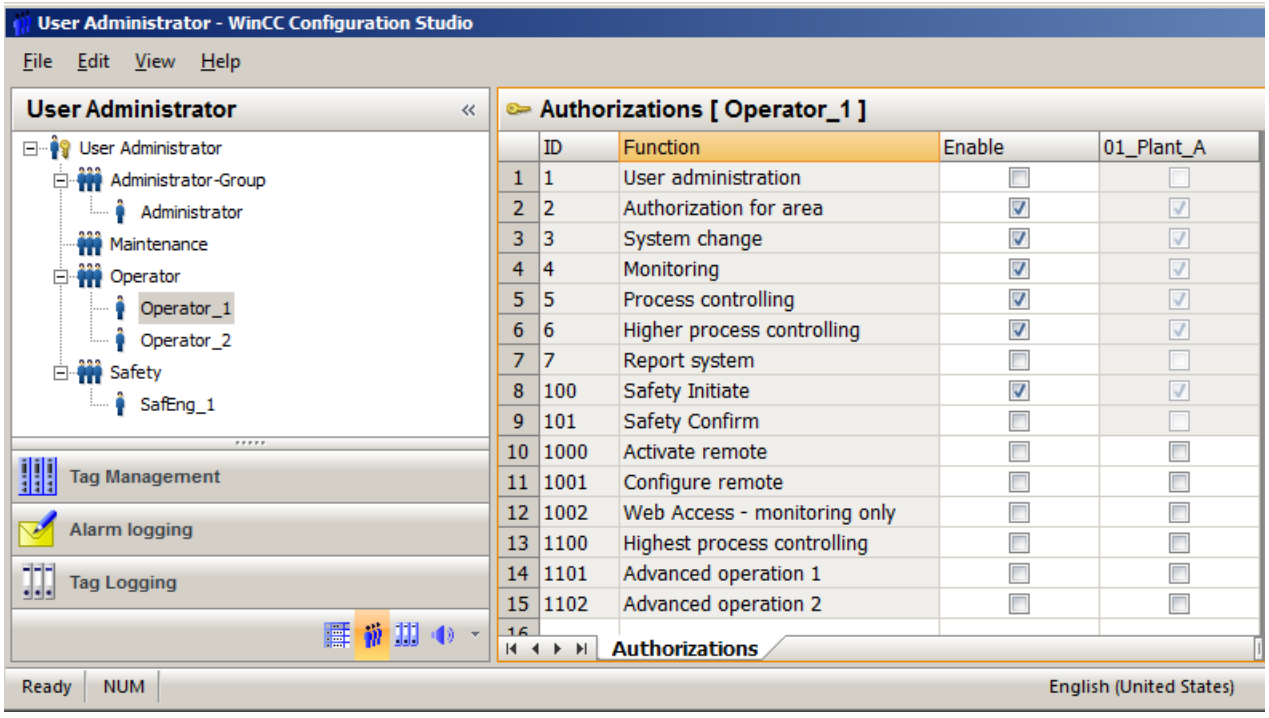
To confirm a transaction (4-eyes principle), a "user" is required who has "Confirmer" (authorization level 101) rights. In addition to "Confirmer", the "User" must be assigned the "Process control" authorization (authorization level 5) and the "Higher-order process control" (authorization level 6).

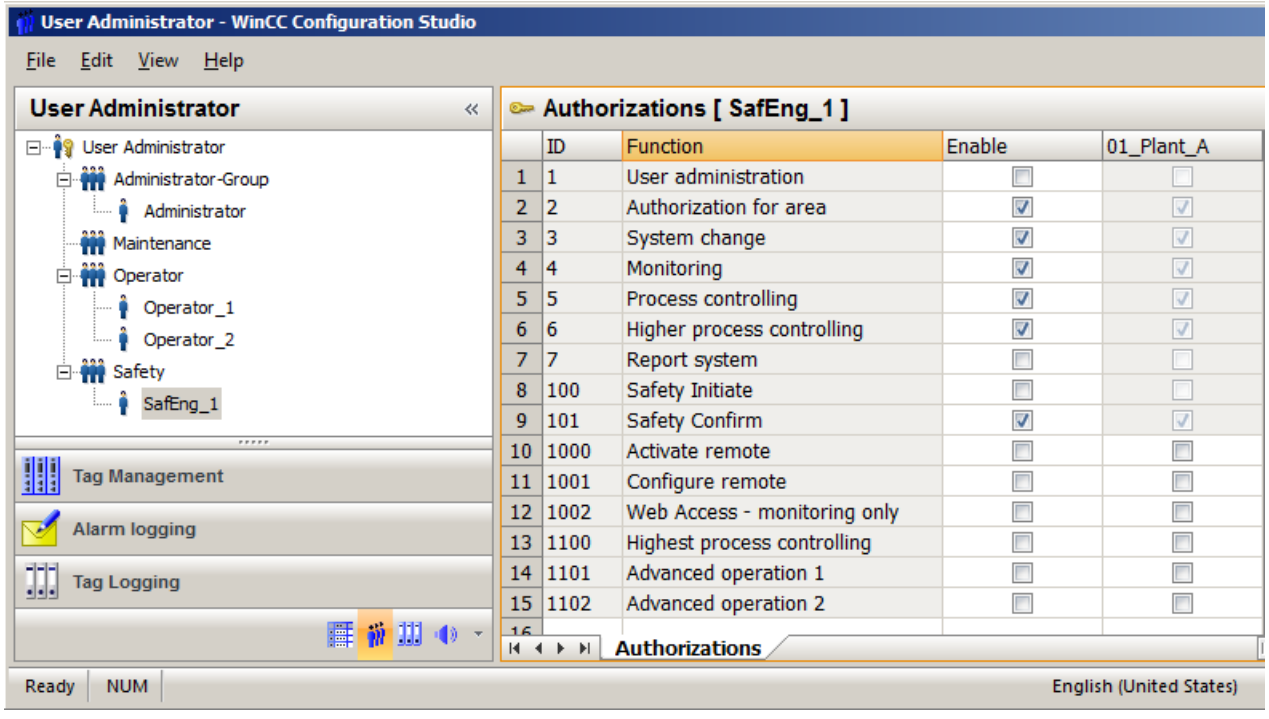
If a "User" is to initiate and confirm a specific action (acknowledgment driver), this action must be assigned its own user level and the "User" must have "Initiator" (authorization level 100) and "Confirmer" (authorization level 101) rights.



Operator roles	Permission levels
Initiator	100
Confirmer	101

Operator control functions	Permission levels
Cause Acknowledge	5
Cause Bypass	5
Cause Tag Bypass	5
Cause Tag Simulation On/Off	5
Cause Tag Simulation Value	5
Cause First-Out Alarm Clear	5
Cause Group Acknowledge	6
Alarm Clear	5
Effect Override	5
Effect Reset	5
Effect Bypass	6
Effect Tag Simulation On/Off	6
Effect Tag Simulation Value	6
Effect Group Reset	6
Events Clear	5
Channel Driver Acknowledge	5


User Administrator - WinCC Configuration Studio
File Edit View Help
User Administrator
User Administrator
Administrator-Group
Administrator
Maintenance
Operator
Operator_1
Operator_2
Safety
SafEng_1
Tag Management
Alarm logging
Tag Logging
Authorizations [Operator_1]
ID Function Enable 01_Plant_A
1 1 User administration
2 2 Authorization for area
3 3 System change
4 4 Monitoring
5 5 Process controlling
6 6 Higher process controlling
7 7 Report system
8 100 Safety Initiate
9 101 Safety Confirm
10 1000 Activate remote
11 1001 Configure remote
12 1002 Web Access - monitoring only
13 1100 Highest process controlling
14 1101 Advanced operation 1
15 1102 Advanced operation 2
Authorizations
Ready NUM English (United States)


User Administrator - WinCC Configuration Studio
File Edit View Help
User Administrator
User Administrator
Administrator-Group
Administrator
Maintenance
Operator
Operator_1
Operator_2
Safety
SafEng_1
Tag Management
Alarm logging
Tag Logging
Authorizations [SafEng_1]
ID Function Enable 01_Plant_A
1 1 User administration
2 2 Authorization for area
3 3 System change
4 4 Monitoring
5 5 Process controlling
6 6 Higher process controlling
7 7 Report system
8 100 Safety Initiate
9 101 Safety Confirm
10 1000 Activate remote
11 1001 Configure remote
12 1002 Web Access - monitoring only
13 1100 Highest process controlling
14 1101 Advanced operation 1
15 1102 Advanced operation 2
Authorizations
Ready NUM English (United States)

8.6 Interconnections between the matrix and safety program

When establishing interconnections between the matrix and the remainder of the safety program, you must ensure that the interconnected blocks are all in the same shutdown group, or that the right communication blocks have been installed between the shutdown groups.

8.7 Using external F-channel drivers in the matrix

There is a difference between internal and external F-channel drivers in the Safety Matrix. Internal F-channel drivers are created by the Safety Matrix during transfer in a "Driver chart" and interconnected with the Safety Matrix. If the Safety Matrix is transferred again, this chart may be regenerated, whereby changed parameters at the inputs of the F-channel drivers are overwritten with the values set in the Safety Matrix. Therefore, you may not change, rename, add or delete any blocks in this "Driver chart". Furthermore, you are not allowed to delete any interconnections. With Safety Matrix V6.3, manually created interconnections at outputs of F-channel drivers are retained.

If parameter changes are required to the F-channel drivers (an extended input signal range for example) or if-signals used by an F-channel driver also used elsewhere, in the program (for example, for display or as interlocking in the standard program) it is recommended to create a CFC for the F-channel driver yourself. In this case, you can activate the "Integrate external channel drivers" function when transferring the matrix to the project.

In this way, not only the process value and its status is interconnected to the Safety Matrix, the inputs "SIM_IN", "SIM_ON", and "SIM_V", which the matrix uses for the maintenance function, as well as "ACK_REI" and "ACK_REQ", are also used to signal an acknowledgment request in the Safety Matrix and perform acknowledgment from here.

To enable the Safety Matrix to integrate external F-channel drivers into its full scope of functions, the "SIM_IN", SIM_ON", "SIM_V", and "ACK_REI" I/Os may not be interconnected, since the Safety Matrix does not change the existing logic and thus cannot interconnect the inputs of the F-channel driver.

Channel drivers of types F_CH...*, F_PA..., F_Q... and F-block types can be incorporated from Safety Matrix V6.2 and higher using the "customer-specific" option.

* however, not those explicitly indicated F_CH_AI, F_CH_DI/DO, F_CH_BI/BO

Note

The max. runtime of the Safety Matrix must be taken into account in the s7ftime.xlsm for the monitoring and system response times. To this end, the number of Causes, Effects and the intersections must be entered in the "max. runtime SM V6.3" table worksheet.

9 Changes, tracking changes, and acceptance

9.1 General information

Operational procedures

During maintenance work in or while making changes to a plant, the operational procedures must be followed at all times.

Before changes can be made to safety-related parts of the plant or functions, a risk assessment relating to the change itself and how it is to be made must be carried out, particularly if it is to be made during operation. Only make changes if a risk assessment has been carried out beforehand and ensure that change instructions resulting from this are followed. If necessary, test program changes by loading them into a test CPU and checking the function.

An S7-400 F/FH system being operated as a safety system is protected by at least two passwords. Make sure you have the required access authorizations.

Note

You can find more information in section Access protection (Page 16).

If changes are to be downloaded during operation, safety mode must be deactivated on the AS and then reactivated once downloading is complete.

Note

You can find more information in section Safety mode and downloading the safety program (Page 171).

9.2 Preparing for changes

Offline/online comparison

Before each CFC change, make sure that the offline and online programs are identical.

- To do this, open a chart from the AS in the CFC editor and switch to online mode.
- If there are differences between the offline and online versions, a message with an additional system prompt will appear; otherwise, the system will switch to online mode without prompting.

In the case of fail-safe functions in the AS, you must also check whether the signature from the last compilation matches the online signature in the AS (see Section Tracking changes in the safety program (Page 253)).

- If the signatures are not identical, or a prompt indicating that there are differences between the programs appears when you switch to online mode, you must determine what has changed and whether these changes can be downloaded.

Version Cross Manager

The "Version Cross Manager" can be used as a tool for comparing two project versions, as well as the current project with a backed-up version of it (see section Tracking changes in the safety program (Page 253)).

- The comparison function in S7 F-Systems can be used to list the differences in the safety program. You can access this comparison function by clicking the "Compare..." button in the "Edit Safety Program" window.
- The next window enables you to choose the versions to be compared.

Do not make any other changes if the offline and online versions are different and you do not know what the differences are.

CPU utilization

Before making any changes, check the CPU utilization with regard to memory and cycle time. You can query how much memory has been allocated using the "Module Information..." function in the CPU.

- To do this, open "Module Information..." in the CPU and check how much memory is allocated at present on the "Memory" tab.
- To determine the cycle utilization, blocks TIME_BEG and TIME_ENG must be installed in the OBs in use and interconnected with one another. In the relevant CFC, check the runtimes of the OBs at output TM_DIFF_TI of the respective TIME_END block. Note that the run times of higher-priority OBs are also measured when this method of measuring the run times of lower-priority OBs is used, and will need to be subtracted accordingly.
  As of PCS V7.0 and an S7-400H CPU as of FW V4.5, the gross and net run times of the cyclic interrupt OBs can also be read at the CPU_RT block.

Note

You can find more information in section Cyclic interrupts (Page 25).

Checking the H parameters

In fault-tolerant systems, you must check the H parameters of the CPU.

- To do this, open the Object Properties of the CPU and switch to the "H Parameters" tab.
- If a "Cyclic interrupt OB with special handling" has been specified here, and the option "Use only calculated values" has been activated, use the "Calculate..." button to open the "Update the Standby CPU: Calculation of Monitoring Times" window.
- Here, check the values in the entry fields "Runtime of the watchdog interrupt concerned [ms]" and "Work memory used for all data blocks in the user program [Kbyte]".
- Compare the runtime entered in the "Runtime of the watchdog interrupt concerned [ms]" field, for the cyclic interrupt OB with special handling, with the measured runtime (TIME_BEG, TIME_END of OB) or the runtime read at the CPU_RT block. The value entered should be approximately 10% greater than the measured one.

- Compare the value for "Work memory used for all data blocks in the user program [Kbyte]" with the object properties of the CPU block folder. There, in the "Blocks" register under "Size in work memory: Data", you will find the amount of memory that is occupied by data blocks (in bytes). This value (expressed in Kbytes), plus some reserve, must be entered in the "Work memory used for all data blocks in the user program [Kbyte]" field.
- If the values in the entry fields do not match the actual values, you must enter the current values and determine the H parameters using the "Calculate..." button.

Note

You can find more information in section Calculating monitoring times (Page 41).

Checking the hardware before downloading

Before downloading the changes - and in particular, before downloading hardware configuration changes with HCiR - make sure that no errors are present in the system.

- The HCiR procedure involves stopping a CPU, performing the download, and then restarting the CPU.
- Immediately after the transition to RUN Redundant, the other CPU is stopped and restarted, during which time it is updated to the current configuration.
- If an error of a redundant component occurs (e. g., the interface module of the ET 200M), this can cause the connection to a PROFIBUS slave to fail and input/output modules to be passivated.

9.3 Changes in CFC

Changing the user program

Before you make changes to the standard or fail-safe program of an S7 F/FH systems, make sure that you can also download and check these changes. Changes to the standard or fail-safe program cannot be compiled or downloaded as part of a separate process. Therefore, you must follow the sequence below in full to make changes:

- Change CFC
- Check
- Compile
- Download
- Offline/online comparison
- Test
- Document

To change or add a fail-safe function, open the relevant CFC or add a new one.

Runtime groups

When a new CFC is added, the system creates a new runtime group with the same name. Check whether its insert position in the editor is the position you require.

When deleting safety functions, empty F-runtime groups may arise, which also have to be deleted. To do this with PCS 7 V7.0 and higher, execute the following command in the CFC editor: "Edit > Delete Empty Runtime Groups".
With PCS 7 V6.1, activate the option "Delete Empty Runtime Groups" when compiling.

Before inserting blocks, establish the predecessor block. When inserting blocks, make sure that the sequence of the blocks corresponds to the signal flow. If necessary, change the block sequence in the runtime editor. The "Optimize run sequence" function does not optimize F-runtime groups. These are excluded from optimization.

Function test

To test your functions, you can use S7 PLCSIM or SIMIT Virtual Controller (VC) depending on your PCS 7 version, you can download your program to a real test AS. Use the "Load to test AS" function. To perform testing with S7-PLCSIM, start S7-PLCSIM and download HW Config and the CFC charts. Depending on the version of S7-PLCSIM you are working with, you may need to enter either the password "plcsim" (up to PLCSIM V5.3) or the configured CPU password (PLCSIM V5.4 and higher) in order to download CFC charts.

You can find information on the configuration and use of the SIMIT Virtual Controller in the manual "SIMATIC SIMIT Simulation Platform" (https://support.industry.siemens.com/cs/ww/en/view/109801804).

A test with S7 PLCSIM or SIMIT Virtual Controller (VC) does not replace the function test in the plant.

9.4 Changes in HW Config

Different changes are possible during operation depending on the I/O line used. Changes to safety-relevant parameters can generally only be loaded in the STOP state of the AS.

When using the ET 200SP HA, you can add F-signal modules at any free slots or remove existing F-signal modules via CiR or H-CiR.

When using the ET 200M, CiR can be used to add or remove F-signal modules at the end of a rack. Using H-CiR, you can add new F-signal modules at any free slots or remove existing F-signal modules.

By removing and adding F-signal modules in two steps, you can change the configuration without the AS in STOP. Re-configuration in one step is not supported.

An attempt to change a parameter on an F-signal module is rejected by the system with an error message during the CiR loading process. As of S7 F Configuration Pack V5.5 SP12, you are notified that loading is only possible in the STOP state of the AS.

Note

Follow the instructions in the manuals:

- "SIMATIC High Availability Systems S7-400H" (https://support.industry.siemens.com/cs/ww/en/view/82478488)
- "SIMATIC PCS 7 Process Control System CPU 410 Process Automation V8 (https://support.industry.siemens.com/cs/ww/en/view/109801828)"

Signature value of the signal module

Safety-related settings of the fail-safe signal modules are entered in the signature of the fail-safe program. The signature value of a fail-safe signal module appears as an input parameter on the F-module driver.

To update this value, after safety-related parameters have been changed in the HW configuration the changes need to be compiled using "Generate module drivers" and downloaded in the CFC editor.

Safety information

In HW Config, you will receive a message when you make changes to safety-related parameters. If you are unable to or do not wish to finalize the changes for the reason specified above, you can cancel them here and close HW Config without saving.

9.5 Downloading changes/Complete downloading

Standard program

In an S7-400 F/FH system with a safety and standard program, changes can be made in the standard program in exactly the same way as with a standard system.

However, since the fail-safe program may also be affected by a program error in the standard program (e.g. an infinite loop in a user block), changes in the standard program should be treated in the same way as changes in the safety program.

Safety program

The procedure for downloading changes/complete downloading of programs with F-blocks is identical to the one used for the standard program. Additionally, safety mode must be deactivated before downloading changes and then reactivated once this is complete. Prior to loading the safety program, perform a consistency test. The signatures in the program information section and in the footer of the safety printout must be the same.

Note

You can find more information in section Safety mode and downloading the safety program (Page 171).

During a complete download, the CPU is stopped and must be restarted once the download is complete. When the CPU starts up, it goes into safety mode.

9.6 Tracking changes in the safety program

Backing up projects

In order to track changes, it is necessary to back up the project at regular intervals both before and after changes are made. A plant-wide decision should be taken regarding where project backups are to be stored and how the individual versions are to be named.

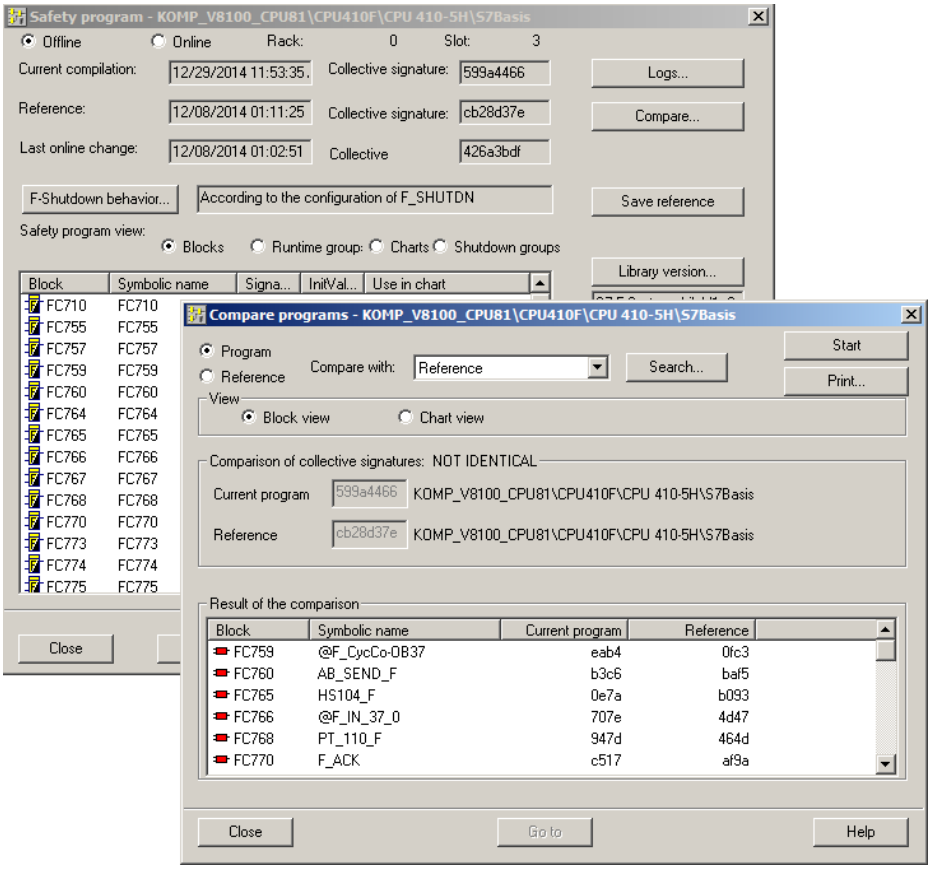
Program comparison

The "Version Cross Manager" can be used for the entire program as a tool for comparing two program versions, as well as for comparing the current project with a backed-up version of it.

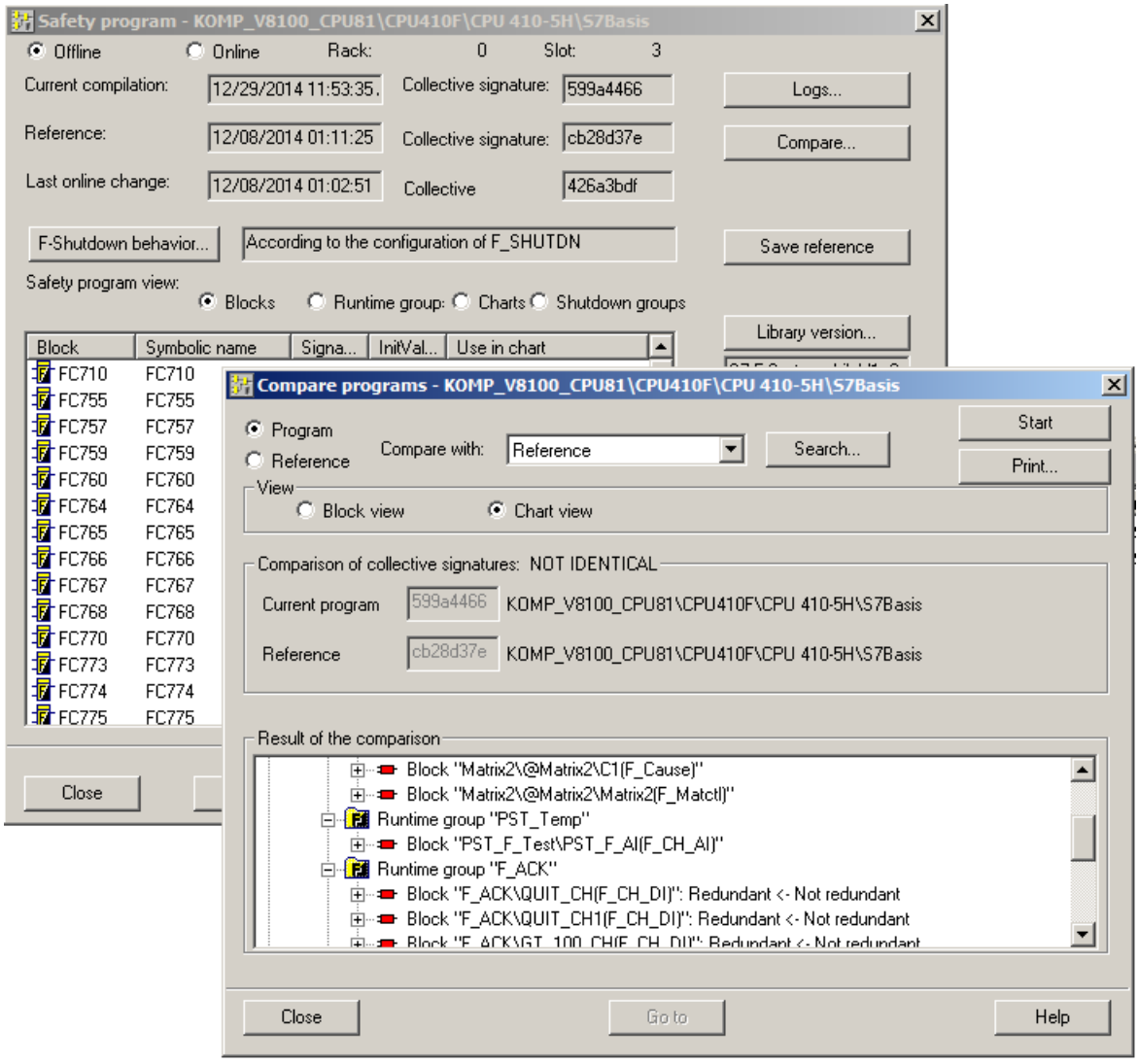
Options for comparing the safety program can be accessed by clicking the "Compare..." button in the "Edit Safety Program" dialog.

You can use this dialog to compare two safety programs and show and print the differences between them.

- Block view



- Chart view


Safety program - KOMP_V8100_CPU81\CPU410F\CPU 410-5H\S7Basis
Offline
Online
Rack: 0
Slot: 3
Current compilation: 12/29/2014 11:53:35
Collective signature: 599a4466
Logs...
Reference: 12/08/2014 01:11:25
Collective signature: cb28d37e
Compare...
Last online change: 12/08/2014 01:02:51
Collective: 426a3bdf
F-Shutdown behavior...
According to the configuration of F_SHUTDN
Save reference
Safety program view:
Blocks
Runtime group
Charts
Shutdown groups
Library version...
Block
Symbolic name
Signa...
InitVal...
Use in chart
FC710 FC710
FC755 FC755
FC757 FC757
FC759 FC759
FC760 FC760
FC764 FC764
FC765 FC765
FC766 FC766
FC767 FC767
FC768 FC768
FC770 FC770
FC773 FC773
FC774 FC774
FC775 FC775
Close
Compare programs - KOMP_V8100_CPU81\CPU410F\CPU 410-5H\S7Basis
Program
Reference
Compare with: Reference
Search...
Start
Print...
View
Block view
Chart view
Comparison of collective signatures: NOT IDENTICAL
Current program 599a4466 KOMP_V8100_CPU81\CPU410F\CPU 410-5H\S7Basis
Reference cb28d37e KOMP_V8100_CPU81\CPU410F\CPU 410-5H\S7Basis
Result of the comparison
Block "Matrix2\@Matrix2\C1(F_Cause)"
Block "Matrix2\@Matrix2\Matrix2(F_Matctl)"
Runtime group "PST_Temp"
Block "PST_F_Test\PST_F_AI(F_CH_AI)"
Runtime group "F_ACK"
Block "F_ACK\QUIT_CH(F_CH_DI)": Redundant <- Not redundant
Block "F_ACK\QUIT_CH1(F_CH_DI)": Redundant <- Not redundant
Close
Go to
Help

Using the "Compare with" drop-down list box, you can determine which programs you intend to compare.

- If you have activated the "Program" option button, you will be able to select one of the following programs here:

Reference	Last reference saved for this program
Last compilation	Last compilation of the program
Online	Program in the state currently downloaded on the F-CPU
Another project	Any offline program, click ("Browse..." to select)

- If you have activated the "Reference" option button, you will be presented with the following selection options:

Current program	Current offline program
Last compilation	Last compilation of the program
Online	Program in the state currently downloaded on the F-CPU
Another project	Any offline program, click ("Browse..." to select)

Signature of the safety program

The program signature is used to identify a safety program. It changes each time a change is made to the safety program. As a result, comparing the signature values of two safety programs provides an initial indication of what changes have been made in the safety program.

The signature of the current safety program in an AS can be found in the "Edit Safety Program" window. To do this, in the SIMATIC Manager select the CPU that contains the safety program and use the "Options > Edit Safety Program" menu command to open the relevant dialog. In this dialog, you can find three signatures with an associated date:

- The date on which CFCs were last compiled and the signature formed. This date is changed after delta compiling with changes to the safety program and after complete compiling without changes to the safety program.
- The date on which a safety program was saved as a reference, and which signature the reference program has.
- The date of the last online change and the signature formed for this. Several online changes may have been made since the last compilation.

Save the program you have checked as a reference using the "Reference" button in the "Edit Safety Program" window; enter the password if requested to do so and answer "Yes" to the query that appears following this.

The signatures shown offline in the "Edit Safety Program" window do not need to match the signature in the AS. It may, for example, be possible that the most recent changes were compiled, but not downloaded and checked.

For this reason, you must also check the signature in the AS.

- In the online view of the "Edit Safety Program" dialog box

  or

- While online, you can view the signature of the safety program in the AS at output F_SIG_OUT of the F_SHUTDN block.

For change tracking purposes, it is worth manually documenting both the signature value of the safety program and the name of the project backup in a log file.

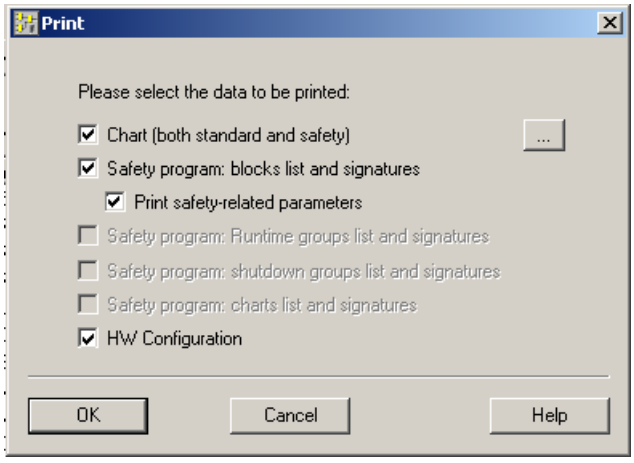
Note

You can find additional information about changing the time stamp and signature in the FAQ "When do the time stamp and signature change in the "Edit Safety Program" dialog?" (https://support.industry.siemens.com/cs/ww/en/view/62046624).

9.7 Printing program data

You can use the "Edit Safety Program" dialog box to view, compare, and document many of the attributes of the safety program. It lists all the blocks that are contained in the safety program. F-runtime groups and charts can also be displayed.

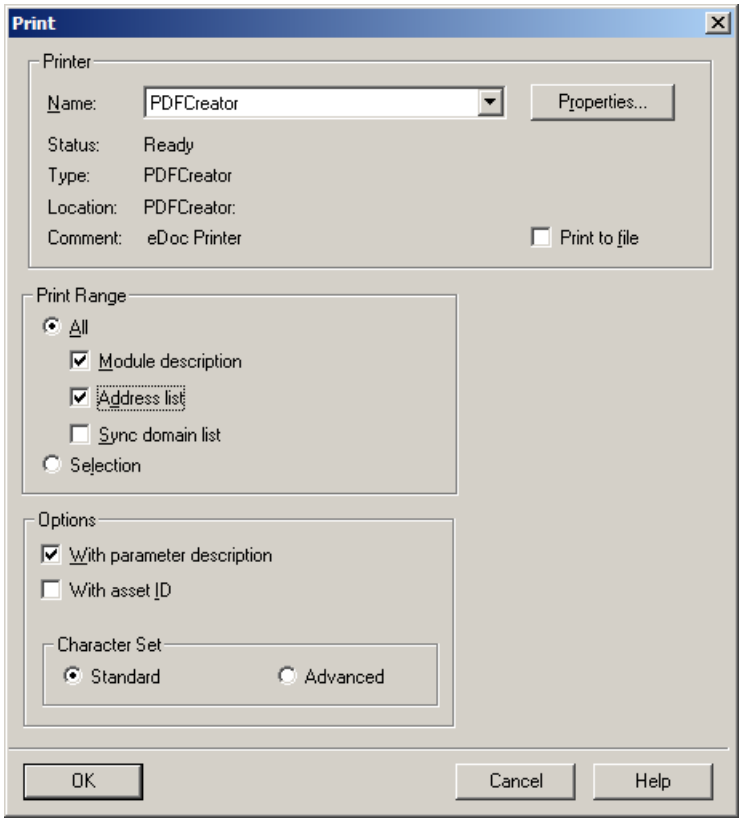
Here, you will also find options for documenting the current safety program:



If you want to print all the charts, select the "Chart (standard and F-chart)" option. Individual charts or all F-charts can be printed from the SIMATIC Manager. If the printout is made from the "Security Program" window, a footer with the S7 F Systems version and the program signature is printed on each page.

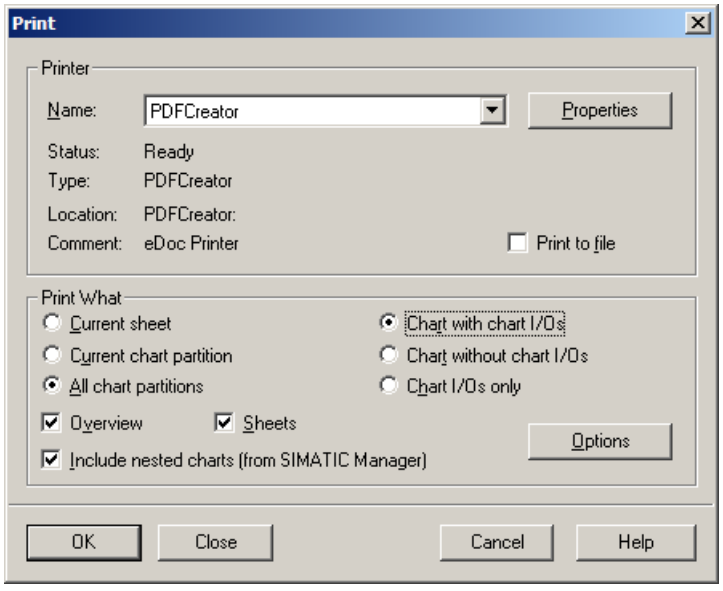
Activate the options shown above to print the safety program and the hardware.

Before the hardware is printed, another dialog appears:



Here, select the "All", "Module description", and "Address list" options.

To print individual or multiple charts from the SIMATIC Manager, you must make the CFC editor settings in the "Print" dialog. For this purpose, open a chart in CFC, go to the "Chart > Print" menu, and then select the printout options shown below.



In the chart directory of your AS, within the SIMATIC Manager you then have the option of highlighting charts for printing purposes, and printing the selected charts using the "File > Print > Object Content" menu command.

9.8 Plant acceptance

Note

The procedure for acceptance of a system, acceptance of changes or acceptance of F-block types as described in the "SIMATIC Industrial Software S7 F/FH Systems - Configuring and Programming" (https://support.industry.siemens.com/cs/ww/en/view/109802562) manual must be followed.

Two checklists are available for system documentation purposes:

- "Process Safety – Configuration" checklist
  This list is used for documenting the system design and the software and hardware settings of the automation system in use.
- "Process Safety – Verification/Testing"
  This list enables you to document that the components in use have been tested against their requirements and specifications, and that the relevant function tests have been performed.

These lists are only templates and may be adapted to the requirements of your plant at any time.

9.9 Replacing fail-safe hardware

If it becomes necessary to replace an F-signal module or F-CPU during plant operation, for example, due to a hardware defect, observe the notes on change management in the context of functional safety management in the relevant standards or guidelines such as IEC 61511 or VDI/VDE 2180.

Basically, the new module must be of the same type and downward compatible to the predecessor module. You can find this information in the technical specifications of the modules at the Industry Online Support Portal (https://support.industry.siemens.com).

If the downward compatibility is ensured and the wiring remains unchanged, it is possible to immediately replace the module without further tests from the product point of view.

10 Service and support

Industry Online Support

Do you have questions or need assistance?

Using the Industry Online Support, you have round-the-clock access to expertise spanning the entire range of service and support, as well as to our services.

Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs and application examples – all information can be accessed with just a few mouse clicks: https://support.industry.siemens.com/.

Industry Online Support App

The "Siemens Industry Online Support" app provides you with optimal support even when you are on the go. The app is available for Apple iOS, Android and Windows Phone: https://support.industry.siemens.com/cs/ww/en/sc/2067

Technical Forum

Exchange your experience and know-how about our products or systems or benefit from the knowledge of others.

Have discussions on special products or general topics, discover new ideas and inspiration and help yourself and others on the Technical Forum (http://www.siemens.com/automation/forum) – free of charge, outside office hours and at the weekend.

Technical Support

The Siemens Industry Technical Support offers you fast and competent support for any technical queries you may have with a number of tailor-made solutions – ranging from basic support to individual support contracts.

Send your queries to Technical Support using the following web form: www.siemens.com/industry/supportrequest.

Range of services

Our range of services includes the following:

- Product training courses
- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog: https://support.industry.siemens.com/cs/sc.

Contact partner

If you have any questions or need support, please contact your local representative, who will put you in contact with the responsible service center. You can find your contact partner in the contact database: www.siemens.com/yourcontact.