SIEMENS

SIMATIC

Process Control System PCS 7 Compendium Part B - Process Safety (V8.2)

Operating Manual

Security information 1

Preface 2

What's new? 3

Installing the fail-safe system 4

Advanced PCS 7 ES settings 5

Configuring S7F/FH hardware 6

Configuring the safety program 7

Configuration with Safety Matrix 8

Changes, tracking changes, and acceptance 9

Service and support 10

Valid for PCS 7 V8.2
SIMATIC F-Systems V6.1 SP2
SIMATIC Safety Matrix V6.2 SP2

07/2016
A5E35031794-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
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E35031794-AB
℗ 07/2016 Subject to change

Table of contents

1 Security information 7

2 Preface 8

3 What's new? 10

4 Installing the fail-safe system 11

4.1 Software components 11

4.2 Installation on the PCS 7 engineering station (ES) 12
4.2.1 Installing S7 F Systems 12
4.2.2 Installing Safety Matrix 13

4.3 Installation on the PCS 7 operator station (OS) 13

4.4 OS client installation 14
4.4.1 Installing S7 F Systems 14
4.4.2 Installing Safety Matrix 14

4.5 Installation steps on an office PC 14

5 Advanced PCS 7 ES settings 15

5.1 Access protection 15
5.1.1 General measures 15
5.1.2 Access protection with SIMATIC Logon 15

5.2 CFC settings for compiling and downloading 16

6 Configuring S7F/FH hardware 18

6.1 Adapting CPU parameters (single F-system) 19
6.1.1 Password and access protection 19
6.1.2 Access protection with SFC 109 20
6.1.3 Cyclic interrupts 23
6.1.4 Diagnostics/Clock 29
6.1.5 H parameters 30

6.2 Adapting CPU parameters (fault-tolerant F system) 32
6.2.1 Reaction to RAM/PIQ comparison error 32
6.2.2 Cyclic interrupt OB with special handling 34
6.2.3 Monitoring times 35
6.2.4 Calculating monitoring times 36

6.3 Communications module parameters/Networks 39

6.4 Setting system parameters for F-signal modules ... 43
6.4.1 Operating mode ... 43
6.4.2 PROFIsafe addresses ... 44
6.4.3 Module parameters - general ... 45
6.4.4 Activating channels ... 47
6.4.5 Parameter assignment for SM326; DI 8 x NAMUR ... 50
6.4.6 Parameter assignment for SM326; DI 24 x DC 24V ... 51
6.4.7 Parameter assignment for SM326; DO 10 x DC 24V/2A (6ES7326-2BF01-0AB0) ... 54
6.4.8 Parameter assignment for SM326; F-DO 10 x DC 24V/2A PP (6ES7326-2BF10-0AB0) ... 55
6.4.9 Parameter assignment for SM326; F-DO 8 x DC24 V/2A PM ... 58
6.4.10 Assigning parameters for the SM336; AI 6 x 13Bit ... 59
6.4.11 Assigning parameters for the SM336; F-AI 6 x 0/4...20mA HART ... 62
6.4.12 Parameter assignment for EM 8 F-DI NAMUR Ex ... 65
6.4.13 Parameter assignment for EM 4 F-DO Ex 17.4V/40mA ... 67
6.4.14 Parameter assignment for EM 4 F-AI Ex HART ... 69

6.5 Configuring redundant F-signal modules ... 72

6.6 Marshalled Termination Assemblies (MTAs) ... 74

6.7 "Wiring and Voting" architectures for ET 200M ... 75
6.7.1 Voting on the module or in the CPU ... 75
6.7.2 2oo3 Voting with F-AI ... 77

7 Configuring the safety program ... 78

7.1 Introduction ... 78

7.2 Creating the safety program ... 80
7.2.1 Defining the program structure ... 81
7.2.2 Creating CFC charts ... 82
7.2.3 Assigning parameters to and interconnecting F-blocks ... 82
7.2.4 Run sequence of F-blocks ... 84
7.2.5 F-runtime groups ... 86
7.2.6 F-shutdown groups ... 89
7.2.7 Data exchange between the F user program and standard user program ... 92
7.2.8 How F-blocks with floating-point operations respond to number range overflows ... 93

7.3 Configuring fail-safe AS-AS communication ... 95
7.3.1 Configuring S7 connections ... 96
7.3.2 Configuring F-communications blocks ... 97

7.4 F-STOP ... 100
7.4.1 Complete shutdown ... 100
7.4.2 Partial shutdown ... 100
7.4.3 Parameter assignment for shutdown behavior ... 101
7.4.4 Causes of errors ... 102
7.4.5 Execution of an F-STOP in S7 F/FH systems ... 103
7.4.6 Exiting an F-STOP ... 104

7.5 F startup and (re)start protection ... 104
7.5.1 F-startup ... 104
7.5.2 (Re)start protection ... 105

7.6 I/O access via F driver blocks ... 106

7.7 Passivation and reintegration of input/output channels 107
7.7.1 Passivation - general 107
7.7.2 Group passivation 108
7.7.3 Reintegration following elimination of errors 109
7.7.4 Automatic reintegration on channel error 109
7.7.5 Programming reintegration following module errors or channel errors requiring acknowledgment 110

7.8 Compiling the F-program 117
7.8.1 Password protection for safety-related functions and settings 117
7.8.2 Parameterizing the maximum F cycle monitoring time 118
7.8.3 Compiling the S7 program 119

7.9 Safety mode and downloading the safety program 121
7.9.1 Information on safety mode 121
7.9.2 Deactivating safety mode 121
7.9.3 Activating safety mode 123
7.9.4 Downloading the safety program 124

7.10 Operating and changing safety-related parameters on a PCS 7 OS 126
7.10.1 Safety Data Write (SDW) 126
7.10.2 F_QUITES 129
7.10.3 Maintenance Override Switch (MOS) 129

7.11 Monitoring times and system response times 133
7.11.1 Diagnostic block "CPU_RT" 134
7.11.2 Calculating the F-cycle monitoring time (for block F_CYC_CO) 136
7.11.3 Communication monitoring time for F CPU/F signal modules 140
7.11.4 Monitoring time for safety-related communication between F-CPUs 149
7.11.5 Monitoring communication between F-shutdown groups 151
7.11.6 Response times of safety functions 152

8 Configuration with Safety Matrix 160

8.1 Creating and configuring a Safety Matrix 160

8.2 Documenting a Safety Matrix 162

8.3 Organizing matrices into different shutdown groups 162

8.4 Duplicating matrices 167

8.5 User authorizations for the Safety Matrix Viewer 169

8.6 Interconnections between the matrix and safety program 171

8.7 Using imported F channel drivers in the matrix 171

8.8 New matrix operating blocks 172

9 Changes, tracking changes, and acceptance 173

9.1 General information 173

9.2 Preparing for changes.... 174

9.3 Changes in CFC.... 176

9.4 Changes in HW Config 177

9.5 Downloading changes/Complete downloading.... 178

9.6 Tracking changes in the safety program.... 178

9.7 Printing program data 182

9.8 Plant acceptance.... 184

10 Service and support....185

Security information 1

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or 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 only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the Internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply 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 http://www.siemens.com/industrialsecurity.

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.

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

It examines the following F-software components:

- S7 F-Systems
- SIMATIC 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 V8.2
- SIMATIC F-Systems V6.1 SP2
- SIMATIC Safety Matrix V6.2 SP2

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.

3 What's new?

The contents of the compendium have been updated in accordance with the new functions and operator input options of SIMATIC PCS 7 V8.2.

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

- Installing the fail-safe system
- Access protection with SFC 109

The section "Creating F block types" has been removed. You can find information on creating F-block types in Section 5.7 of the manual

"SIMATIC Industrial Software S7 F/FH Systems – Configuring and Programming" (https://support.industry.siemens.com/cs/ww/en/view/101509838)

Installing the fail-safe system 4

4.1 Software components

This documentation is based on PCS 7 version V8.2 and the following additional software components:

- S7 F-Systems
  - S7 F Configuration Pack V5.5 SP12
  - S7 F-Systems V6.1 SP2
  - S7 F-Systems Lib V1_3 SP1 Upd. 1
  - S7 F-Systems HMI V6.1 SP2
- Safety Matrix
  - Safety Matrix Engineering Tool V6.2 SP2
  - Safety Matrix Viewer V6.2 SP2
  - Safety Matrix AS-OS Engineering V6.2 SP3

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:

- S7 F/FH Systems Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/101509838)
- Industrial Software Safety Matrix (https://support.industry.siemens.com/cs/ww/en/view/100675874)

4.2 Installation on the PCS 7 engineering station (ES)

4.2.1 Installing S7 F Systems

Procedure

1. Run SETUP.EXE to start the installation and follow the instructions in the setup program.
2. Select the "Engineering" package for installation on the ES . The following components are selected for installation in the next window:
   - F Systems V6.1 SP2
   - F Systems HMI V6.1 SP2
   - S7 F-Systems Lib V1_3 SP1 Upd.1
   - S7 F-ConfigurationPack V5.5 SP11
3. Deactivate the option for the S7 F-Configuration Pack V5.5 SP11
4. Carry out the installation.
5. Download the S7 F Configuration Pack V5.5 SP12 via the Siemens Industry Online Support:
   - Download S7 F Configuration Pack V5.5 SP12 (https://support.industry.siemens.com/cs/ww/en/view/15208817)
6. Run SETUP.EXE to start the installation and follow the instructions in the setup program.

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.

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

4.2.2 Installing Safety Matrix

Procedure

Safety Matrix Engineering requires an installation of F-System. 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" package. The following components are selected for installation in the next window:
   - Safety Matrix Engineering Tool V6.2 SP2
   - Safety Matrix Viewer V6.2 SP2
   - Safety Matrix AS-OS Engineering V6.2 SP3
3. Download the Safety Matrix AS-OS Engineering V6.2 SP3 via the Siemens Industry Online Support:
   - Download Safety Matrix AS-OS Engineering V6.2 SP3 (https://support.industry.siemens.com/cs/ww/en/view/109482577)
   - You require only the following file for PCS 7 V8.2: Update software Safety Matrix AS-OS Engineering V6.2 SP3 "S7FSMTXMAP_V62_SP3.zip".
4. Unzip the archive file.
5. Run SETUP.EXE to start the installation and follow the instructions in the setup program.

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 S7 F Systems

Procedure

If you are using SDW or MOS, run SETUP.EXE to start the installation and select the "Runtime" package: The following components are selected for installation in the next dialog:

- S7 F-Systems HMI V6.1 SP2

4.4.2 Installing Safety Matrix

Procedure

Run SETUP.EXE to start the installation. Follow the instructions in the setup program and select the "Runtime" package: The following components are selected for installation in the next dialog:

- Safety Matrix Viewer V6.2 SP2

4.5 Installation steps on an office PC

Procedure

You can install the Safety Matrix Editor on an office PC to design safety features.

1. Start the installation using SETUP.EXE.
2. Follow the instructions of the setup program and select the "Editor" package. The following components are selected for installation in the next window:

- Safety Matrix Editor V6.2 SP2
- Automation License Manager V5.3

Advanced PCS 7 ES settings 5

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

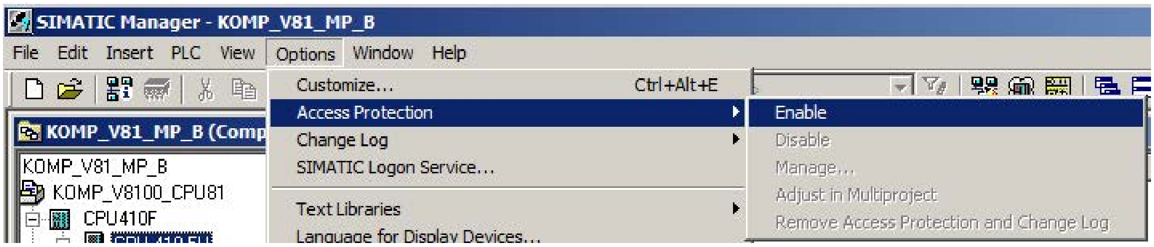
With PCS 7 V7.0 and higher, it is possible to set up access protection for individual subprojects with SIMATIC Logon. With a station-selective multiproject structure, this means that it is possible to assign access rights for protecting AS projects with F program.

Requirement

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

Procedure

1. In the SIMATIC Manager, activate access protection on a selected project node via "Options > Access Protection".



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.

5.2 CFC settings for compiling and downloading

Procedure

1. For compiling programs with F-blocks, set the threshold for generating the warning based on the number of blocks per sequence group. The default value is 50.

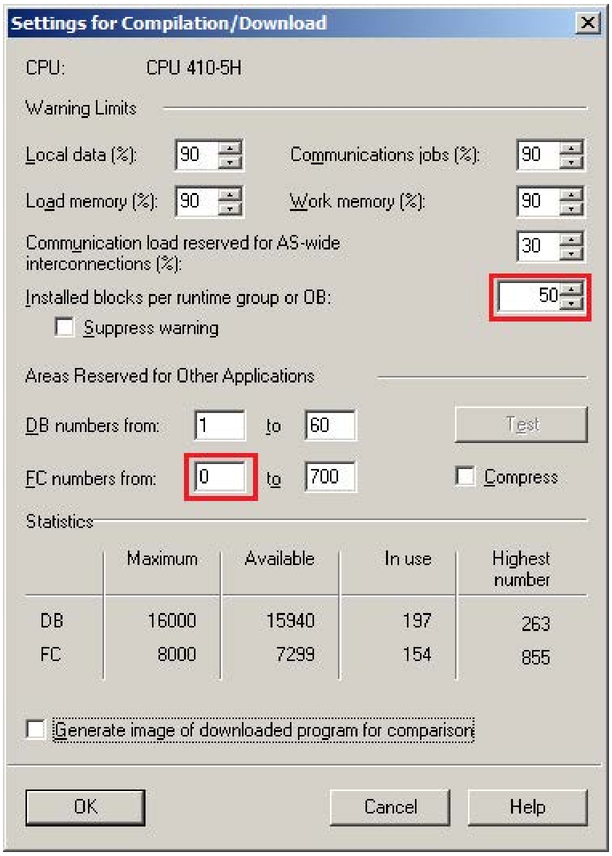
Note

This value applies for any project that is compiled on the ES and should be reset for the purpose of compiling standard programs.

The warning limit is designed to prevent creation of blocks with more than 64 KB. The compiler aborts with an error in this case because blocks with more than 64 KB are not possible. You can set the warning limit individually (1 – 32767), for example, after empirical determination. To determine the warning limit empirically, the program must be compiled at regular intervals during the configuration. Then you can check in the block folder of the program whether a block (Task FC) is approaching the maximum allowable size of 64 KB. If the block size is close to this limit, the warning limit is set too high. If the block size is well below the limit of 64 KB, the warning limit can be increased.

If a block is close to the limit of 64 KB, you can reduce the required memory by inserting new sequence groups or by moving blocks/sequence groups to a cyclic interrupt.

You can find additional information on this topic in the FAQ "Why does the error message "Maximum length of code area reached (max. 64 KB)" or "Insufficient main memory" appear when the CFC charts are compiled?" (https://support.industry.siemens.com/cs/ww/en/view/771569).



Settings for Compilation/Download

CPU: CPU 410-5H

Warning Limits

Local data (%): 90

Communications jobs (%): 90

Load memory (%): 90

Work memory (%): 90

Communication load reserved for AS-wide interconnections (%): 30

Installed blocks per runtime group or OB: 50

□ Suppress warning

Areas Reserved for Other Applications

DB numbers from: 1 to 60

FC numbers from: 0 to 700

□ Compress

Statistics

	Maximum	Available	In use	Highest number
DB	16000	15940	197	263
FC	8000	7299	154	855

□ Generate image of downloaded program for comparison

2. In the "Areas Reserved for Other Applications" field, set the value for "FC numbers from:" to 0. The default setting is 60.

Configuring S7F/FH hardware 6

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

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

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.

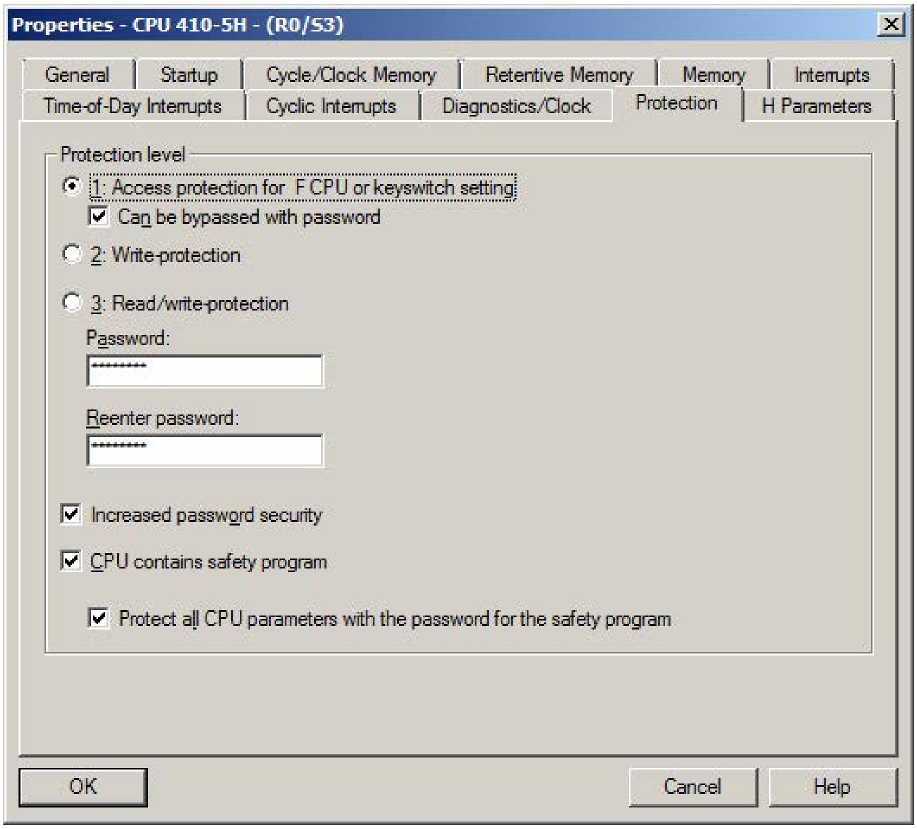
6.1 Adapting CPU parameters (single F-system)

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.



Protection level

● 1: Access protection for F CPU or keyswitch setting

☑ Can be bypassed with password

○ 2: Write-protection

○ 3: Read/write-protection

Password: *********

Reenter password: *********

☑ Increased password security

☑ CPU contains safety program

☑ Protect all 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

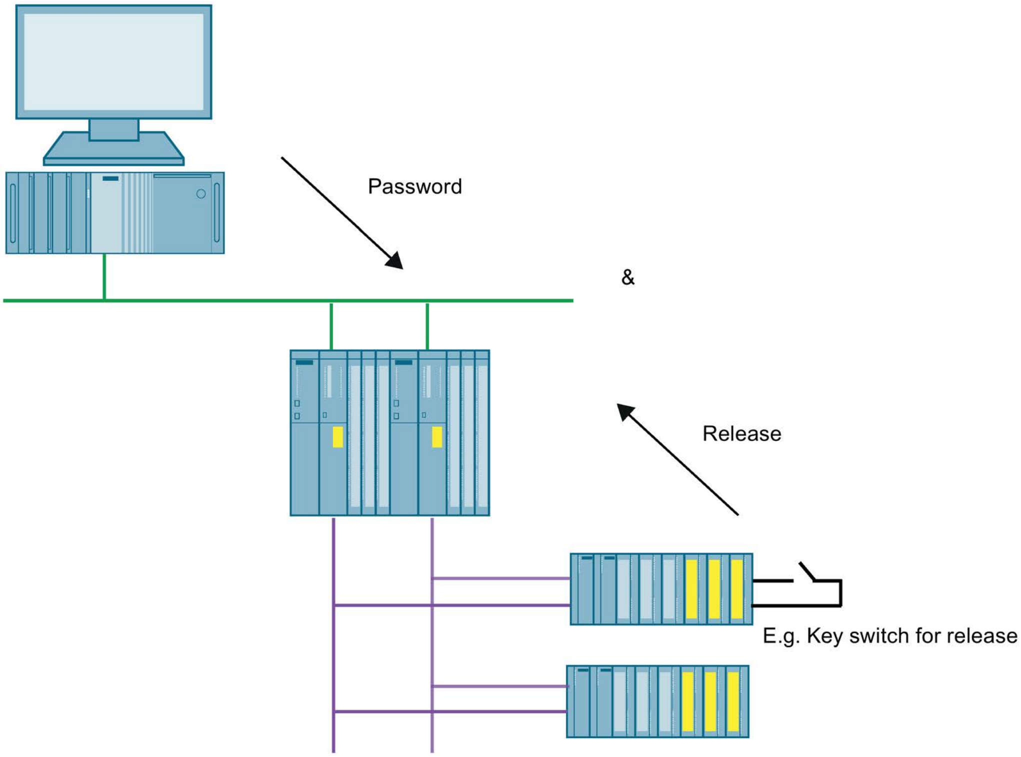
Setting the protection level: Any applicable block that is present on password authorization is lifted through this call.

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.

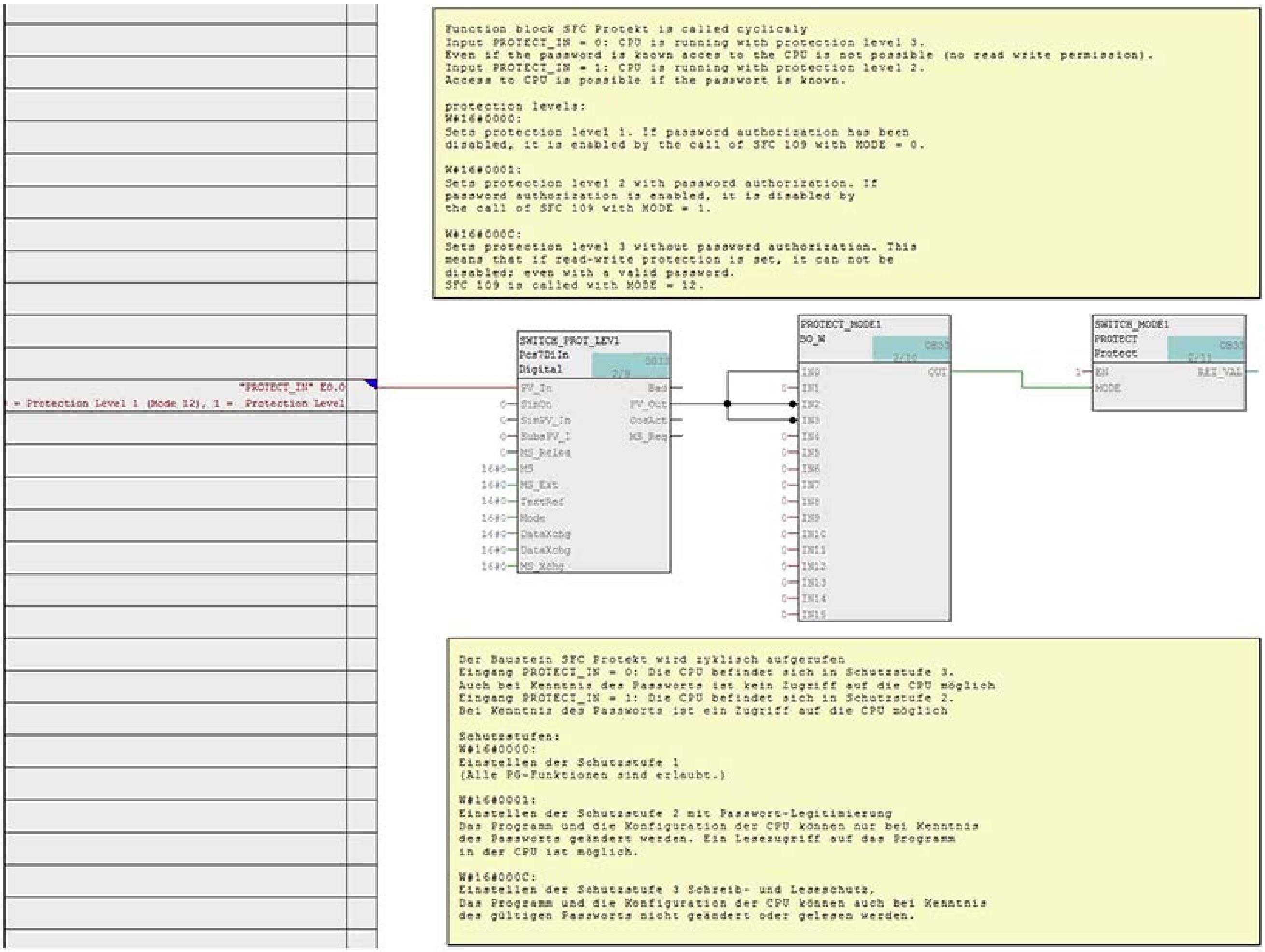
Calling of SFC 109 with MODE=12

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.



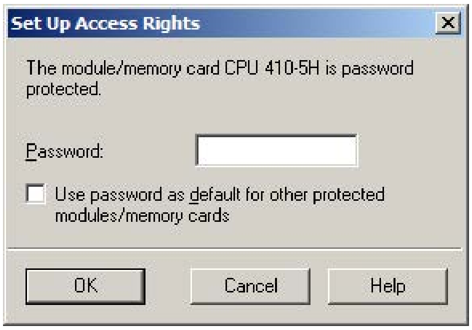
```
Function block SFC Protekt is called cyclicaly
Input PROTECT_IN = 0: CPU is running with protection level 3.
Even if the password is known acces to the CPU is not possible (no read write permission).
Input PROTECT_IN = 1: CPU is running with protection level 2.
Access to CPU is possible if the passwort is known.

protection levels:
W#16#0000:
Sets protection level 1. If password authorization has been
disabled, it is enabled by the call of SFC 109 with MODE = 0.

W#16#0001:
Sets protection level 2 with password authorization. If
password authorization is enabled, it is disabled by
the call of SFC 109 with MODE = 1.

W#16#000C:
Sets protection level 3 without password authorization. This
means that if read-write protection is set, it can not be
disabled; even with a valid password.
SFC 109 is called with MODE = 12.
```

```
Der Baustein SFC Protekt wird zyklisch aufgerufen
Eingang PROTECT_IN = 0: Die CPU befindet sich in Schutzstufe 3.
Auch bei Kenntnis des Passworts ist kein Zugriff auf die CPU möglich
Eingang PROTECT_IN = 1: Die CPU befindet sich in Schutzstufe 2.
Bei Kenntnis des Passworts ist ein Zugriff auf die CPU möglich

Schutzstufen:
W#16#0000:
Einstellen der Schutzstufe 1
(Alle PG-Funktionen sind erlaubt.)

W#16#0001:
Einstellen der Schutzstufe 2 mit Passwort-Legitimierung
Das Programm und die Konfiguration der CPU können nur bei Kenntnis
des Passworts geändert werden. Ein Lesezugriff auf das Programm
in der CPU ist möglich.

W#16#000C:
Einstellen der Schutzstufe 3 Schreib- und Leseschutz,
Das Programm und die Konfiguration der CPU können auch bei Kenntnis
des gültigen Passworts nicht geändert oder gelesen werden.
```

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.



Set Up Access Rights

The module/memory card CPU 410-5H is password protected.

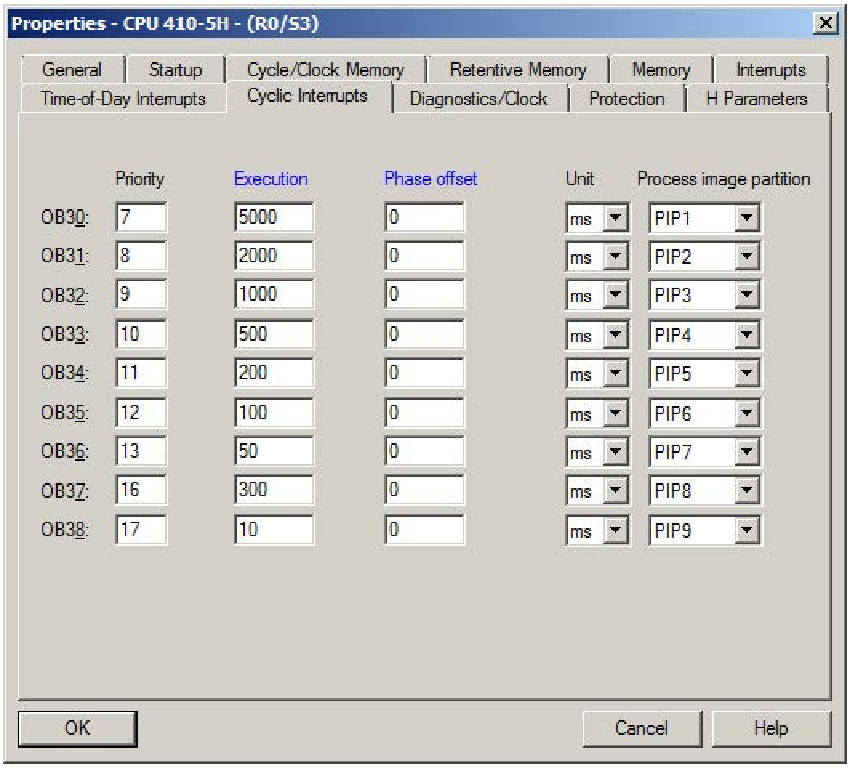
Password:

□ Use password as default for other protected modules/memory cards

6.1.3 Cyclic interrupts

Parameter assignment

Process image partitions do not need to be configured for F-program parts, because F-signal modules in S7 F/FH systems are not accessed using the process image, but rather through F-module drivers. When a process image is assigned to an F-module, it must match the process image of the cyclic interrupt in which the F-module driver is processed.



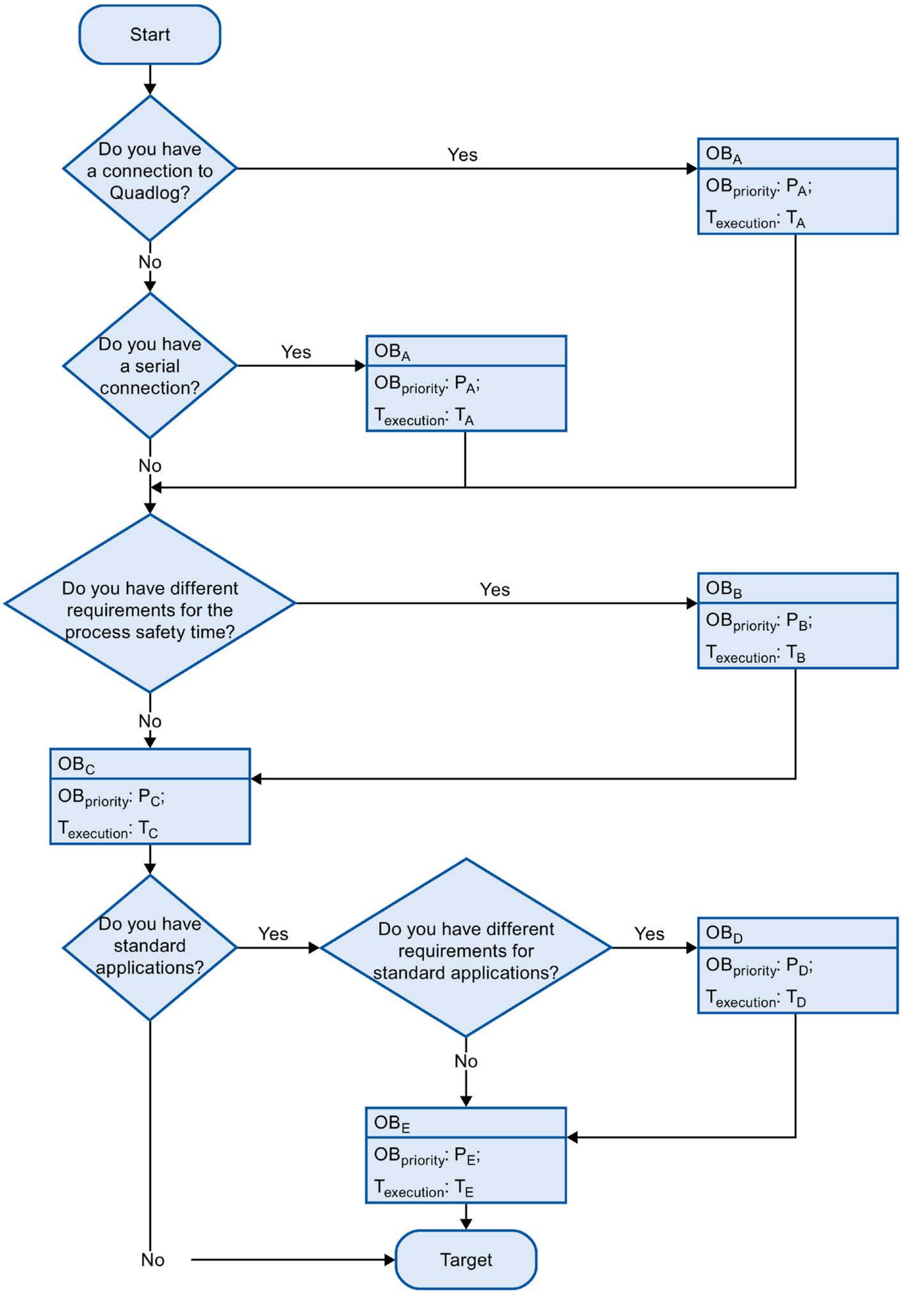
Properties - CPU 410-5H - (R0/S3)

	Priority	Execution	Phase offset	Unit	Process image partition
OB30:	7	5000	0	ms	PIP1
OB31:	8	2000	0	ms	PIP2
OB32:	9	1000	0	ms	PIP3
OB33:	10	500	0	ms	PIP4
OB34:	11	200	0	ms	PIP5
OB35:	12	100	0	ms	PIP6
OB36:	13	50	0	ms	PIP7
OB37:	16	300	0	ms	PIP8
OB38:	17	10	0	ms	PIP9

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 (cyclic interrupt with special treatment)
  - For example pressure protection functions
- OB_C
  - (Slow) F-applications
  - If there is only one cyclic interrupt for F-applications, then it will be the cyclic interrupt OB with special treatment.
  - 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.)

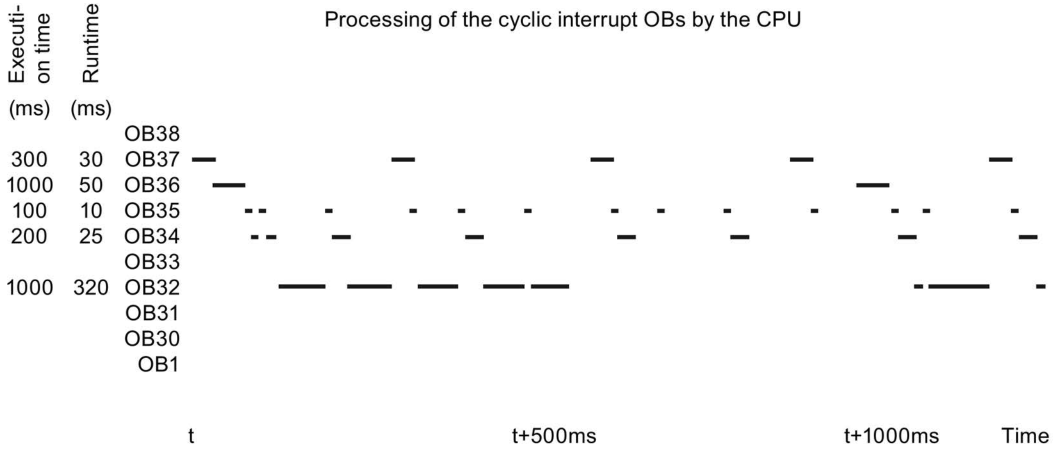
Example 1: Reconfiguration (no Quadlog connection, no serial communication)

OB	Prio	Call interval	Purpose	Comment
OB 38	15	10 ms	Empty	
OB 37	17	300 ms	Fast F-application	OB with special handling
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 time stamping of the IM module, 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 with special handling
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 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 with special handling
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 time stamping of the IM module, 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 SP1 and an S7-400H CPU with FW 4.5 and higher, the run times for the cyclic interrupt OBs and the complete utilization of the AS may also 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.

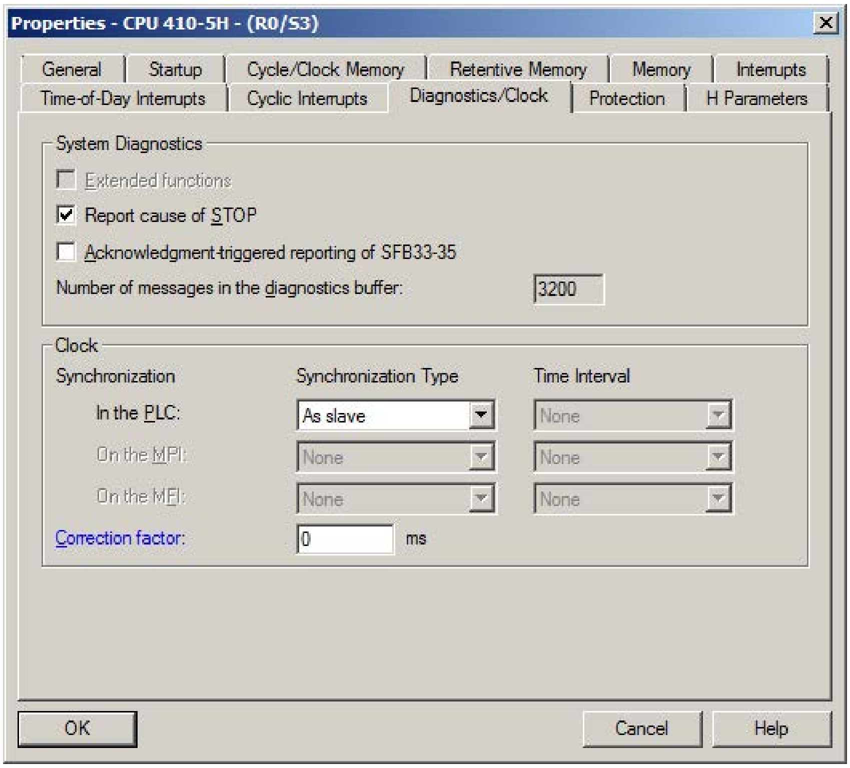
Alternatively, you can disable stop prevention altogether by setting the parameter for input Max_RTRG of block CPU_RT to 0. You can find this block in the @CPU_RT chart.

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. This usually involves an OS server or an external clock (SICLOCK) taking on the role of the time master. All other operator stations and automation systems on the plant bus then have the time from this time master and, therefore, identical time.

This is why the synchronization in the AS is always set to the "As slave" synchronization type for each AS/CPU in a time-synchronized PCS 7 plant.



System Diagnostics

☐ Extended functions

☑ Report cause of STOP

☐ Acknowledgment-triggered reporting of SFB33-35

Number of messages in the diagnostics buffer: 3200

Clock

Synchronization	Synchronization Type	Time Interval
In the PLC:	As slave	None
On the MPI:	None	None
On the MFI:	None	None

Correction factor: 0 ms

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

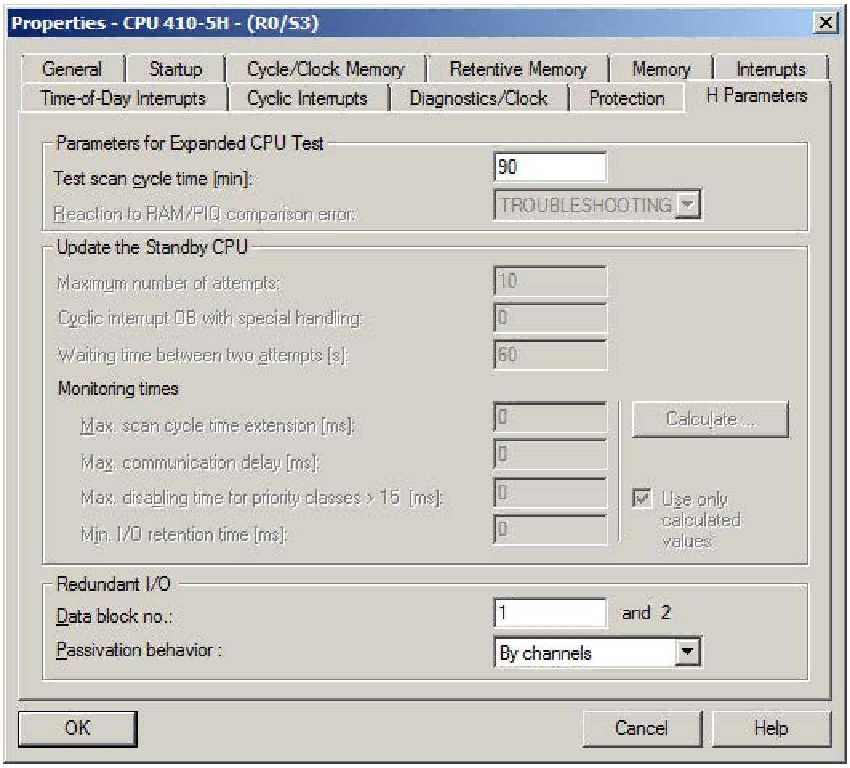
The test cycle time (default setting: 90 minutes) indicates the time taken for a complete background self-test.

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).



Properties - CPU 410-5H - (R0/S3)

Parameters for Expanded CPU Test

Test scan cycle time [min]: 90

Reaction to RAM/PIQ comparison error: TROUBLESHOOTING

Update the Standby CPU

Maximum number of attempts: 10

Cyclic interrupt OB with special handling: 0

Waiting time between two attempts [s]: 60

Monitoring times

Max. scan cycle time extension [ms]: 0

Max. communication delay [ms]: 0

Max. disabling time for priority classes > 15 [ms]: 0

Min. I/O retention time [ms]: 0

☑ Use only calculated values

Redundant I/O

Data block no.: 1 and 2

Passivation behavior : By channels

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

  To find out which events trigger the TROUBLESHOOTING operating state, please refer to the "SIMATIC S7-400H Fault-tolerant Systems" (https://support.industry.siemens.com/cs/ww/en/view/82478488) manual.

- 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).

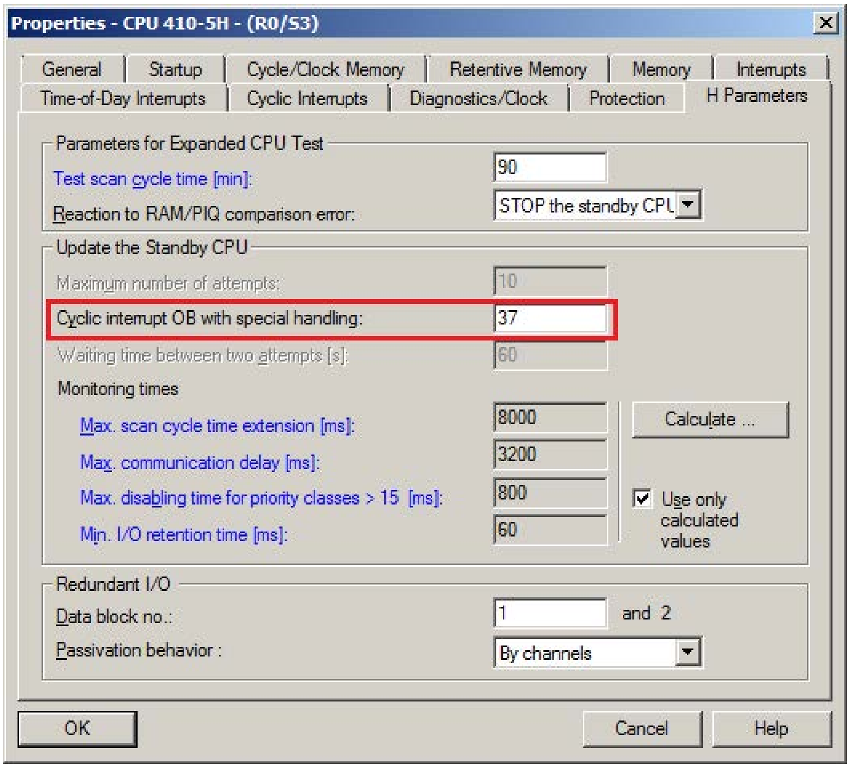
If this is only to occur at certain times defined by the plant operator, "Standby STEO" must be selected as the error reaction. Following this, maintenance personnel must carry out a self-test on both CPUs at an appropriate point in time, by performing a non-buffered CPU startup.

6.2.2 Cyclic interrupt OB with special handling

Priority class

In order to prevent time monitoring (F-CYC_CO 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.



Parameters for Expanded CPU Test

Test scan cycle time [min]: 90

Reaction to RAM/PIQ comparison error: STOP the standby CPU

Update the Standby CPU

Maximum number of attempts: 10

Cyclic interrupt OB with special handling: 37

Waiting time between two attempts [s]: 60

Monitoring times

Max. scan cycle time extension [ms]: 8000

Max. communication delay [ms]: 3200

Max. disabling time for priority classes > 15 [ms]: 800

Min. I/O retention time [ms]: 60

☑ Use only calculated values

Redundant I/O

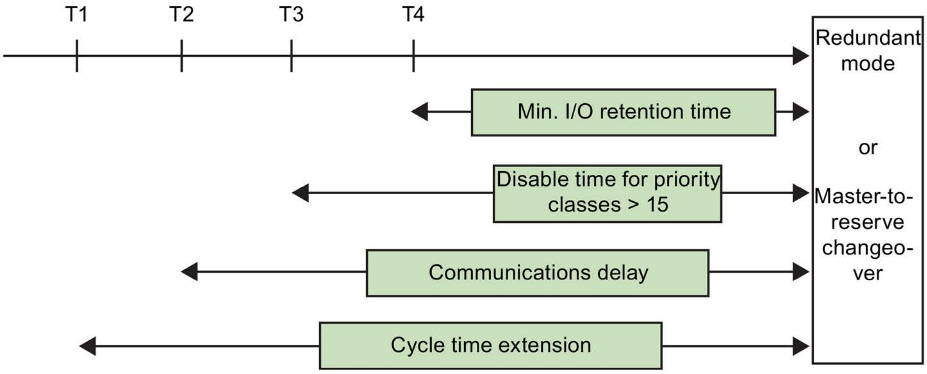
Data block no.: 1 and 2

Passivation behavior : By channels

6.2.3 Monitoring times

While the standby CPU is being updated, the FH system checks that the scan cycle time extension, the communication delay, and the disabling time for priority classes > 15 do not exceed the maximum values you have set. It also ensures that the minimum I/O retention time that has been configured is observed.

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 reserve 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 reserve CPU once the specified wait time has elapsed.

Note

For more information, see manual "SIMATIC S7-400H Fault-tolerant Systems" (https://support.industry.siemens.com/cs/ww/en/view/82478488).

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

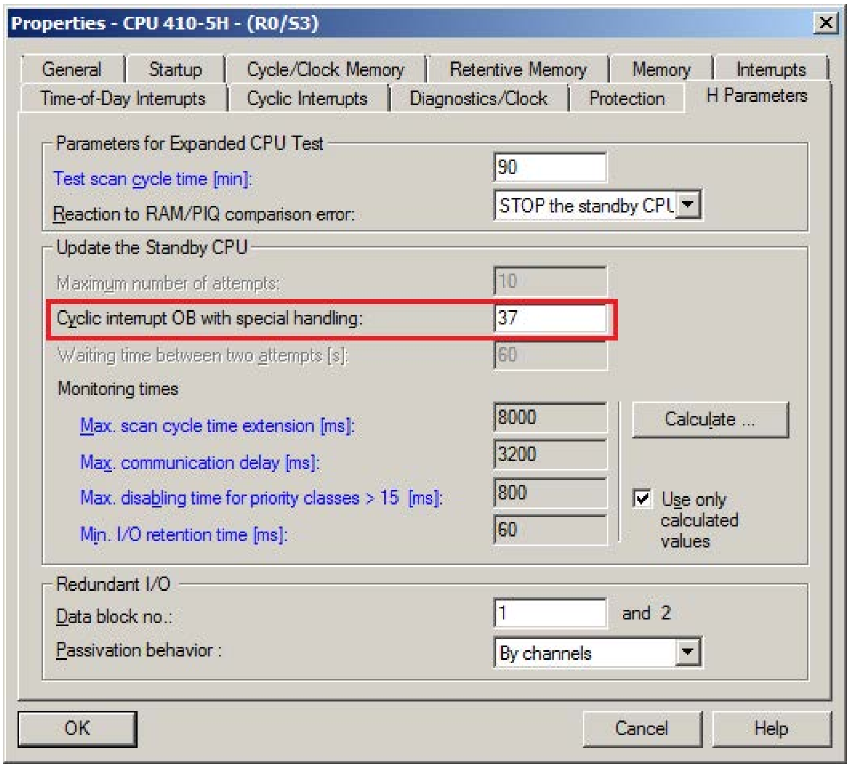
Calculation

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.



Properties - CPU 410-5H - (R0/S3)

Parameters for Expanded CPU Test
Test scan cycle time [min]: 90
Reaction to RAM/PIQ comparison error: STOP the standby CPU

Update the Standby CPU
Maximum number of attempts: 10
Cyclic interrupt OB with special handling: 37
Waiting time between two attempts [s]: 60
Monitoring times
Max. scan cycle time extension [ms]: 8000
Max. communication delay [ms]: 3200
Max. disabling time for priority classes > 15 [ms]: 800
Min. I/O retention time [ms]: 60
☑ Use only calculated values

Redundant I/O
Data block no.: 1 and 2
Passivation behavior : By channels

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

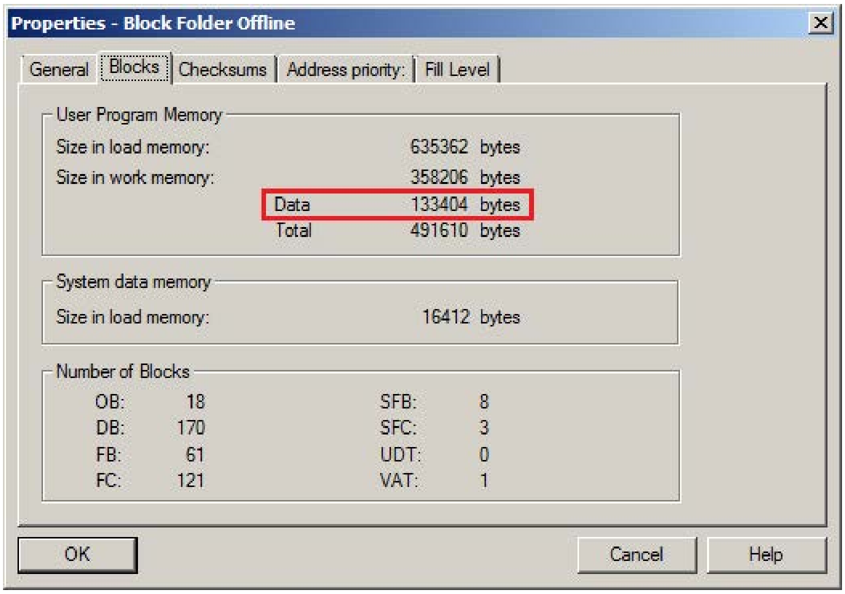
The runtime can be calculated using the TIME_BEG and TIME_END blocks.
You can find information on this in the "How do I set the runtime and time scale of a cyclic interrupt OB?" (https://support.industry.siemens.com/cs/ww/en/view/1023077) FAQ.

From PCS 7 V7.0 and higher, and an S7-400H CPU with FW V4.5 and higher, the runtimes 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".



User Program Memory

Size in load memory:	635362	bytes
Size in work memory:	358206	bytes
Data	133404	bytes
Total	491610	bytes

System data memory

Size in load memory:	16412	bytes

Number of Blocks

OB:	18	SFB:	8
DB:	170	SFC:	3
FB:	61	UDT:	0
FC:	121	VAT:	1

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).
- In the diagnostic buffer of the master CPU, search for messages relating to the master CPU's "Transition from coupling to updating", as well as for the message "Redundant mode".
- The "Maximum disabling time for priority classes > 15" must be greater than the time difference between the two messages. Make sure you factor reserve time of approximately 20% into your setting.

Note

For more information and corrective measures, see manual "SIMATIC S7-400H Fault-tolerant Systems" (https://support.industry.siemens.com/cs/ww/en/view/82478488).

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 on PROFINET IO in the system description PROFINET (https://support.industry.siemens.com/cs/ww/en/view/19292127).

Requirements for using PROFINET with F Systems

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

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

Recommended software requirements:

- PCS 7 V8.0 SP2 or higher
- S7 F Systems V6.1 SP1 or higher
- S7 F Systems Lib V1.3 or higher
- S7 F Configuration Pack V5.5 SP11 or higher

Hardware requirements:

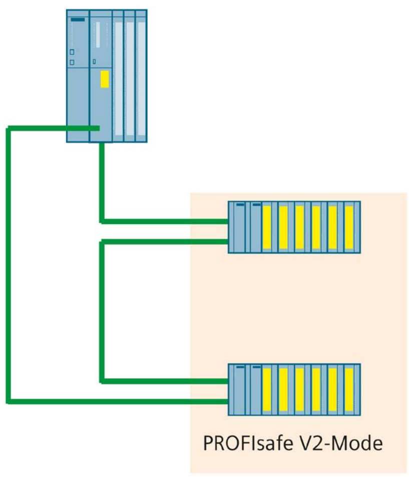
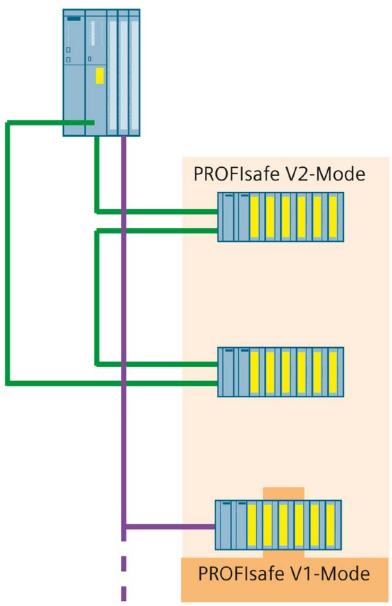
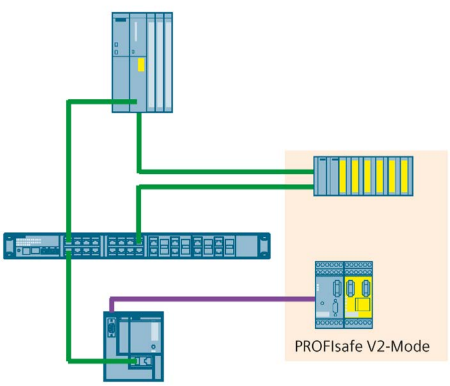
- CPU (CPU 412-5H, CPU 414-5H, CPU 416-5H, CPU 417-5H or CPU 410-5H)
- I/O modules:
  - SM 326F, DI 24xDC24V (6ES7 326-1BK02-0AB0)
  - SM 326F, DO 10xDC24V/2A, P-switching (6ES7 326-2BF10-0AB0)
  - SM 326F, DO 8xDC24V/2A, P-M-switching (6ES7 326-2BF41-0AB0)
  - SM 336F, AI 6x0/4...20mA HART (6ES7 336-4GE00-0AB0)

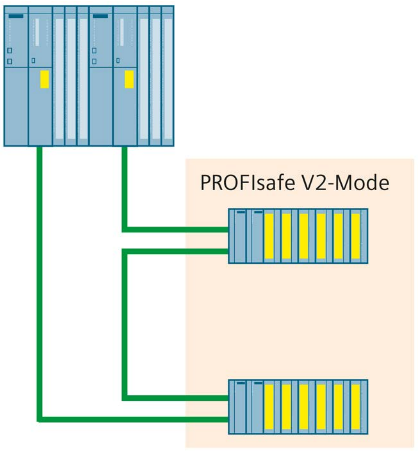
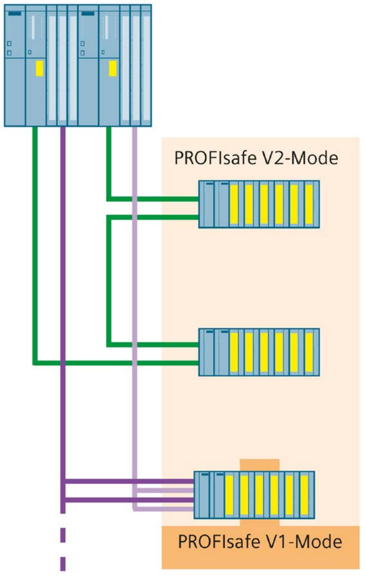
Note

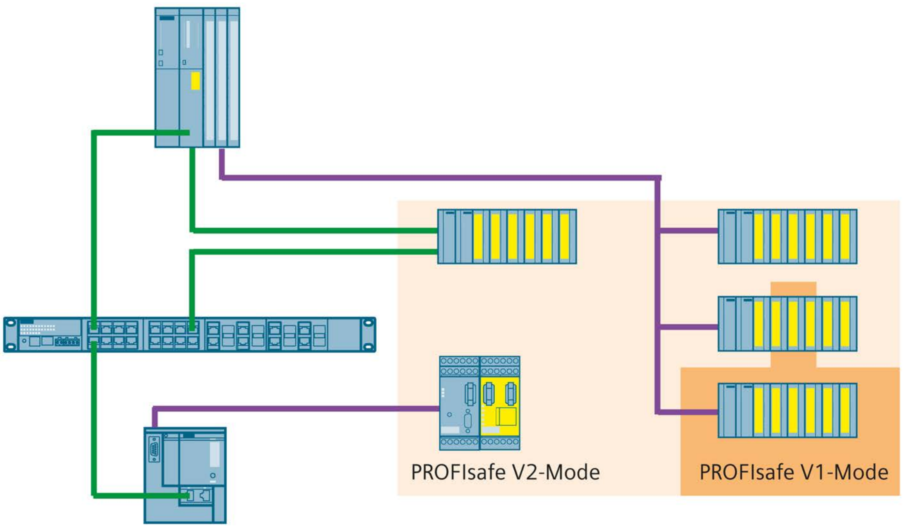
Before you use the fail-safe devices make sure that they support PROFIsafe V2 mode (F_Par_Version = 1) on PROFINET IO as well as in the downstream networks (PROFINET IO or PROFIBUS DP).

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	

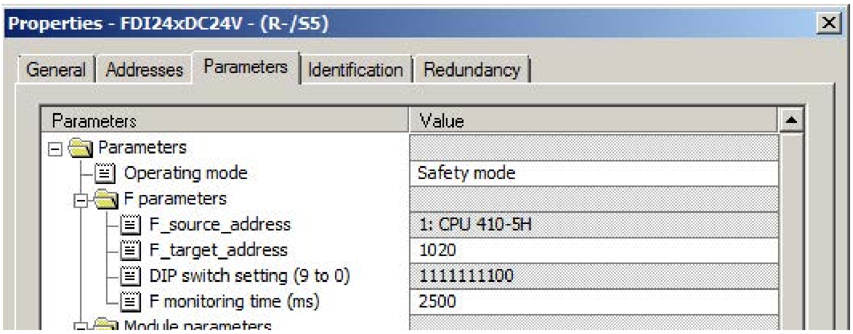
6.4 Setting system parameters for F-signal modules

Similar to standard modules, F-signal modules are configured in HW Config. This requires the corresponding F-Configuration 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 ET 200M 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.



Parameters	Value
Parameters	
Operating mode	Safety mode
F parameters	
F_source_address	1: CPU 410-5H
F_target_address	1020
DIP switch setting (9 to 0)	1111111100
F monitoring time (ms)	2500
Module parameters	

6.4.1 Operating mode

Safety mode

"Safety mode" is to be set for the signal modules.

6.4.2 PROFIsafe addresses

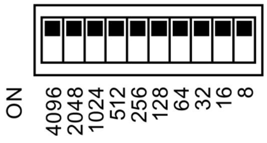
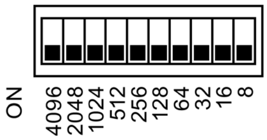
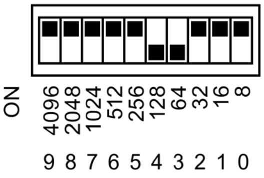
F source and destination addresses

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.

DIP switch settings

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
 ON 4096 2048 1024 512 256 128 64 32 16 8 or  ON 4096 2048 1024 512 256 128 64 32 16 8	All possible combinations that do not correspond to standard mode  ON 4096 2048 1024 512 256 128 64 32 16 8 9 8 7 6 5 4 3 2 1 0 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.

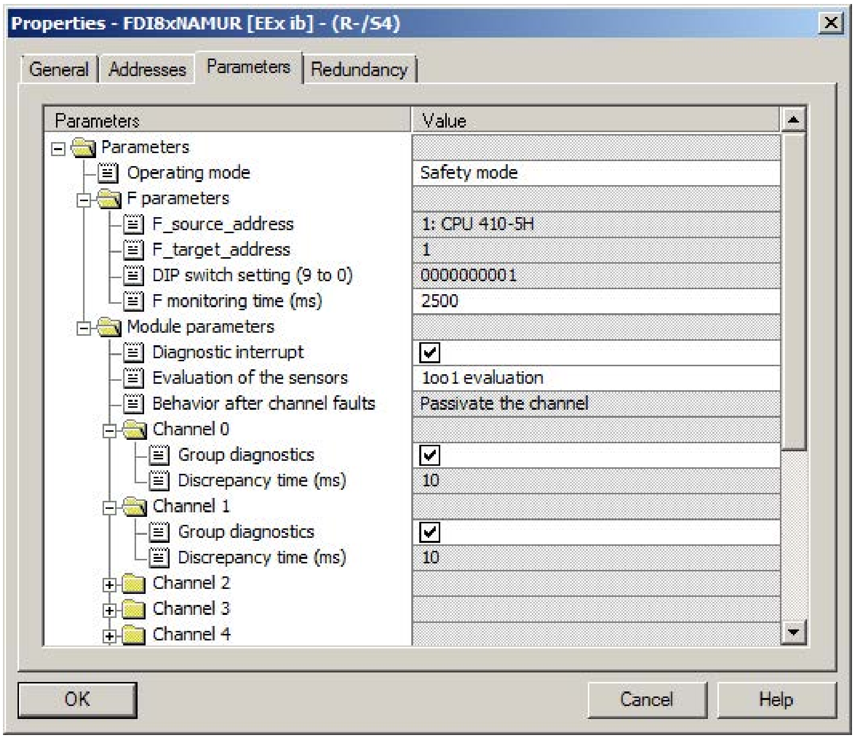
F monitoring time

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 133)" section.

6.4.3 Module parameters - general



Properties - FDI8xNAMUR [EEx ib] - (R-/S4)

Parameters	Value
Parameters	
Operating mode	Safety mode
F parameters	
F_source_address	1: CPU 410-5H
F_target_address	1
DIP switch setting (9 to 0)	0000000001
F monitoring time (ms)	2500
Module parameters	
Diagnostic interrupt	☑
Evaluation of the sensors	1oo1 evaluation
Behavior after channel faults	Passivate the channel
Channel 0	
Group diagnostics	☑
Discrepancy time (ms)	10
Channel 1	
Group diagnostics	☑
Discrepancy time (ms)	10
Channel 2	
Channel 3	
Channel 4	

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 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, group diagnostics needs to be activated whenever 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)
- 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

Due to the structure of fail-safe signal modules, it is not possible to make changes to their hardware configuration or to download them without the module being passivated. Passivating output modules involves establishing a safe state on all outputs, while passivating input modules involves the input drivers outputting the value 0.

In order to be able to use free channels on F-signal modules for expansion during operation, the channels in HW Config must be activated beforehand. 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.

SM326; DI 8 x NAMUR [EEx ib] (6ES7 326-1RF00-0AB0 / 6ES7 326-1RF01-0AB0)

- Determine operating mode
- Determine operating parameters
- Determine module parameters
- Activate group diagnostics for the channel
- Connect the channel to a resistor (e.g. 1 kohm)

SM326; DI 24 x DC 24V (6ES7 326-1BK00-0AB0 / 6ES7 326-1BK01-0AB0 / 6ES7 326-1BK02-0AB0)

- 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 kohm)

SM326; DO 10 x DC 24V/2A (6ES7 326-2BF01-0AB0)

- Determine operating mode
- Determine module parameters
- Activate group diagnostics for the channel
- To simulate an actuator, interconnect output with a resistor (e.g. 2.7 kilohms) downstream of the ground connection

SM326; F-DO 10 x DC 24V/2A PP (6ES7 326-2BF10-0AB0)

- Determine module parameters
- Activate group diagnostics for the channel
- To simulate an actuator, interconnect output with a resistor (e.g. 2.7 kilohms) downstream of the ground connection

M326; F-DO 8 x DC 24V/2A PM (6ES7 326-2BF40-0AB0 / 6ES7 326-2BF41-0AB0)

- Determine module parameters
- Activate group diagnostics for the channel
- To simulate an actuator, interconnect output with a resistor (e.g. 2.7 kilohms) downstream of the ground connection

SM 336; F-AI 6 x 13 Bit (6ES7 336-1HE00-0AB0)

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

SM 336; F-AI 6 x 0/4...20mA HART (6ES7 336-4GE00 0AB0)

- Determine module parameters
- Determine type of sensor interconnection
- Make channel-specific settings
- Make HART communication settings
- Interconnect plus input of channel with supply voltage via a resistor (e.g. 3.9 kilohms) and connect minus input to ground

EM; F-DI 8 x NAMUR Ex (6ES7 138-7FN00 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
- Provided the sensor supply comes from the module: Connect input to the sensor supply via a resistor
(e.g.: 1 kohm)

EM; F-DO 4 x 17.4V/40mA Ex (6ES7 138-7FD00 0AB0)

- Determine module parameters
- Activate group diagnostics for the channel
- To simulate an actuator, interconnect output with a resistor (e.g. 2.7 kilohms) downstream of the ground connection

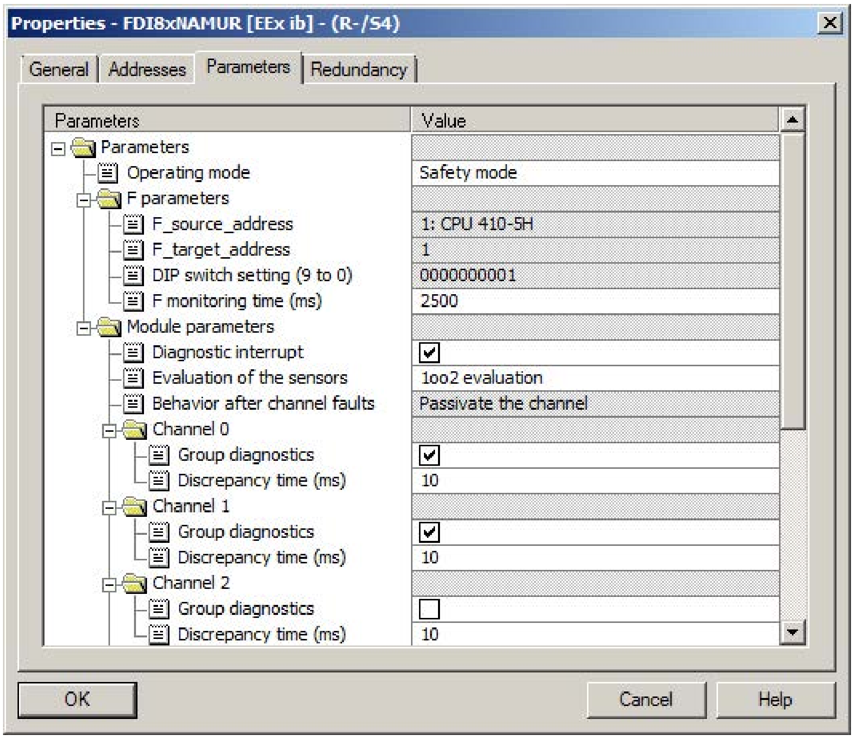
EM; F-AI 4 x 0/4...20mA Ex HART (6ES7 138-7FA00 0AB0)

- Determine module parameters
- Make channel-specific settings
- Make HART communication settings
- Connect the plus input of the channel via a resistor (for example 3.9 Kilohm) to the minus input of the channel

Note

You can find more information on activating channels during operation in the "Programming with F/FH systems - Changing parameters on fail-safe I/Os" (https://support.industry.siemens.com/cs/ww/en/view/21382997) FAQ.

6.4.5 Parameter assignment for SM326; DI 8 x NAMUR



Properties - FDI8xNAMUR [EEx ib] - (R-/S4)

Parameters	Value
Parameters	
Operating mode	Safety mode
F parameters	
F_source_address	1: CPU 410-5H
F_target_address	1
DIP switch setting (9 to 0)	0000000001
F monitoring time (ms)	2500
Module parameters	
Diagnostic interrupt	☑
Evaluation of the sensors	1oo2 evaluation
Behavior after channel faults	Passivate the channel
Channel 0	
Group diagnostics	☑
Discrepancy time (ms)	10
Channel 1	
Group diagnostics	☑
Discrepancy time (ms)	10
Channel 2	
Group diagnostics	☐
Discrepancy time (ms)	10

Sensor evaluation

- 1oo1 (1v1) evaluation

  A sensor connected to the F signal module via a single channel

- 1oo2 (2v2) 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 by means of voting in the CPU.
- 2-channel – SIL 3 (voting on module)

Group diagnostics

Group diagnostics must be activated for all used channels.

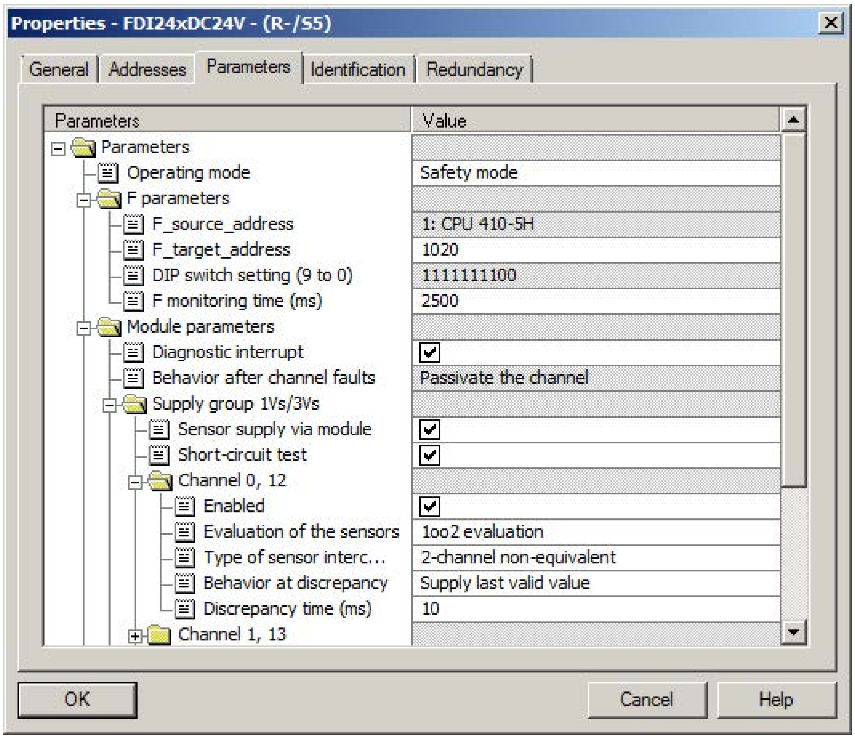
Discrepancy time

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.

6.4.6 Parameter assignment for SM326; DI 24 x DC 24V



Parameters	Value
Parameters	
Operating mode	Safety mode
F parameters	
F_source_address	1: CPU 410-5H
F_target_address	1020
DIP switch setting (9 to 0)	1111111100
F monitoring time (ms)	2500
Module parameters	
Diagnostic interrupt	☑
Behavior after channel faults	Passivate the channel
Supply group 1Vs/3Vs	
Sensor supply via module	☑
Short-circuit test	☑
Channel 0, 12	
Enabled	☑
Evaluation of the sensors	1oo2 evaluation
Type of sensor interc...	2-channel non-equivalent
Behavior at discrepancy	Supply last valid value
Discrepancy time (ms)	10
Channel 1, 13	

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 module.

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 diagnostics interrupt on the CPU and send a corresponding process control message to the OS.

Sensor evaluation

- 1oo1 (1v1) evaluation
  A sensor connected to the F signal module via a single channel.
- 1oo2 (2v2) 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 by means of voting in the CPU.
- 2-channel – SIL 3 (voting 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 parameterized, 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.

- "Provide last valid value" or
- "provide 0 value"

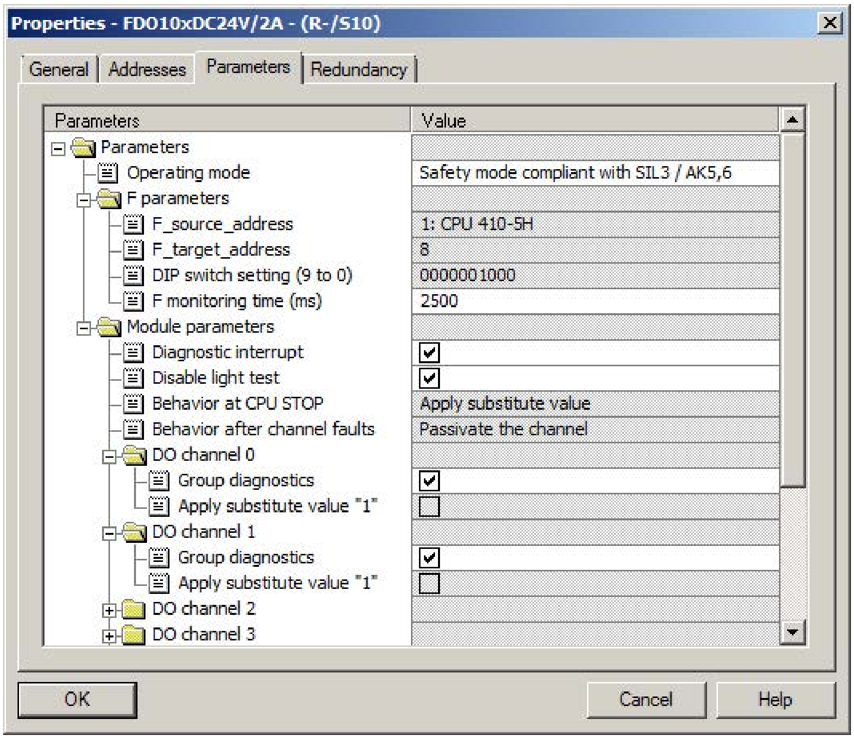
Discrepancy time

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.

6.4.7 Parameter assignment for SM326; DO 10 x DC 24V/2A (6ES7326-2BF01-0AB0)



Parameters	Value
Parameters	
Operating mode	Safety mode compliant with SIL3 / AK5,6
F parameters	
F_source_address	1: CPU 410-5H
F_target_address	8
DIP switch setting (9 to 0)	0000001000
F monitoring time (ms)	2500
Module parameters	
Diagnostic interrupt	☑
Disable light test	☑
Behavior at CPU STOP	Apply substitute value
Behavior after channel faults	Passivate the channel
DO channel 0	
Group diagnostics	☑
Apply substitute value "1"	☐
DO channel 1	
Group diagnostics	☑
Apply substitute value "1"	☐
DO channel 2	
DO channel 3	

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

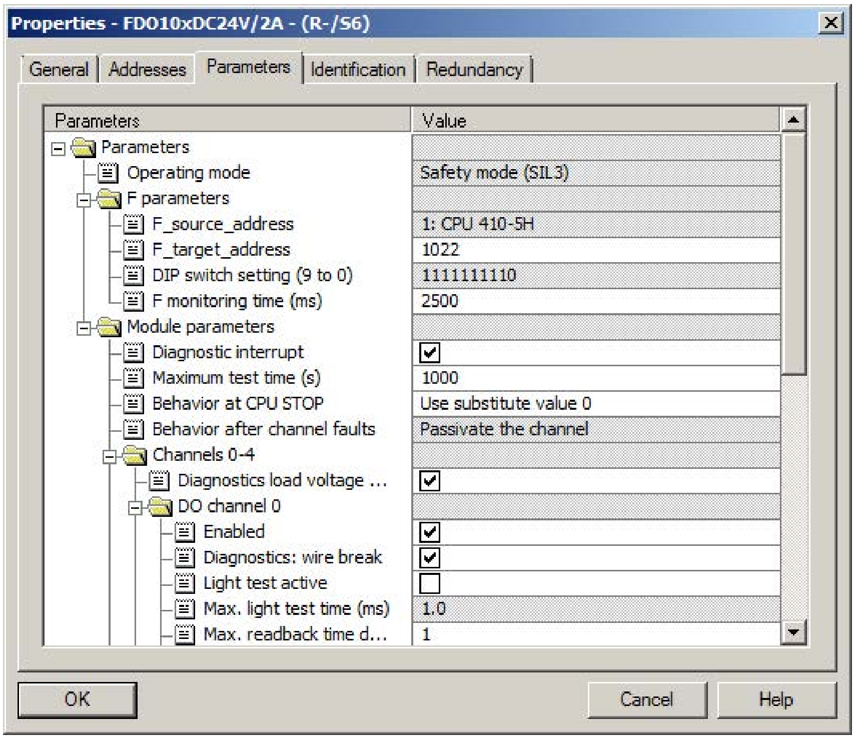
Deactivating the light test

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.

6.4.8 Parameter assignment for SM326; F-DO 10 x DC 24V/2A PP (6ES7326-2BF10-0AB0)



Parameters	Value
Parameters	
Operating mode	Safety mode (SIL3)
F parameters	
F_source_address	1: CPU 410-5H
F_target_address	1022
DIP switch setting (9 to 0)	1111111110
F monitoring time (ms)	2500
Module parameters	
Diagnostic interrupt	☑
Maximum test time (s)	1000
Behavior at CPU STOP	Use substitute value 0
Behavior after channel faults	Passivate the channel
Channels 0-4	
Diagnostics load voltage ...	☑
DO channel 0	
Enabled	☑
Diagnostics: wire break	☑
Light test active	□
Max. light test time (ms)	1.0
Max. readback time d...	1

Figure 6-1

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 long enough if the affected channel activates large capacitive loads. If the maximum light test time is set too short for a controlled capacitive load, the output channel is passivated, because loading does not occur within the parameterized 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 response time is extended by the configured maximum light test time, the light test 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 maximum light test time which leads to the output channel becoming passivated sporadically, set the next highest value of the maximum light period.

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.

The maximum readback time should be set sufficiently long enough if the affected channel activates large capacitive loads. If the maximum readback time is set too short for a connected capacitive load, the output channel is passivated, because discharge does not occur within the parameterized 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 which leads to the output channel becoming passivated sporadically, set the next highest value of the 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).

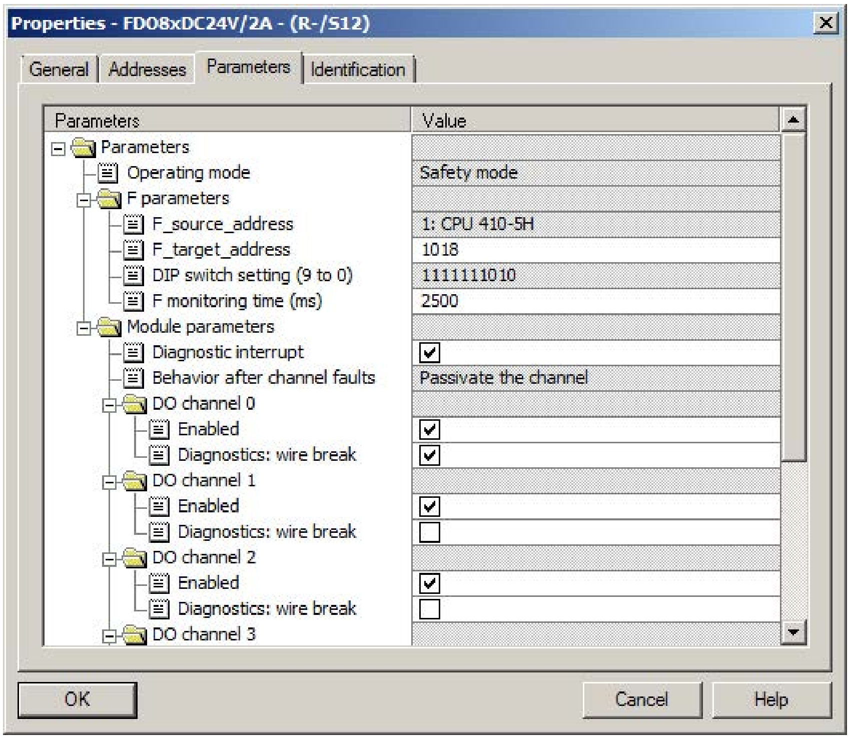
Redundant interconnection

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.

6.4.9 Parameter assignment for SM326; F-DO 8 x DC24 V/2A PM



Properties - FDO8xDC24V/2A - (R-/S12)

Parameters	Value
Parameters	
Operating mode	Safety mode
F parameters	
F_source_address	1: CPU 410-5H
F_target_address	1018
DIP switch setting (9 to 0)	1111111010
F monitoring time (ms)	2500
Module parameters	
Diagnostic interrupt	☑
Behavior after channel faults	Passivate the channel
DO channel 0	
Enabled	☑
Diagnostics: wire break	☑
DO channel 1	
Enabled	☑
Diagnostics: wire break	□
DO channel 2	
Enabled	☑
Diagnostics: wire break	□
DO channel 3	

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.

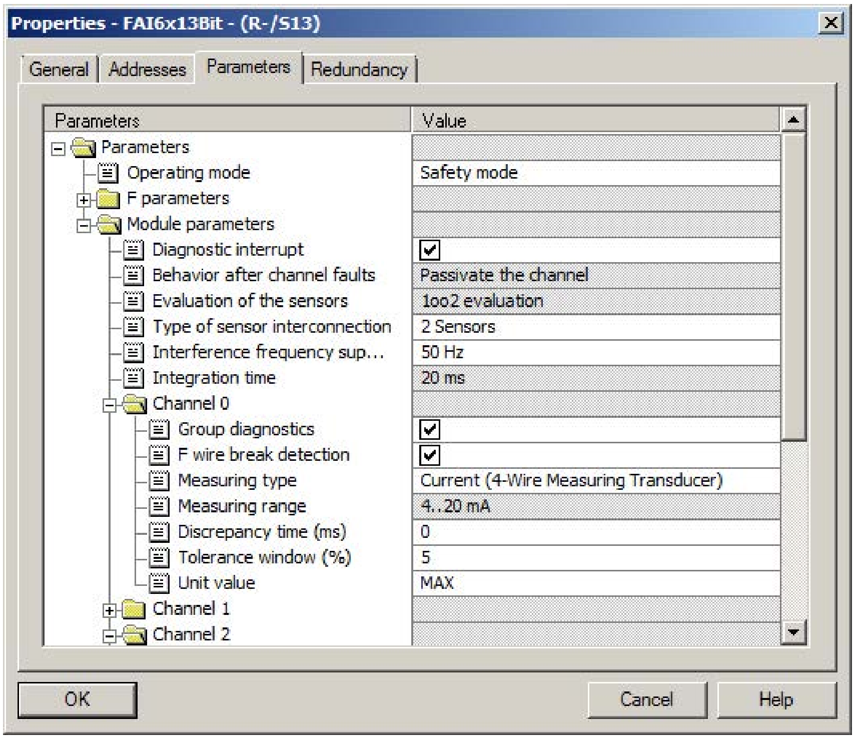
Activated

Activates channel processing

Diagnostics: Wire break

Activates wire-break monitoring on the channel

6.4.10 Assigning parameters for the SM336; AI 6 x 13Bit



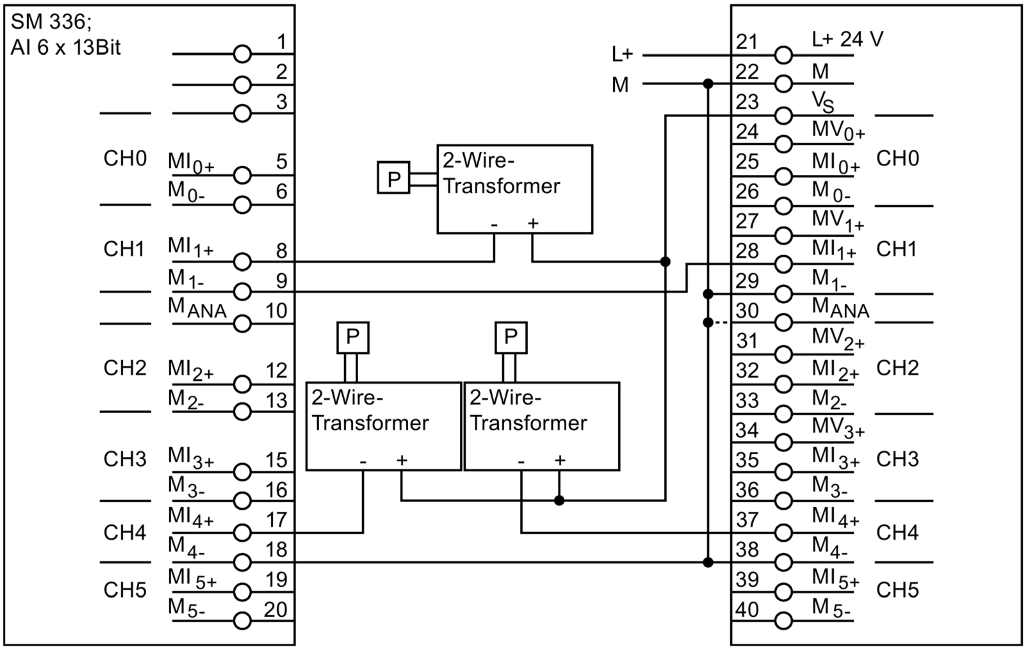
Parameters	Value
Parameters	
Operating mode	Safety mode
F parameters	
Module parameters	
Diagnostic interrupt	☑
Behavior after channel faults	Passivate the channel
Evaluation of the sensors	1oo2 evaluation
Type of sensor interconnection	2 Sensors
Interference frequency sup...	50 Hz
Integration time	20 ms
Channel 0	
Group diagnostics	☑
F wire break detection	☑
Measuring type	Current (4-Wire Measuring Transducer)
Measuring range	4..20 mA
Discrepancy time (ms)	0
Tolerance window (%)	5
Unit value	MAX
Channel 1	
Channel 2	

Sensor evaluation (analog inputs)

- 1oo2 evaluation

  1 sensor connected to the module via a single-channel redundant connection (voting on module). The module has 6 redundant SIL 3-compatible 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, however, the type of sensor you are using (e.g. a gas sensor) means that you do need to process signals that fall below this range, you can deactivate F wire-break detection. In this case, a current of < 1.18 mA will produce an underflow message.

For more information, please refer to the following FAQ: "How can process signals that are less than 4 mA be used with a 4 to 20 mA analog input module (F technology)?" (https://support.industry.siemens.com/cs/ww/en/view/23707365).

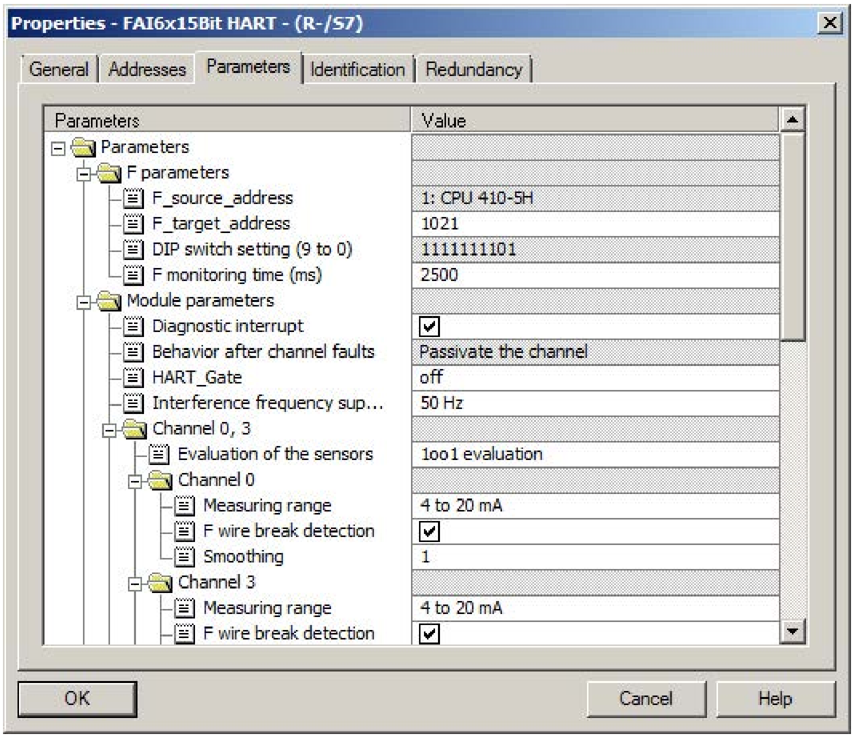
Discrepancy handling (analog inputs)

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

For details of possible types of interconnection, please refer to the FAQ titled "Wiring & Voting Architectures for ET 200M F-AIs".
(https://support.industry.siemens.com/cs/ww/en/view/24690377)

6.4.11 Assigning parameters for the SM336; F-AI 6 x 0/4...20mA HART



Parameters	Value
Parameters	
F parameters	
F_source_address	1: CPU 410-5H
F_target_address	1021
DIP switch setting (9 to 0)	1111111101
F monitoring time (ms)	2500
Module parameters	
Diagnostic interrupt	☑
Behavior after channel faults	Passivate the channel
HART_Gate	off
Interference frequency sup...	50 Hz
Channel 0, 3	
Evaluation of the sensors	1oo1 evaluation
Channel 0	
Measuring range	4 to 20 mA
F wire break detection	☑
Smoothing	1
Channel 3	
Measuring range	4 to 20 mA
F wire break detection	☑

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).

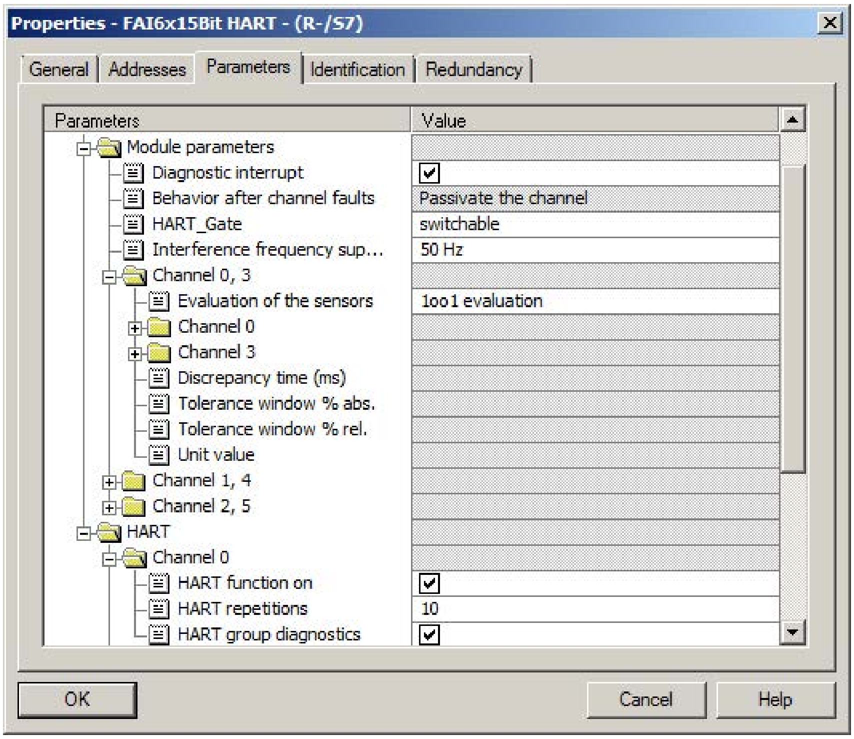
Filter

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.



Parameters	Value
Module parameters	
Diagnostic interrupt	☑
Behavior after channel faults	Passivate the channel
HART_Gate	switchable
Interference frequency sup...	50 Hz
Channel 0, 3	
Evaluation of the sensors	1oo1 evaluation
Channel 0	
Channel 3	
Discrepancy time (ms)	
Tolerance window % abs.	
Tolerance window % rel.	
Unit value	
Channel 1, 4	
Channel 2, 5	
HART	
Channel 0	
HART function on	☑
HART repetitions	10
HART group diagnostics	☑

HART

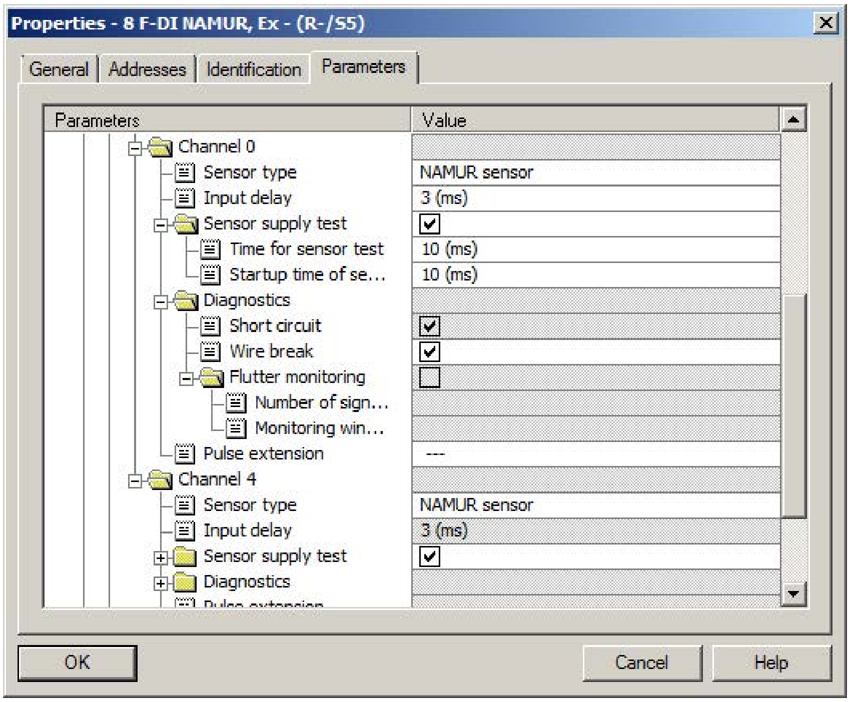
Here, you can switch off HART communication on specific channels in a non-safety-related manner, as well as enable HART diagnostics options and determine how often the module will attempt to establish HART communication with the transducer before a message is issued.

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

See also

Software components (Page 11)

6.4.12 Parameter assignment for EM 8 F-DI NAMUR Ex

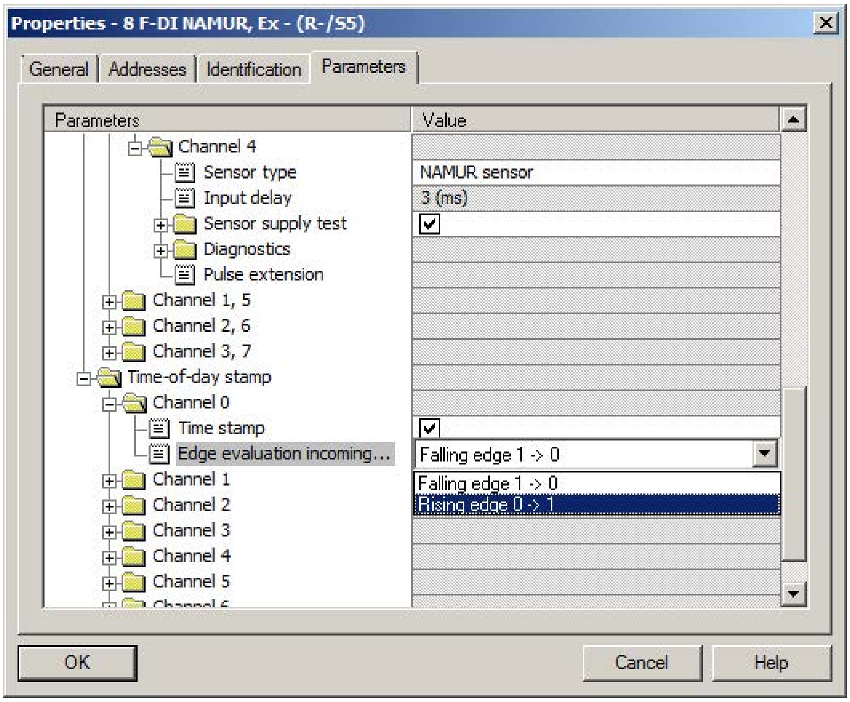


Parameters	Value
Channel 0	
Sensor type	NAMUR sensor
Input delay	3 (ms)
Sensor supply test	☑
Time for sensor test	10 (ms)
Startup time of se...	10 (ms)
Diagnostics	
Short circuit	☑
Wire break	☑
Flutter monitoring	□
Number of sign...	
Monitoring win...	
Pulse extension	---
Channel 4	
Sensor type	NAMUR sensor
Input delay	3 (ms)
Sensor supply test	☑
Diagnostics	
Pulse extension	

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 necessary"
  If you have configured "Test 0 signal necessary", 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 (2v2) non-equivalent evaluation" – then a 0 signal must be present at the lower value channel of the pair.
- "Test 0 signal not necessary"
  If you have configured "Test 0 signal not necessary", a discrepancy error is considered lifted if no discrepancy is present any more at both input channels.



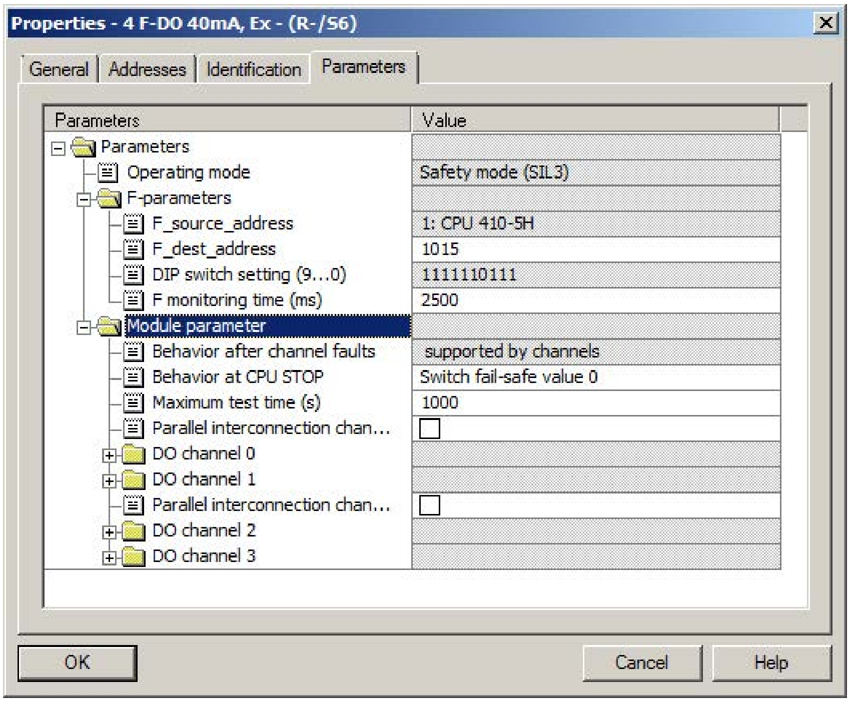
Properties - 8 F-DI NAMUR, Ex - (R-/S5)

Parameters	Value
Channel 4	
Sensor type	NAMUR sensor
Input delay	3 (ms)
Sensor supply test	☑
Diagnostics	
Pulse extension	
Channel 1, 5	
Channel 2, 6	
Channel 3, 7	
Time-of-day stamp	
Channel 0	
Time stamp	☑
Edge evaluation incoming...	Falling edge 1 -> 0
Channel 1	Falling edge 1 -> 0 Rising edge 0 -> 1
Channel 2	
Channel 3	
Channel 4	
Channel 5	
Channel 6	

Time stamp

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

6.4.13 Parameter assignment for EM 4 F-DO Ex 17.4V/40mA



Parameters	Value
Parameters	
Operating mode	Safety mode (SIL3)
F-parameters	
F_source_address	1: CPU 410-5H
F_dest_address	1015
DIP switch setting (9...0)	1111110111
F monitoring time (ms)	2500
Module parameter	
Behavior after channel faults	supported by channels
Behavior at CPU STOP	Switch fail-safe value 0
Maximum test time (s)	1000
Parallel interconnection chan...	□
DO channel 0	
DO channel 1	
Parallel interconnection chan...	□
DO channel 2	
DO channel 3	

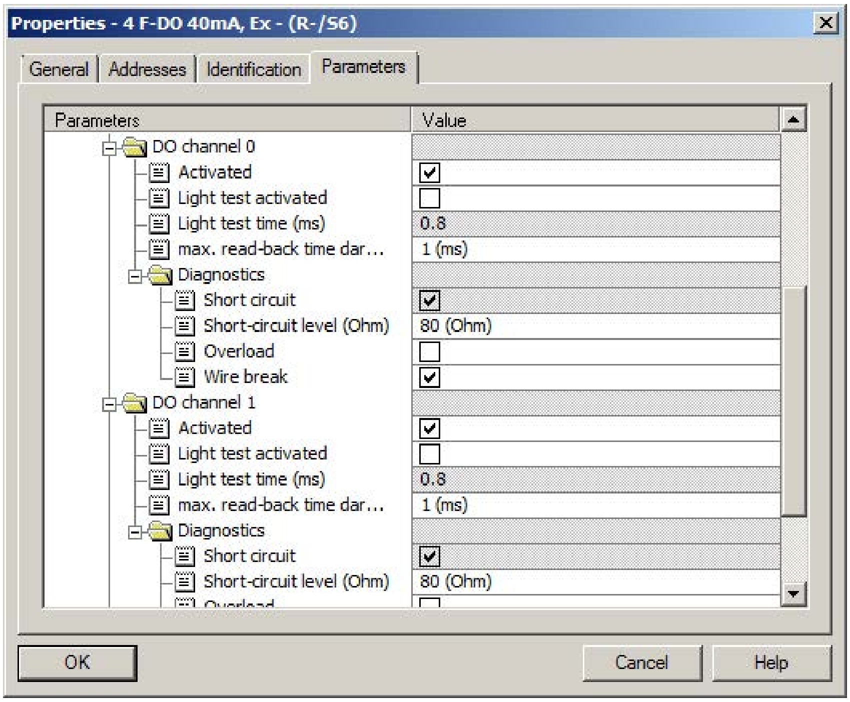
"Maximum test time" parameter

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



Properties - 4 F-DO 40mA, Ex - (R-/S6)

Parameters	Value
DO channel 0	
Activated	☑
Light test activated	□
Light test time (ms)	0.8
max. read-back time dar...	1 (ms)
Diagnostics	
Short circuit	☑
Short-circuit level (Ohm)	80 (Ohm)
Overload	□
Wire break	☑
DO channel 1	
Activated	☑
Light test activated	□
Light test time (ms)	0.8
max. read-back time dar...	1 (ms)
Diagnostics	
Short circuit	☑
Short-circuit level (Ohm)	80 (Ohm)
Overload	□

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.

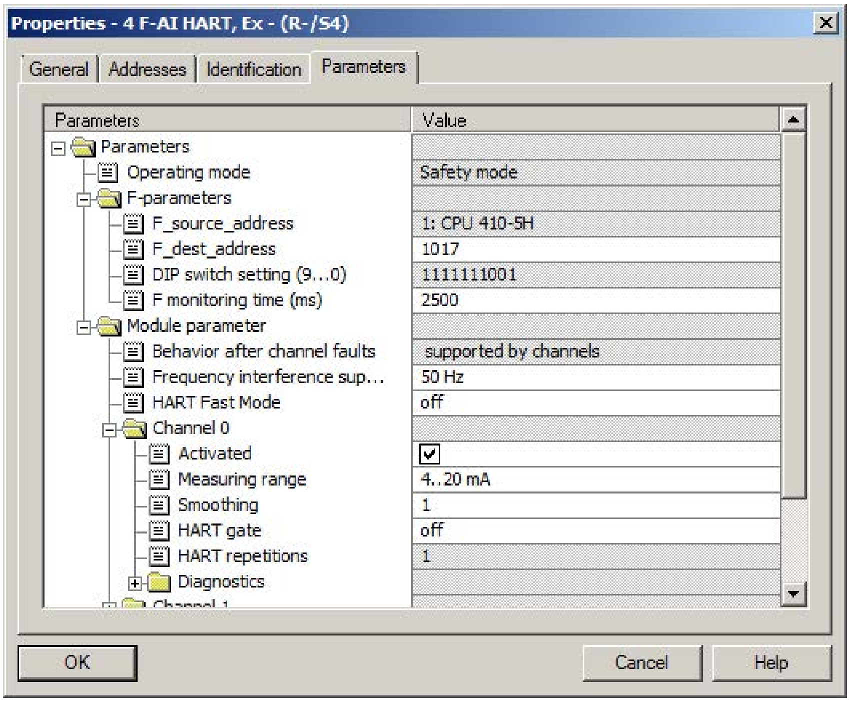
This means that in the range between employing the current limiting (the inflection point on the output curve) and the reaching of the short-circuit level, no diagnostics are transmitted. The channel remains switched on until the load undershoots the short-circuit level.

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 diagnostic 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.

6.4.14 Parameter assignment for EM 4 F-AI Ex HART



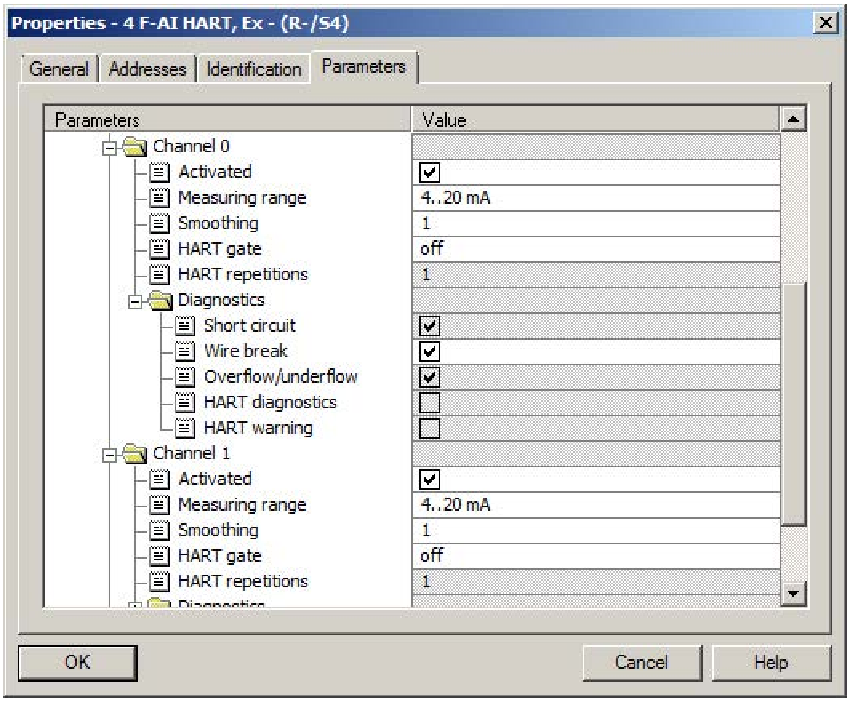
Properties - 4 F-AI HART, Ex - (R-/S4)

Parameters	Value
Parameters	
Operating mode	Safety mode
F-parameters	
F_source_address	1: CPU 410-5H
F_dest_address	1017
DIP switch setting (9...0)	1111111001
F monitoring time (ms)	2500
Module parameter	
Behavior after channel faults	supported by channels
Frequency interference sup...	50 Hz
HART Fast Mode	off
Channel 0	
Activated	☑
Measuring range	4..20 mA
Smoothing	1
HART gate	off
HART repetitions	1
Diagnostics	
Channel 1	

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 every further HART command with a set SHC bit, the electronic module reserves the HART command processing for this channel again for another 2 seconds. If a HART command is detected for this channel without a set SHC bit, or if no further command for this channel arrives within 2 seconds of the previous HART command, then the electronic module reverts to "normal" HART command processing. Result: All HART channels are re-processed.



Parameters	Value
Channel 0	
Activated	☑
Measuring range	4..20 mA
Smoothing	1
HART gate	off
HART repetitions	1
Diagnostics	
Short circuit	☑
Wire break	☑
Overflow/underflow	☑
HART diagnostics	☐
HART warning	☐
Channel 1	
Activated	☑
Measuring range	4..20 mA
Smoothing	1
HART gate	off
HART repetitions	1
Diagnostics	

HART diagnostics

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

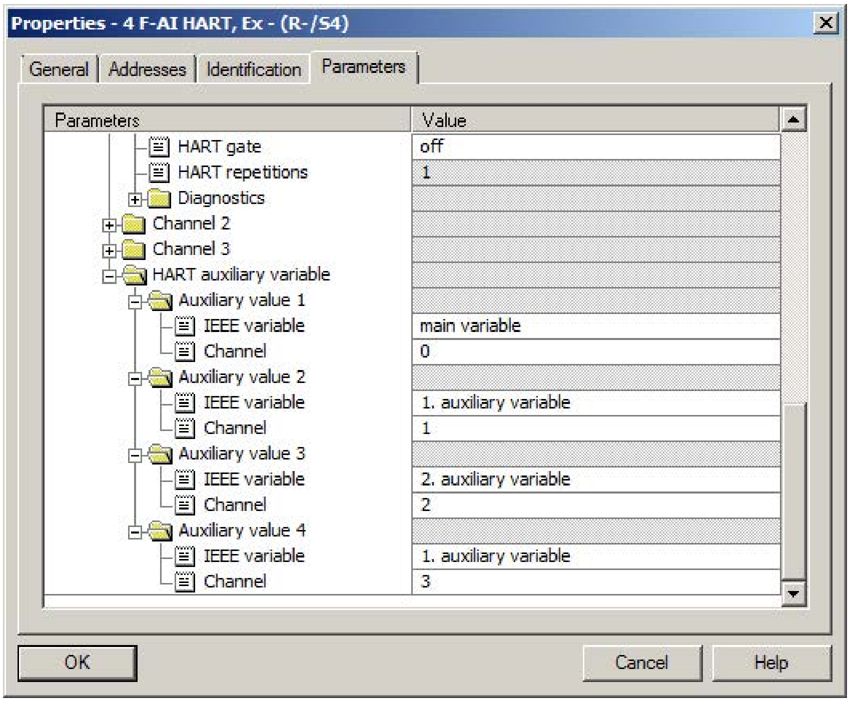
- HART analog output current specified
- HART analog output current saturated
- HART communication error
- HART primary variable outside limits
- HART secondary variable outside limits
- HART error function HART device

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



Parameters	Value
HART gate	off
HART repetitions	1
Diagnostics	
Channel 2	
Channel 3	
HART auxiliary variable	
Auxiliary value 1	
IEEE variable	main variable
Channel	0
Auxiliary value 2	
IEEE variable	1. auxiliary variable
Channel	1
Auxiliary value 3	
IEEE variable	2. auxiliary variable
Channel	2
Auxiliary value 4	
IEEE variable	1. auxiliary variable
Channel	3

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

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 or several different ET 200Ms. Where F signal modules configured with redundancy are concerned, 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.

Where fail-safe signal input modules configured with redundancy are concerned, it is possible to draw a distinction between 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).

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 undergo further processing in the logic or be reported with a message block, e.g. MESSAGE.

The F_CH_AI does not perform a discrepancy analysis. 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.

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.

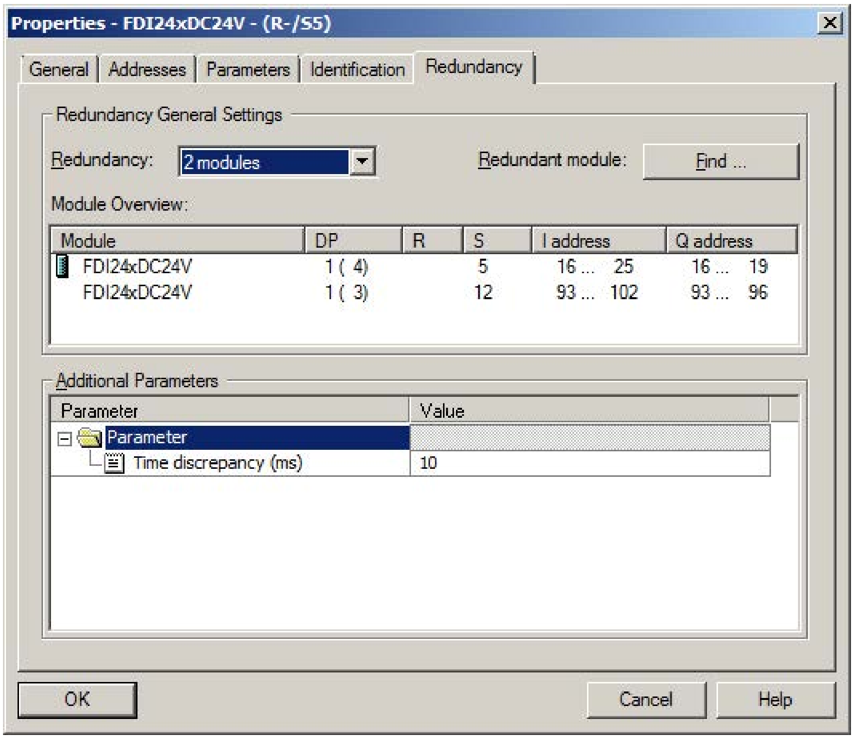
Procedure

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 applied automatically 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.



Properties - FDI24xDC24V - (R-/S5)

Redundancy: 2 modules

Module Overview:

Module	DP	R	S	I address	Q address
FDI24xDC24V	1 (4)		5	16 ... 25	16 ... 19
FDI24xDC24V	1 (3)		12	93 ... 102	93 ... 96

Parameter	Value
Parameter	
Time discrepancy (ms)	10

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. In both modules, configure a "HART field device" on the relevant 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

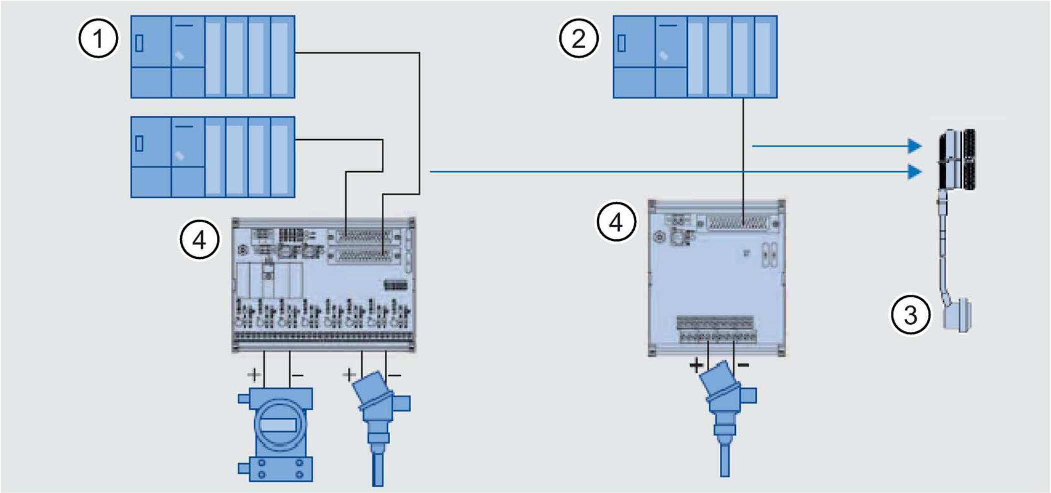
You can find additional information on configuring redundant I/O modules in the "SIMATIC Process Control System PCS 7 Compendium Part A - Configuration Guidelines".

6.6 Marshalled Termination Assemblies (MTAs)

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

For more information, please refer to the "ET 200M Marshalled Termination Assemblies Remote I/O Modules" (https://support.industry.siemens.com/cs/ww/en/view/22091986) FAQ.

6.7 "Wiring and Voting" architectures for ET 200M

Note

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

- Wiring & Voting Architectures for ET 200M F-AIs (https://support.industry.siemens.com/cs/ww/en/view/24690377)
- F systems: "Wiring and Voting" architectures for ET200M F-DIs und F-DOs (https://support.industry.siemens.com/cs/ww/en/view/37236961)

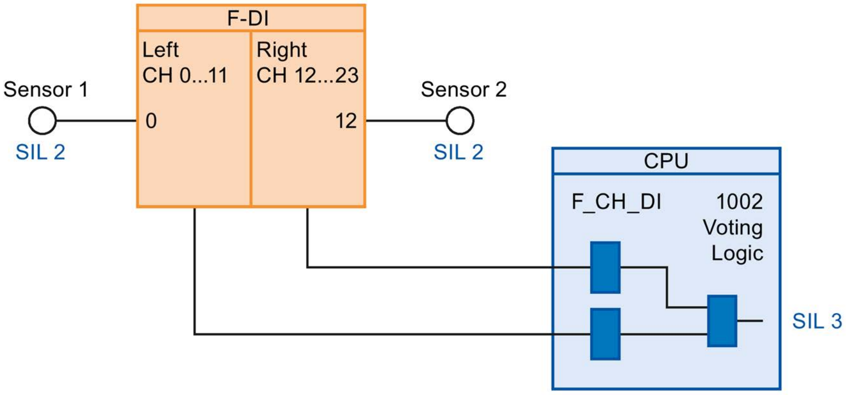
1oo2 voting of fail-safe input signals can be implemented in both the F signal module and the user program.

2oo3 voting of three fail-safe signals can be implemented in CFC using a function block, or in the Safety Matrix.

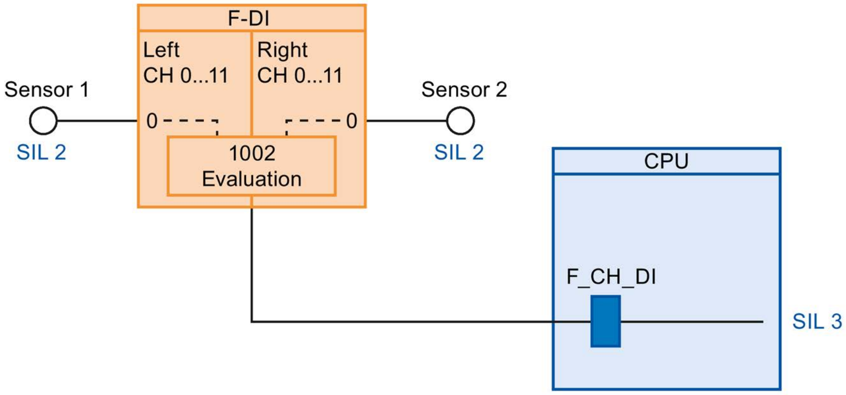
6.7.1 Voting on the module or in the CPU

Various types of voting are shown in the examples below.

SIL 3 by means of voting in the F-user program



SIL 3 by means of voting in module



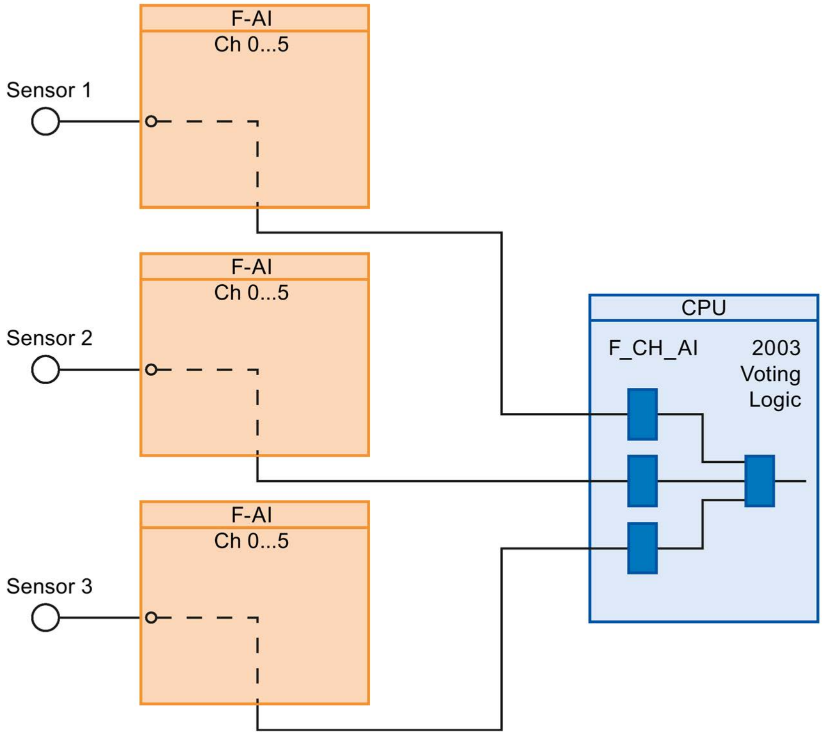
Note

Suitable sensors are required to achieve this SIL3 wiring.

6.7.2 2oo3 Voting 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.

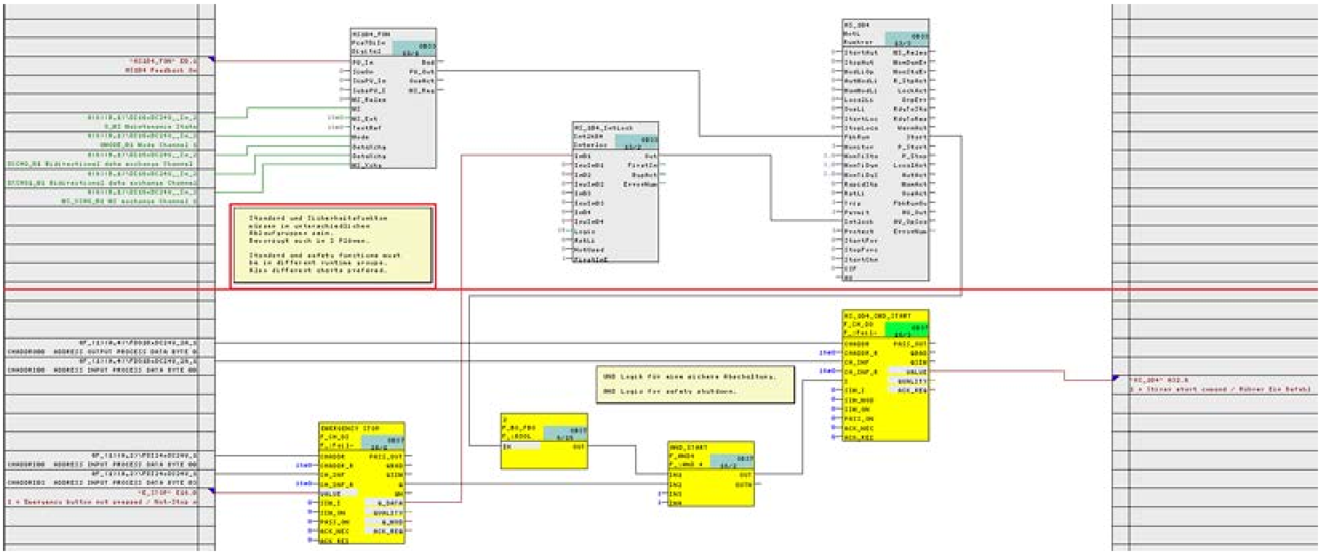


Configuring the safety program 7

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.



Standard and safety functions must be in different runtime groups. Also different charts prefered.
Logic for safety shutdown.
EMERGENCY STOP

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.

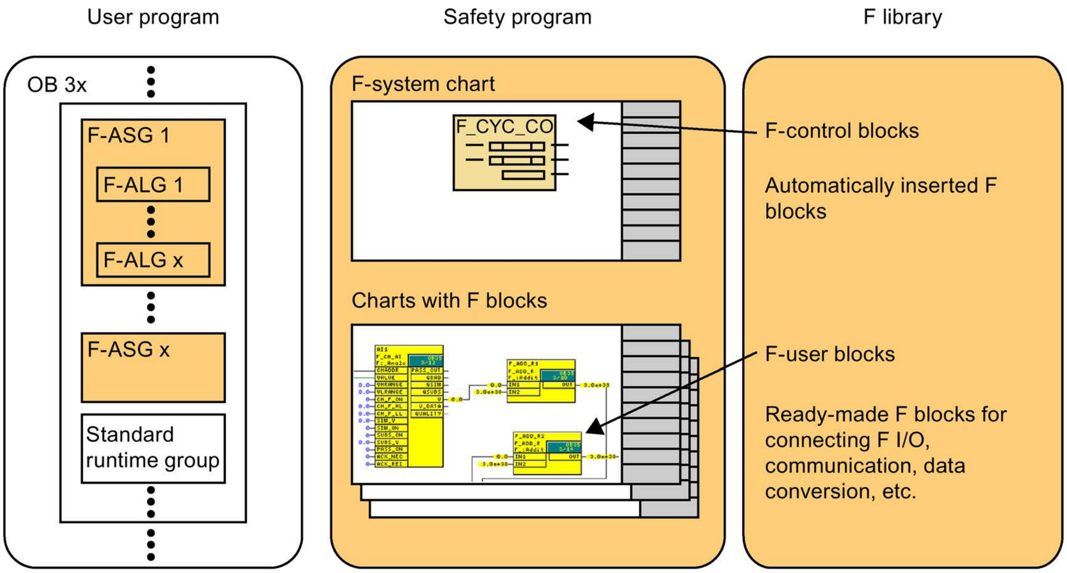
The user program in the CPU can be created from F-and non-F blocks. The F-program is configured in separate runtime groups.

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.

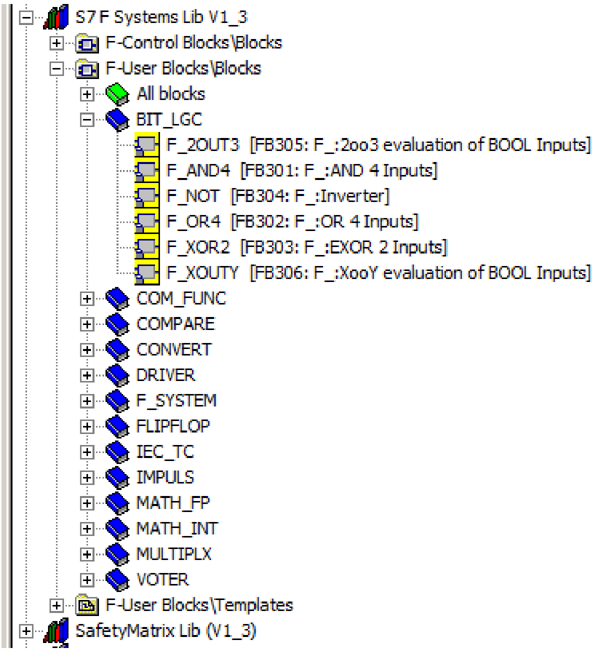
7.2 Creating the safety program

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 a CPU 41x-xH.

Library

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



- S7 F Systems Lib V1_3
  - F-Control Blocks\Blocks
  - F-User Blocks\Blocks
    - All blocks
    - BIT_LGC
      - F_2OUT3 [FB305: F_:2oo3 evaluation of BOOL Inputs]
      - F_AND4 [FB301: F_:AND 4 Inputs]
      - F_NOT [FB304: F_:Inverter]
      - F_OR4 [FB302: F_:OR 4 Inputs]
      - F_XOR2 [FB303: F_:EXOR 2 Inputs]
      - F_XOUTY [FB306: F_:XooY evaluation of BOOL Inputs]
    - COM_FUNC
    - COMPARE
    - CONVERT
    - DRIVER
    - F_SYSTEM
    - FLIPFLOP
    - IEC_TC
    - IMPULS
    - MATH_FP
    - MATH_INT
    - MULTIPLX
    - VOTER
  - F-User Blocks\Templates
- SafetyMatrix Lib (V1_3)

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 chart container "Insert New Object > CFC" in the SIMATIC Manager
- Directly in the PH or process object view in the relevant hierarchy folder "Insert New Object > CFC"

Inserting F blocks

Blocks are dragged from the "S7 F Systems Lib V1_3" library ("Failsafe Blocks (V1_2)" > "F-User Blocks") and dropped into the chart. 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

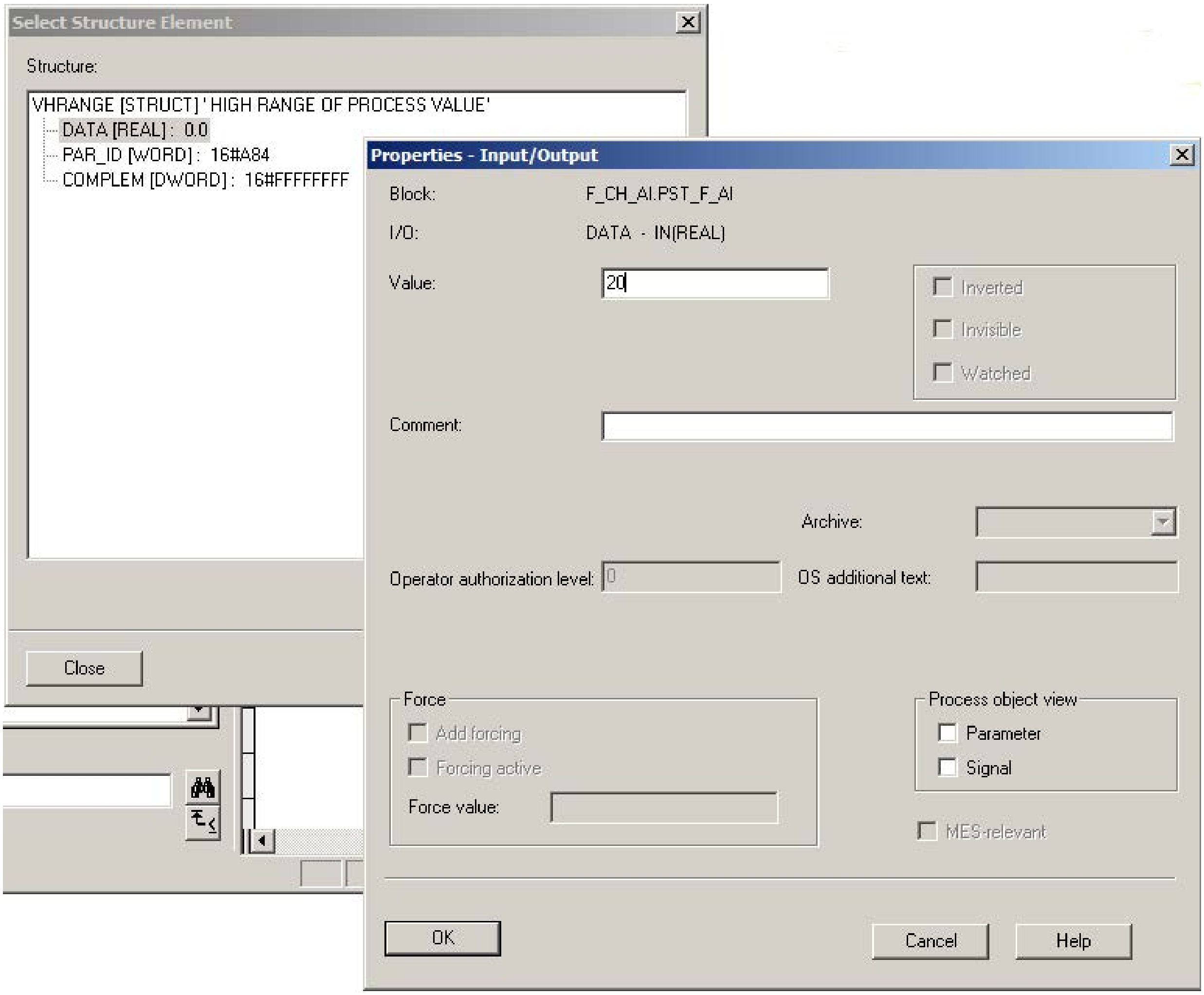
F block inputs and outputs are parameterized and interconnected using the standard CFC procedure.

Note

You are not permitted to interconnect EN/ENO connections 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 connections. The safety data format enables data and address errors to be detected.

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



VHRANGE [STRUCT] ' HIGH RANGE OF PROCESS VALUE'
DATA [REAL] : 0.0
PAR_ID [WORD] : 16#A84
COMPLEM [DWORD] : 16#FFFFFFFF

Block: F_CH_AI.PST_F_AI

I/O: DATA - IN(REAL)

Value: 20

Operator authorization level: 0

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 connection 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

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.

With F-Systems Lib V1_3 and higher, separate runtime groups are created for the F-blocks listed under points 1 and 5 the first time compiling is performed.

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.

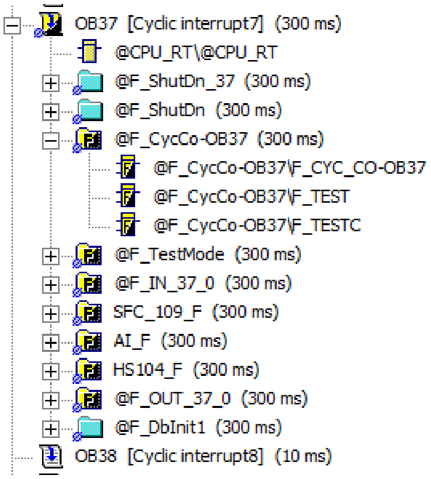
Note

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.



```
OB37  [Cyclic interrupt7]  (300 ms)
    @CPU_RT\@CPU_RT
    @F_ShutDn_37  (300 ms)
    @F_ShutDn  (300 ms)
    @F_CycCo-OB37  (300 ms)
        @F_CycCo-OB37\F_CYC_CO-OB37
        @F_CycCo-OB37\F_TEST
        @F_CycCo-OB37\F_TESTC
    @F_TestMode  (300 ms)
    @F_IN_37_0  (300 ms)
    SFC_109_F  (300 ms)
    AI_F  (300 ms)
    HS104_F  (300 ms)
    @F_OUT_37_0  (300 ms)
    @F_DbInit1  (300 ms)
OB38  [Cyclic interrupt8]  (10 ms)
```

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.

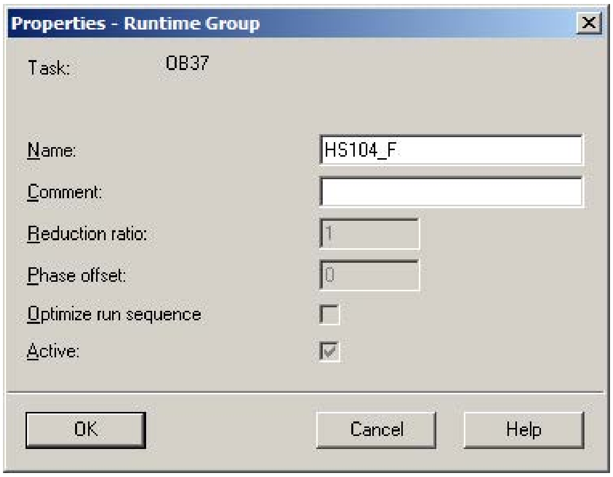
There should only be one @F_IN_xx_y runtime group before the first F-user runtime group and one @F_OUT_xx_y runtime group after the last F-use runtime group. If the safety program consist of several shutdown groups (see section 6.2.6 (Page 89)), there is the @F_IN_xx_y and @F_OUT_xx_y runtime group both 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



Properties - Runtime Group

Task: OB37

Name: HS104_F

Comment:

Reduction ratio: 1

Phase offset: 0

Optimize run sequence □

Active: ☑

- 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

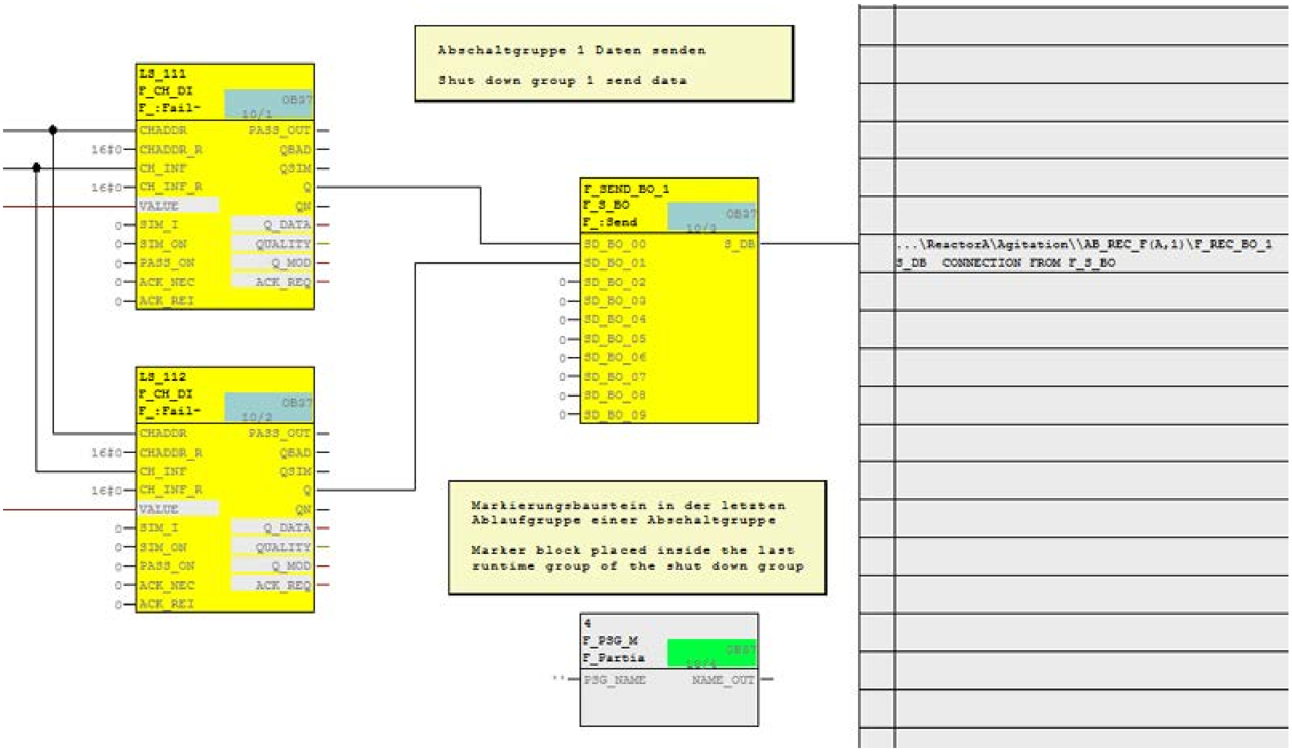
If you wish to exchange data between two F-shutdown groups, you are not permitted to interconnect the inputs and outputs directly. You need to use the following F-system blocks for data exchange between F blocks in different F-shutdown groups:

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:



Abschaltgruppe 1 Daten senden

Shut down group 1 send data

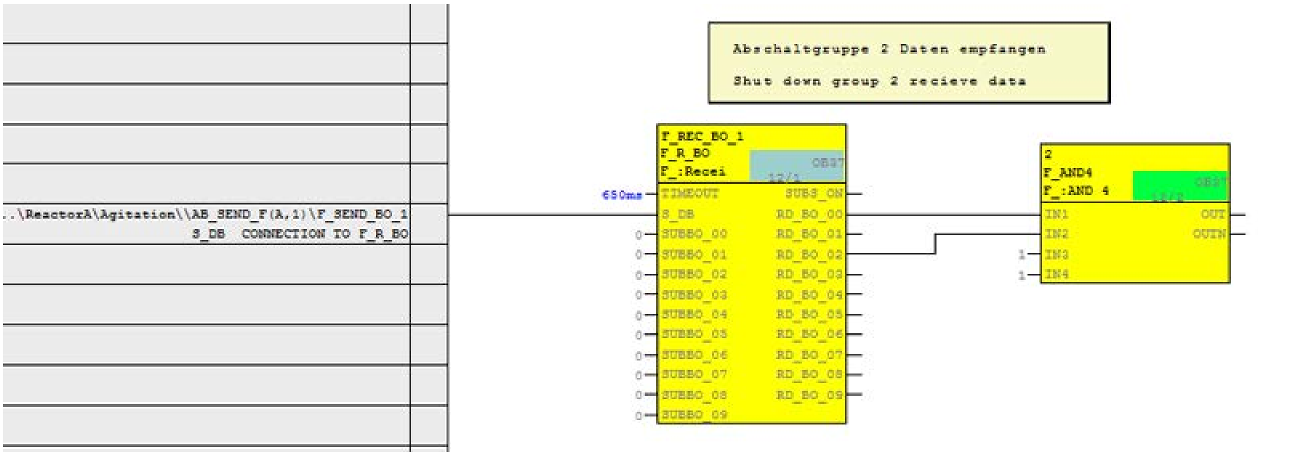
Markierungsbaustein in der letzten
Ablaufgruppe einer Abschaltgruppe

Marker block placed inside the last
runtime group of the shut down group

...\ReactorA\Agitation\\AB_REC_F(A,1)\F_REC_BO_1
S_DB CONNECTION FROM F_S_BO

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:



Abschaltgruppe 2 Daten empfangen

Shut down group 2 recieve data

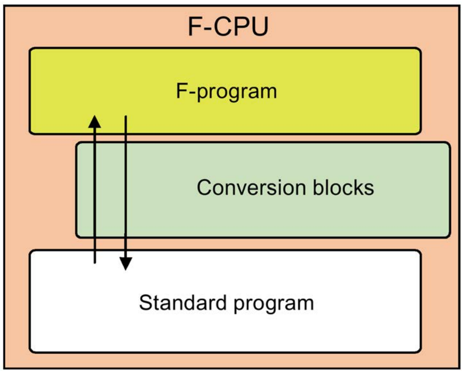
..\ReactorA\Agitation\\AB_SEND_F(A,1)\F_SEND_BO_1
S_DB CONNECTION TO F_R_BO

See also

Monitoring times and system response times (Page 133)

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

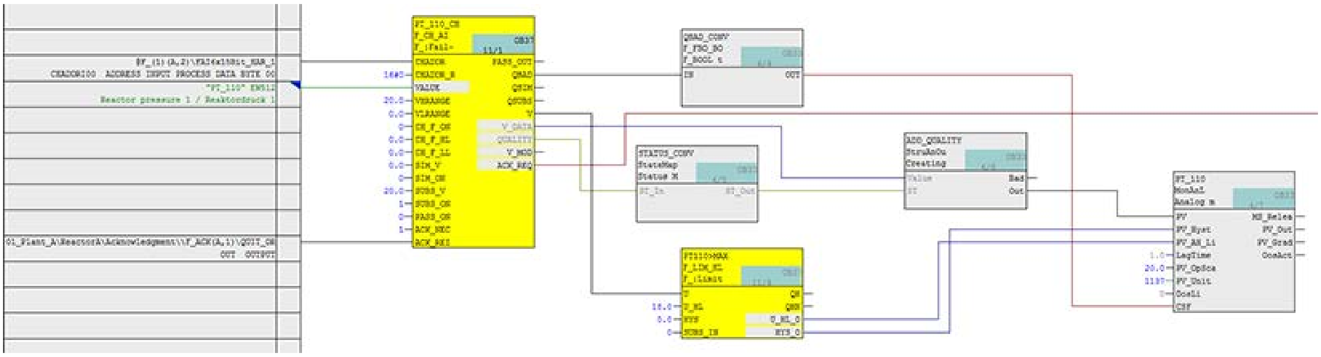
The standard program and the F-program use different data formats. Accordingly, special conversion blocks have to be used for data exchange.



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, EventMESSAGE 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.

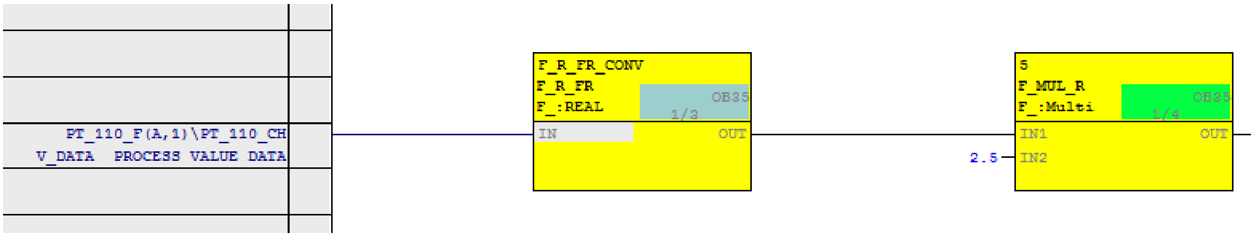
If parameters cannot be directly further interconnected due to the safety data format, the conversion blocks described above can be used.

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:

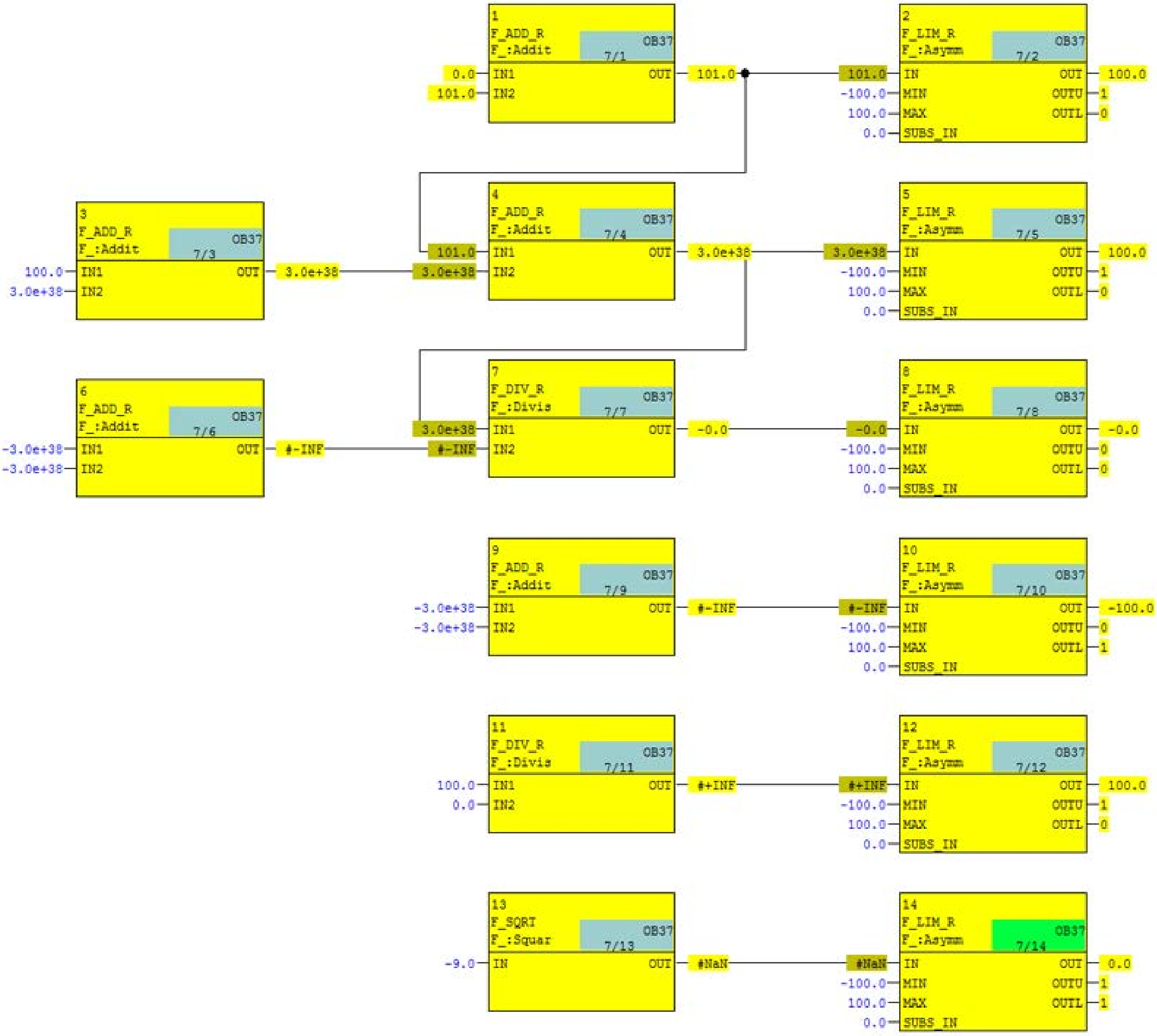
- Either output at the output and can be processed further by subsequent F blocks
- Or signaled to special outputs. A substitute value is output if necessary.

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 diagnostic buffer:

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

You can use this entry in the diagnostic 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 "S7 F/FH Systems – Configuring and Programming" (https://support.industry.siemens.com/cs/ww/en/view/101509838) manual.

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.

In the case of F Systems V6.0 with S7 F Systems Lib V1_3 and higher, 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.

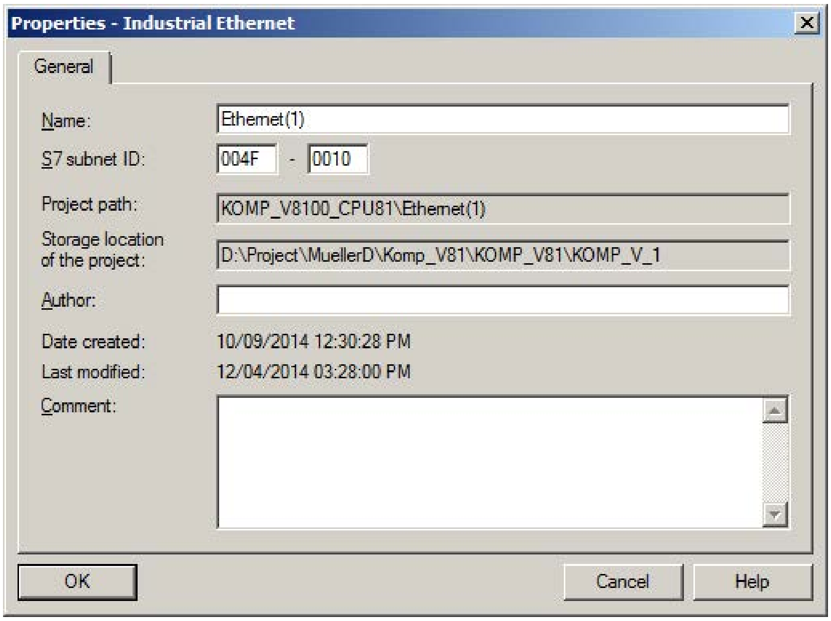
7.3.1 Configuring S7 connections

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".

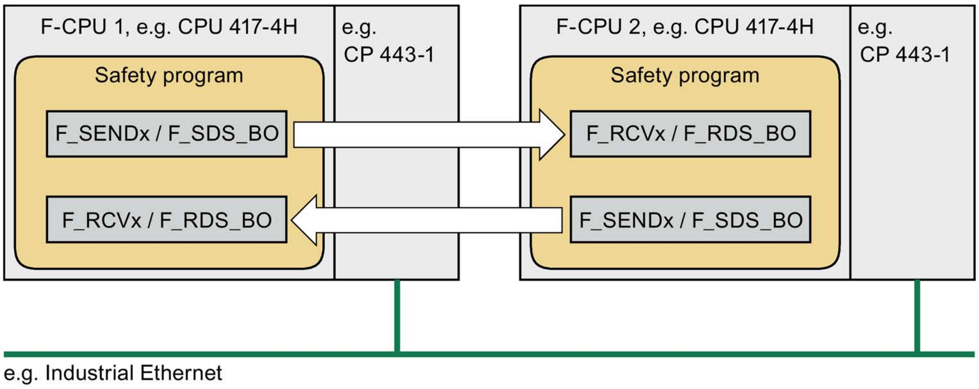
During communication between automation systems in various subprojects, please make sure that the S7 subnet ID is the same in each of the respective projects. This ID is involved in the calculation of the CRC sum at the send and receive blocks and must, therefore, be the same in each case.



Name: Ethernet(1)
S7 subnet ID: 004F - 0010
Project path: KOMP_V8100_CPU81\Ethernet(1)
Storage location of the project: D:\Project\MuellerD\Komp_V81\KOMP_V81\KOMP_V_1
Author:
Date created: 10/09/2014 12:30:28 PM
Last modified: 12/04/2014 03:28:00 PM
Comment:

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 (F Systems V6.0 and higher)	Fail-safe sending of 32 F_BOOL data type objects to another F-CPU
F_RDS_BO (F Systems V6.0 and higher)	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.

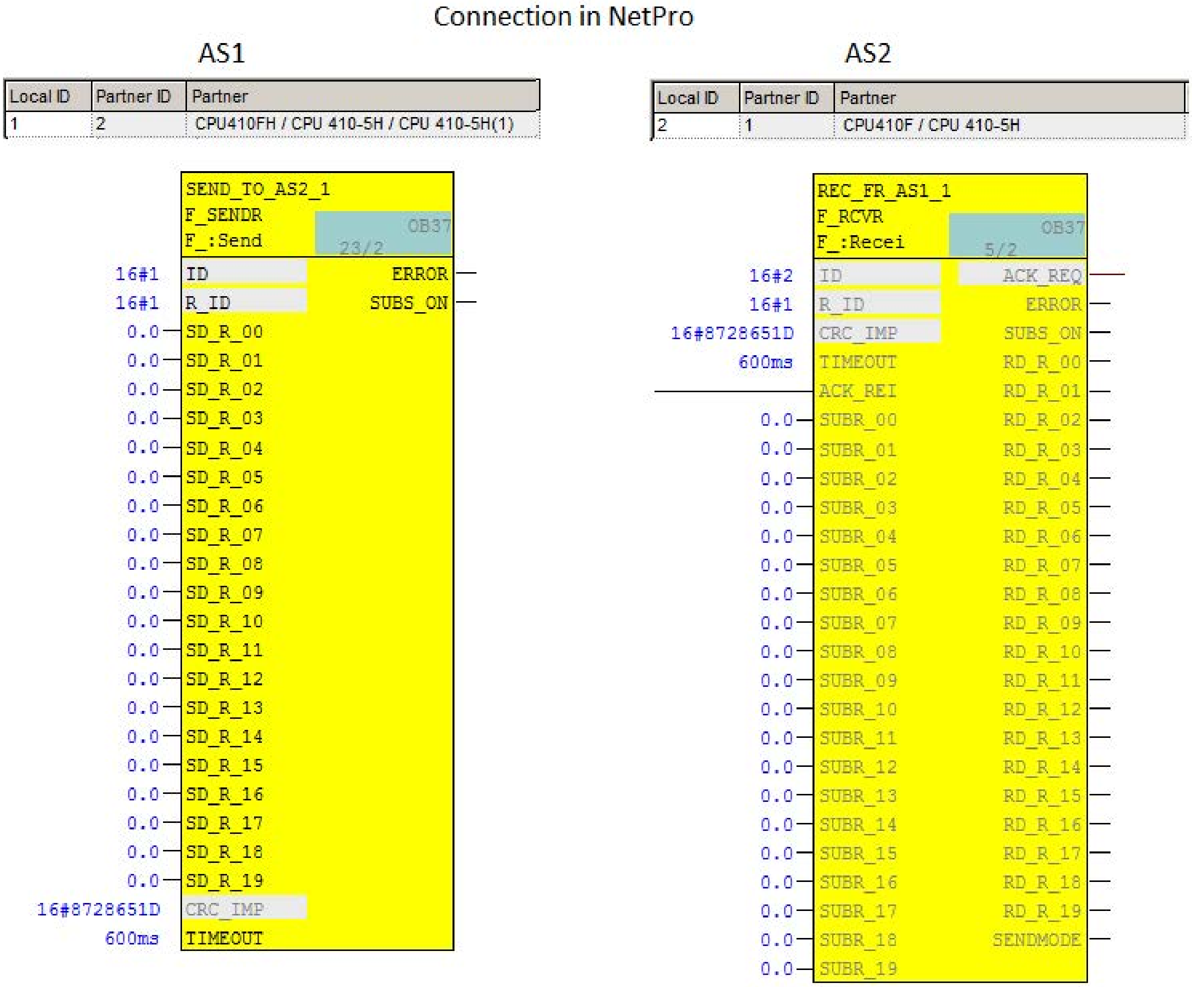
Procedure

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 AS4 is sender, partner AS3 is recipient



Connection in NetPro

AS1

Local ID	Partner ID	Partner
1	2	CPU410FH / CPU 410-5H / CPU 410-5H(1)

AS2

Local ID	Partner ID	Partner
2	1	CPU410F / CPU 410-5H

SEND_TO_AS2_1
F_SENDR
F_:Send
OB37
23/2

	Input	Output
16#1	ID	ERROR
16#1	R_ID	SUBS_ON
0.0	SD_R_00	
0.0	SD_R_01	
0.0	SD_R_02	
0.0	SD_R_03	
0.0	SD_R_04	
0.0	SD_R_05	
0.0	SD_R_06	
0.0	SD_R_07	
0.0	SD_R_08	
0.0	SD_R_09	
0.0	SD_R_10	
0.0	SD_R_11	
0.0	SD_R_12	
0.0	SD_R_13	
0.0	SD_R_14	
0.0	SD_R_15	
0.0	SD_R_16	
0.0	SD_R_17	
0.0	SD_R_18	
0.0	SD_R_19	
16#8728651D	CRC_IMP	
600ms	TIMEOUT	

REC_FR_AS1_1
F_RCVR
F_:Recei
OB37
5/2

	Input	Output
16#2	ID	ACK_REQ
16#1	R_ID	ERROR
16#8728651D	CRC_IMP	SUBS_ON
600ms	TIMEOUT	RD_R_00
	ACK_REI	RD_R_01
0.0	SUBR_00	RD_R_02
0.0	SUBR_01	RD_R_03
0.0	SUBR_02	RD_R_04
0.0	SUBR_03	RD_R_05
0.0	SUBR_04	RD_R_06
0.0	SUBR_05	RD_R_07
0.0	SUBR_06	RD_R_08
0.0	SUBR_07	RD_R_09
0.0	SUBR_08	RD_R_10
0.0	SUBR_09	RD_R_11
0.0	SUBR_10	RD_R_12
0.0	SUBR_11	RD_R_13
0.0	SUBR_12	RD_R_14
0.0	SUBR_13	RD_R_15
0.0	SUBR_14	RD_R_16
0.0	SUBR_15	RD_R_17
0.0	SUBR_16	RD_R_18
0.0	SUBR_17	RD_R_19
0.0	SUBR_18	SENDMODE
0.0	SUBR_19	

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 being used by more than one block. [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%.

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 controlled by the F-shutdown group are passivated.
- With S7 F Systems Lib V1_3 and higher, the F channel drivers of the F-shutdown group set the QBAD outputs 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. In the case of S7 F Systems Lib V1_3, the messages contain the following 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:

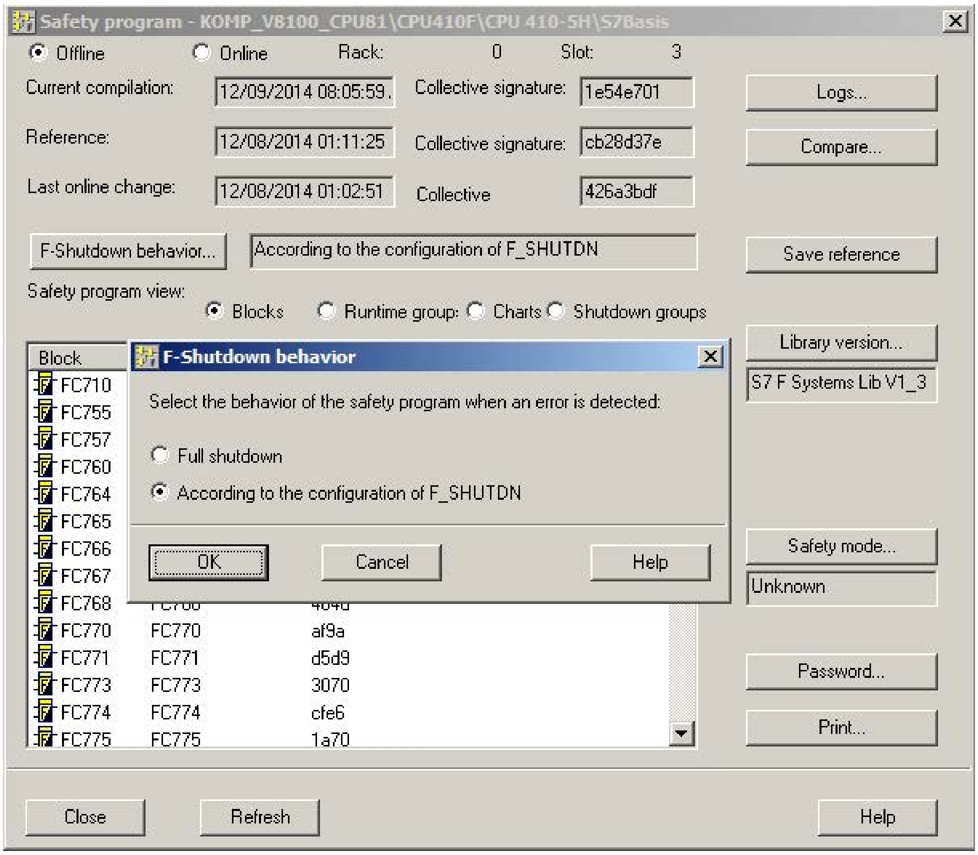
- First, the F-shutdown group in which the error was detected is shut down.
- All other F-shutdown groups are then shut down within double the time period you set as the F monitoring time for the slowest cyclic interrupt OB.

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.



Safety program - KOMP_V8100_CPU81\CPU410F\CPU 410-5H\S7Basis

● Offline ○ Online Rack: 0 Slot: 3

Current compilation: 12/09/2014 08:05:59 Collective signature: 1e54e701

Reference: 12/08/2014 01:11:25 Collective signature: cb28d37e

Last online change: 12/08/2014 01:02:51 Collective 426a3bdf

F-Shutdown behavior...: According to the configuration of F_SHUTDN

Safety program view: ● Blocks ○ Runtime group: ○ Charts ○ Shutdown groups

Library version...: S7 F Systems Lib V1_3

Safety mode...: Unknown

Block		
FC710		
FC755		
FC757		
FC760		
FC764		
FC765		
FC766		
FC767		
FC768	FC768	4040
FC770	FC770	af9a
FC771	FC771	d5d9
FC773	FC773	3070
FC774	FC774	cfe6
FC775	FC775	1a70

F-Shutdown behavior

Select the behavior of the safety program when an error is detected:

○ Full shutdown

● According to the configuration of F_SHUTDN

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:

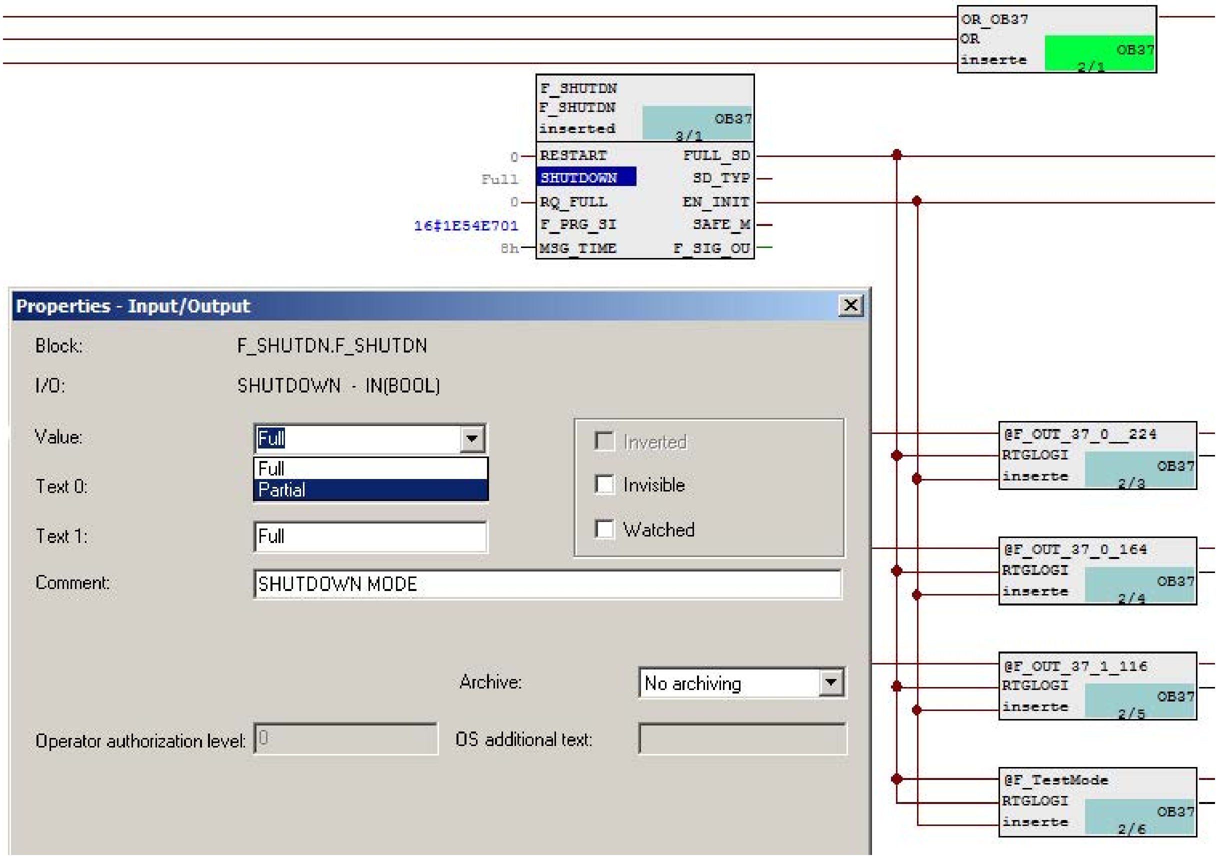
  – "Partial":

    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.



Properties - Input/Output

Block: F_SHUTDN.F_SHUTDN

I/O: SHUTDOWN - IN(BOOL)

Value: Full

Full
Partial

Text 0:

Text 1: Full

Comment: SHUTDOWN MODE

□ Inverted
□ Invisible
□ Watched

Archive: No archiving

Operator authorization level: 0

OS additional text:

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

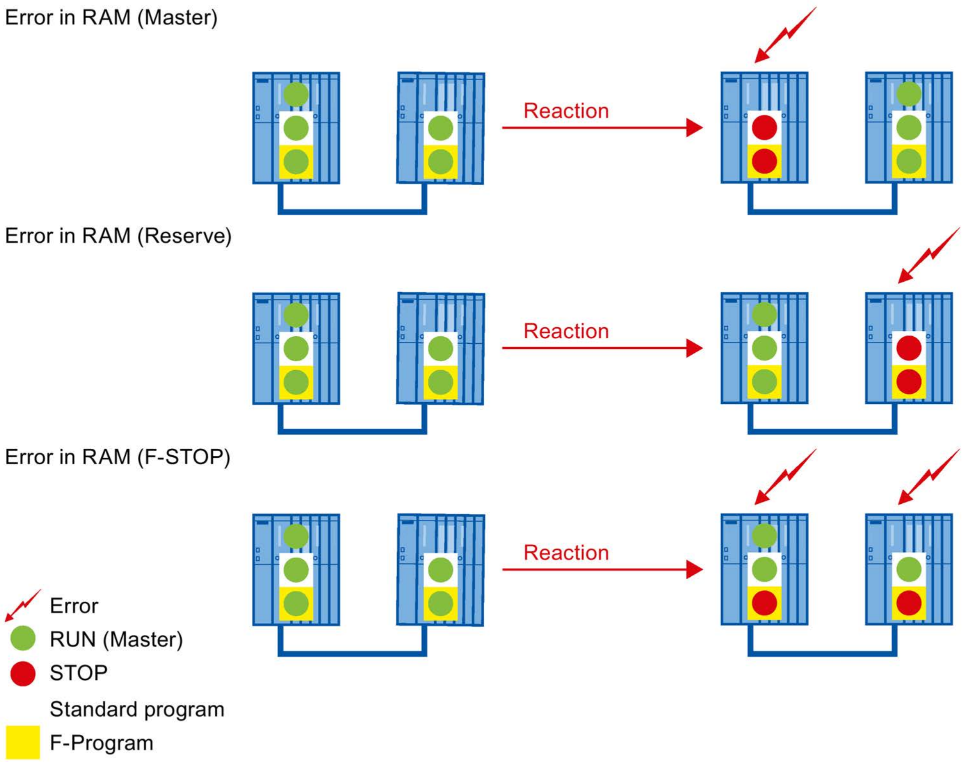
- Distortion of:
  - Data
  - Program sequence
  - Code
- CPU error

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

You can find more information in the manual titled "SIMATIC Fault-tolerant Systems S7-400H" (https://support.industry.siemens.com/cs/ww/en/view/82478488).

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. The F_CHG_BO, F_CHG_R (part of the Safety Data Write function), and F_MOV_R (S7 F-Systems Lib V1_3 and higher) F-blocks are exceptions to this rule.

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.

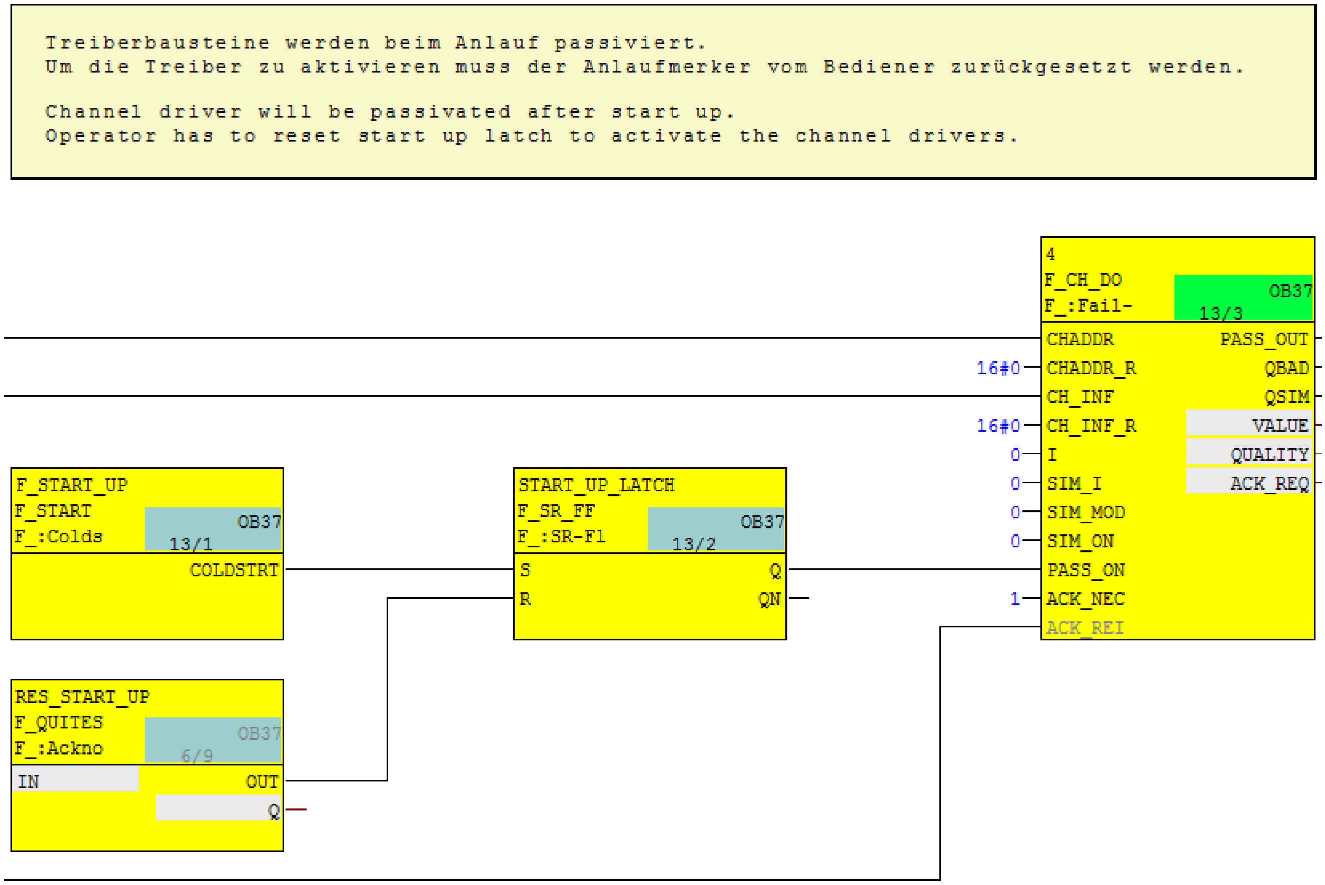
An F-startup is performed:

- 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.



```
Treiberbausteine werden beim Anlauf passiviert.
Um die Treiber zu aktivieren muss der Anlaufmerker vom Bediener zurückgesetzt werden.

Channel driver will be passivated after start up.
Operator has to reset start up latch to activate the channel drivers.
```

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 (F_QUITES block).

Note

For more options when programming (re)start protection, please refer to the "SIMATIC Industrial Software S7 F/FH Systems – Configuring and Programming" (https://support.industry.siemens.com/cs/ww/en/view/101509838) manual.

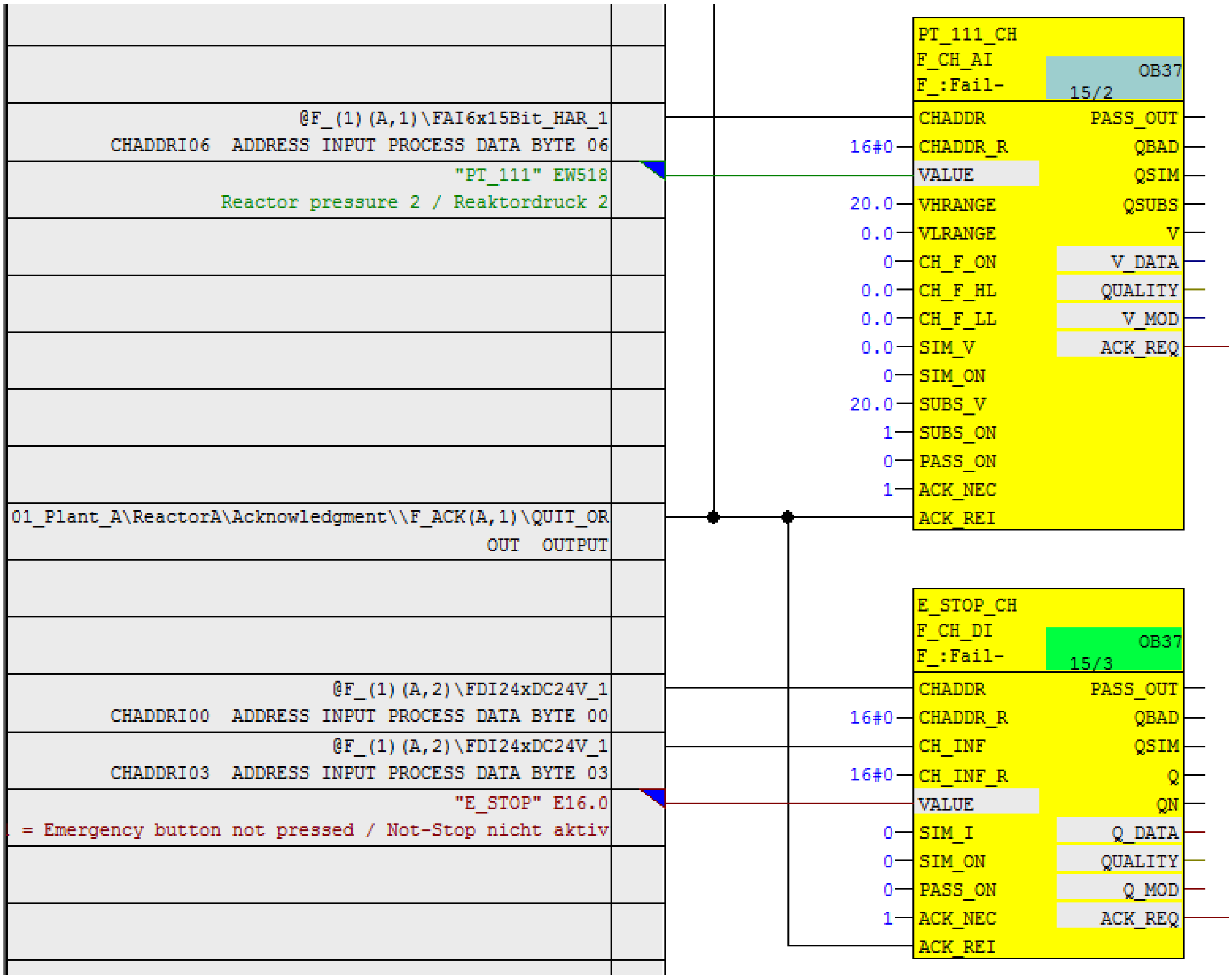
7.6 I/O access via F driver blocks

In S7 F-systems, F-signal modules are accessed via F-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.



@F_(1)(A,1)\FAI6x15Bit_HAR_1
CHADDRI06 ADDRESS INPUT PROCESS DATA BYTE 06

"PT_111" EW518
Reactor pressure 2 / Reaktordruck 2

01_Plant_A\ReactorA\Acknowledgment\\F_ACK(A,1)\QUIT_OR
OUT OUTPUT

@F_(1)(A,2)\FDI24xDC24V_1
CHADDRI00 ADDRESS INPUT PROCESS DATA BYTE 00

@F_(1)(A,2)\FDI24xDC24V_1
CHADDRI03 ADDRESS INPUT PROCESS DATA BYTE 03

"E_STOP" E16.0
. = Emergency button not pressed / Not-Stop nicht aktiv

PT_111_CH
F_CH_AI
F_:Fail-
OB37
15/2

CHADDR — PASS_OUT
16#0 — CHADDR_R — QBAD
VALUE — QSIM
20.0 — VHRANGE — QSUBS
0.0 — VLRANGE — V
0 — CH_F_ON — V_DATA
0.0 — CH_F_HL — QUALITY
0.0 — CH_F_LL — V_MOD
0.0 — SIM_V — ACK_REQ
0 — SIM_ON
20.0 — SUBS_V
1 — SUBS_ON
0 — PASS_ON
1 — ACK_NEC
ACK_REI

E_STOP_CH
F_CH_DI
F_:Fail-
OB37
15/3

CHADDR — PASS_OUT
16#0 — CHADDR_R — QBAD
CH_INF — QSIM
16#0 — CH_INF_R — Q
VALUE — QN
0 — SIM_I — Q_DATA
0 — SIM_ON — QUALITY
0 — PASS_ON — Q_MOD
1 — ACK_NEC — ACK_REQ
ACK_REI

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

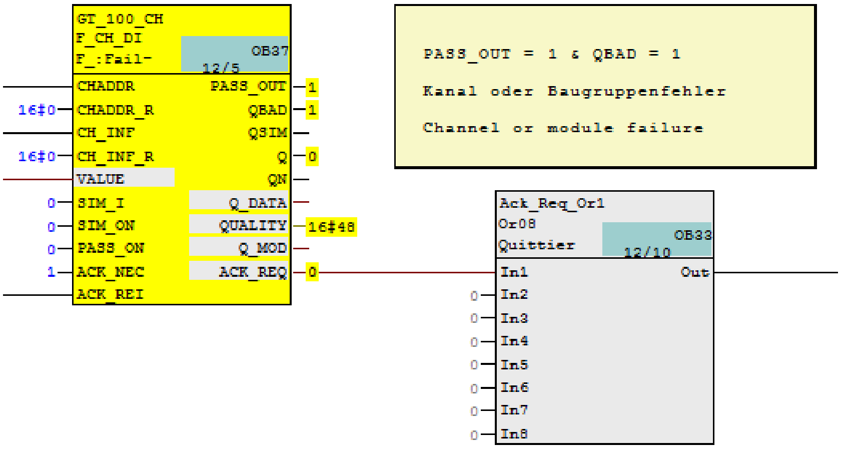
7.7 Passivation and reintegration of input/output channels

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.



PASS_OUT = 1 & QBAD = 1

Kanal oder Baugruppenfehler

Channel or module failure

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

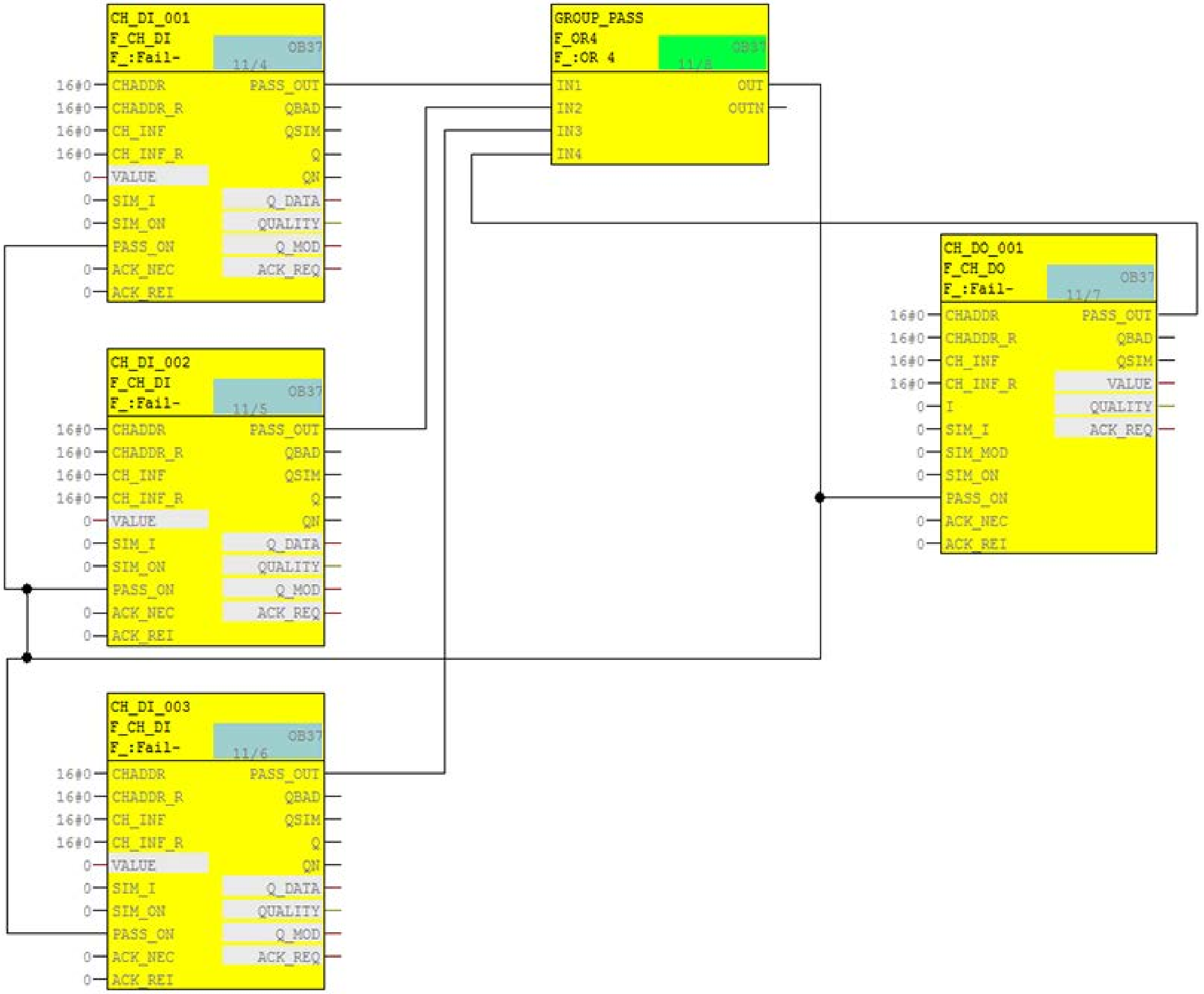
F startup and (re)start protection (Page 104)

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, for example, be used to force simultaneous reintegration of all F-I/Os after the F-system has been started up.

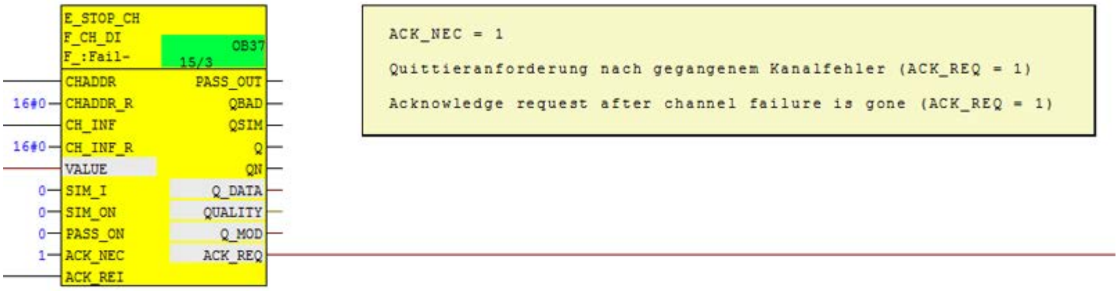
To enable group passivation, you must link all PASS_OUT outputs of the F-channel drivers in this group with F_OR4 F-blocks, and interconnect the OUT output result of F_OR4 with all PASS_ON inputs of the F-channel drivers in this group.



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



ACK_NEC = 1

Quittieranforderung nach gegangenem Kanalfehler (ACK_REQ = 1)

Acknowledge request after channel failure is gone (ACK_REQ = 1)

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.

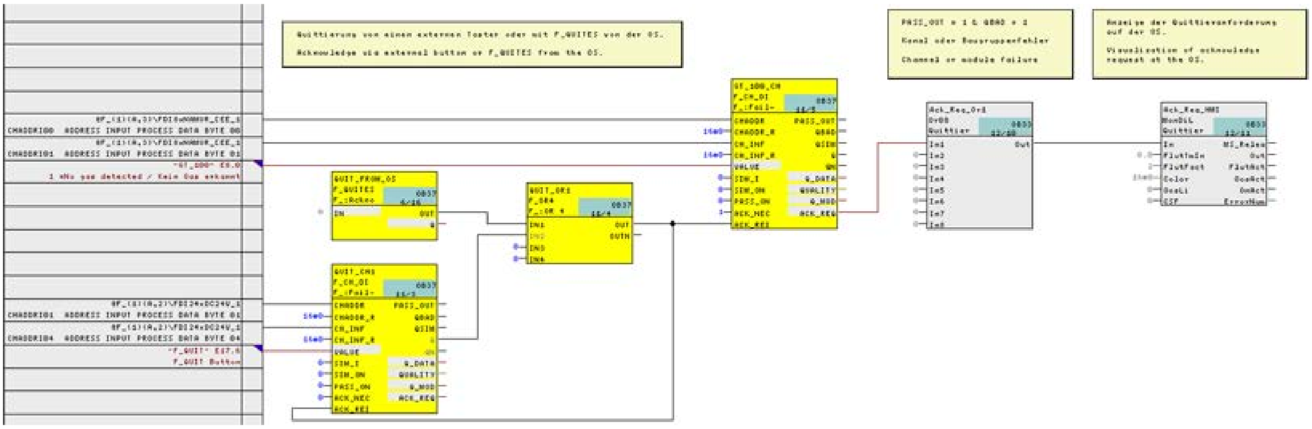
7.7.5 Programming reintegration following module errors or channel errors requiring acknowledgment

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

- Connection of an acknowledgment button to a fail-safe digital input module.
- Manual input from an ES/OS station using the F_QUITES block



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: using an "F_QUITES" block.

Therefore, in cases where you are setting up acknowledgment for reintegration of an F-signal module group to which an acknowledgment key is connected, we recommend providing another means of acknowledgment via an OS.

Note

Automatic user acknowledgment is not permitted.

How to program user acknowledgment via an OS

1. Add the F_QUITES F-block to your safety program. You can access the acknowledgment signal for evaluation for user acknowledgments at the output OUT of F_QUITES.
2. Interconnect the OUT output of F_QUITES with the ACK_REI input of the F-channel drivers.
3. Configure a button on your OS for writing the "Acknowledge value" "6" (first acknowledgment step) and a second button for writing "Acknowledge value" "9" (second acknowledgment step). Connect the buttons to the IN input of F_QUITES.
4. Optional: On your OS, evaluate the output Q of F_QUITES to show the time window within which the 2nd. acknowledgment step must be completed (making the second button visible) or to show that the 1st acknowledgment step has already been completed.

Note

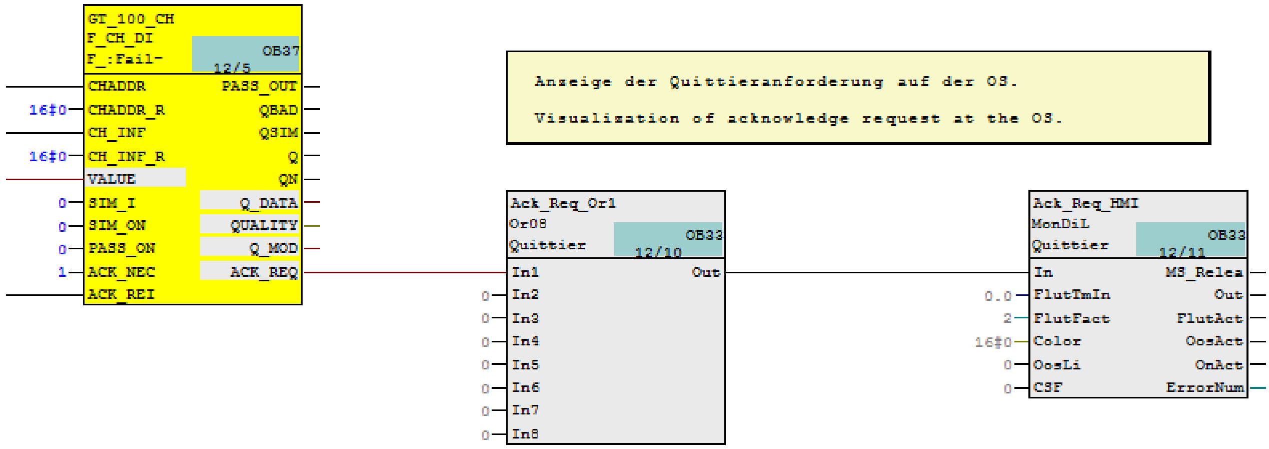
Automatic reintegration using F_QUITES:

The non-safety-related input IN of F_QUITES must not be interconnected with a signal or described by a signal which generates the above condition (change from 6 to 9 within a minute) automatically for a fail-safe acknowledgment.

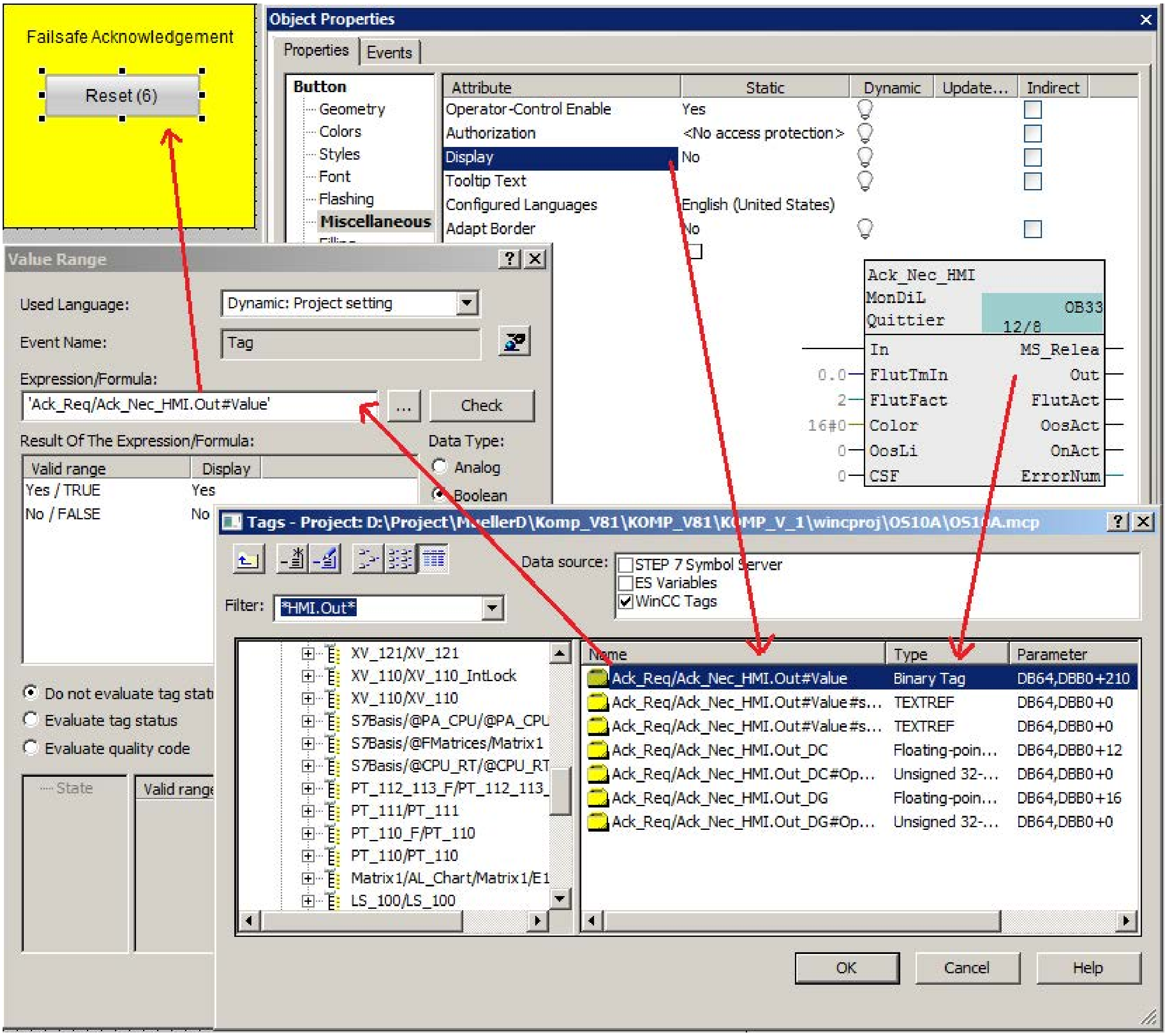
Fail-safe acknowledgment must only be generated by means of a conscious manual entry on the ES/OS (not automatically in the program).

Example: Implementing F-user acknowledgment in the OS

All "ACK_REQ" channel driver outputs are grouped by means of an OR in the standard user program and made available to the OS via a DIG_MON block.



If an acknowledgment prompt is pending (ACK_REQ=1) the acknowledge field (yellow) and the "reset (6)" button will appear on the OS.



Failsafe Acknowledgement

Reset (6)

Object Properties

Properties | Events

Button: Geometry, Colors, Styles, Font, Flashing, Miscellaneous

Attribute	Static	Dynamic	Update...	Indirect
Operator-Control Enable	Yes			□
Authorization	<No access protection>			□
Display	No			□
Tooltip Text				□
Configured Languages	English (United States)			
Adapt Border	No			□

Value Range

Used Language: Dynamic: Project setting

Event Name: Tag

Expression/Formula: 'Ack_Req/Ack_Nec_HMI.Out#Value'

Result Of The Expression/Formula:

Valid range	Display
Yes / TRUE	Yes
No / FALSE	No

Data Type: ○ Analog ● Boolean

● Do not evaluate tag stat
○ Evaluate tag status
○ Evaluate quality code

State | Valid range

```
Ack_Nec_HMI
MonDiL                OB33
Quittier              12/8
    In              MS_Relea
0.0 FlutTmIn             Out
  2 FlutFact         FlutAct
16#0 Color           OosAct
  0 OosLi             OnAct
  0 CSF            ErrorNum
```

Tags - Project: D:\Project\MuellerD\Komp_V81\KOMP_V81\KOMP_V_1\wincproj\OS10A\OS10A.mcp

Data source: □ STEP 7 Symbol Server □ ES Variables ☑ WinCC Tags

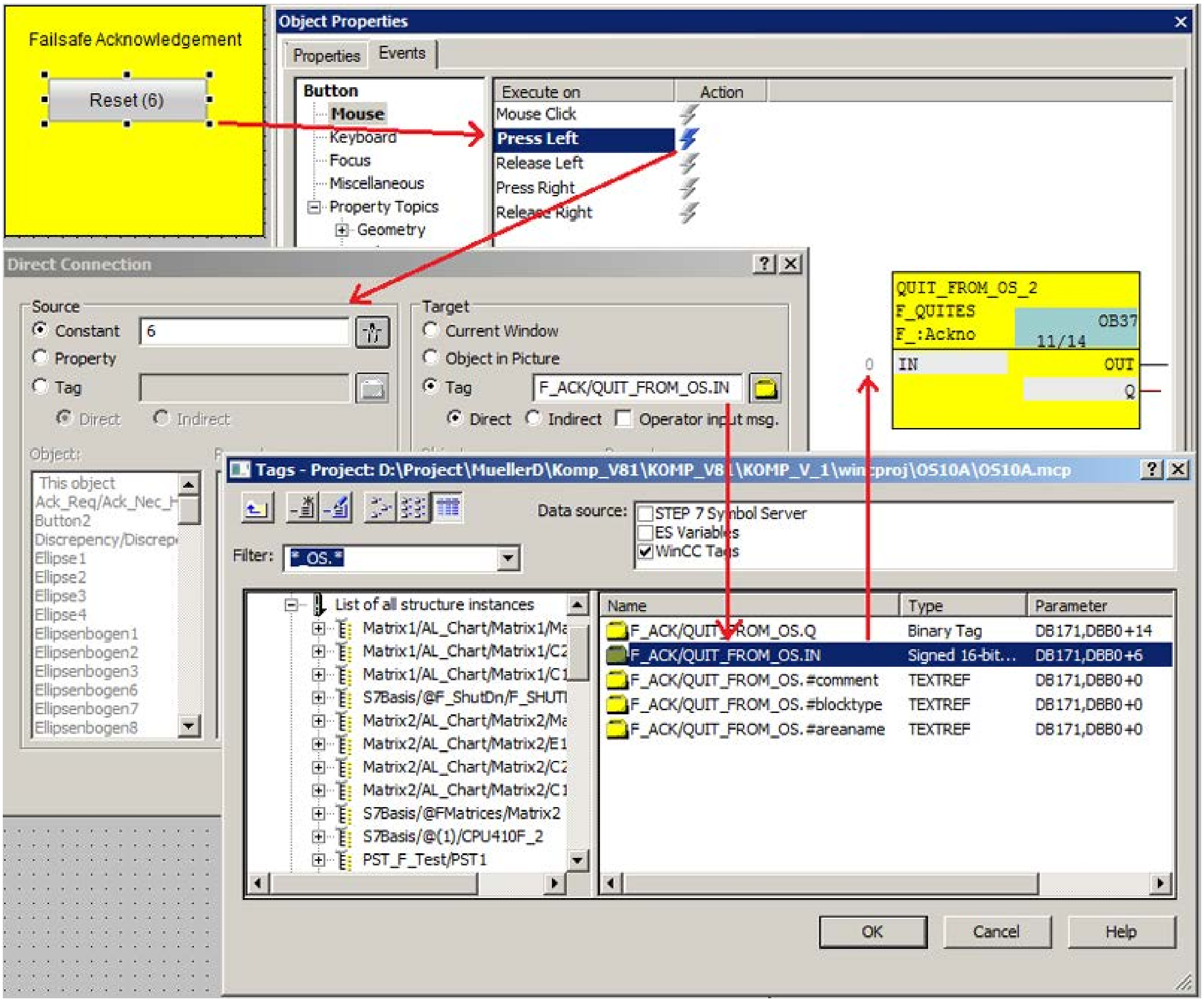
Filter: *HMI.Out*

XV_121/XV_121
XV_110/XV_110_IntLock
XV_110/XV_110
S7Basis/@PA_CPU/@PA_CPU
S7Basis/@FMatrices/Matrix1
S7Basis/@CPU_RT/@CPU_RT
PT_112_113_F/PT_112_113_
PT_111/PT_111
PT_110_F/PT_110
PT_110/PT_110
Matrix1/AL_Chart/Matrix1/E1
LS_100/LS_100

Name	Type	Parameter
Ack_Req/Ack_Nec_HMI.Out#Value	Binary Tag	DB64,DBB0+210
Ack_Req/Ack_Nec_HMI.Out#Value#s...	TEXTREF	DB64,DBB0+0
Ack_Req/Ack_Nec_HMI.Out#Value#s...	TEXTREF	DB64,DBB0+0
Ack_Req/Ack_Nec_HMI.Out_DC	Floating-poin...	DB64,DBB0+12
Ack_Req/Ack_Nec_HMI.Out_DC#Op...	Unsigned 32-...	DB64,DBB0+0
Ack_Req/Ack_Nec_HMI.Out_DG	Floating-poin...	DB64,DBB0+16
Ack_Req/Ack_Nec_HMI.Out_DG#Op...	Unsigned 32-...	DB64,DBB0+0

Procedure

1. Press the first acknowledge button, "reset (6)", to write the value 6 to the "IN" input of the F_QUITES block.



Source: ● Constant 6 ○ Property ○ Tag (● Direct ○ Indirect)

Target: ○ Current Window ○ Object in Picture ● Tag F_ACK/QUIT_FROM_OS.IN ● Direct ○ Indirect □ Operator input msg.

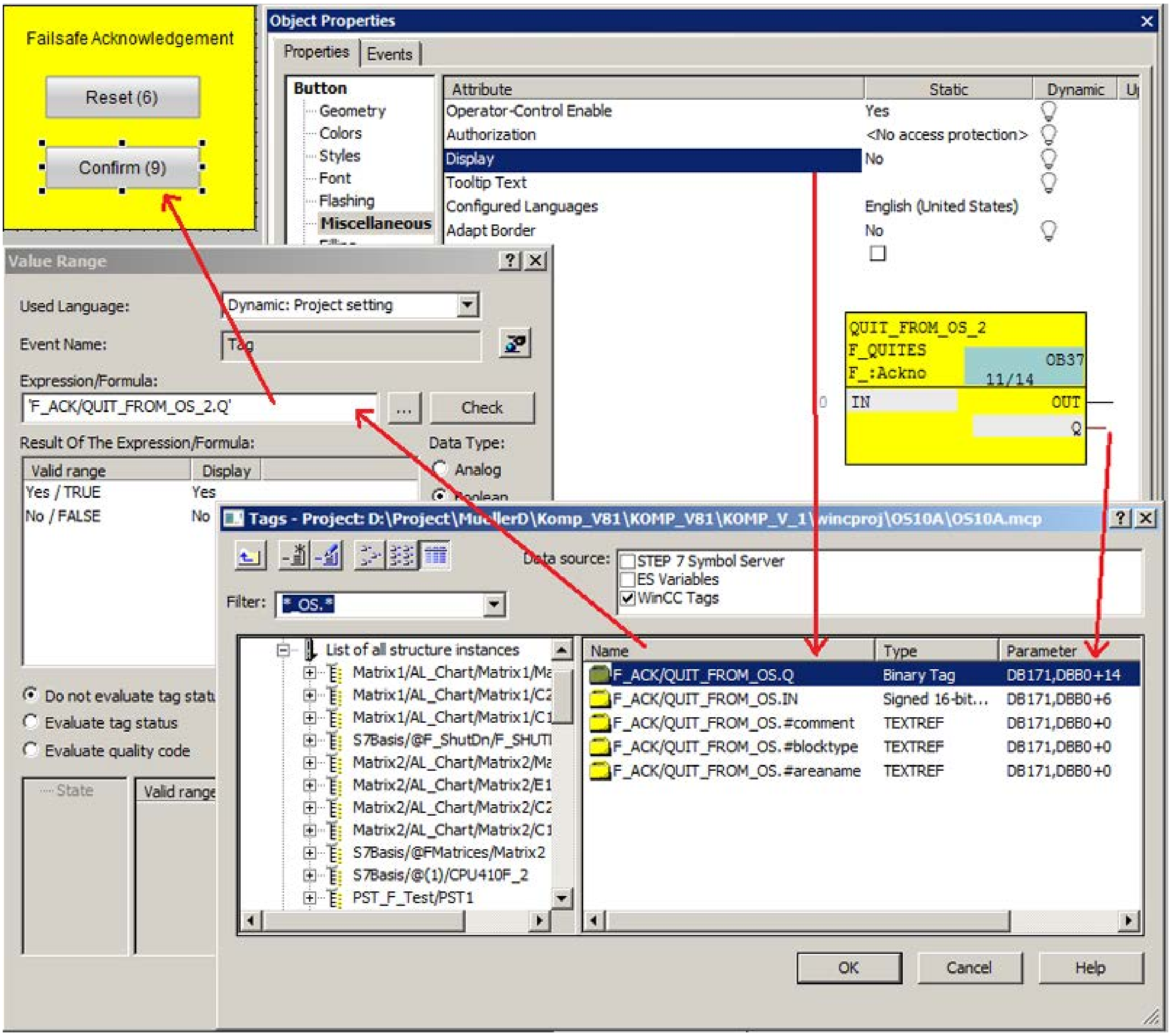
Tags - Project: D:\Project\MuellerD\Komp_V81\KOMP_V81\KOMP_V_1\wincproj\OS10A\OS10A.mcp

Data source: □ STEP 7 Symbol Server □ ES Variables ☑ WinCC Tags

Filter: *OS.*

Name	Type	Parameter
F_ACK/QUIT_FROM_OS.Q	Binary Tag	DB171,DBB0+14
F_ACK/QUIT_FROM_OS.IN	Signed 16-bit...	DB171,DBB0+6
F_ACK/QUIT_FROM_OS.#comment	TEXTREF	DB171,DBB0+0
F_ACK/QUIT_FROM_OS.#blocktype	TEXTREF	DB171,DBB0+0
F_ACK/QUIT_FROM_OS.#areaname	TEXTREF	DB171,DBB0+0

The second acknowledge button, "reset (9)", appears if the "Q" output of the F_QUITES block has been set. This output remains set for 60 seconds.



Attribute	Static	Dynamic
Operator-Control Enable	Yes	
Authorization	<No access protection>	
Display	No	
Tooltip Text		
Configured Languages	English (United States)	
Adapt Border	No	

Used Language: Dynamic: Project setting

Event Name: Tag

Expression/Formula: 'F_ACK/QUIT_FROM_OS_2.Q'

Result Of The Expression/Formula:

Valid range	Display
Yes / TRUE	Yes
No / FALSE	No

● Do not evaluate tag statu

○ Evaluate tag status

○ Evaluate quality code

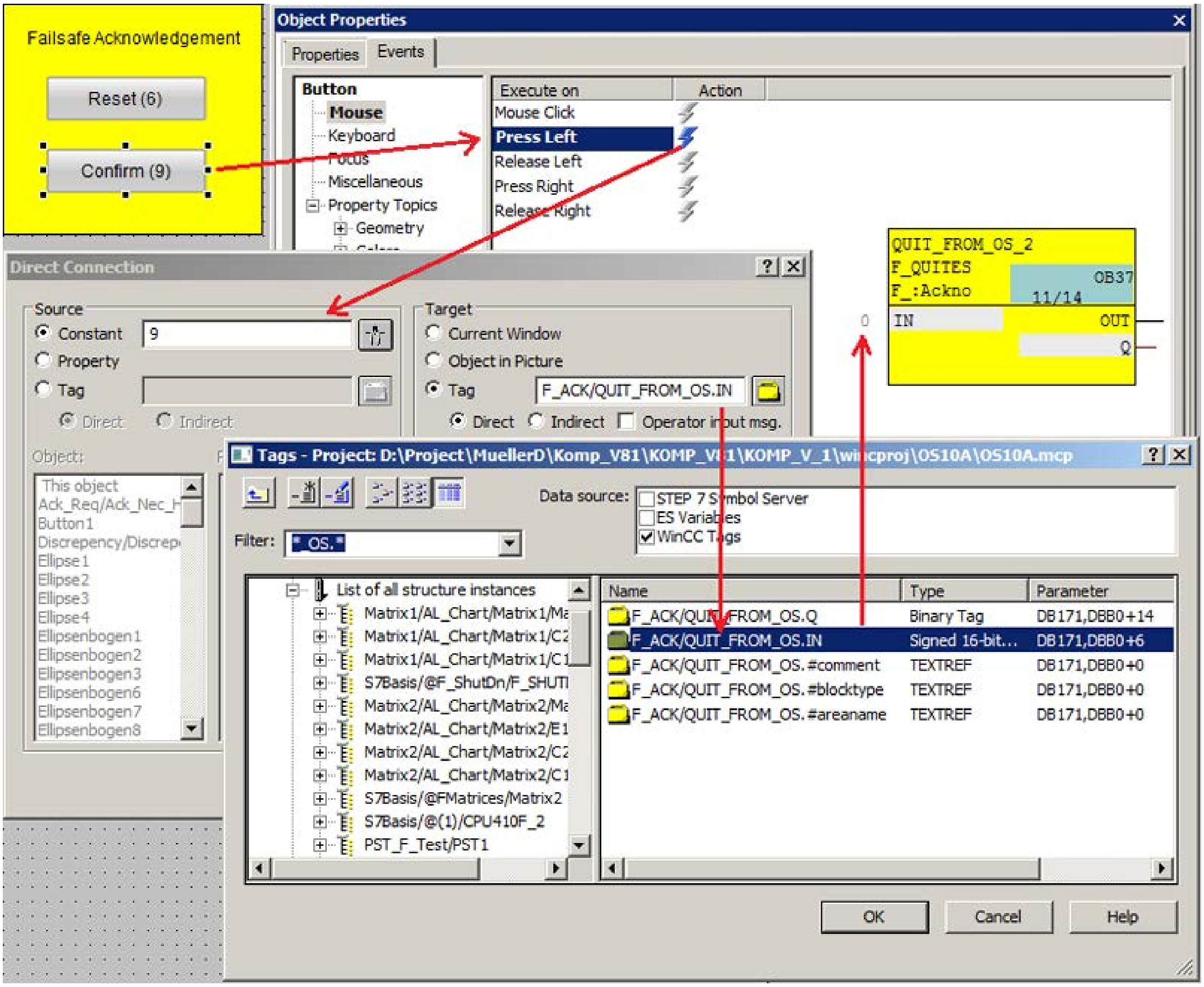
Data source: ☐ STEP 7 Symbol Server ☐ ES Variables ☑ WinCC Tags

Filter: *_OS.*

List of all structure instances
- Matrix1/AL_Chart/Matrix1/Ma
- Matrix1/AL_Chart/Matrix1/C2
- Matrix1/AL_Chart/Matrix1/C1
- S7Basis/@F_ShutDn/F_SHUT
- Matrix2/AL_Chart/Matrix2/Ma
- Matrix2/AL_Chart/Matrix2/E1
- Matrix2/AL_Chart/Matrix2/C2
- Matrix2/AL_Chart/Matrix2/C1
- S7Basis/@FMatrices/Matrix2
- S7Basis/@(1)/CPU410F_2
- PST_F_Test/PST1

Name	Type	Parameter
F_ACK/QUIT_FROM_OS.Q	Binary Tag	DB171,DBB0+14
F_ACK/QUIT_FROM_OS.IN	Signed 16-bit...	DB171,DBB0+6
F_ACK/QUIT_FROM_OS.#comment	TEXTREF	DB171,DBB0+0
F_ACK/QUIT_FROM_OS.#blocktype	TEXTREF	DB171,DBB0+0
F_ACK/QUIT_FROM_OS.#areaname	TEXTREF	DB171,DBB0+0

2. Press the second acknowledge button, "reset (9)", to write the value 9 to the "IN" input of the F_QUITES block.



Source: ● Constant 9; ○ Property; ○ Tag; ● Direct ○ Indirect

Object: This object, Ack_Req/Ack_Nec_H, Button1, Discrepency/Discrep, Ellipse1, Ellipse2, Ellipse3, Ellipse4, Ellipsenbogen1, Ellipsenbogen2, Ellipsenbogen3, Ellipsenbogen6, Ellipsenbogen7, Ellipsenbogen8

Target: ○ Current Window; ○ Object in Picture; ● Tag F_ACK/QUIT_FROM_OS.IN; ● Direct ○ Indirect □ Operator input msg.

Data source: □ STEP 7 Symbol Server; □ ES Variables; ☑ WinCC Tags

Filter: *_OS.*

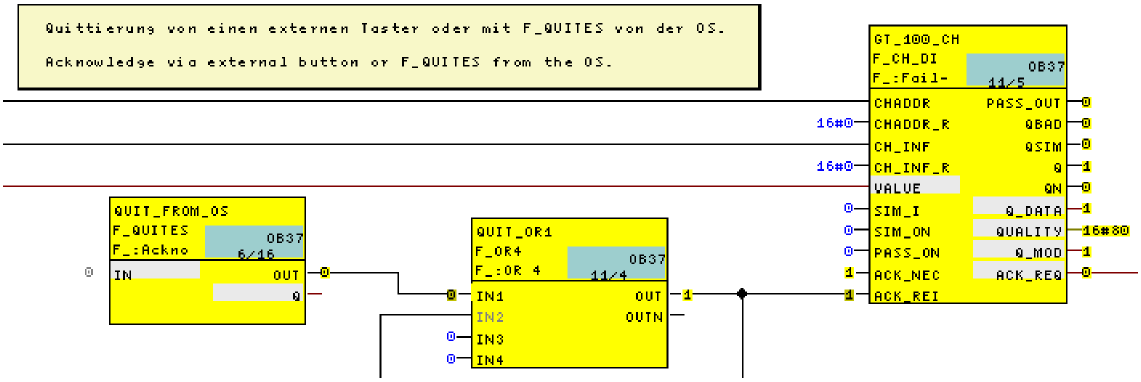
List of all structure instances: Matrix1/AL_Chart/Matrix1/Ma, Matrix1/AL_Chart/Matrix1/C2, Matrix1/AL_Chart/Matrix1/C1, S7Basis/@F_ShutDn/F_SHUT, Matrix2/AL_Chart/Matrix2/Ma, Matrix2/AL_Chart/Matrix2/E1, Matrix2/AL_Chart/Matrix2/C2, Matrix2/AL_Chart/Matrix2/C1, S7Basis/@FMatrices/Matrix2, S7Basis/@(1)/CPU410F_2, PST_F_Test/PST1

Name	Type	Parameter
F_ACK/QUIT_FROM_OS.Q	Binary Tag	DB171,DBB0+14
F_ACK/QUIT_FROM_OS.IN	Signed 16-bit...	DB171,DBB0+6
F_ACK/QUIT_FROM_OS.#comment	TEXTREF	DB171,DBB0+0
F_ACK/QUIT_FROM_OS.#blocktype	TEXTREF	DB171,DBB0+0
F_ACK/QUIT_FROM_OS.#areaname	TEXTREF	DB171,DBB0+0

The "OUT" output of F_QUITES is set to 1 for one cycle and the F-channel drivers are reintegrated.

Result

If the value 6 is written to the "IN" input of the F_QUITES block, followed by the value 9 within 60 seconds, the "OUT" output of F_QUITES is set to 1 for one cycle. The F-channel drivers connected to this output (at the "ACK_REI" input) are reintegrated if they are ready for acknowledgment (ACK_REQ = 1).



Quittierung von einen externen Taster oder mit F_QUITES von der OS.

Acknowledge via external button or F_QUITES from the OS.

If the acknowledgment prompt is no longer pending, the buttons on the OS are hidden again.

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

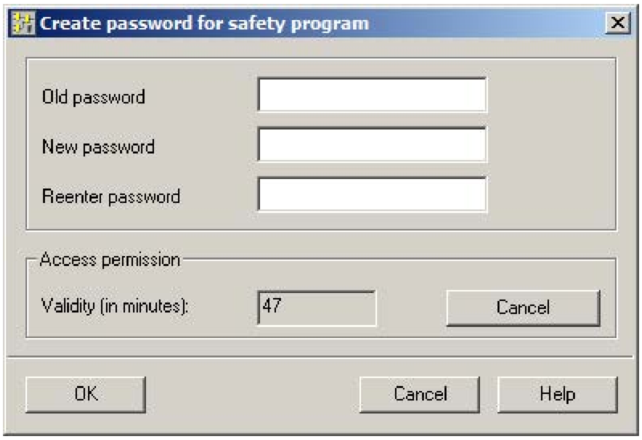
A password protects the fail-safe program and the parameters of the F-modules against unauthorized changes. The password is requested when you attempt to access fail-safe parts of the system, for example, when opening a fail-safe CFC, when compiling changes in the safety program, or when opening the properties of a fail-safe module of the runtime editor from a standard CFC.

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.


Create password for safety program

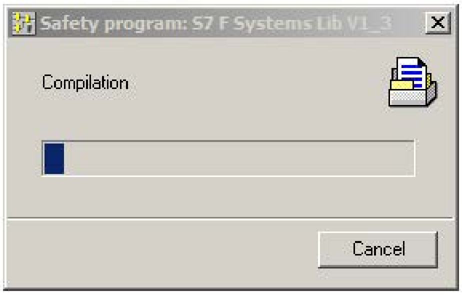
Old password
New password
Reenter password

Access permission
Validity (in minutes): 47

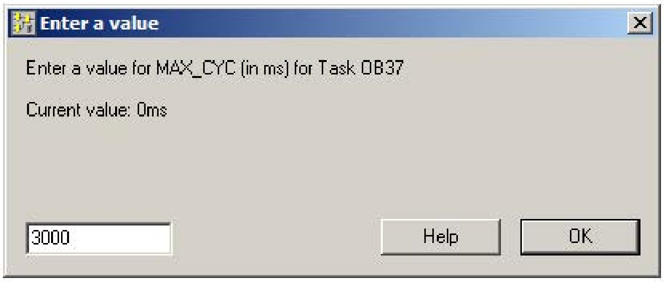
If a standard user program and a fail-safe program are running in one CPU, changes to the standard part can be compiled without the need to enter the F-password. This assumes that no changes have been made to the safety program.

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.



Compilation



Enter a value for MAX_CYC (in ms) for Task OB37

Current value: 0ms

3000

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

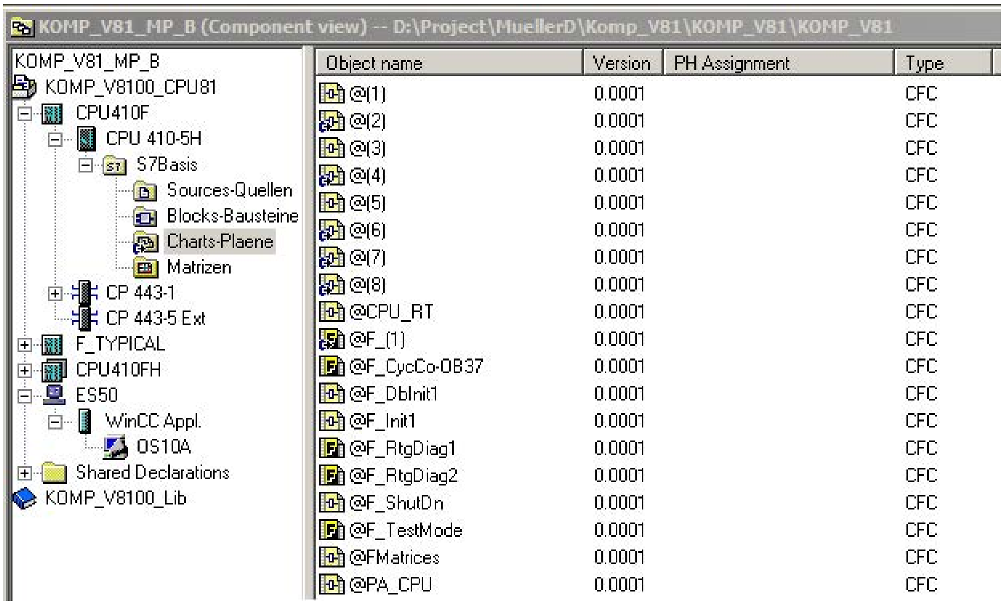
You can change the default value at the MAX_CYC input of the F_CYC_CO block in chart @F_CycCo-OB3x whenever you wish.

You can find information about setting the F-monitoring time and response times in section "Monitoring times and system response times (Page 133)".

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.



KOMP_V81_MP_B (Component view) -- D:\Project\MuellerD\Komp_V81\KOMP_V81\KOMP_V81

- KOMP_V81_MP_B
  - KOMP_V8100_CPU81
    - CPU410F
      - CPU 410-5H
        - S7Basis
          - Sources-Quellen
          - Blocks-Bausteine
          - Charts-Plaene
          - Matrizen
      - CP 443-1
      - CP 443-5 Ext
    - F_TYPICAL
    - CPU410FH
    - ES50
      - WinCC Appl.
        - OS10A
    - Shared Declarations
  - KOMP_V8100_Lib

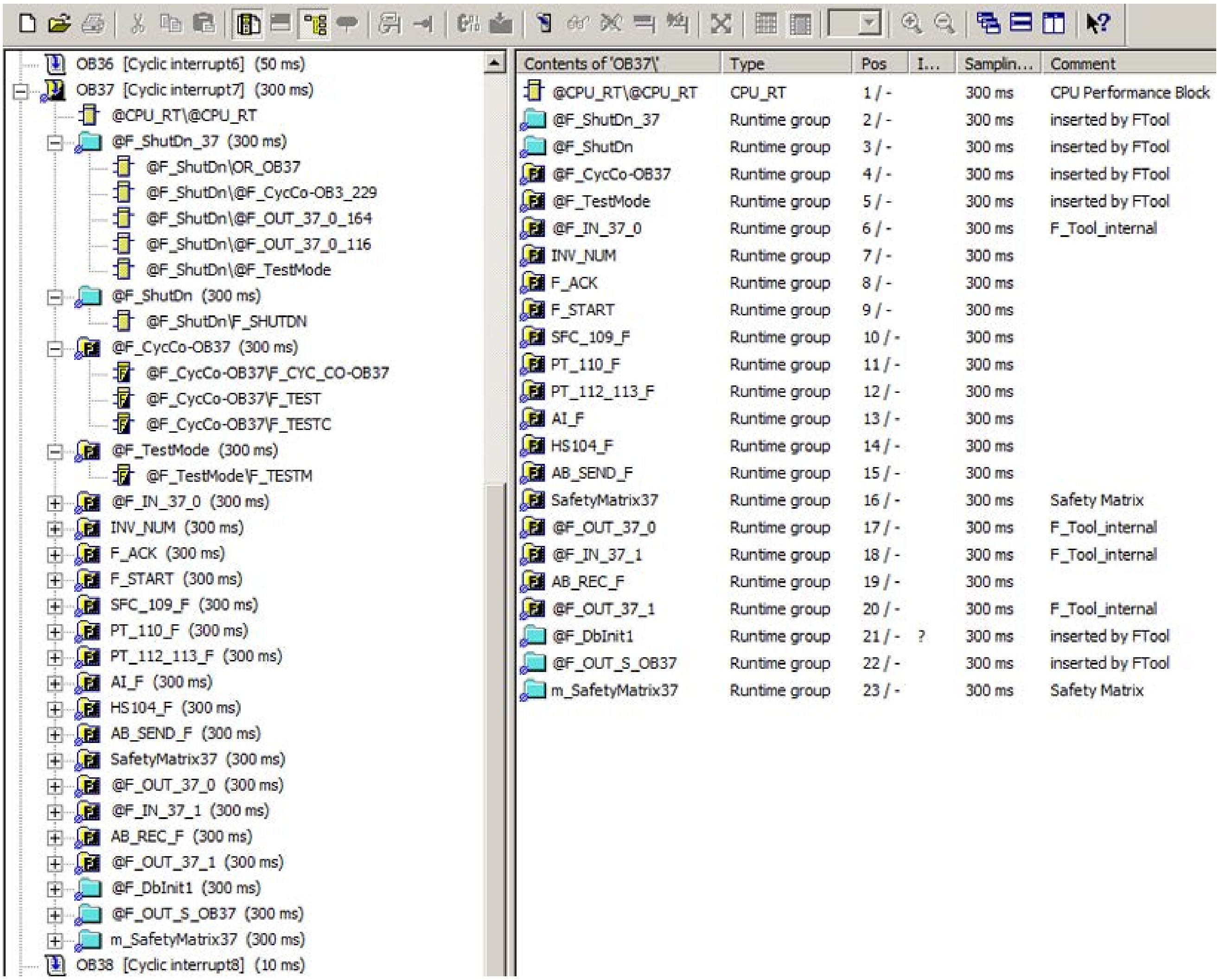
Object name	Version	PH Assignment	Type
@(1)	0.0001		CFC
@(2)	0.0001		CFC
@(3)	0.0001		CFC
@(4)	0.0001		CFC
@(5)	0.0001		CFC
@(6)	0.0001		CFC
@(7)	0.0001		CFC
@(8)	0.0001		CFC
@CPU_RT	0.0001		CFC
@F_(1)	0.0001		CFC
@F_CycCo-OB37	0.0001		CFC
@F_DbInit1	0.0001		CFC
@F_Init1	0.0001		CFC
@F_RtgDiag1	0.0001		CFC
@F_RtgDiag2	0.0001		CFC
@F_ShutDn	0.0001		CFC
@F_TestMode	0.0001		CFC
@FMatrices	0.0001		CFC
@PA_CPU	0.0001		CFC

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_".



```
OB36  [Cyclic interrupt6]  (50 ms)
OB37  [Cyclic interrupt7]  (300 ms)
    @CPU_RT\@CPU_RT
    @F_ShutDn_37  (300 ms)
        @F_ShutDn\OR_OB37
        @F_ShutDn\@F_CycCo-OB3_229
        @F_ShutDn\@F_OUT_37_0_164
        @F_ShutDn\@F_OUT_37_0_116
        @F_ShutDn\@F_TestMode
    @F_ShutDn  (300 ms)
        @F_ShutDn\F_SHUTDN
    @F_CycCo-OB37  (300 ms)
        @F_CycCo-OB37\F_CYC_CO-OB37
        @F_CycCo-OB37\F_TEST
        @F_CycCo-OB37\F_TESTC
    @F_TestMode  (300 ms)
        @F_TestMode\F_TESTM
    @F_IN_37_0  (300 ms)
    INV_NUM  (300 ms)
    F_ACK  (300 ms)
    F_START  (300 ms)
    SFC_109_F  (300 ms)
    PT_110_F  (300 ms)
    PT_112_113_F  (300 ms)
    AI_F  (300 ms)
    HS104_F  (300 ms)
    AB_SEND_F  (300 ms)
    SafetyMatrix37  (300 ms)
    @F_OUT_37_0  (300 ms)
    @F_IN_37_1  (300 ms)
    AB_REC_F  (300 ms)
    @F_OUT_37_1  (300 ms)
    @F_DbInit1  (300 ms)
    @F_OUT_S_OB37  (300 ms)
    m_SafetyMatrix37  (300 ms)
OB38  [Cyclic interrupt8]  (10 ms)
```

Contents of 'OB37\'	Type	Pos	I...	Samplin...	Comment
@CPU_RT\@CPU_RT	CPU_RT	1 / -		300 ms	CPU Performance Block
@F_ShutDn_37	Runtime group	2 / -		300 ms	inserted by FTool
@F_ShutDn	Runtime group	3 / -		300 ms	inserted by FTool
@F_CycCo-OB37	Runtime group	4 / -		300 ms	inserted by FTool
@F_TestMode	Runtime group	5 / -		300 ms	inserted by FTool
@F_IN_37_0	Runtime group	6 / -		300 ms	F_Tool_internal
INV_NUM	Runtime group	7 / -		300 ms	
F_ACK	Runtime group	8 / -		300 ms	
F_START	Runtime group	9 / -		300 ms	
SFC_109_F	Runtime group	10 / -		300 ms	
PT_110_F	Runtime group	11 / -		300 ms	
PT_112_113_F	Runtime group	12 / -		300 ms	
AI_F	Runtime group	13 / -		300 ms	
HS104_F	Runtime group	14 / -		300 ms	
AB_SEND_F	Runtime group	15 / -		300 ms	
SafetyMatrix37	Runtime group	16 / -		300 ms	Safety Matrix
@F_OUT_37_0	Runtime group	17 / -		300 ms	F_Tool_internal
@F_IN_37_1	Runtime group	18 / -		300 ms	F_Tool_internal
AB_REC_F	Runtime group	19 / -		300 ms	
@F_OUT_37_1	Runtime group	20 / -		300 ms	F_Tool_internal
@F_DbInit1	Runtime group	21 / -	?	300 ms	inserted by FTool
@F_OUT_S_OB37	Runtime group	22 / -		300 ms	inserted by FTool
m_SafetyMatrix37	Runtime group	23 / -		300 ms	Safety Matrix

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

An S7-400 F/FH system containing a fail-safe program automatically goes into safety mode when it starts up. 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 modify the safety program in active operation (RUN).

In order to make online changes to fail-safe parameters from the CFC online, or to download changes in the fail-safe program, part of the diagnostics functions must be switched off.

Safety mode must be deactivated for this purpose, before changes are made online or downloaded.

Prior to deactivating safety mode, you must ensure that the process is in a non-critical state and is being monitored by an operator during this time (monitored operation).

To download program changes in deactivated safety mode, the monitoring parts are switched off, which would detect software changes and trigger an F-STOP. "Random hardware faults" continue to be detected and the diagnostics for the modules remain active. The safety program continues to be processed to ensure that a "Demand" from the field leads to 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.

The risk analysis may reveal details of other measures that are required.

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.

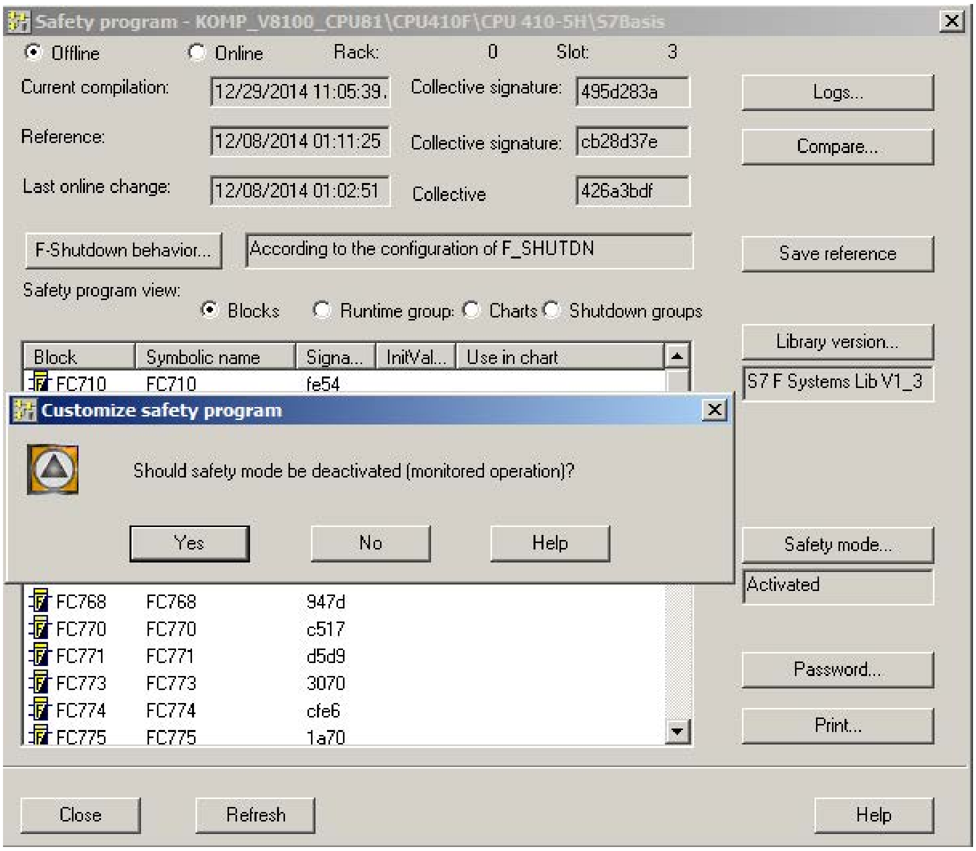
The safety mode status is entered in the CPU diagnostic buffer and reported on the OS, and can be checked in chart @F_Shutdn at the SAFE_M output of the F_SHUTDN block.

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".



Safety program - KOMP_V8100_CPU81\CPU410F\CPU 410-5H\S7Basis

● Offline ○ Online Rack: 0 Slot: 3

Current compilation: 12/29/2014 11:05:39. Collective signature: 495d283a

Reference: 12/08/2014 01:11:25 Collective signature: cb28d37e

Last online change: 12/08/2014 01:02:51 Collective 426a3bdf

F-Shutdown behavior... According to the configuration of F_SHUTDN

Safety program view: ● Blocks ○ Runtime group: ○ Charts ○ Shutdown groups

Block	Symbolic name	Signa...	InitVal...	Use in chart
FC710	FC710	fe54		
FC768	FC768	947d		
FC770	FC770	c517		
FC771	FC771	d5d9		
FC773	FC773	3070		
FC774	FC774	cfe6		
FC775	FC775	1a70		

Library version: S7 F Systems Lib V1_3

Safety mode: Activated

Customize safety program

Should safety mode be deactivated (monitored operation)?

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.
- The changes must undergo a function test that complies with relevant standards (e.g. IEC 61511-1) before the program can be imported into the active plant.
  As a general principle, the effect of changes on the system characteristics (program runtime, etc.) must be analyzed. 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.

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 following 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. On S7 F/FH systems, you need to run this comparison for both CPUs.

See also

Tracking changes in the safety program (Page 178)

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

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

- Safety Data Write (SDW)
- Safety Matrix
- F_QUITES for fail-safe acknowledgment
- Maintenance Override Switch (MOS)

7.10.1 Safety Data Write (SDW)

Introduction

The "Safety Data Write" function enables safety-related changes to be made to F-parameters in the safety program of an F-CPU via 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. Modified values of F-parameters can also be retained following a restart (warm restart) of F/FH systems.

S7 F-systems offers the following for SDW:

- Two F-blocks, which you integrate into the CFC charts in your safety program
  - F_CHG_R: SDW for F_REAL data type F-parameters
  - F_CHG_BO: SDW for F_BOOL data type F-parameters
- Associated faceplates, which you integrate into your OS. Two identification values (Safe_ID1 and Safe_ID2) are used to uniquely assign each faceplate to a block in an AS.

Transaction for SDW

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

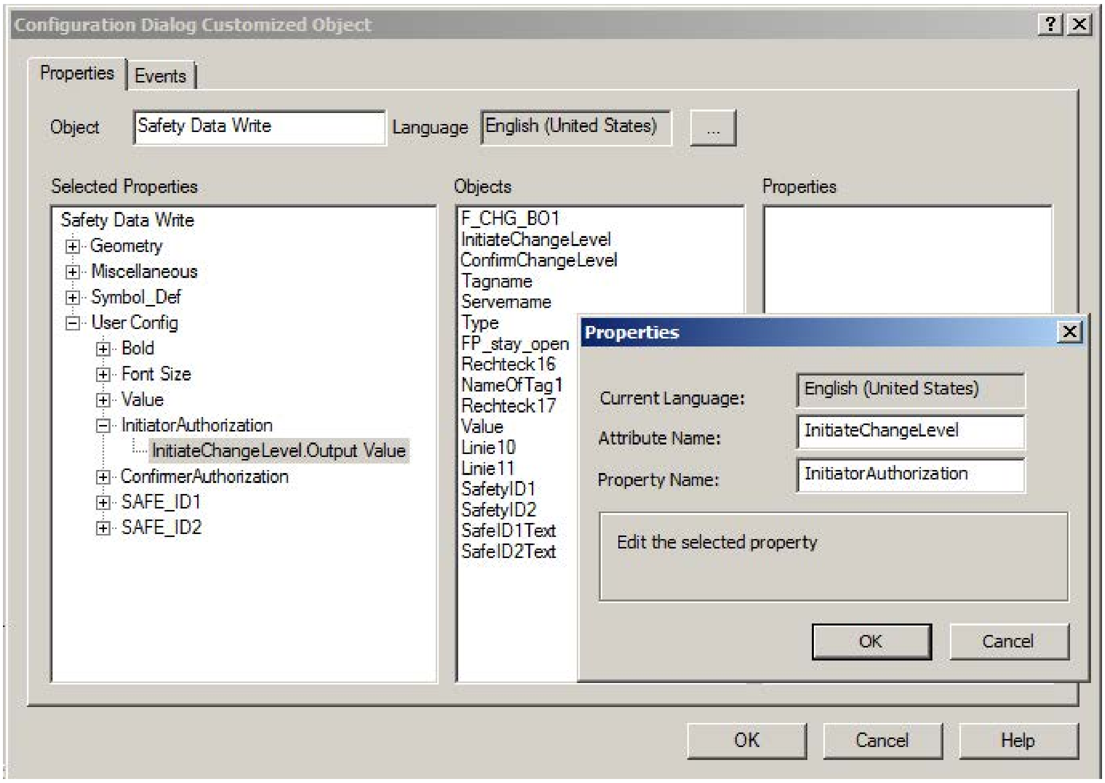
Operator types for SDW

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 authorizations and Safe_IDs are set in the faceplate properties. They are overwritten with the default settings whenever the faceplates are updated, however. To prevent this, enter the parameters in the file @@PCS7Typicals.CFG.

which you can find in the project path of the OS server project on the ES, under wincproj\<OSname>\WScripts.

The names of these attributes and properties can be found in the configuration dialog of the block icon, by selecting the block icon followed by "Configuration dialog..." in the context menu.


Configuration Dialog Customized Object

Object: Safety Data Write
Language: English (United States)

Selected Properties

- Safety Data Write
  - Geometry
  - Miscellaneous
  - Symbol_Def
  - User Config
    - Bold
    - Font Size
    - Value
    - InitiatorAuthorization
      - InitiateChangeLevel.Output Value
    - ConfirmerAuthorization
    - SAFE_ID1
    - SAFE_ID2

Objects

F_CHG_BO1
InitiateChangeLevel
ConfirmChangeLevel
Tagname
Servername
Type
FP_stay_open
Rechteck16
NameOfTag1
Rechteck17
Value
Linie10
Linie11
SafetyID1
SafetyID2
SafeID1Text
SafeID2Text

Properties

Current Language: English (United States)
Attribute Name: InitiateChangeLevel
Property Name: InitiatorAuthorization

Edit the selected property

In file @@PCS7Typicals.CFG, you will need to extend the [Columns] and [Column00] sections. The name of the property is entered in [Columns] and the attribute name in [Column00]. The sections should then appear as shown below (please note that they are case-sensitive).

Since the sections already contain entries for properties and attributes, you need to proceed to the last line in each case. Start with the first unused number (in the example: last number used = 10, first unused number = 11 = N), and increase the number for each entry.

```
[Columns]
…(existing entries)
ColumnN = SAFE_ID1
TypeN = 3
ColumnN+1 = SAFE_ID2
TypeN+1 = 3
ColumnN+2 = InitiatorAuthorization
TypeN+2 = 3
ColumnN+3 = ConfirmerAuthorization
TypeN+3 = 3
```

```
[Column00]
…(existing entries)
[ColumnN]
Property0 = SAFE_ID1
[ColumnN+1]
Property0 = SAFE_ID2
[ColumnN+2]
Property0 = InitiateChangeLevel
[ColumnN+3]
Property0 = ConfirmChangeLevel
```

Note

For more details on SDW, please refer to the "SIMATIC Industrial Software S7 F/FH Systems – Configuring and Programming" (https://support.industry.siemens.com/cs/ww/en/view/101509838) manual.

For more information on the structure of the @@PCS7Typicals.CFG file, refer to the WinCC Information System (Start > Simatic > WinCC > WinCC Information System in the contents under Options > Options for Process Control > Graphic Object Update Wizard > Structure of the Configuration File).

7.10.2 F_QUITES

Using the "F_QUITES" F block, the OS can generate fail-safe pulses in the F program of the automation system. You can find an application example for F_QUITES in "Implementing F user acknowledgment in the OS", in Section Programming reintegration following module errors or channel errors requiring acknowledgment (Page 110).

7.10.3 Maintenance Override Switch (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.

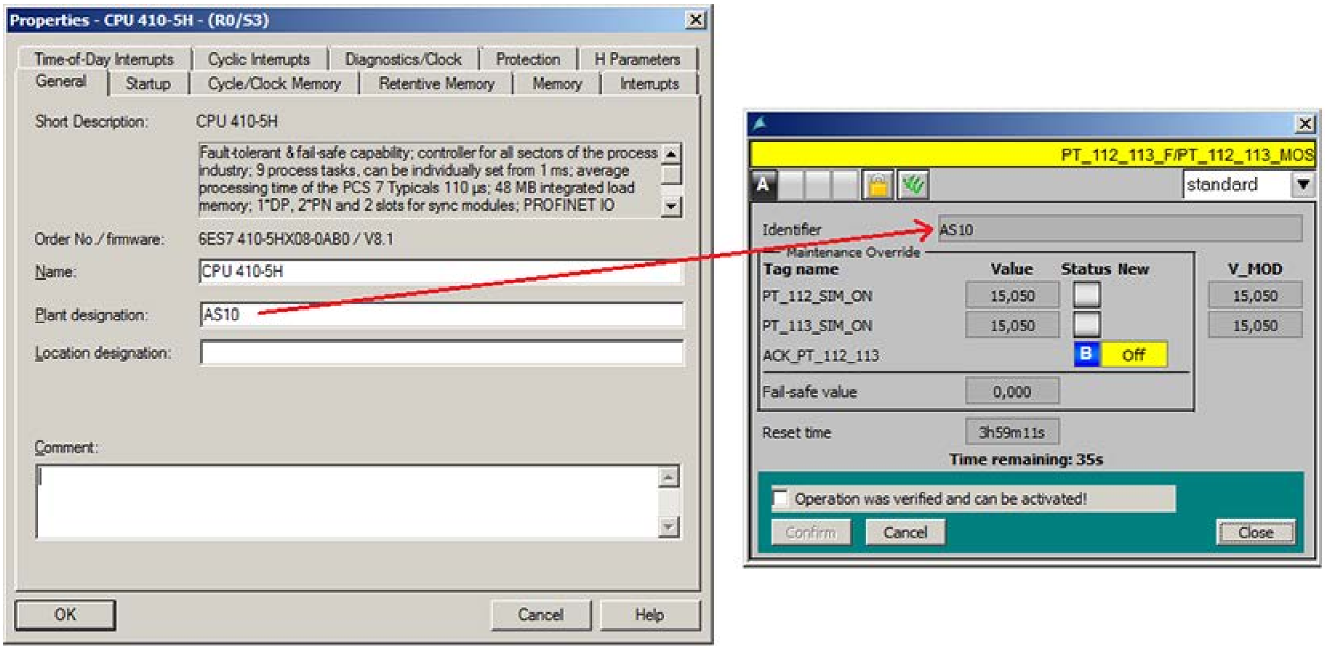
Transaction for MOS

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 authorizations are set in the faceplate properties. The connection IDs are generated by the system automatically, in contrast with SDW. 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.


Properties - CPU 410-5H - (R0/S3)

Short Description: CPU 410-5H

Fault-tolerant & fail-safe capability; controller for all sectors of the process industry; 9 process tasks, can be individually set from 1 ms; average processing time of the PCS 7 Typicals 110 µs; 48 MB integrated load memory; 1*DP, 2*PN and 2 slots for sync modules; PROFINET IO

Order No./ firmware: 6ES7 410-5HX08-0AB0 / V8.1

Name: CPU 410-5H

Plant designation: AS10

Location designation:

Comment:

PT_112_113_F/PT_112_113_MOS

standard

Identifier: AS10

Maintenance Override

Tag name	Value	Status	New	V_MOD
PT_112_SIM_ON	15,050	□		15,050
PT_113_SIM_ON	15,050	□		15,050
ACK_PT_112_113		B	Off	
Fail-safe value	0,000			

Reset time: 3h59m11s

Time remaining: 35s

□ Operation was verified and can be activated!

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.

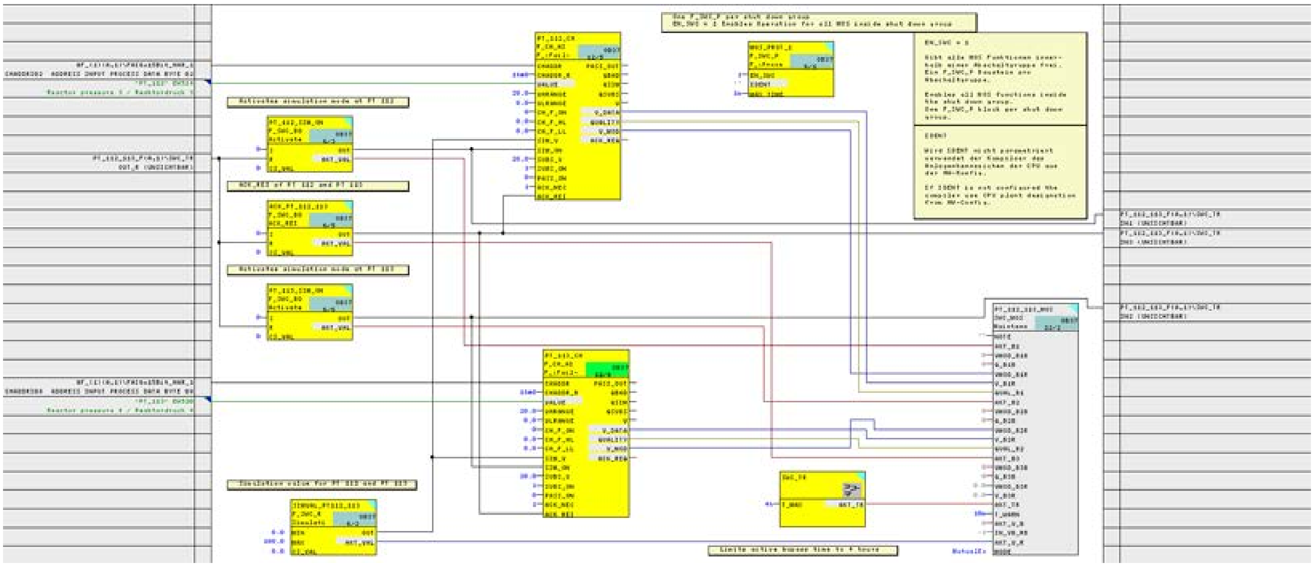
At the "MODE" input of the "SWC_MOS" block, it is determined whether all three BOOL values can be activated at the same time ("Norestrictions"), or if just one ("MutualExclBypass") BOOL value can be activated in each case.

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:

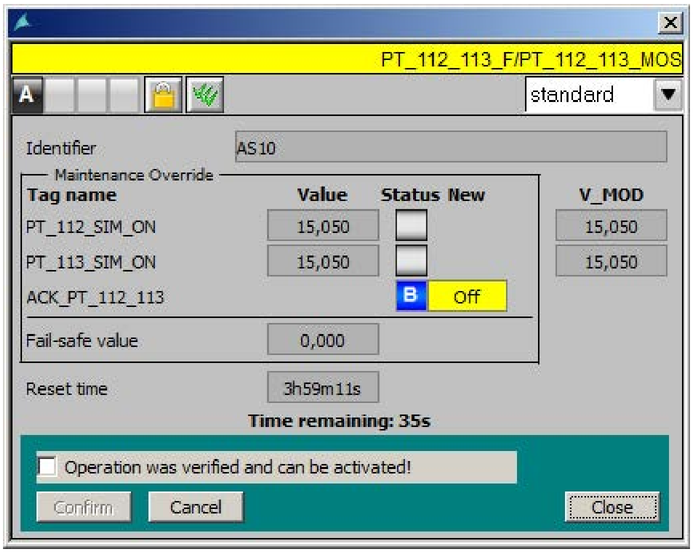


Note

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.



PT_112_113_F/PT_112_113_MOS

Identifier: AS10

Maintenance Override

Tag name	Value	Status New	V_MOD
PT_112_SIM_ON	15,050	□	15,050
PT_113_SIM_ON	15,050	□	15,050
ACK_PT_112_113		B Off	
Fail-safe value	0,000		

Reset time: 3h59m11s

Time remaining: 35s

□ Operation was verified and can be activated!

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.

Both the availability and the safety of the F/FH system must be taken into account when configuring monitoring times.

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

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

The Excel file "s7ftimea.xlsm" is used for the purpose of calculating the monitoring and response times 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-SG (Lib V1_3)
  Here, you will find the runtimes of the F-blocks from F-library 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.
- max. runtime F-SG (Lib V1_2)
  Here, you will find the runtimes of the F-blocks from F-library V1_2 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.
- Typ. Response times
  A wizard for estimating the typical response time

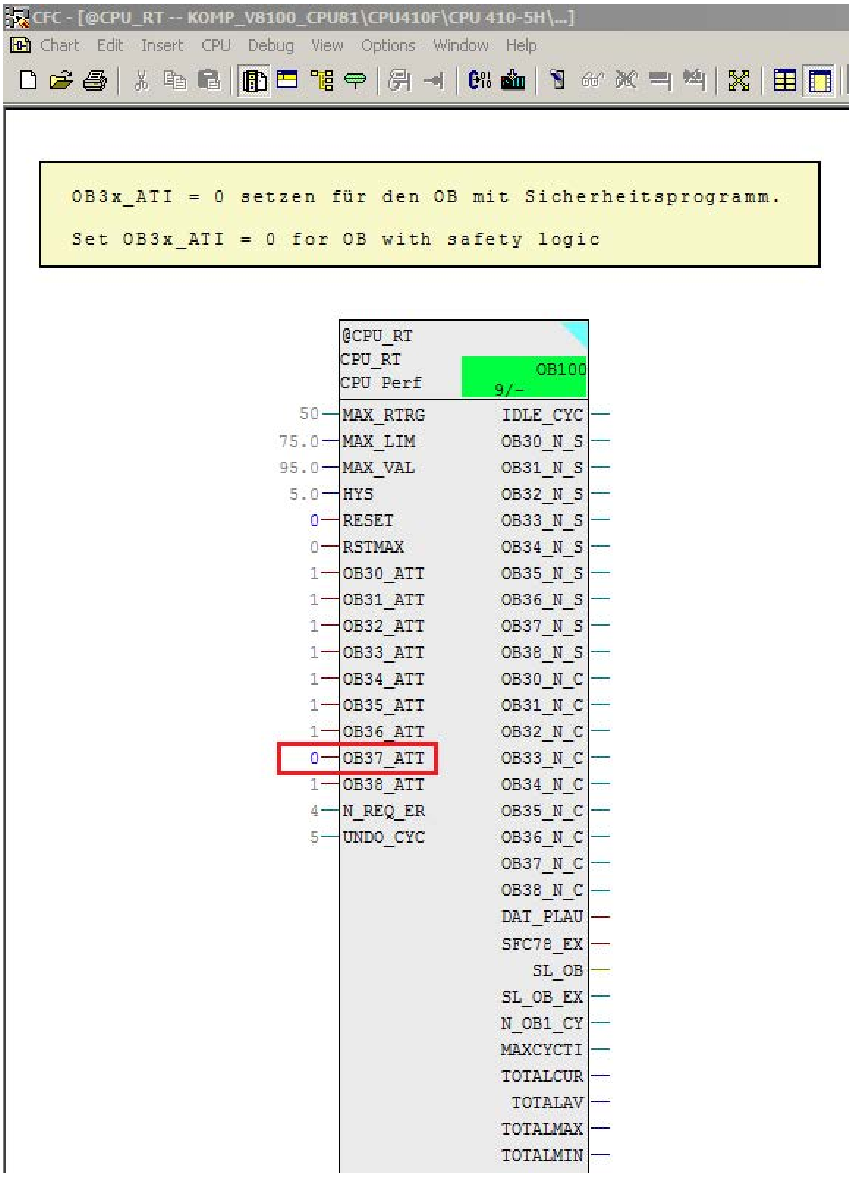
7.11.1 Diagnostic block "CPU_RT"

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.



OB3x_ATI = 0 setzen für den OB mit Sicherheitsprogramm.

Set OB3x_ATI = 0 for OB with safety logic

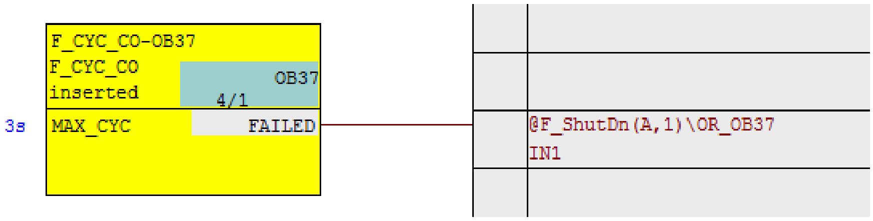
```
  50—MAX_RTRG
75.0—MAX_LIM
95.0—MAX_VAL
 5.0—HYS
   0—RESET
   0—RSTMAX
   1—OB30_ATT
   1—OB31_ATT
   1—OB32_ATT
   1—OB33_ATT
   1—OB34_ATT
   1—OB35_ATT
   1—OB36_ATT
   0—OB37_ATT
   1—OB38_ATT
   4—N_REQ_ER
   5—UNDO_CYC
```

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/109738089) 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

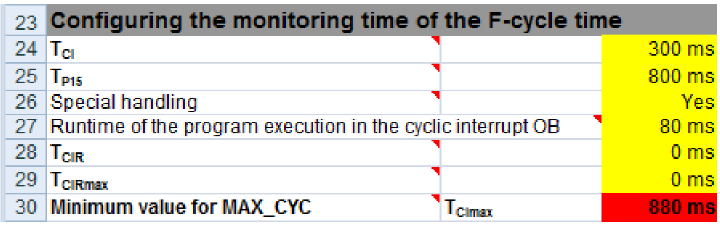
The first time the F-program is compiled, you will be prompted to enter a value for the maximum cycle time (MAX_CYC) which may elapse between two calls to this cyclic interrupt OB. The default for the maximum F-cycle time is 3000 ms.

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 "s7ftimea.xlsm" Excel file:

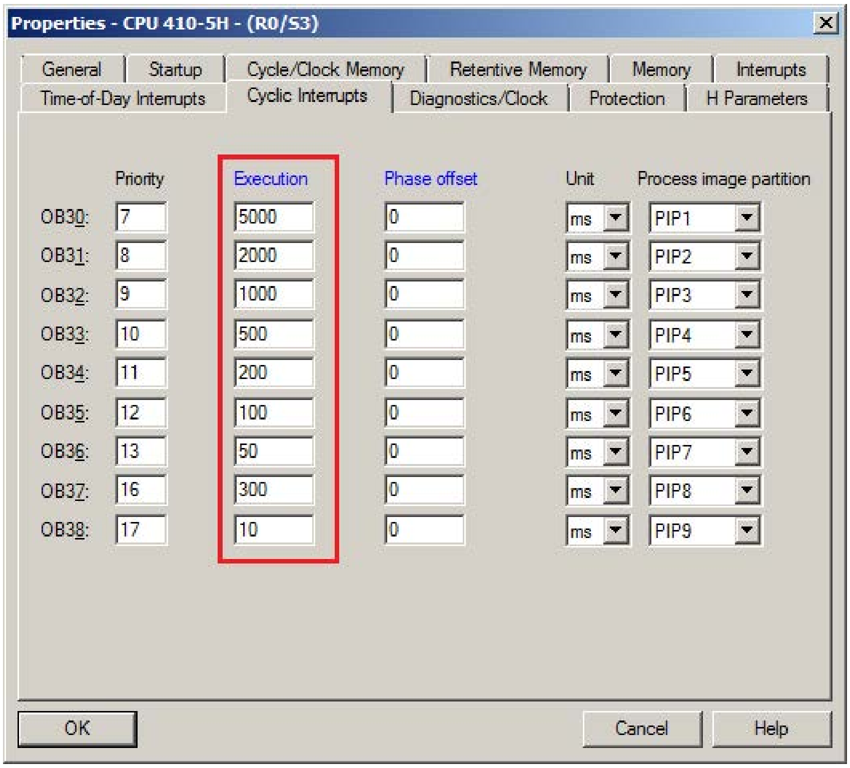


23	**Configuring the monitoring time of the F-cycle time**		
24	T_{CI}		300 ms
25	T_{P15}		800 ms
26	Special handling		Yes
27	Runtime of the program execution in the cyclic interrupt OB		80 ms
28	T_{CIR}		0 ms
29	T_{CIRmax}		0 ms
30	**Minimum value for MAX_CYC**	T_{CImax}	880 ms

To prevent monitoring from being triggered when no errors are present, MAX_CYC must be set higher than the T_{CImax} calculated for the corresponding cyclic interrupt OB.

- For non-redundant S7 F/FH systems:
  - The setting for T_{CImax} must be at least as high as the configured execution time (T_{CI}) 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.

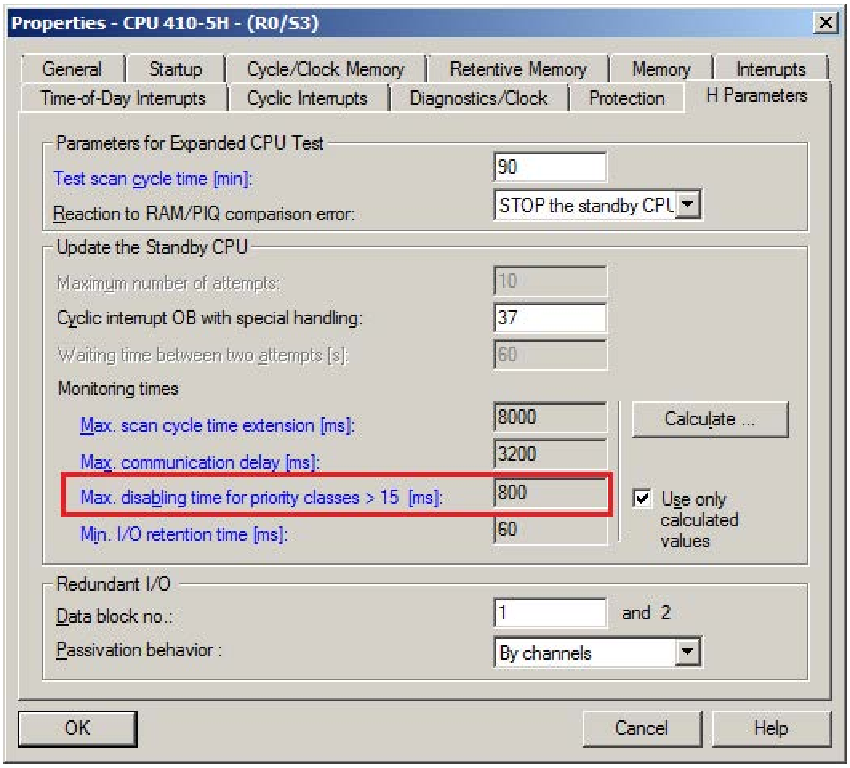
You can find the value for T_{CI} in the "Execution" column of the relevant cyclic interrupt OB, located on the "Cyclic Interrupts" tab in the CPU properties.



Properties - CPU 410-5H - (R0/S3)

	Priority	Execution	Phase offset	Unit	Process image partition
OB30:	7	5000	0	ms	PIP1
OB31:	8	2000	0	ms	PIP2
OB32:	9	1000	0	ms	PIP3
OB33:	10	500	0	ms	PIP4
OB34:	11	200	0	ms	PIP5
OB35:	12	100	0	ms	PIP6
OB36:	13	50	0	ms	PIP7
OB37:	16	300	0	ms	PIP8
OB38:	17	10	0	ms	PIP9

Parameter T_{P15} is the same as the "Max. disabling time for priority classes > 15" parameter from the H parameters of the CPU.



Parameters for Expanded CPU Test
Test scan cycle time [min]: 90
Reaction to RAM/PIQ comparison error: STOP the standby CPU

Update the Standby CPU
Maximum number of attempts: 10
Cyclic interrupt OB with special handling: 37
Waiting time between two attempts [s]: 60
Monitoring times
Max. scan cycle time extension [ms]: 8000
Max. communication delay [ms]: 3200
Max. disabling time for priority classes > 15 [ms]: 800
Min. I/O retention time [ms]: 60
☑ Use only calculated values

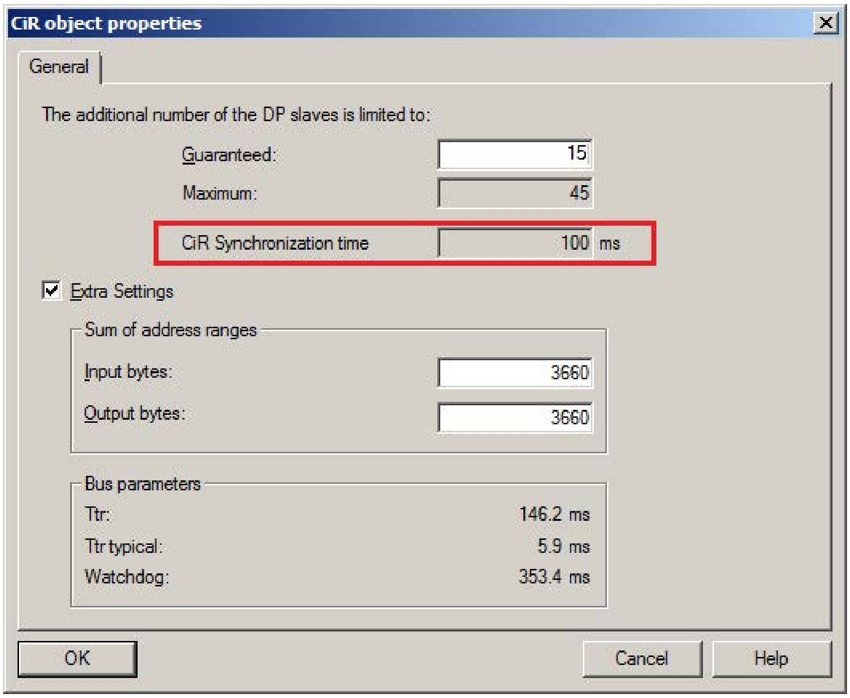
Redundant I/O
Data block no.: 1 and 2
Passivation behavior : By channels

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.



CiR object properties

General

The additional number of the DP slaves is limited to:

Guaranteed: 15

Maximum: 45

CiR Synchronization time 100 ms

☑ Extra Settings

Sum of address ranges

Input bytes: 3660

Output bytes: 3660

Bus parameters

Ttr: 146.2 ms

Ttr typical: 5.9 ms

Watchdog: 353.4 ms

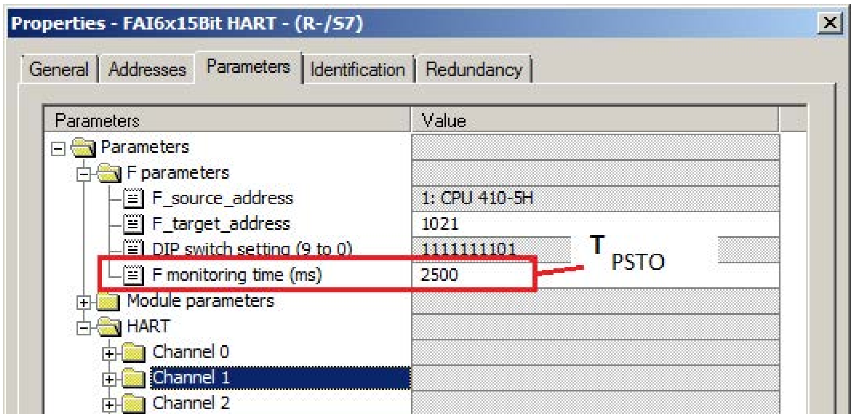
Note

For more information on CiR, refer to the "SIMATIC STEP7 V5.5 Modifying the System during Operation via CiR" (https://support.industry.siemens.com/cs/ww/en/view/45531308) manual.

7.11.3 Communication monitoring time for F CPU/F signal modules

Time monitoring of PROFIsafe or PROFINET communication is implemented in the F-signal modules 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.

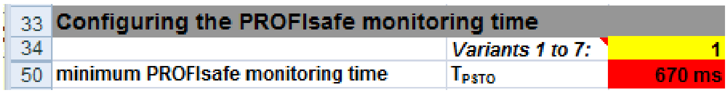


Properties - FAI6x15Bit HART - (R-/S7)

Parameters	Value
Parameters	
F parameters	
F_source_address	1: CPU 410-5H
F_target_address	1021
DIP switch setting (9 to 0)	1111111101
F monitoring time (ms)	2500
Module parameters	
HART	
Channel 0	
Channel 1	
Channel 2	

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.

You can determine the shortest possible F-monitoring time using S7tftimea.xlsm.



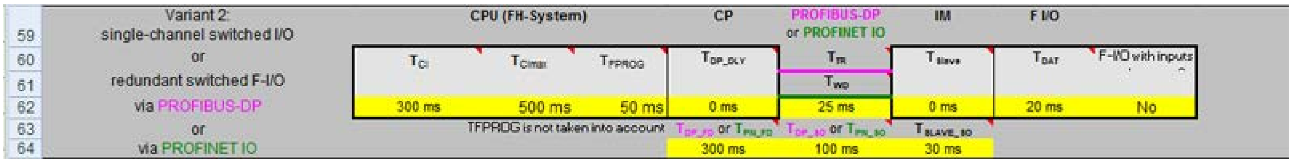
33	**Configuring the PROFIsafe monitoring time**		
34		*Variants 1 to 7:*	1
50	minimum PROFIsafe monitoring time	T_{PSTO}	670 ms

Depending on the hardware configuration in question, S7ftimea.xlsm distinguishes between 7 different options:

- Variant 1:
  Singular system with F-signal modules in PROFIBUS DP or PROFINET IO slaves
- Variant 2:
  Redundant system with F-signal modules in a switched (ET 200M) PROFIBUS DP slave or PROFINET IO slaves
- Variant 3:
  Singular system with F-PA devices on a PROFIBUS DP/PA coupler
- Variant 4:
  Singular system with F-PA devices on a PROFIBUS DP/PA link
- Variant 5:
  Redundant system with F-PA devices on a switched PROFIBUS DP/PA link
- Variant 6:
  Redundant system with F-DP devices on a switched PROFIBUS Y link
- Version 7:

  Single or redundant system with F-DP devices on an IE/PB link PCS 7 does not support the variant.

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.



59	Variant 2: single-channel switched I/O	CPU (FH-System)			CP	PROFIBUS-DP or PROFINET IO	IM	F I/O	
60	or	T_{CI}	T_{CImax}	T_{FPROG}	T_{DP_DLY}	T_{TR}	T_{Slave}	T_{DAT}	F-I/O with inputs
61	redundant switched F-I/O					T_{WD}			
62	via PROFIBUS-DP	300 ms	500 ms	50 ms	0 ms	25 ms	0 ms	20 ms	No
63	or	TFPROG is not taken into account			T_{DP_FD} or T_{PN_FD}	T_{DP_SO} or T_{PN_SO}	T_{SLAVE_SO}		
64	via PROFINET IO				300 ms	100 ms	30 ms		

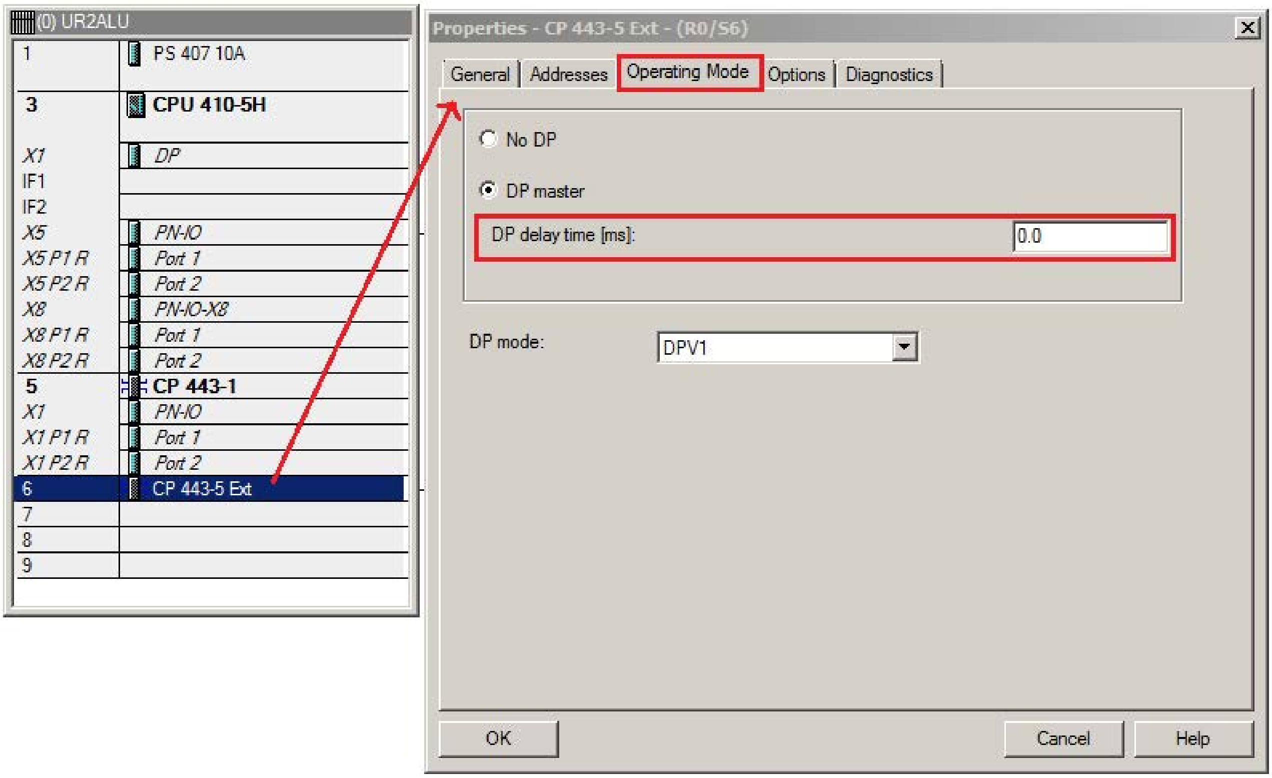
You need the following parameters for the calculation depending on the variant:

T_{CI}	Configured execution time of the cyclic interrupt OB in which the F-module driver is processed
T_{PROG}	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_{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.
$T_{F\text{-}SIGNAL\ MODULE,\ ACK}$	Maximum acknowledgment time of the fail-safe I/O module in safety mode (F signal module group data sheet)
T_{DP_DLY}	Additional delay time with external DP interface (via CP 443-5 Extended)

When Profinet IO is used, the following PROFINET network parameters are required	
T_{WD}	Watchdog time of PROFINET IO devices. This can be found in the "IO cycle" tab in the properties of the PROFINET IO device. If no watchdog time is specified for the IO device, use three times the update time from the properties of the PROFINET IO system.
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.



(0) UR2ALU	
1	PS 407 10A
3	CPU 410-5H
X1	DP
IF1	
IF2	
X5	PN-IO
X5 P1 R	Port 1
X5 P2 R	Port 2
X8	PN-IO-X8
X8 P1 R	Port 1
X8 P2 R	Port 2
5	CP 443-1
X1	PN-IO
X1 P1 R	Port 1
X1 P2 R	Port 2
6	CP 443-5 Ext
7	
8	
9	

Properties - CP 443-5 Ext - (R0/S6)

○ No DP

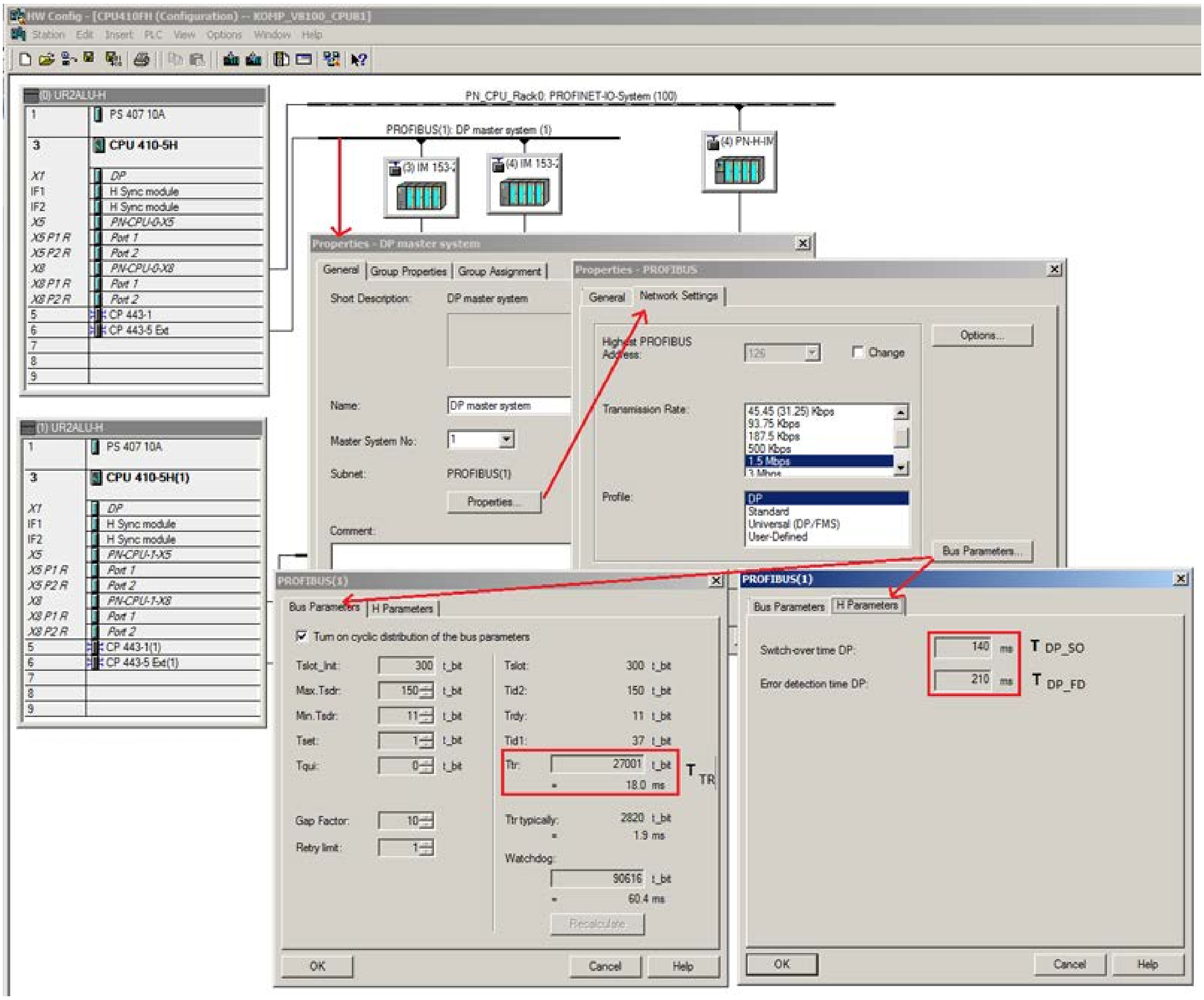
● DP master

DP delay time [ms]: 0.0

DP mode: DPV1

$T_{TR7TR1/TR2}$/T_{DP_FD}/T_{DP_SO} parameter

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:



Properties - DP master system

General | Group Properties | Group Assignment

Short Description: DP master system

Name: DP master system

Master System No.: 1

Subnet: PROFIBUS(1)

Properties...

Comment:

Properties - PROFIBUS

General | Network Settings

Highest PROFIBUS Address: 126 □ Change

Transmission Rate: 45.45 (31.25) Kbps, 93.75 Kbps, 187.5 Kbps, 500 Kbps, **1.5 Mbps**, 3 Mbps

Profile: **DP**, Standard, Universal (DP/FMS), User-Defined

Options... | Bus Parameters...

PROFIBUS(1)

Bus Parameters | H Parameters

☑ Turn on cyclic distribution of the bus parameters

Tslot_Init:	300	t_bit	Tslot:	300	t_bit
Max. Tsdr:	150	t_bit	Tid2:	150	t_bit
Min. Tsdr:	11	t_bit	Trdy:	11	t_bit
Tset:	1	t_bit	Tid1:	37	t_bit
Tqui:	0	t_bit	Ttr:	27001	t_bit
			=	18.0	ms
Gap Factor:	10		Ttr typically:	2820	t_bit
Retry limit:	1		=	1.9	ms
			Watchdog:	90616	t_bit
			=	60.4	ms

T_{TR}

Recalculate

OK | Cancel | Help

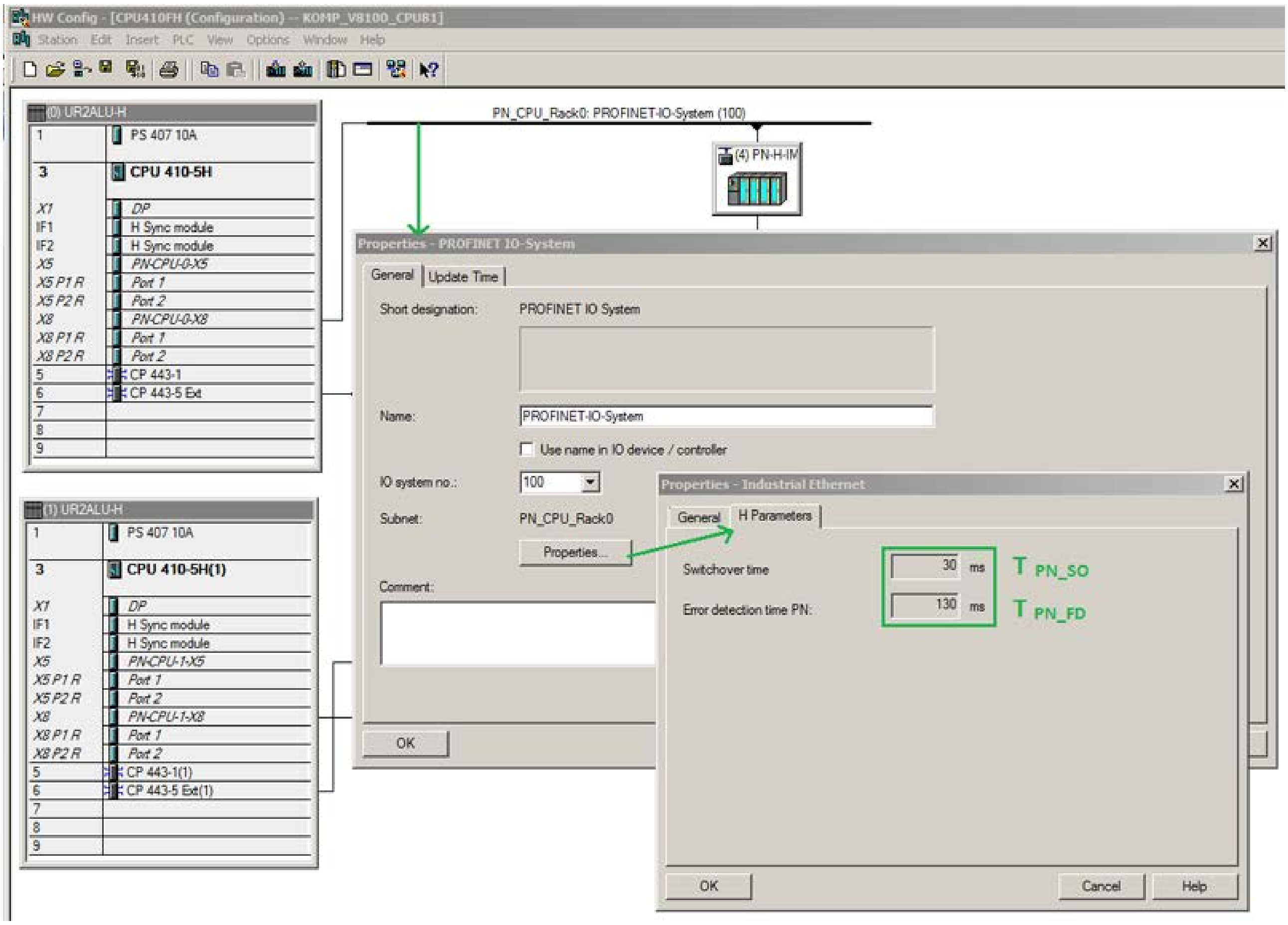
PROFIBUS(1)

Bus Parameters | H Parameters

Switch-over time DP: 140 ms T_{DP_SO}

Error detection time DP: 210 ms T_{DP_FD}

OK | Cancel | Help


HW Config - [CPU410FH (Configuration) -- KOMP_V8100_CPU81]
Station Edit Insert PLC View Options Window Help
PN_CPU_Rack0: PROFINET-IO-System (100)
(4) PN-H-IM
Properties - PROFINET IO-System
General
Update Time
Properties...
OK
Properties - Industrial Ethernet
General
H Parameters
OK
Cancel
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	

Short designation: PROFINET IO System

Name: PROFINET-IO-System

□ Use name in IO device / controller

IO system no.: 100

Subnet: PN_CPU_Rack0

Comment:

Switchover time: 30 ms T_{PN_SO}

Error detection time PN: 130 ms T_{PN_FD}

T_{SLAVE_SO} parameter

T_{SLAVE_SO} depends on the IM used.

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 modules
	-2Bx00	30 ms	Any configuration
	-2Bxx1	30 ms	Without F, FM, or HART modules
	-2Bxx2	30 ms	

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_{Slave} parameter

Maximum delay time with the IM:

- 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/98821323)).

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

$T_{Y\_L\_DLY}$ parameter

- Additional delay time with a Y link in the redundant system

Precondition	Switchover time
Delay time with a Y link	5 ms

T_{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:

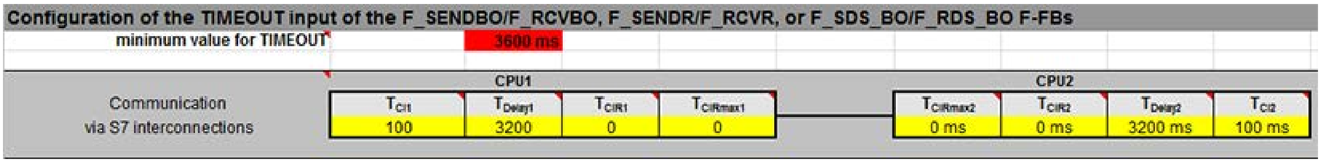
Module	Acknowledgment time in safety mode
SM326; DI x 24 DC 24V 6ES7326-1BK01-0AB0	With sensor evaluation 1oo1 (1v1): Max. 29 ms
	With sensor evaluation 1oo2 (2v2): Max. 30 ms
SM326; DI x 24 DC 24V 6ES7326-1BK02-0AB0	With sensor evaluation 1oo1 (1v1): Max. 29 ms
	With sensor evaluation 1oo2 (2v2): Max. 29 ms
SM326; DI 8 x NAMUR 6ES7326-1RF00-0AB0 6ES7326-1RF01-0AB0	Max. 68 ms
SM326; DO 10 x DC 24V/2A 6ES7326-2BF01-0AB0	Max. 20 ms
SM326; F-DO 10 x DC 24V/2A PP 6ES7326-2BF10-0AB0	Max. 10 ms
SM326; F-DO 8 x DC 24V/2A PM 6ES7326-2BF40-0AB0	Max. 14 ms
SM326; F-DO 8 x DC 24V/2A PM 6ES7326-2BF41-0AB0	Max. 18 ms
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
SM336; F-AI 6 x 0/4 ... 20 mA HART 6ES7336-4GE00-0AB0	100 ms
EM 8 F-DI Ex NAMUR 6ES7138-7FN00-0AB0	Max. 26 ms

Module	Acknowledgment time in safety mode
EM 4 F-DO Ex 17.4V/40mA 6ES7138-7FD00-0AB0	Max. 59 ms
EM 4 F-AI Ex HART 6ES7138-7FA00-0AB0	• Typ. response 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 S7ftimea.xlsm.



Configuration of the TIMEOUT input of the F_SENDBO/F_RCVBO, F_SENDR/F_RCVR, or F_SDS_BO/F_RDS_BO F-FBs

minimum value for TIMEOUT 3600 ms

	CPU1				CPU2			
	T_{CI1}	T_{Delay1}	T_{CiR1}	$T_{CiRmax1}$	$T_{CiRmax2}$	T_{CiR2}	T_{Delay2}	T_{CI2}
Communication via S7 interconnections	100	3200	0	0	0 ms	0 ms	3200 ms	100 ms

You will need the following parameters to calculate the "TIMEOUT" parameter:

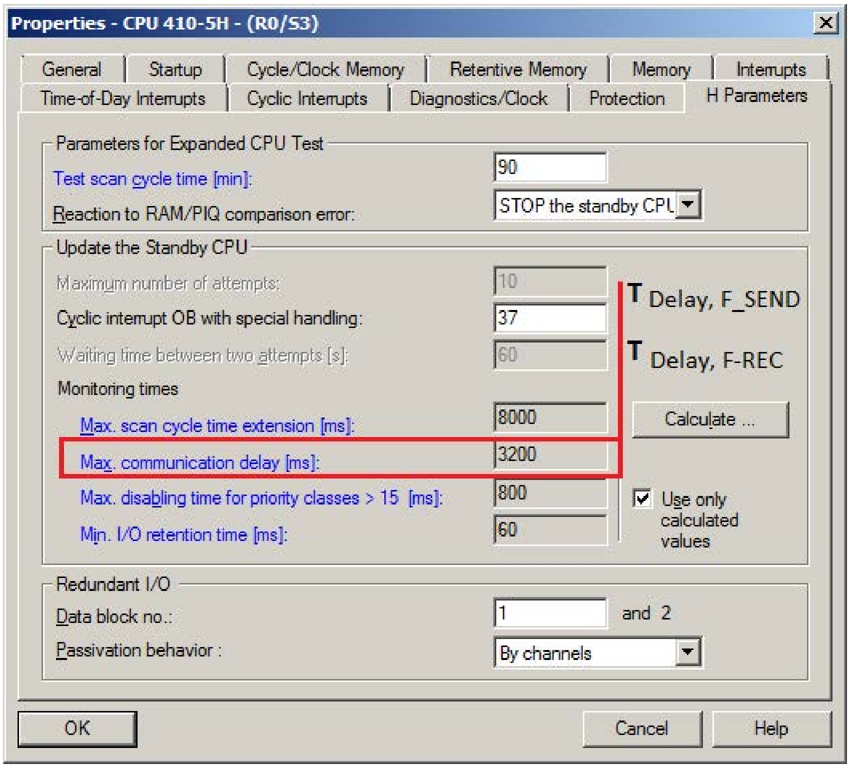
Communication between F-CPUs (TIMEOUT parameter)	
CPU 1, sender	
T_{CI1}	Configured cycle time of the cyclic interrupt OB in which the send blocks F_SENDBO or F_SENDR are called.
$T_{Delay1,\ F\_SEND}$	Maximum communication delay when updating the standby in the S7 FH system with call of F_SENDBO or 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.
$T_{Delay2,\ F\text{-}Rec}$	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 133).

$T_{Delay1/Delay2}$ parameters

You can find these parameters in the H parameters within the CPU properties.



Properties - CPU 410-5H - (R0/S3)

Parameters for Expanded CPU Test

Test scan cycle time [min]: 90

Reaction to RAM/PIQ comparison error: STOP the standby CPU

Update the Standby CPU

Maximum number of attempts: 10

Cyclic interrupt OB with special handling: 37

Waiting time between two attempts [s]: 60

Monitoring times

Max. scan cycle time extension [ms]: 8000

Max. communication delay [ms]: 3200

Max. disabling time for priority classes > 15 [ms]: 800

Min. I/O retention time [ms]: 60

☑ Use only calculated values

Redundant I/O

Data block no.: 1 and 2

Passivation behavior : By channels

T Delay, F_SEND

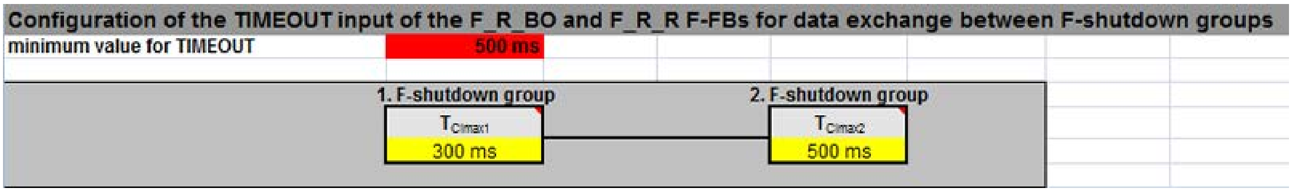
T Delay, F-REC

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_R F FBs and configured at the "TIMEOUT" input parameter of the receive block.

To prevent time monitoring from being triggered when no errors are present, 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 time can be determined using S7ftimea.xls.



Configuration of the TIMEOUT input of the F_R_BO and F_R_R F-FBs for data exchange between F-shutdown groups

minimum value for TIMEOUT 500 ms

1. F-shutdown group
T_{CImax1}
300 ms

2. F-shutdown group
T_{CImax2}
500 ms

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 process safety time depends on the type of process and must be specified individually.

How to calculate the response time

In S7ftimea.xlsm, the route of a signal from the sensor to the actuator via the system can be broken down into five possible sections:

1. Input:
   Runtime from sensor to user program
2. Processing in the 1st F-CPU:
   Cycle time and run time 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 run time 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:

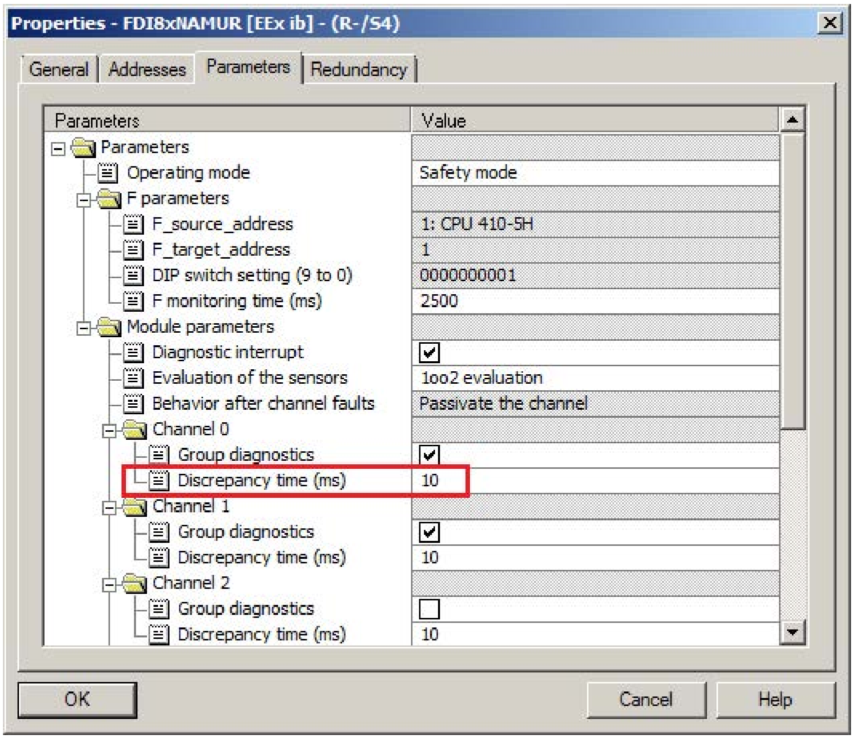
$T_{Sensor\_DLY}/T_{Actuator\_DLY}$	Delay time of sensor or actuator
T_{DIS}	Maximum discrepancy time
T_{WCDT}	Worst Case Delay Time Maximum response time when no errors are present
T_{OFDT}	One Fault Delay Time Maximum response time when an error is present
T_{DAT}	Maximum acknowledgment time of the 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_{DP_DLY}	Additional delay time with external DP interface (via CP 443-5 Extended)

$T_{Sensor\_DLY}/T_{Actuator\_DLY}$ 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 (2v2) has been selected in the hardware configuration of the F-signal module.



Properties - FDI8xNAMUR [EEx ib] - (R-/S4)

Parameters	Value
Parameters	
Operating mode	Safety mode
F parameters	
F_source_address	1: CPU 410-5H
F_target_address	1
DIP switch setting (9 to 0)	0000000001
F monitoring time (ms)	2500
Module parameters	
Diagnostic interrupt	☑
Evaluation of the sensors	1oo2 evaluation
Behavior after channel faults	Passivate the channel
Channel 0	
Group diagnostics	☑
Discrepancy time (ms)	10
Channel 1	
Group diagnostics	☑
Discrepancy time (ms)	10
Channel 2	
Group diagnostics	□
Discrepancy time (ms)	10

Enter 0 if:

- No 1oo2 (2v2) evaluation is performed on the module.
- The value 0 is immediately output in the event of a discrepancy.

T_{WCDT}/T_{OFDT} 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 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)

<table>
<tr><th>F signal module</th><th>T_{WCDT}</th><th>T_{OFDT}</th></tr>
<tr><td rowspan="2">DI 24 x DC 24 V
6ES7326-1BK02-0AB0</td><td rowspan="2">= Max. internal processing time + input delay + short-circuit test time
= 23 ms + 3 ms + 6 ms = 32 ms</td><td>= 31 ms with 1oo1 evaluation</td></tr>
<tr><td>= 29 ms with 1oo2 evaluation
With parameter assignment: "Provide last valid value", the set discrepancy time has to be added.</td></tr>
<tr><td>DI 8 x NAMUR
6ES7326-1RF00-0AB0
6ES7326-1RF01-0AB0</td><td colspan="2">= 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 (2v2)- evaluation" of the sensors was configured.</td></tr>
<tr><td>F-DO 8 x DC 24V/2A PM
6ES7326-2BF40-0AB0</td><td colspan="2">= Max. internal processing time
=14 ms</td></tr>
<tr><td>F-DO 8 x DC 24V/2A PM
6ES7326-2BF41-0AB0</td><td colspan="2">= Max. internal processing time
=14 ms</td></tr>
<tr><td>DO 10 x DC 24V/2A
6ES7326-2BF01-0AB0</td><td colspan="2">= Internal processing time =24 ms</td></tr>
<tr><td>F-DO 10 x DC 24V/2A PP
6ES7326-2BF10-0AB0</td><td colspan="2">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</td></tr>
<tr><td>AI 6 x 13Bit
6ES7336-1HE00-0AB0</td><td colspan="2">= 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).</td></tr>
<tr><td>F-AI 6 x 0/4 ... 20 mA HART
6ES7336-4GE00-0AB0</td><td>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</td><td>= 2 × conversion cycle time
E.g.: interference frequency of 50 Hz, 3 active channel pairs
= 2 × (3 x 25 ms + 50 ms)
= 250 ms</td></tr>
</table>

<table>
<tr><th>F signal module</th><th>T_{WCDT}</th><th colspan="3">T_{OFDT}</th></tr>
<tr><td rowspan="2"></td><td>With 1oo2 (2v2):
= 2 × conversion cycle time × filter + 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</td><td colspan="3"></td></tr>
<tr><td colspan="4">• Conversion cycle time = (Basic response time + N × response time per channel pair) (N = Number of activated channel pairs)</td></tr>
<tr><td rowspan="5">EM 8 F-DI Ex NAMUR
6ES7138-7FN00-0AB0</td><td colspan="4">Internal processing time</td></tr>
<tr><td colspan="2"></td><td>Sensor supply test
Deactivated</td><td>Sensor supply test
Activated</td></tr>
<tr><td colspan="2">1oo1 evaluation</td><td>22 ms</td><td>25 ms</td></tr>
<tr><td colspan="2">1oo2 (2v2) evaluation with discrepancy behavior = "Provide 0 value"</td><td>22 ms</td><td>25 ms</td></tr>
<tr><td colspan="2">1oo2 (2v2) evaluation with discrepancy behavior = "Provide last valid value"</td><td>35 ms</td><td>48 ms</td></tr>
</table>

<table>
<tr><th>F signal module</th><th>T_{WCDT}</th><th>T_{OFDT}</th></tr>
<tr><td></td><td colspan="2">• Response time with 1oo1 evaluation (operation with and without errors)
Response time = Internal processing time[1] + Input delay + {Time for sensor test + start-up time of the sensor after sensor test}2)
• Response time at 1oo2 (2v2) evaluation with discrepancy behavior = "provide 0 value" (operation with and without errors)
Response time = Internal processing time[1] + input delay + MAX { (time for sensor test CHANNEL(n) + start-up time of the sensor after sensor testCHANNEL(n))[2], (time for sensor testCHANNEL(n+4) + start-up time of the sensor after sensor testCHANNEL(n+4))[2,3] }
• Response time at 1oo2 (2v2) evaluation with discrepancy behavior = "Provide last valid value" (operation without errors)
Response time = Internal processing time[1] + input delay + discrepancy time + (time for sensor test CHANNEL(n) + start-up time of the sensor after sensor testCHANNEL(n))[2] + (time for sensor test CHANNEL(n+4) + start-up time of the sensor after sensor testCHANNEL(n+4))[2,3] If there is an error with the sensor supply test, the test is repeated. This repetition only has an effect on the response time for 1oo2 (2v2) evaluation with discrepancy behavior = "Provide last valid value".
• Response time for 1oo2 (2v2) evaluation with discrepancy behavior = "provide last valid value" (operation with errors)
Response time = Internal processing time[1] + input delay + discrepancy time + 2 x { (time for sensor testCHANNEL(n) + start-up time of the sensor after sensor testCHANNEL(n))[2] + (time for sensor testCHANNEL(n+4) + start-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 parameter at 1oo2 (2v2):
• 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</td></tr>
</table>

F signal module	T_{WCDT}	T_{OFDT}
	Example calculation of the response time of EM 8 F-DI Ex NAMUR: • Parameter assignment: – 1oo2 (2v2) evaluation (equivalent or non-equivalent) – Discrepancy behavior: Provide last valid value – Discrepancy time: 400 ms – Sensor supply at 1oo2 (2v2): Sensor n and n+4 to Vs n – Input delay: 3 ms – Sensor supply test: Activated – Time for sensor test: 10 ms – Start-up time of the sensor after sensor test: 100 ms • Response time = Internal processing time + input delay + discrepancy time + (time for sensor testCHANNEL(n) + start-up time of the sensor after sensor testCHANNEL(n)) + (time for sensor testCHANNEL(n+4) + start-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) + start-up time of the sensor after sensor testCHANNEL(n)) + (time for sensor testCHANNEL(n+4) + start-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	
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 read-back 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	
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

The 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
$T_{CImax.proj.}$ / $T_{CImax.proj.1}$ / $T_{CI\ max.proj.2}$	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

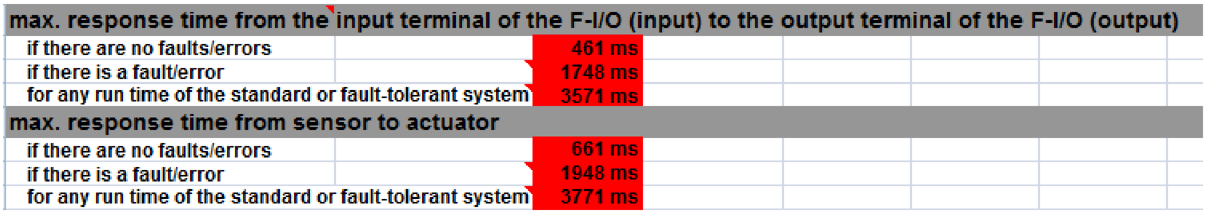
CPU-to-CPU communication (optional)

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", is not be taken into account during calculation in this case

Result

As the result, S7ftimea.xls returns two groups with 3 times each.



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	461 ms
if there is a fault/error	1748 ms
for any run time of the standard or fault-tolerant system	3571 ms
max. response time from sensor to actuator	
if there are no faults/errors	661 ms
if there is a fault/error	1948 ms
for any run time of the standard or fault-tolerant system	3771 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.

Configuration with Safety Matrix 8

8.1 Creating and configuring a Safety Matrix

Note

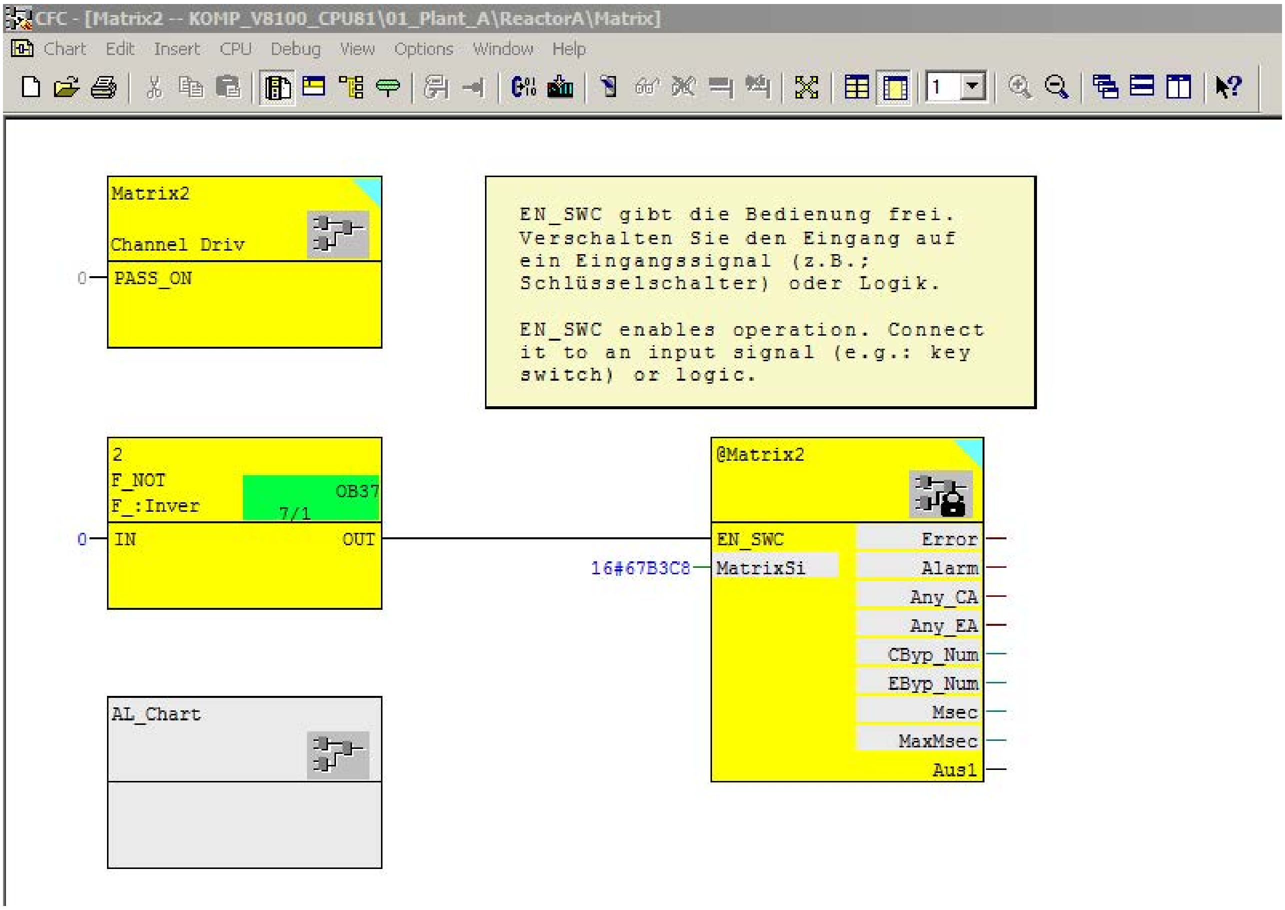
You can find information on creating and configuring a Safety Matrix in the "SIMATIC Industrial Software Safety Matrix" (https://support.industry.siemens.com/cs/ww/en/view/100675874) manual.

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 permission 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. You can thus prevent a configured "1" from being overwritten when transferring the Safety Matrix to the CFC.



EN_SWC gibt die Bedienung frei. Verschalten Sie den Eingang auf ein Eingangssignal (z.B.; Schlüsselschalter) oder Logik.

EN_SWC enables operation. Connect it to an input signal (e.g.: key switch) or logic.

8.2 Documenting a Safety Matrix

A Safety Matrix is documented via menu item "Options > Reports > Configuration Report".

This displays all of the configurations in 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,

or a hard copy of it can be printed out via the menu item "File > Print...". In order to ensure that as much information as possible is retained in this printout, activate all options on the "General" tab prior to printing (accessible via "View > Adapt > Layout"); otherwise, fields that are not visible will not be printed. Please note that this type of printout does not meet the criteria of an acceptance document, as it lacks key information such as a signature and cyclic interrupt OB.

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.

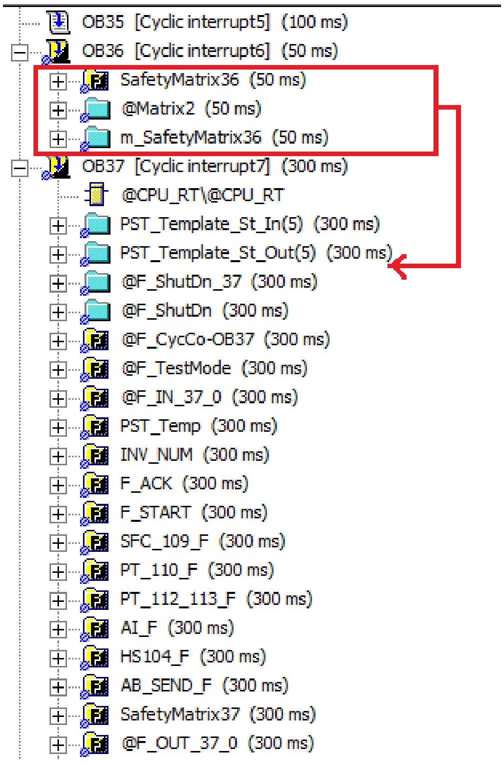
Creating shutdown groups

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.

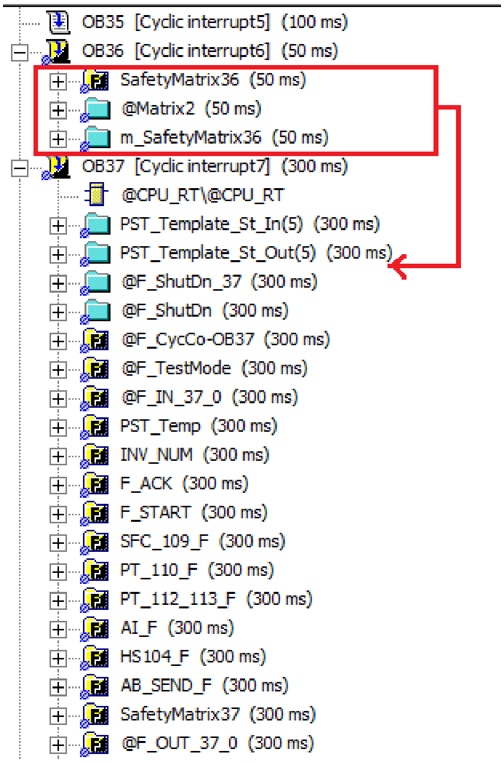


```
OB35  [Cyclic interrupt5]  (100 ms)
OB36  [Cyclic interrupt6]  (50 ms)
    SafetyMatrix36  (50 ms)
    @Matrix2  (50 ms)
    m_SafetyMatrix36  (50 ms)
OB37  [Cyclic interrupt7]  (300 ms)
    @CPU_RT\@CPU_RT
    PST_Template_St_In(5)  (300 ms)
    PST_Template_St_Out(5)  (300 ms)
    @F_ShutDn_37  (300 ms)
    @F_ShutDn  (300 ms)
    @F_CycCo-OB37  (300 ms)
    @F_TestMode  (300 ms)
    @F_IN_37_0  (300 ms)
    PST_Temp  (300 ms)
    INV_NUM  (300 ms)
    F_ACK  (300 ms)
    F_START  (300 ms)
    SFC_109_F  (300 ms)
    PT_110_F  (300 ms)
    PT_112_113_F  (300 ms)
    AI_F  (300 ms)
    HS104_F  (300 ms)
    AB_SEND_F  (300 ms)
    SafetyMatrix37  (300 ms)
    @F_OUT_37_0  (300 ms)
```

Inserting a new matrix in a new shutdown group.

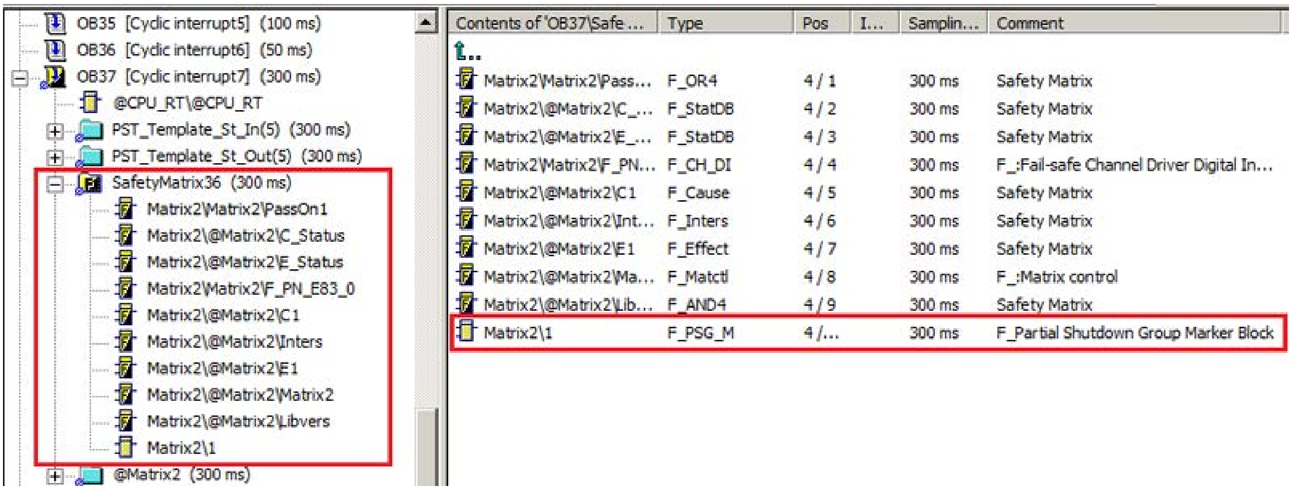
To insert a new matrix and assign it to a new shutdown group, proceed as outlined below.

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.



```
OB35 [Cyclic interrupt5] (100 ms)
OB36 [Cyclic interrupt6] (50 ms)
    SafetyMatrix36 (50 ms)
    @Matrix2 (50 ms)
    m_SafetyMatrix36 (50 ms)
OB37 [Cyclic interrupt7] (300 ms)
    @CPU_RT\@CPU_RT
    PST_Template_St_In(5) (300 ms)
    PST_Template_St_Out(5) (300 ms)
    @F_ShutDn_37 (300 ms)
    @F_ShutDn (300 ms)
    @F_CycCo-OB37 (300 ms)
    @F_TestMode (300 ms)
    @F_IN_37_0 (300 ms)
    PST_Temp (300 ms)
    INV_NUM (300 ms)
    F_ACK (300 ms)
    F_START (300 ms)
    SFC_109_F (300 ms)
    PT_110_F (300 ms)
    PT_112_113_F (300 ms)
    AI_F (300 ms)
    HS104_F (300 ms)
    AB_SEND_F (300 ms)
    SafetyMatrix37 (300 ms)
    @F_OUT_37_0 (300 ms)
```

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.

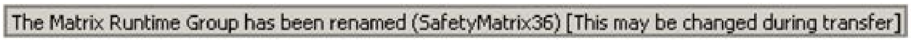


OB35 [Cyclic interrupt5] (100 ms)
OB36 [Cyclic interrupt6] (50 ms)
OB37 [Cyclic interrupt7] (300 ms)
- @CPU_RT\@CPU_RT
- PST_Template_St_In(5) (300 ms)
- PST_Template_St_Out(5) (300 ms)
- SafetyMatrix36 (300 ms)
  - Matrix2\Matrix2\PassOn1
  - Matrix2\@Matrix2\C_Status
  - Matrix2\@Matrix2\E_Status
  - Matrix2\Matrix2\F_PN_E83_0
  - Matrix2\@Matrix2\C1
  - Matrix2\@Matrix2\Inters
  - Matrix2\@Matrix2\E1
  - Matrix2\@Matrix2\Matrix2
  - Matrix2\@Matrix2\Libvers
  - Matrix2\1
- @Matrix2 (300 ms)

Contents of 'OB37\Safe ...	Type	Pos	I...	Samplin...	Comment
Matrix2\Matrix2\Pass...	F_OR4	4 / 1		300 ms	Safety Matrix
Matrix2\@Matrix2\C_...	F_StatDB	4 / 2		300 ms	Safety Matrix
Matrix2\@Matrix2\E_...	F_StatDB	4 / 3		300 ms	Safety Matrix
Matrix2\Matrix2\F_PN...	F_CH_DI	4 / 4		300 ms	F_:Fail-safe Channel Driver Digital In...
Matrix2\@Matrix2\C1	F_Cause	4 / 5		300 ms	Safety Matrix
Matrix2\@Matrix2\Int...	F_Inters	4 / 6		300 ms	Safety Matrix
Matrix2\@Matrix2\E1	F_Effect	4 / 7		300 ms	Safety Matrix
Matrix2\@Matrix2\Ma...	F_Matctl	4 / 8		300 ms	F_:Matrix control
Matrix2\@Matrix2\Lib...	F_AND4	4 / 9		300 ms	Safety Matrix
Matrix2\1	F_PSG_M	4 /...		300 ms	F_Partial Shutdown Group Marker Block

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).

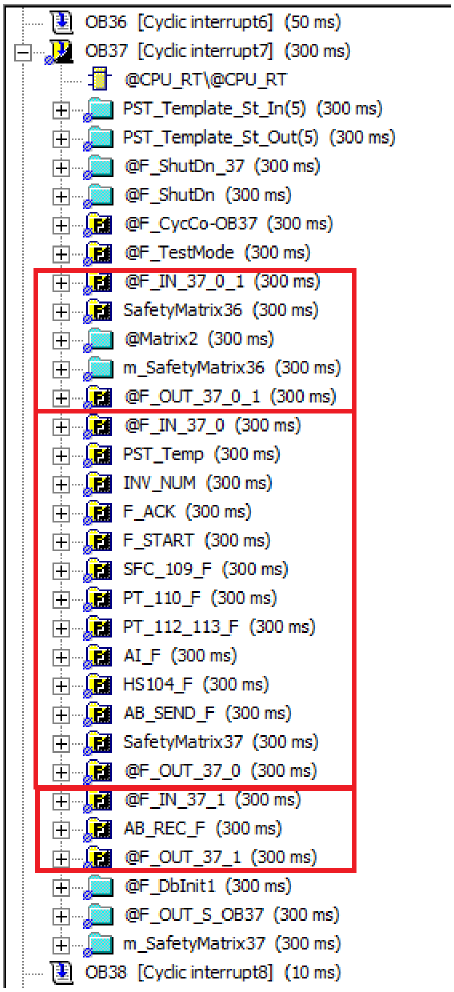
6. Transfer the matrix with the modified cyclic interrupt OB setting to the project. When changes are transferred, the engineering tool will locate the runtime group that has been created and moved, and transfer changes to it as well. The following information appears briefly in the status bar of the Safety Matrix engineering tool:



The Matrix Runtime Group has been renamed (SafetyMatrix36) [This may be changed during transfer]

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.



```
OB36  [Cyclic interrupt6]  (50 ms)
OB37  [Cyclic interrupt7]  (300 ms)
    @CPU_RT\@CPU_RT
    PST_Template_St_In(5)  (300 ms)
    PST_Template_St_Out(5)  (300 ms)
    @F_ShutDn_37  (300 ms)
    @F_ShutDn  (300 ms)
    @F_CycCo-OB37  (300 ms)
    @F_TestMode  (300 ms)
    @F_IN_37_0_1  (300 ms)
    SafetyMatrix36  (300 ms)
    @Matrix2  (300 ms)
    m_SafetyMatrix36  (300 ms)
    @F_OUT_37_0_1  (300 ms)
    @F_IN_37_0  (300 ms)
    PST_Temp  (300 ms)
    INV_NUM  (300 ms)
    F_ACK  (300 ms)
    F_START  (300 ms)
    SFC_109_F  (300 ms)
    PT_110_F  (300 ms)
    PT_112_113_F  (300 ms)
    AI_F  (300 ms)
    HS104_F  (300 ms)
    AB_SEND_F  (300 ms)
    SafetyMatrix37  (300 ms)
    @F_OUT_37_0  (300 ms)
    @F_IN_37_1  (300 ms)
    AB_REC_F  (300 ms)
    @F_OUT_37_1  (300 ms)
    @F_DbInit1  (300 ms)
    @F_OUT_S_OB37  (300 ms)
    m_SafetyMatrix37  (300 ms)
OB38  [Cyclic interrupt8]  (10 ms)
```

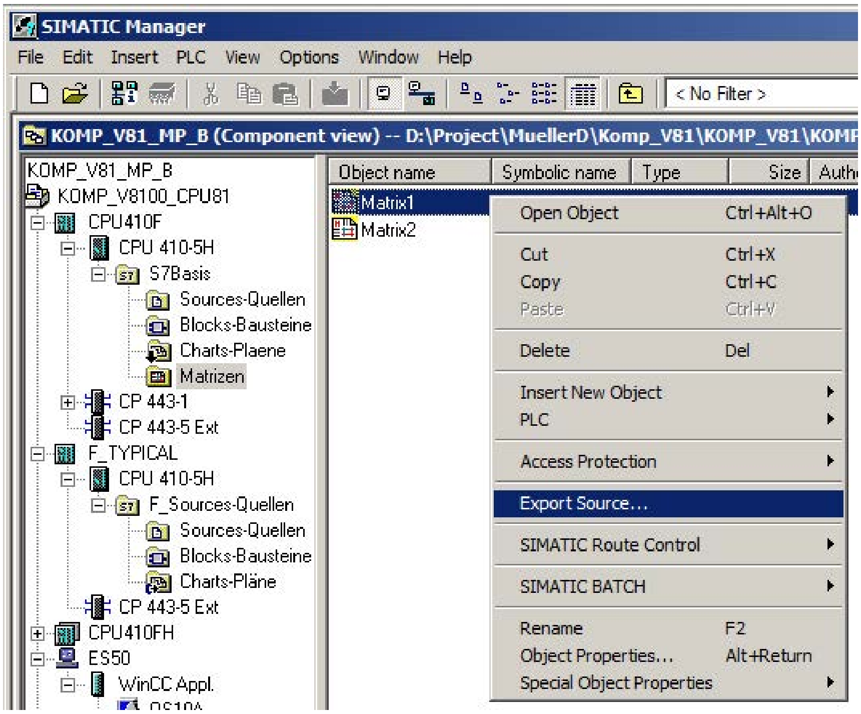
Note

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 Duplicating matrices

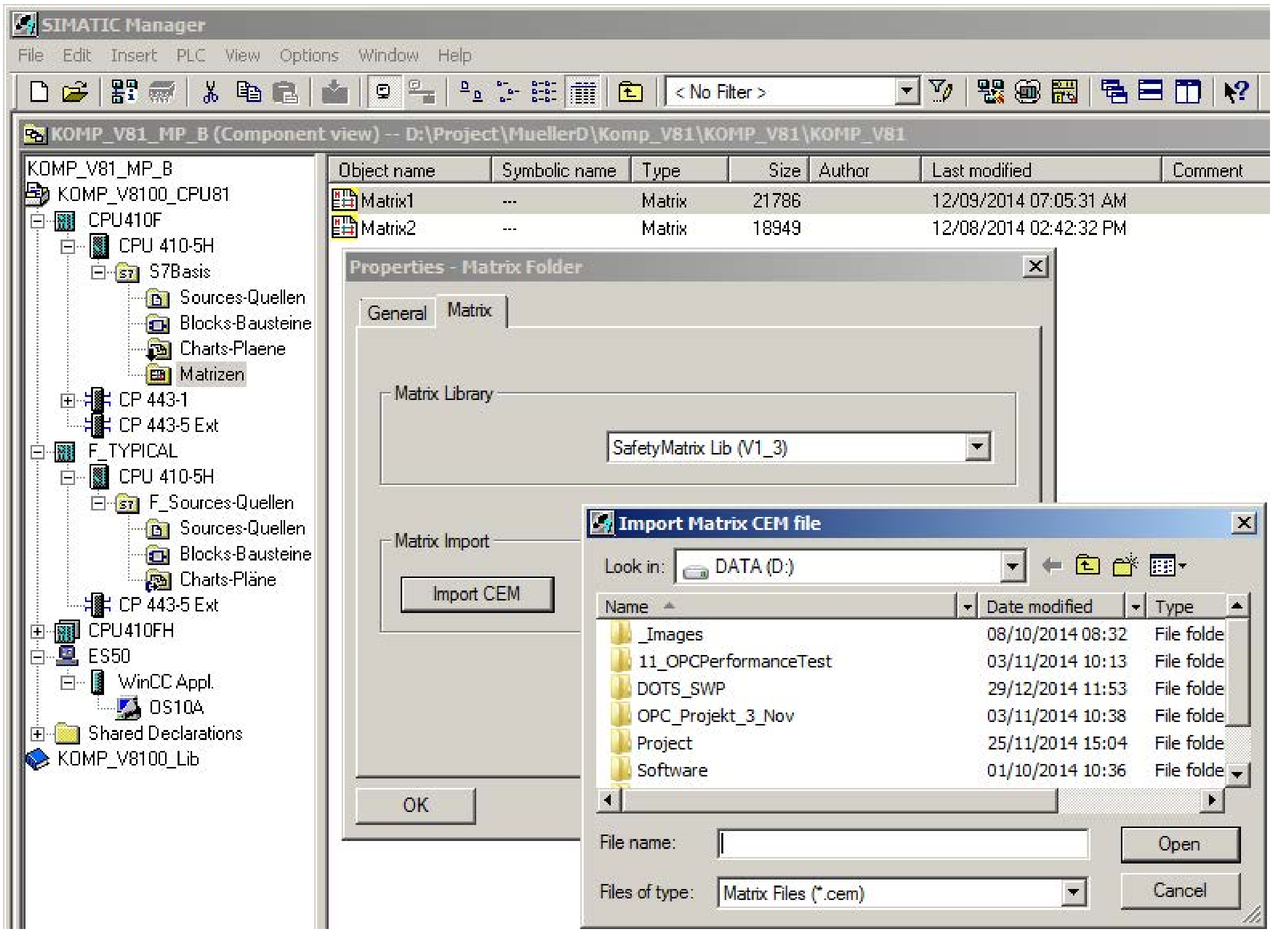
In order to keep the same selected settings, such as SIF assignments (safety instrumented function groups), in another matrix, it is possible to duplicate the matrix template. To do this, proceed as follows:

1. In the matrix folder of the CPU, select the matrix you wish to use as a template and export it as a source via the context menu.



2. Select a destination folder and save the file here under a new name. Renaming the file is important as, if you do not do this, your template file will be overwritten when you carry out an import.

3. To import a template file of this kind, open the object properties of the matrix folder and go to the "Matrix" tab. You can use the "Import CEM" button to add the saved matrix template to a matrix folder.



Object name	Symbolic name	Type	Size	Author	Last modified	Comment
Matrix1	---	Matrix	21786		12/09/2014 07:05:31 AM	
Matrix2	---	Matrix	18949		12/08/2014 02:42:32 PM	

SafetyMatrix Lib (V1_3)

Look in: DATA (D:)

Name	Date modified	Type
_Images	08/10/2014 08:32	File folde
11_OPCPerformanceTest	03/11/2014 10:13	File folde
DOTS_SWP	29/12/2014 11:53	File folde
OPC_Projekt_3_Nov	03/11/2014 10:38	File folde
Project	25/11/2014 15:04	File folde
Software	01/10/2014 10:36	File folde

File name:

Files of type: Matrix Files (*.cem)

4. 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

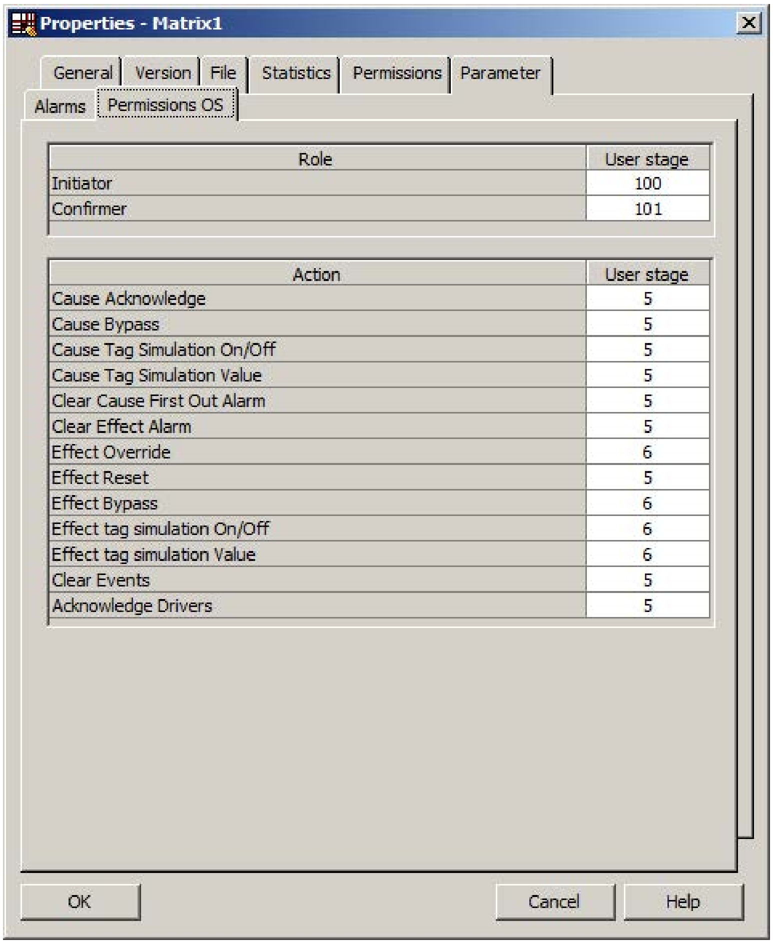
In the properties of the Safety Matrix in the Safety Matrix Engineering Tool, you can set up a separate user authorization for each action and assign it to selected users.

Here, it is also possible to enter the authorization level for the initiator and confirmer for each OS operation. To split operator authorizations across two different users (i.e. for doubly-assured authorization by two users), you can assign the initiator level to one user and the confirmer level to the other,

meaning that each relevant matrix transaction must be initiated by the first user and confirmed by the second.

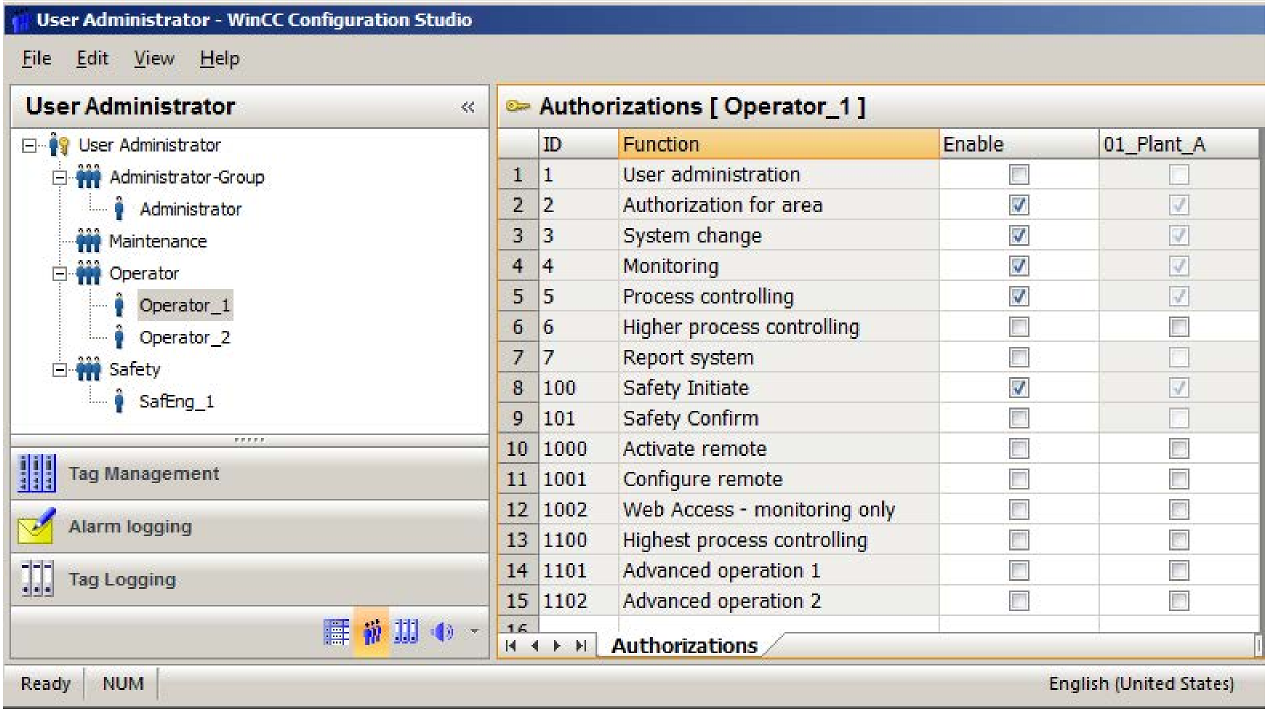
The example configuration below involves a "user" who has process operator authorization (authorization level 5) and therefore possesses both "initiator" (authorization level 100) and "confirmer" (authorization level 101) rights at this level.

However, this "user" is only permitted to execute acknowledgments. In order to execute "higher-level process operations" (authorization level 6) in the matrix, an "initiator" (authorization level 100) and "confirmer" (authorization level 101) are required.



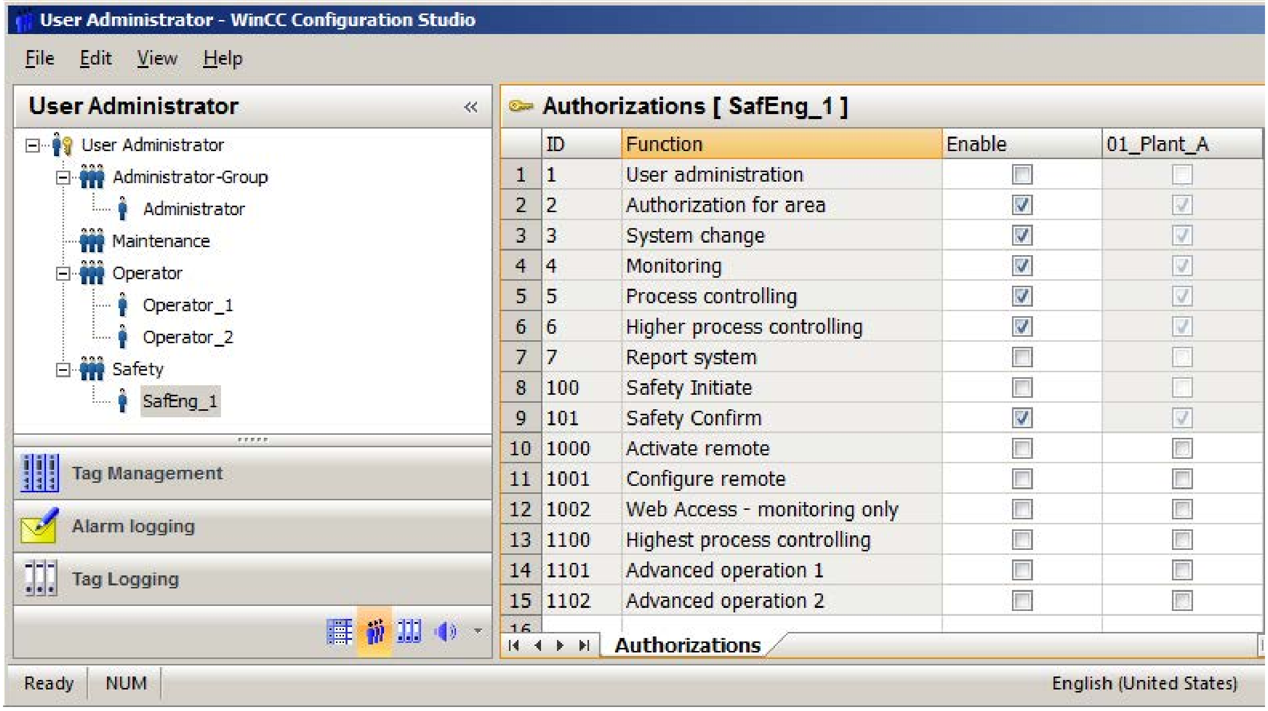
Role	User stage
Initiator	100
Confirmer	101

Action	User stage
Cause Acknowledge	5
Cause Bypass	5
Cause Tag Simulation On/Off	5
Cause Tag Simulation Value	5
Clear Cause First Out Alarm	5
Clear Effect Alarm	5
Effect Override	6
Effect Reset	5
Effect Bypass	6
Effect tag simulation On/Off	6
Effect tag simulation Value	6
Clear Events	5
Acknowledge Drivers	5



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	□	□
16				



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	□	□
16				

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 imported 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. Internal F-channel drivers are recreated whenever any changes affecting the "chart and parameters" are made, whereby any interconnections previously established are lost and changed parameters to the inputs of the F-channel drivers are overwritten with the default values. This is why you are not allowed to change parameters or perform interconnections in this driver chart.

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 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 the display or interlocking in the standard program), it is recommended that you create a process tag (CFC) for the signal. In this case, you can enable the "Imported channel drivers (IEA support)" 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-typicals 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

8.8 New matrix operating blocks

In order to use the Safety Matrix Viewer in a PCS 7 version from V7.1 or higher, the following images have to be converted to the current WinCC version:

- @PG_F_MATCTL*
- @PG_F_MA_AL*
- @PG_F_SC_AL*
- @PG_F_SE_AL*
- @PCS7Typicals_S7FSMTX.PDL

The converted images should subsequently be stored in the root directory of the installation. You can find this in the installation directory of the Siemens software under:
C:\...\Siemens\WinCC\Options\PDL\Faceplatedesigner_V6\

You can find further information in the section "Inserting the new safety matrix block icon in the PCS 7 OS" in the "SIMATIC Industrial Software Safety Matrix" (https://support.industry.siemens.com/cs/ww/en/view/100675874) manual.

Changes, tracking changes, and acceptance

9

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 15).

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 121).

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 178)).

- 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 178)).

- 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. Please note that the runtimes of higher-priority OBs are also measured when this method of measuring the runtimes of lower-priority OBs is used, and will need to be subtracted accordingly.
  With PCS V7.0 SP1 and higher, and an S7-400H CPU with FW V4.5 and higher, the gross and net runtimes of the cyclic interrupt OBs can also be read at block CPU_RT.

Note

You can find more information in section Cyclic interrupts (Page 23).

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 Reserve: 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 36).

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 there is an error in a redundant component (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, depending on your PCS 7 version, you can download your program to a real test AS. Use the "Load to test AS" function in both cases. 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. Testing with S7-PLCSIM is not a substitute for carrying out a function test in the plant.

9.4 Changes in HW Config

CIR allows your to add or remove F-signal modules at the end of an ET 200M rack. When parameters are changed on a F-signal module, the download process is rejected by the system with an error message. When using the S7 F Configuration Pack V5.5 SP12, you will receive a note informing you that download is only possible when the AS is in STOP.

F-signal modules can be added or removed in the HW Config in a fault-tolerant system. Changes to the configuration of a existing F-signal module lead to passivation of the module after the hardware configuration has been downloaded. The changes in the CFC must be compiled and downloaded. All F-channel drivers of the module must then be acknowledged or the module must be unplugged and plugged back in again. If changes are required, check of the signals are necessary for the process that is currently running. Establish (within the context of a risk assessment, if necessary) whether signal simulation is permissible.

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 121).

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.

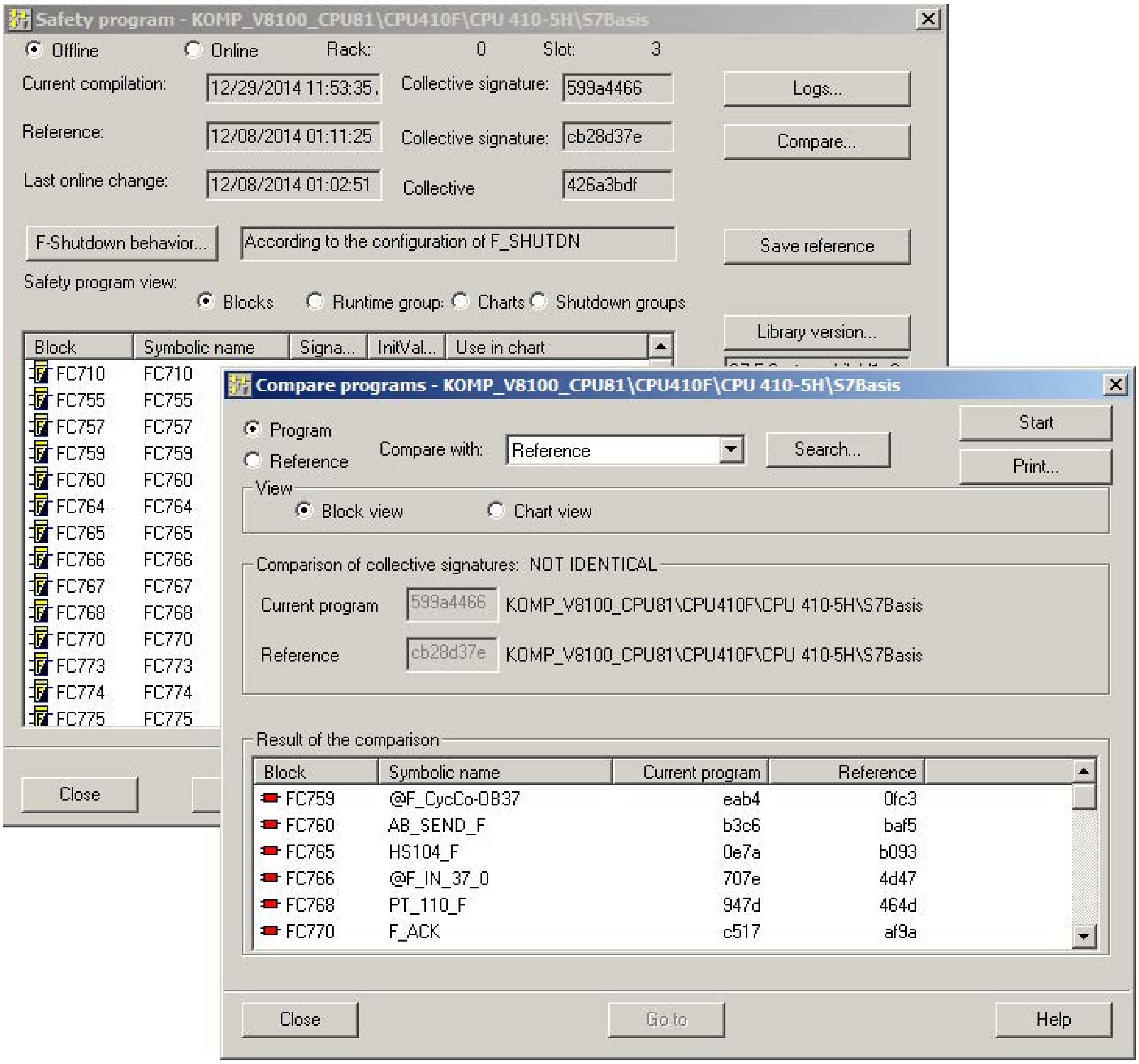
Program comparison

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



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

Reference: 12/08/2014 01:11:25 Collective signature: cb28d37e

Last online change: 12/08/2014 01:02:51 Collective 426a3bdf

F-Shutdown behavior... According to the configuration of F_SHUTDN

Safety program view: ● Blocks ○ Runtime group ○ Charts ○ Shutdown groups

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			

Compare programs - KOMP_V8100_CPU81\CPU410F\CPU 410-5H\S7Basis

● Program
○ Reference

Compare with: Reference

View: ● Block view ○ Chart view

Comparison of collective signatures: NOT IDENTICAL

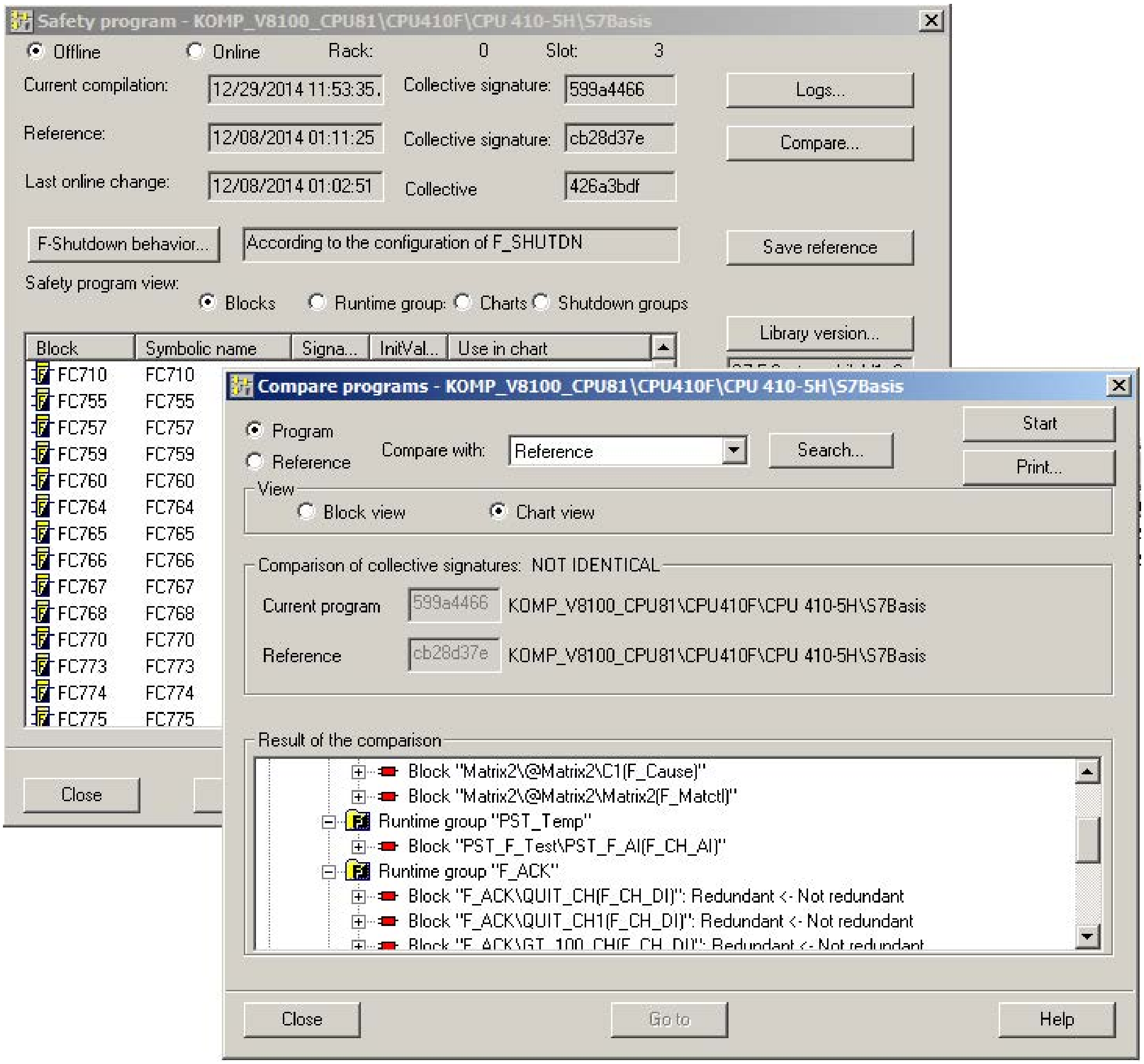
Current program 599a4466 KOMP_V8100_CPU81\CPU410F\CPU 410-5H\S7Basis

Reference cb28d37e KOMP_V8100_CPU81\CPU410F\CPU 410-5H\S7Basis

Result of the comparison

Block	Symbolic name	Current program	Reference
🟥 FC759	@F_CycCo-OB37	eab4	0fc3
🟥 FC760	AB_SEND_F	b3c6	baf5
🟥 FC765	HS104_F	0e7a	b093
🟥 FC766	@F_IN_37_0	707e	4d47
🟥 FC768	PT_110_F	947d	464d
🟥 FC770	F_ACK	c517	af9a

- 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

Reference: 12/08/2014 01:11:25 Collective signature: cb28d37e

Last online change: 12/08/2014 01:02:51 Collective 426a3bdf

F-Shutdown behavior... According to the configuration of F_SHUTDN

Safety program view: ● Blocks ○ Runtime group: ○ Charts ○ Shutdown groups

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			

Compare programs - KOMP_V8100_CPU81\CPU410F\CPU 410-5H\S7Basis

● Program ○ Reference Compare with: Reference

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
    Block "F_ACK\GT_100_CH(F_CH_DI)": Redundant <- Not redundant
```

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. There, you will see three signatures, each with a corresponding date:

- The most recent date on which the CFC charts with changes to the safety program were compiled, and the signature formed for this.
- 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 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.

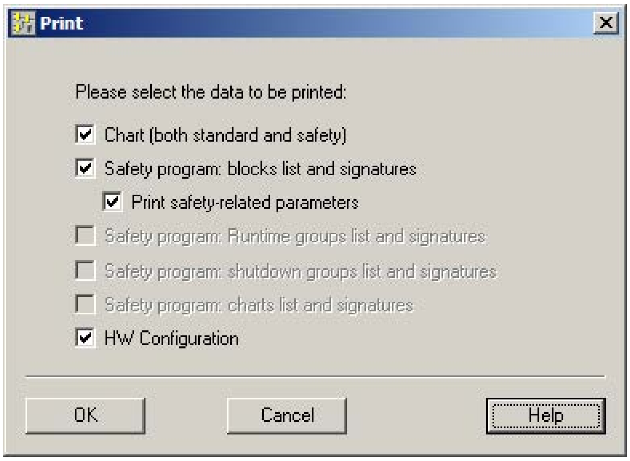
- To do this, go online in CFC and open the @F_Shtdn chart.
- While online, you can view the signature of the safety program in the AS at output F_SIG_OUT of the F_SHUTDN block.

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.

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:



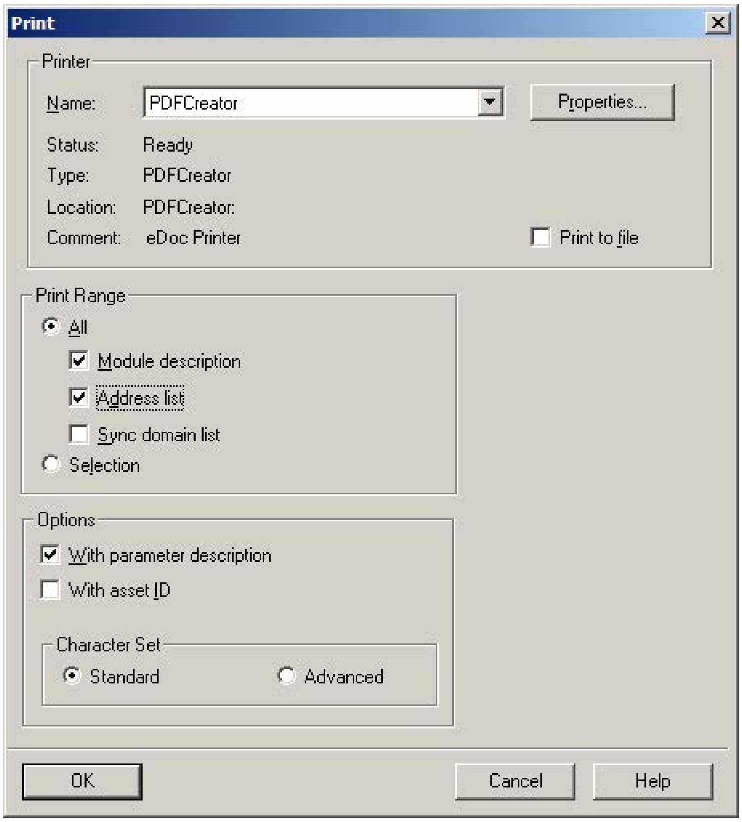
Please select the data to be printed:

☑ Chart (both standard and safety)
☑ Safety program: blocks list and signatures
☑ Print safety-related parameters
□ Safety program: Runtime groups list and signatures
□ Safety program: shutdown groups list and signatures
□ Safety program: charts list and signatures
☑ HW Configuration

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 "Safety Program" window, a footer containing the F-system 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:



Print

Printer

Name: PDFCreator

Status: Ready
Type: PDFCreator
Location: PDFCreator:
Comment: eDoc Printer

□ Print to file

Print Range

● All

☑ Module description

☑ Address list

□ Sync domain list

○ Selection

Options

☑ With parameter description

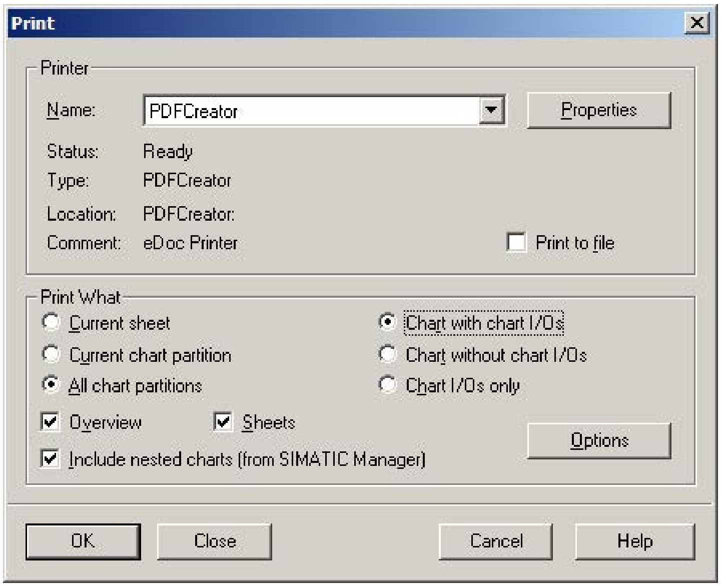
□ With asset ID

Character Set

● Standard ○ Advanced

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.



Print

Printer

Name: PDFCreator

Status: Ready

Type: PDFCreator

Location: PDFCreator:

Comment: eDoc Printer

□ Print to file

Print What

- ○ Current sheet
- ○ Current chart partition
- ● All chart partitions
- ● Chart with chart I/Os
- ○ Chart without chart I/Os
- ○ Chart I/Os only

☑ Overview ☑ Sheets

☑ Include nested charts (from SIMATIC Manager)

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

You can find information on acceptance of a plant, changes, or F block types in the "SIMATIC Industrial Software S7 F/FH Systems - Configuring and Programming" (https://support.industry.siemens.com/cs/ww/en/view/101509838) manual.

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.

Service and support 10

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.