SIEMENS

SIMATIC

Industrial software SIMATIC S7 F/FH Systems - Configuring and Programming

Programming and Operating Manual

02/2020

A5E49169662-AA

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 Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E49169662-AA
℗ 02/2020 Subject to change

Table of contents

Security information 1

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

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

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

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

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

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

Preface 2

2.1 Preface

Purpose of this documentation

The information in this manual enables you to configure and program fail-safe S7 F/FH Systems using "S7 F Systems" V6.3.

As a supplement, you need the " Safety Engineering in SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/12490443) " system manual.

Basic Knowledge Requirements

General basic knowledge of automation engineering is needed to understand this documentation. Basic knowledge of the following is also necessary:

- Fail-safe automation systems
- S7-400 Automation Systems
- Distributed I/O systems on PROFIBUS DP / PROFINET IO
- STEP 7 basic software, particularly:
  - Working with SIMATIC Manager
  - Hardware configuration with HW Config
  - Communication between CPUs
  - CFC optional software

Scope of this documentation

	Article number	As of product version	License type (location)
Optional package "SIMATIC S7 F Systems" V6.3 including License Key V6.3	• Full version: 6ES7833-1CC36-0YA5	V6.3	Floating, Trial (14 days)
	• Upgrade version of V6.2: 6ES7833-1CC36-0YE5		Floating (as upgrade), trial (14 days)
S7 F Systems RT Licence (Copy Licence)	• 6ES7833-1CC00-6YX0	V5.0	CPU label

The "SIMATIC S7 F Systems" optional package is used for configuring and programming S7 F/FH Systems. The integration of the following F-I/Os in S7 F/FH Systems is also viewed in this context:

- ET 200S fail-safe I/O modules
- ET 200SP fail-safe I/O modules
- ET 200SP HA fail-safe I/O modules

- ET 200eco fail-safe I/O modules
- ET 200pro fail-safe I/O modules
- ET 200iSP fail-safe I/O modules
- Fail-safe signal modules S7-300 (used in ET 200M)
- Fail-safe DP standard slaves/IO standard devices
- Fail-safe PA field devices

What's New?

The new features and changes in "S7 F Systems" V6.3 are described below:

- New F-blocks of the F-library to support the PROFIsafe Profile V2.6.1 XP (Expanded Protocol):
  - F_PS_13: F-control block "F_module driver" PROFIsafe profile V2.6.1 XP
  - F_CH_QBI: F-channel driver for inputs of data type BOOL (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices
  - F_CH_QBO: F-channel driver for outputs of data type BOOL (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices
  - F_CH_QII: F-channel driver for inputs of data type INT (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices
  - F_CH_QIO: F-channel driver for outputs of data type INT (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices
- New block in the F-library:
  - F_MNR_H: F-control block
- Support of "Web Option for OS" for operating and monitoring via Intranet/Internet on a PCS 7 web client
- Support for F I/O modules of the ET 200SP HA
  - Digital input module F-DI 16x24VDC HA
  - Digital output module F-DQ 10x24VDC/2A PP HA
- The password of the safety program can be changed for F-libraries or projects without a configured CPU
- Support of additional fail-safe DP standard slaves/IO standard devices

Approvals

S7 F/FH Systems and the F-I/O are certified for use in safety mode for:

- Safety Integrity Level SIL3 according to IEC 61508:2010
- Performance Level (PL) e and Category 4 according to ISO 13849-1:2015 or EN ISO 13849-1:2015

Position in the information landscape

Depending on your application, you will need the following supplementary documentation when working with *S7 F/FH Systems*.

This documentation includes references to the supplementary documentation where appropriate.

Documentation for	Brief Description of Relevant Contents
Safety Engineering in SIMATIC S7	The "Safety Engineering in SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/12490443)" system manual provides an informational overview of the use, installation, and mode of operation of the S7 Distributed Safety and S7 F/FH Systems fail-safe automation systems, and describes basic properties and technical information about these F-systems.
S7 F/FH Systems	• The "Automation System S7-400 Hardware and Installation (https://support.industry.siemens.com/cs/ww/en/view/1117849)" installation manual describes the assembly and wiring of S7-400 systems. • The "Automation System S7-400H Fault-Tolerant Systems (https://support.industry.siemens.com/cs/en/en/view/82478488)" manual describes the CPU 41x-H central processing units and the tasks required to set up and commission an S7-400H fault-tolerant system.
S7 Distributed Safety	The following elements are described in the " S7 Distributed Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/22099875) " operating manual and online help: • Configuration of the F-CPU and the F-I/O • Programming of the F-CPU in F-FBD or F-LAD
S7-300 Automation System, ET 200M I/O Device	The "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)" manual describes the hardware of the fail-safe signal modules in S7-300 (including setup, wiring and technical specifications). The signal modules of the S7-300 are also used in the ET 200M.
ET 200S Distributed I/O System	The "ET 200S Distributed I/O System - Fail-Safe Modules (https://support.industry.siemens.com/cs/ww/en/view/12490437)" operating instructions describe the hardware of the ET 200S fail-safe modules (including installation, wiring and technical specifications).
ET 200SP Distributed I/O System	The Manual Collection "SIMATIC ET 200SP Manual Collection (https://support.industry.siemens.com/cs/ww/en/view/84133942)" contains all important information about the I/O system.
ET 200SP HA Distributed I/O system	The operating instructions "Distributed I/O System ET 200SP HA (https://support.industry.siemens.com/cs/ww/en/view/109761547)": Describes the hardware of the fail-safe modules ET 200SP HA (including setup, wiring and technical specifications).
ET 200pro Distributed I/O System	The "ET 200pro Distributed I/O Device - Fail-Safe Modules (https://support.industry.siemens.com/cs/ww/en/view/22098524)" operating instructions describe the hardware of the ET 200pro fail-safe modules (including installation, wiring and technical specifications).
ET 200eco Distributed I/O System	The "ET 200eco Distributed I/O Station Fail-safe I/O Module (http://support.automation.siemens.com/WW/view/en/19033850)" manual describes the hardware of the fail-safe I/O module ET 200eco (including setup, wiring and technical specifications).

Documentation for	Brief Description of Relevant Contents
ET 200iSP Distributed I/O System	The "ET 200iSP Distributed I/O Device - Fail-safe Modules (https://support.industry.siemens.com/cs/ww/en/view/47357221)" operating instructions describe the hardware of the ET 200iSP fail-safe modules (including installation, wiring and technical specifications).
STEP 7 manuals	• The "Configuring hardware and communication connections with STEP 7 (http://support.automation.siemens.com/WW/view/en/109751824)"manual describes how to use the corresponding standard tools of STEP 7. • The "System software for S7 300/400 System and Standard Functions (https://support.industry.siemens.com/cs/ww/en/view/109751826)" reference manual describes access/diagnostic functions of the distributed I/O / CPU. • The "Programming with STEP 7 (http://support.automation.siemens.com/WW/view/en/109751825)" manual describes programming procedures in STEP 7. • The "SIMATIC Process Control System PCS 7 CFC for SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/109765729)"manual / online help provides a description of programming with CFC. • The "Modifying the System during Operation via CiR (https://support.industry.siemens.com/cs/ww/en/view/45531308)" manual
STEP 7 Online Help	• Describes the operation of STEP 7 standard tools • Contains information on configuring and assigning parameters for I/Os with HW Config.
PCS 7	• The "PCS 7 manuals (www.siemens.com/pcs7-documentation)"describe operation of the PCS 7 process control system (required when the S7 F/FH System is integrated into a higher-level control system). The documents "PCS 7 Compendium Part B - Process Safety" and "PCS 7 Compendium Part F - Industrial Security" are also available at the following link.

Guide

This documentation describes how to work with the "S7 F Systems" optional package. It includes both instructional material and reference material (description of fail-library blocks).

The following topics are addressed:

- Configuration of S7 F Systems
- Access protection for S7 F Systems
- Programming of the safety program (safety-related user program)
- Safety-related communication
- Support for the system acceptance test
- Operation and maintenance of S7 F Systems
- F-Libraries

Conventions

The following terms are used in this documentation...

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

Additional support

If you have further questions about the use of products presented in this manual, contact your local Siemens representative:

You will find information on who to contact on the Web (http://www.siemens.com/automation/partner).

A guide to the technical documentation for the various SIMATIC products and systems is available on the Web (https://support.industry.siemens.com/cs/ww/en/view/109742705).

You will find the online catalog and online ordering system on the Web (https://mall.industry.siemens.com).

Training center

We offer courses to help you get started with the SIMATIC S7 automation system. Contact your regional training center or the central training center in D -90327 Nuremberg, Federal Republic of Germany.

You will find more information on the Web (https://new.siemens.com/global/en/products/services/industry/sitrain.html).

Technical Support

You can contact Technical Support for all Industry Automation products using the Support Request (https://support.industry.siemens.com/cs/ww/en/sc/4868).

You can find additional information about our Technical Support on the Web (https://support.industry.siemens.com/cs/ww/en/).

Service & Support on the Internet

In addition to our paper documentation, our complete knowledge base is available to you on the Web (http://www.siemens.com/automation/service&support).

There, you will find the following information:

- The newsletter providing the latest information on your products
- The right documents for you, using our Service & Support search engine
- A forum in which users and specialists worldwide exchange their know-how
- Your local contact partner for Industry Automation products in our Contact Partners database
- Information about on-site service, repairs, spare parts, and much more under "Repairs, spare parts, and consulting"

Important notes for maintaining operational safety of your plant

Note

Operation of safety-related systems

Systems with safety-related characteristics are subject to special operational safety requirements on the part of the operator. The supplier is also obliged to comply with special product monitoring measures. For this reason, we provide you with information on product developments and product features that are (or could be) relevant to operation of safety-related systems. In order to obtain the latest information on this topic and to enable you to undertake modifications to your system you must subscribe to the corresponding notifications. To subscribe, go to the Internet (https://support.industry.siemens.com/My/ww/de/).

Register on this website and under "Notifications" select the notifications for the following topics, for example:

- S7-300/S7-300F
- S7-400/S7-400H/S7-400F/FH
- Distributed I/O
- SIMATIC Industrial Software
- Safety Matrix
- S7 F/FH Systems

You can find more information on setting up notifications on the page "Helpful functions in Online Support (https://support.industry.siemens.com/cs/ww/en/sc/2063)".

Safety concepts and communication

The PCS 7 safety concepts described in the document "PCS 7 Compendium Part F - Industrial Security" must be observed for safe operation of the system.

Additional information on this document is available in the table above under "PCS 7".

In particular we recommend the following:

- The protection of the devices/systems, e.g. PCS 7 OS server and clients
- Ensuring the integrity and confidentiality of the communication between the devices/systems, e.g.:
  - By means of encrypted and authenticated communication between the systems involved, such as PCS 7 OS system and/or also between engineering stations (ES)
  - When using Industrial Ethernet CPs through VPN tunnels between the OS systems and/or automation systems (AS).

2.2 Warnings index

Warnings in the main part of the document

FSW	Warning	Section
	Section: Product Overview	
1	S7 F/FH systems operation	3.2
	Section: Configuration	
3	An F-CPU containing a safety program must have a password.	5.3
4	Configuring a protection level	5.3
5	"Group diagnostics" for fail-safe F-SMs in safety mode	5.4.2
6	Address assignment in subnets only and in mixed configurations	5.4.3
7	Uniqueness of PROFIsafe addresses across stations required	5.4.4
8	Identification and acknowledgment of the F-I/O	5.4.4.1
9	Devices and "F_Par_Version" parameter for a mixed configuration	5.5
	Section: Access Protection	
10	Limiting accessing using the engineering system	6.2
11	Transferring the safety program to multiple F-CPUs	6.2
12	Password protection	6.2
13	Limiting accessing using the engineering system	6.3
14	Passwords must be unique	6.3
	Section: Programming	
15	Default setting of the maximum MAX_CYC	7.2.3
16	Do not change values created during compilation	7.2.4
17	Call interval of cyclic interrupt OB 3x is monitored for the maximum value	7.2.4
18	Compression changes the signature	7.2.5
19	Effect of optimizing the runtime sequence in the CFC	7.2.7
20	Entries for F-Blocks in the symbol table must not be changed	7.3.1
21	Illegal changes to input parameters of F-Blocks can cause a shutdown of the safety program and its outputs	7.3.2
22	Do not change automatically inserted F-Control blocks.	7.4
23	Saved error information is lost during an F-Startup	7.5
24	Outputs of F-blocks always use the predefined initial values	7.7.2
25	Validity check	7.9.2
26	The two acknowledgment steps must not be triggered with a single operation.	7.10
27	Execution of the two acknowledgment steps, if access to several F-CPUs is possible.	7.10
	Section: F-I/O access	
28	F-I/O with digital inputs of the BOOL data type	8.3
	Section: Programming communication	
29	CPU-CPU communication and public networks	9.1.1
30	Value for the respective address relationship	9.1.3
31	Duration of the signal level to be transmitted	9.1.3
32	Data reception when safety mode is deactivated	9.1.3
33	The S7 program must be recompiled if the S7 connections for communication between F-CPUs have been changed.	9.1.3

FSW	Warning	Section
	Section: Operator inputs with the "Secure Write Command++" function	
34	The "Secure Write Command++" functionality allows changes to the safety program to be made during RUN mode	10.4.2.1
35	Warnings in the descriptions of the F-blocks	10.4.2.2 to 10.4.2.7
37	Initiator and confirmer must not accept an invalid value	10.5.1
38	Technological assignment must be appropriate for the environment	10.5.1
39	Transaction for changing an F-Parameter	10.5.1
	Section: Safety Data Write function	
40	Warnings in the descriptions of the F-blocks	11.2.2
41	Static values of the SAFE_ID1 and SAFE_ID2 attributes	11.2.4
42	Initiator and confirmer must not accept an invalid value	11.3.1
43	Technological assignment must be appropriate for the environment	11.3.1
44	Transaction for changing an F-Parameter	11.3.1
	Section: Compiling and commissioning an S7 program	
45	Deactivating safety mode	12.5.1
46	Do not copy F-Blocks with SIMATIC Manager	12.6
47	Safety program on a memory card	12.6.1
48	Downloading the safety program with multiple F-CPUs	12.6.1
49	Shutdown of the safety program following a change to the fail-safe outputs	12.7
50	A simulation is no substitute for a function test!	12.7.1
51	Changing the collective signature for changes in CFC test mode	12.8.1
52	Do not change values created during compilation	12.8.1
53	Download operation aborted	12.8.2
54	Moving F-Blocks or F-Runtime groups	12.8.2
55	Modifying the safety program in RUN mode	12.8.2
	Section: Acceptance of the system	
56	Address assignment in subnets only and in mixed configurations	13.2.1
	Section: Operation and maintenance	
57	Safety of the F-system when using simulation devices / simulation programs	14.1
58	STOP not as a safety condition	14.1
59	STOP state, which was initiated with SFC 46 "STP", is not a safety-related STOP	14.1
60	Two F-CPUs not simultaneously as master system	14.1
61	Using the "F-Forcing" function	14.3

Warnings in the appendix of the document

FSW	Warning	Section
	Section: F-Libraries	
101	Values of PAR_ID and COMPLEM must not be changed	A.1.2
102	Value for the respective address relationship	A.2.2.2 to A.2.2.7

FSW	Warning	Section
103	Detecting and transmitting a signal level	A.2.2.2 to A.2.2.7
104	User acknowledgment is always required for communication errors	A.2.2.3; A.2.2.5; A.2.2.7
105	Fail-safe user times	A.2.4.1 to A.2.4.3
120	Validity check	A.2.5.1
121	The "Secure Write Command++" functionality allows changes to the safety program to be made during RUN mode	A.2.5.2 to A.2.5.6
122	The CHANGED input cannot be evaluated in the safety program.	A.2.5.2
123	Interconnection input CS_VAL	A.2.5.2
124	F-Startup	A.2.5.2 A.2.5.3
126	The CHANGED input cannot be evaluated in the safety program.	A.2.5.3
127	Interconnection inputs CS_VAL, MIN, MAX and MAXDELTA	A.2.5.3
131	Interconnection input CS_VAL	A.2.5.5
132	F-startup	A.2.5.5
134	Interconnection inputs CS_VAL, MIN and MAX	A.2.5.6
135	F-Startup	A.2.5.6
136	Reintegration through user acknowledgment with F_QUITES	A.2.5.11
137	The "Safety Data Write" functionality makes changes in the safety program during RUN mode	A.2.5.16
138	The CHANGED output cannot be evaluated in the safety program	A.2.5.16
139	Interconnection inputs MIN, MAX and MAXDELTA	A.2.5.16
140	SAFE_ID1 and SAFE_ID2 parameters	A.2.5.16
141	F-Startup	A.2.5.16
142	The "Safety Data Write" functionality makes changes in the safety program during RUN mode	A.2.5.17
143	The CHANGED output cannot be evaluated in the safety program	A.2.5.17
144	SAFE_ID1 and SAFE_ID2 parameters	A.2.5.17
145	F-Startup	A.2.5.17
146	Parameter assignment input ACK_NEC	A.2.6.1 to A.2.6.16
147	Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device	A.2.6.1 to A.2.6.4 A.2.6.10 to A.2.6.16
148	Startup protection for short-term power failure of the fail-safe PA field device	A.2.6.5 to A.2.6.6
149	Startup protection for short-term power failure of the F-I/O	A.2.6.7 to A.2.6.9
170	Fail-safe user times	A.2.9.2 to A.2.9.4 A.2.10.1; A.2.10.2
175	F-Startup	A.2.13.2

FSW	Warning	Section
176	Safety note: Do not change automatically inserted F-control blocks	A.3 A.3.1 to A.3.20
177	Default setting of the maximum MAX_CYC	A.3.3
	Section: Requirements for virtual environments and remote access	
301	Use of virtual environments in ES/OS	C.2.1
302	Remote access from higher-level control room and Engineering Center	C.2.2
303	The "S7 F Systems HMI" and "Safety Matrix Viewer" functionality makes changes in the safety program during RUN mode.	C.2.2

Product Overview 3

3.1 Overview

S7 F/FH Systems fail-safe systems

The fail-safe automation systems ("F-Systems") S7 F/FH Systems are used in systems with stringent safety requirements. The objective of S7 F/FH systems is to control processes with an immediately achievable safe state. In other words, F-Systems control processes in which an immediate shutdown does not endanger people or the environment.

The "SIMATIC S7 F Systems" optional package comprises the following components:

- SIMATIC S7 F systems
- SIMATIC S7 F Systems HMI
- SIMATIC S7 F Systems Library
- SIMATIC S7 F Device Integration Pack
- SIMATIC S7 F Configuration Pack
- Automation License Manager

The related version designations can be found in the readme file.

Achievable safety requirements

With S7 F/FH Systems, you achieve the following safety requirements:

- Safety Integrity Level SIL3 according to IEC 61508:2010
- Performance Level (PL) e and Category 4 according to ISO 13849-1:2015 or EN ISO 13849-1:2015

The principle of safety functions in S7 F/FH Systems

Functional safety is implemented principally through safety functions in the software. Safety functions are performed by S7 F/FH Systems whenever a dangerous event occurs:

- To place the system in a safe state
  or
- To keep the system in a safe state

Safety functions are contained mainly in the following components:

- In the safety-related user program (safety program) in the fail-safe CPU (F-CPU)
- In the fail-safe inputs and outputs (F-I/O)

The F-I/O ensures safe processing of field information (such as temperature and level monitoring). They have all of the required hardware and software components for safe processing, in accordance with the required safety class. You only have to program the user safety function. The safety function for the process can be provided through a user safety function or a fault reaction function. In the event of a fault, if the F-system can no longer execute its actual user safety function, it executes the fault reaction function. For more information, refer to section "F-STOP (Page 99)".

Example of user safety functions and fault reaction functions

In the event of overpressure, the F-system opens a valve (user safety function). In the event of a dangerous fault in the F-CPU, all outputs are switched off (fault reaction function). The valve is opened and the other actuators also achieve a safe state. If the F-system is intact, only the valve would be opened.

Fail-safety and availability

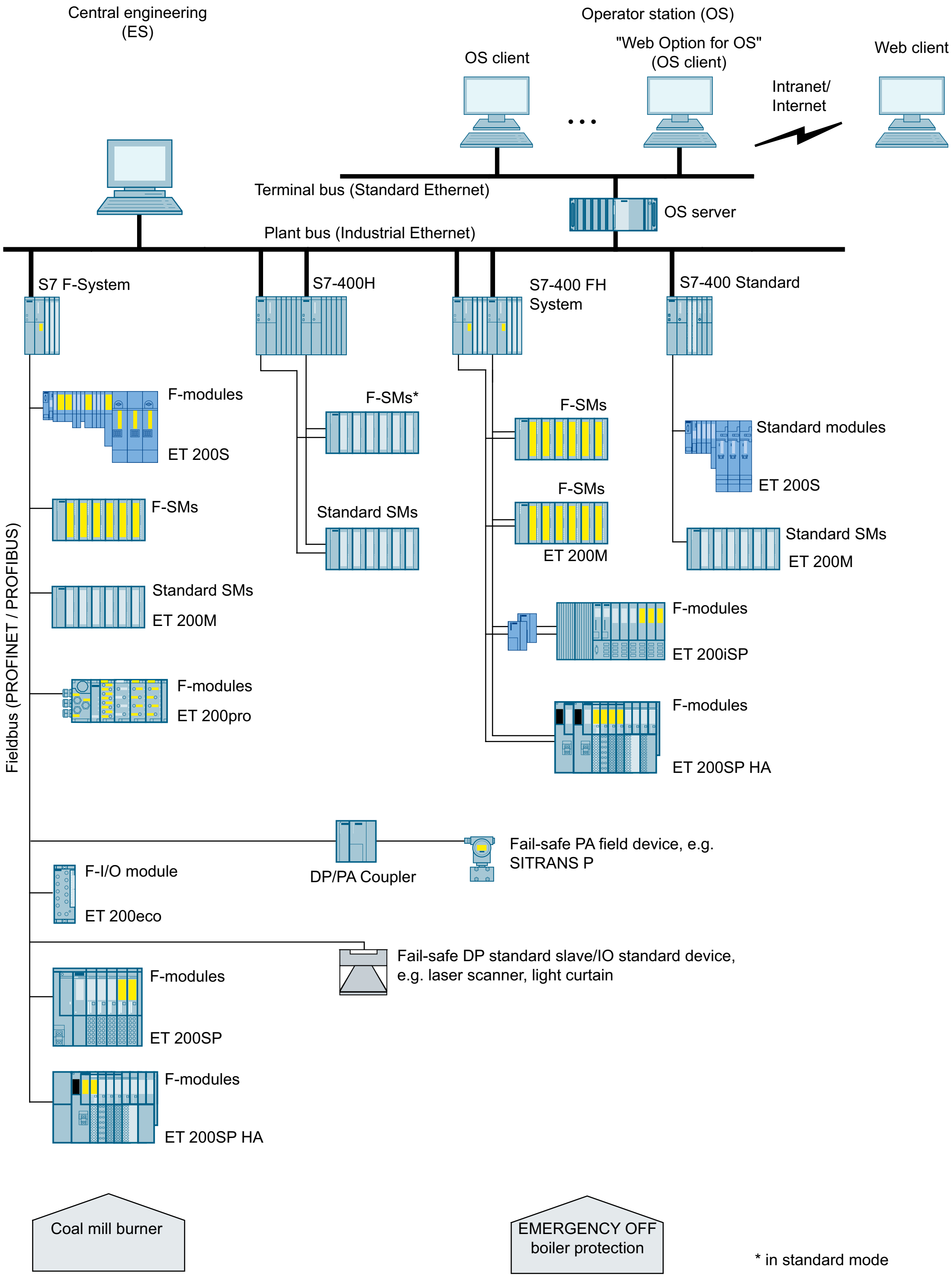
To increase availability of the automation system and, thus, to prevent process failures due to faults in the F-System, you can optionally equip fail-safe systems with a fault-tolerant feature. You achieve this increased availability through component redundancy:

- Power supply
- Central processing unit
- Communication
- F-I/O

With fail-safe, high-availability S7 F/FH Systems, you can resume production without harming people or the environment.

Use in process engineering

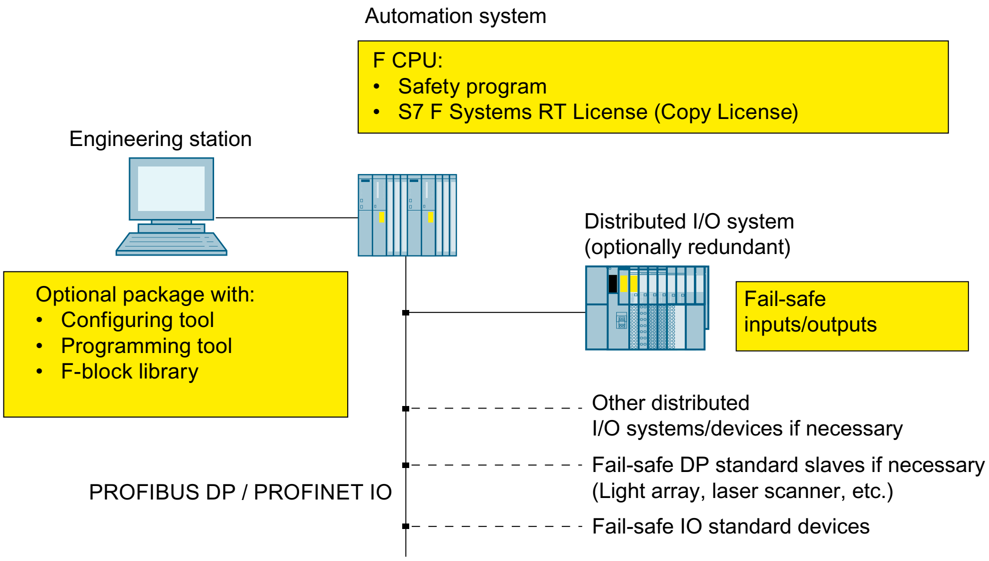
The figure below shows you the possible ways of integrating S7 F/FH Systems into you process automation system with PCS 7.



3.2 Hardware and software components

Hardware and software components of S7 F/FH systems

The following figure gives you an overview of hardware and software components you need to set up and operate S7 F/FH systems.



Hardware components

The hardware components of S7 F/FH systems include:

- F-CPU (CPU 412-5H, CPU 414-5H, CPU 416-5H, CPU 417-5H, CPU 410-5H, CPU 410SIS, CPU 410E)
- Fail-safe inputs/outputs (F-I/O), for example:
  - S7-300 fail-safe signal modules in ET 200M (distributed configuration)
  - Fail-safe power and electronic modules in ET 200S
  - Fail-safe power and I/O modules in ET 200SP
  - Fail-safe I/O modules in ET 200SP HA
  - ET 200eco fail-safe I/O modules
  - ET 200pro fail-safe I/O modules
  - ET 200iSP fail-safe modules
  - Fail-safe DP standard slaves
  - Fail-safe IO standard devices
  - Fail-safe PA field devices

You can expand the configuration with standard I/O.

Note

F-I/O for PCS 7

For information on the F-I/O released for PCS 7, please refer to the "Process Control System PCS 7 Released Modules" manual for the respective PCS 7 version.

Software components

⚠ **WARNING**

S7 F/FH systems operation

You may only operate S7 F/FH systems in the approved system environments.

Operation in a virtual environment or remote access are permitted under the conditions listed in section "Requirements for virtual environments and remote access (Page 487)".

FSW-001

The software components of S7 F/FH systems include:

- The "SIMATIC S7 F Systems" optional package on the engineering station for configuring and programming the F-system.
- The safety program in the F-CPU
- "SIMATIC S7 F Systems HMI" for displaying the fail-safe operator control blocks on the OS

You also need the STEP 7 basic software and CFC optional software on the ES for configuration and programming.

Optional package "SIMATIC S7 F Systems"

This documentation describes S7 F Systems. S7 F Systems is the configuration and programming software for S7 F/FH systems.

With S7 F Systems, you obtain:

- Support in the configuration of the F-I/O in STEP 7 with HW Config
- Support in creating the safety program and integrating error detection functions in the safety program
- The F-library with F-blocks that you can use in your safety program.
- S7 F Systems also offers functions for comparing safety programs and to assist you in the acceptance of your plant.
- Support for controlling fail-safe parameters of a PCS 7 OS during operation (Secure Write Command/Safety Data Write).
- Support for safety-related changes of F-parameters in the safety program of the F-CPU from a PCS 7 OS (Maintenance Override).
- Support for fail-safe acknowledgment from a PCS 7 OS (with SWC_QOS).

- Support for operation and maintenance with F-forcing.
- Support for assigning the PROFIsafe address for the F-/O from the engineering system

Safety program

You can create a safety program with the CFC Editor in STEP 7 from the F-blocks that are included in an F-library with the "SIMATIC S7 F Systems" optional package.

When you compile the S7 program, safety checks are automatically performed and additional F-blocks for fault detection and fault response are installed. This ensures that failures and errors are detected and appropriate reactions triggered. This keeps the F-system in a safe state or brings the system to a safe state.

The S7 program in the CPU is comprised of fail-safe (safety program) and non-fail-safe (standard user program) components.

Data can be exchanged between safety and standard user programs in the F-CPU using special F-blocks for data conversion.

Installing

4

4.1 Installing the S7 F Systems optional package

Software requirements

In order to operate S7 F Systems V6.3, the following software packages must be installed:

- On the ES:
  - PCS 7 or SIS compact
    Or
  - STEP 7 and CFC
- On the OS (for SIMATIC S7 F Systems HMI)
  - PCS 7
    Or
  - SIS compact
- For offline testing
  - S7-PLCSIM

You can find the corresponding versions and requirements in the readme file.

Available installation units

S7 F Systems comprises the following installation units:

The related version designations can be found in the readme file.

- "Engineering AS OS"
  - S7 F Systems
  - S7 F Systems HMI
  - S7 F Systems Library
  - S7 F Device Integration Pack
  - S7 F Configuration Pack
  - Automation License Manager
- "Engineering AS"
  - S7 F Systems
  - S7 F Systems Library
  - S7 F Device Integration Pack
  - S7 F Configuration Pack

- "Engineering OS"
  - S7 F Systems HMI
- "Runtime"
  - S7 F Systems HMI

The "Automation License Manager" application can be optionally installed.

Read the installation notes in section 3 of the "SIMATIC S7 F Configuration Pack - Readme" file for S7 F Configuration Pack.

Reading readme files

You can find important information about the delivered software in the following readme files:

- "SIMATIC S7 F Systems - Readme"
- "SIMATIC S7 F Configuration Pack - Readme"
- "SIMATIC S7 F Systems HMI - Readme"
- "SIMATIC S7 F Systems Library - Readme"
- "SIMATIC S7 F Device Integration Pack - Readme".

You can display these files at the end of the corresponding setup program. At a later point, you can open the readme file by selecting **Siemens Automation > Documentation** in the Windows Start menu.

Installation options

The following options are available in the setup:

Option	Description
Engineering AS OS	The option is used to install all S7 F Systems components on the ES, i.e. if the computer is used for AS and OS engineering. This option is used for the installation under SIMATIC PCS 7.
Engineering AS	The option is used to install the S7 F Systems components on the ES, i.e. when the computer is used for engineering the AS. This option is used: • For installation under SIMATIC STEP 7. • For updating S7 F Systems Engineering including S7 F Systems Library, S7 F Device Integration Pack, S7 F Configuration Pack under SIMATIC PCS 7.
Engineering OS	The option is used for installation of OS components on the ES, which means the computer is used for the configuration of AS and OS and when only the OS is to be updated. This option is used for the installation of the OS components S7 F Systems HMI under SIMATIC PCS 7.
Runtime	The option is used to install the OS components S7 F Systems HMI: • On the OS, i.e. when the computer is only used as OS (for example, in OS single station system, OS server, or OS with Web server).

The optional packages from S7 F Systems can also be installed via SIMATIC Management Console.

Installing S7 F Systems on the ES

1. Start the Engineering station.
2. Save your changes in the "S7 F Systems Library" before installation.
3. Ensure that no STEP 7 applications are open.
4. Insert the "SIMATIC S7 F Systems" product CD.
5. Initiate the SETUP.EXE program on the CD.
6. Follow the instructions of the setup program.
   Select a program package with the engineering components of SIMATIC S7 F Systems in the setup.
   - "Engineering AS OS"
   - "Engineering OS"
   - "Engineering AS"

   Detailed information on the options/program packages is available in the "Installation options" table above.

Installing S7 F Systems on the OS

1. Start your OS. Ensure that no SIMATIC applications are open.
2. Insert the "SIMATIC S7 F Systems" product CD.
3. Initiate the SETUP.EXE program on the CD.
4. Follow the setup program instructions.
   Select the following program package in the setup:
   - "Runtime"

   Detailed information on the options/program packages is available in the "Installation options" table above.

Starting S7 F Systems

The "SIMATIC S7 F Systems" optional package does not contain any applications that you must start specifically. Support for the configuration and programming of F-Systems is integrated into:

- SIMATIC Manager
- HW Config
- CFC Editor
- PCS 7-OS

Displaying integrated Help

Context-sensitive Help is provided for the dialogs of the optional package. You can access this Help at every stage of configuring and programming using the F1 key or the "Help" button. For advanced help, select **Help > Contents > Calling Help on Optional Packages > S7 F/FH Systems - Working with F Systems**.

License key (usage authorization)

A license key is required for the "SIMATIC S7 F Systems" optional package. This license key is installed in the same way as for STEP 7 and the optional packages. For information on installing and working with license keys, refer to the readme file and the STEP 7 basic help.

S7 F Systems RT License (Copy License)

The S7 F Systems RT license (copy license) allows you to use a CPU as an F-CPU (for example, to run a safety program on it).

4.2 Uninstalling the S7 F Systems optional package

Removing S7 F Systems

The "S7 F Systems" optional package comprises the following components:

- S7 F Systems
- S7 F Systems HMI
- S7 F Systems Library
- S7 F Device Integration Pack
- S7 F Configuration Pack

It is recommended not to uninstall the SIMATIC S7 F Systems components as this can lead to problems with your configuration.

If you want to remove SIMATIC S7 F Systems or one of the components, place it on a basic image of your system and reinstall the required components.

4.3 Upgrade to S7 F Systems V6.3

4.3.1 Overview of upgrading

Introduction

Before upgrading from an existing project to S7 F Systems V6.3, read the following section carefully. This section contains the following important information:

- Basic upgrade information
- Effects of upgrading
- User scenarios for upgrades

Note

S7 F Systems V6.3 supports more F-I/Os than PCS 7. If necessary, consult the documentation for PCS 7.

With these F-I/O, however, only the processing with S7 F Systems and not the diagnostic functionality of PCS 7 is generated during compilation. For this reason, the message "Module is not supported" appears on the "Module drivers" tab when compiling.

Note

If you want to use the new features, upgrading from S7 F Systems to V6.3 also requires upgrading the S7 F Systems Library to V1.3 SP3.

Note

Specific notes on compatibility

- S7 F Systems Library V1.3 or higher is used as the F-library in the S7 project.

Upgrading to S7 F Systems V6.3

Note

Proceed with the upgrade according to the scenarios described here. Do not use the "Update block types" function even for multiprojects. Proceed as described in section "Updating a multiproject master data library (Page 45)" to update a multiproject master data library.

Effects of the upgrade

Before you upgrade a certain project to S7 F Systems V6.3, consider the following consequences:

Installation variant	**Consequences**	
	Advantages	**Disadvantages**
"Engineering OS" or "Runtime" options (only installation of the OS component S7 F Systems HMI)	• Safety program is unchanged, which means a CPU STOP is not necessary. • New OS functions can be used in full	• No new functions in the safety program • New OS functions can be used in full • OS compilation required
"Engineering AS" or "Engineering AS OS" options Update of the S7 F Systems Library	• Expanded engineering • Expanded functionality for operator control and monitoring • Full scope of functions	• Modified safety program and modified collective signature • Complete compiling and complete downloading with CPU-STOP required • OS compilation required
"Engineering AS OS" option; Update of the S7 F Systems Library	• Safety program is unchanged, which means a CPU STOP is not necessary. • New OS functions can be used in full	• No new functions in the safety program • OS compilation required
"Engineering AS" option without updating the S7 F Systems Library	• Safety program is unchanged, which means a CPU STOP is not necessary.	• No new functions in the safety program • New OS functions cannot be used

Note

"S7 F Systems Lib V1_3" library

In the following descriptions and user scenarios, the library name "S7 F Systems Lib V1.3" is used and applies to the following versions.

- S7 F Systems Library V1.3
- S7 F Systems Library V1.3 SP1
- S7 F Systems Library V1.3 SP1 Update 1
- S7 F Systems Library V1.3 SP2
- S7 F Systems Library V1.3 SP3

You can find the installed version in the Windows Start menu in subdirectory "Siemens Automation > SIMATIC > Installed software".

User scenarios for upgrading

Proceed as described in the user scenarios relevant for you.

The following sections give you a description of the user scenarios.

Upgrade of S7 F Systems V6.x	Update of the S7 F Systems Library	To S7 F Systems V6.3
Only upgrade of the OS component "S7 F Systems HMI" on ES and OS	No	User scenario 1 (Page 38)
Upgrade ES and OS	No	User scenario 2 (Page 40)
Upgrade ES	Yes	User scenario 3 (Page 41)
Upgrade ES and OS	Yes	User scenario 4 (Page 43)

Requirements:

- The S7 project is created with S7 F Systems as of V6.0.
- S7 F Systems Library V1.3 or higher is used as the F-library.

Note

Before using S7 F Systems, please check if the ES/OS operating system meets the minimum requirements of S7 F Systems V6.3. If necessary, you need to upgrade your operating system to the ES/OS and then install S7 F Systems V6.3.

Note

See also the section "Differences between the S7 F Systems Lib F-libraries (Page 478)".

4.3.2 User scenario 1

Objective

Upgrading the OS component "S7 F Systems HMI" to ES and OS without program modification.

Introduction

This user scenario helps you to upgrade the OS component S7 F Systems HMI to ES and OS.

There is no upgrade of S7 F Systems or the S7 F Systems Library.

By upgrading according to this user scenario, you maintain compatibility with your previous version.

Requirement

Your S7 program must be compiled, downloaded and executable for the original S7 F Systems Lib V1.3. Ensure this through a printout of the safety program and an online comparison.

There must not be any offline changes that are not downloaded online.

Consequences

- Safety program is not changed
- No change of the collective signature of the safety program
- No new functionality
- Compilation and download of the OS required

Procedure

1. Start the installation program of S7 F Systems V6.3.
   Select a program package with the OS component "S7 F Systems HMI" in the setup.
   - "Engineering OS" on the ES
   - "Runtime" on the OS

   Detailed information on the options/program packages is available in the section "Installing the S7 F Systems optional package (Page 31)" in the "Installation options" table.
   The selected program package is installed on the computer.
2. Prior to the initial compilation, save the current version of your safety program as a reference ("Save reference" in the "Safety program" dialog) so that it will be available for future comparisons.
3. You can now compile your S7 program again.

Take the following steps to use the new S7 F Systems HMI faceplates in a project already existing.

1. Launch the WinCC Explorer for the OS assigned to the S7 F Systems project.
2. Open the OS Project Editor and click OK.
   The project is reconfigured and the new block icons are applied.
3. Open the Global Script C Editor and select the menu command "**Options > Regenerate Header**".

Authorizations at the block icons (e.g. LevelInitiate, LevelBypass) may need to be configured again.

Result

Once you have performed these steps, the new OS functions can be used in the project.

In order to use the OS functions, you must compile and download the OS for the relevant project.

4.3.3 User scenario 2

Objective

Upgrade ES and OS from S7 F Systems V6.x to V6.3 without upgrading the S7 F Systems Library.

Introduction

This user scenario helps you upgrade from ES and OS to S7 F Systems V6.3 without upgrading the S7 F Systems Library.

Since the blocks of the S7 F Systems Library are not upgraded to V1.3 SP3, you cannot use new functions of the F-library S7 F Systems Library V1.3 SP3.

Requirements

- S7 F Systems Library V1.3 or higher is used as the F-library in the S7 project.

Consequences

- No change of the collective signature of the safety program
- Safety program is not changed
- Compilation and download of the OS required

You can find additional information on the possible consequences in the section "Acceptance test following system upgrade (Page 227)".

Procedure

1. Create a backup copy of the entire S7 project for comparison purposes before you install S7 F Systems V6.3.
2. Start the S7 F Systems V6.3 installation program on the ES or OS.
3. Select the following program package in the setup:
   - "Engineering AS OS" on the ES
   - "Runtime" on the OS

   Detailed information on the options/program packages is available in the section "Installing the S7 F Systems optional package (Page 31)" in the "Installation options" table.
4. Prior to the initial compilation, save the current version of your safety program as a reference ("Save reference" in the "Safety program" dialog) so that it will be available for future comparisons.
5. Compile and load your S7 program.

Take the following steps to use the new S7 F Systems HMI faceplates in a project already existing.

1. Launch the WinCC Explorer for the OS assigned to the S7 F Systems project.
2. Open the OS Project Editor and click OK.
   The project is reconfigured and the new block icons are applied.
3. Open the Global Script C Editor and select the menu command "**Options > Regenerate Header**".

Authorizations at the block icons (e.g. LevelInitiate, LevelBypass) may need to be configured again.

Result

ES and OS are upgraded to S7 F Systems V6.3.

The S7 F Systems Library has not been upgraded.

In order to use the OS functions, you must compile and download the OS for the relevant project.

4.3.4 User scenario 3

Objective

Only upgrade ES from S7 F Systems V6.x to V6.3 with upgrade of S7 F Systems Library V1.3.x to V1.3 SP3.

Introduction

This user scenario helps you to upgrade the ES to S7 F Systems V6.3 with upgrading the S7 F Systems Library to V1.3 SP3.

Since the blocks of the S7 F Systems Library are upgraded to V1.3 SP3, you can use the new functions of the F-library S7 F Systems Library V1.3 SP3.

When you migrate from S7 F Systems Library V1.3.x to V1.3 SP3, the F-FBs in your safety program are overwritten by F-blocks with different block signatures. This means that the collective signature will change.

Requirements

- S7 F Systems Library V1.3 or higher is used as the F-library in the S7 project.
- If custom F-block types are used in your project, you must re-create these with S7 F Systems Library V1.3 SP3 beforehand. To do this, follow the procedure outlined in section "Updating custom F-block types (Page 45)".

Consequences

- Change of the collective signature of the safety program
- Change the safety program
- Complete download with STOP of F-CPU required
- Compilation and download of the OS required

You can find additional information on the possible consequences in the section "Acceptance test following system upgrade (Page 227)".

Procedure

1. Create a backup copy of the entire S7 project for comparison purposes before you install S7 F Systems V6.3.
2. Start the S7 F Systems V6.3 installation program on the ES.
3. Select the following program package in the setup:
   – "Engineering AS"
4. Detailed information on the options/program packages is available in the section "Installing the S7 F Systems optional package (Page 31)" in the "Installation options" table.
5. Prior to the initial compilation, save the current version of your safety program as a reference ("Save reference" in the "Safety program" dialog) so that it will be available for future comparisons.
6. Select the "S7 F Systems Lib V1.3" F-library in the "Safety Program" dialog.
   To do so, click the "Library Version" button in the "Edit safety program" dialog.
7. In the S7 program, update the existing F-block types. See section "Updating custom F-block types (Page 45)" for more on this.
8. Update all block types in the CFC Editor by selecting **Options > Block Types** and clicking "New Version".
9. In the CFC Editor under **Options > Block Types**, click "Clean Up".
10. Compile and download your hardware configuration.
11. Compile and load your S7 program.

Result

The ES is upgraded from S7 F Systems V6.x to V6.3 including the upgrade of S7 F Systems Library V1.3.x to V1.3 SP3.

4.3.5 User scenario 4

Objective

Upgrade ES and OS from S7 F Systems V6.x to V6.3 with upgrade of S7 F Systems Library V1.3.x to V1.3 SP3.

Introduction

This user scenario helps you upgrade from ES and OS to S7 F Systems V6.3 by upgrading the S7 F Systems Library to V1.3 SP3.

Since the blocks of the S7 F Systems Library are upgraded to V1.3 SP3, you can use the new functions of the F-library S7 F Systems Library V1.3 SP3.

When you migrate from S7 F Systems Library V1.3.x to V1.3 SP3, the F-FBs in your safety program are overwritten by F-blocks with different block signatures. This means that the collective signature will change.

Requirements

- S7 F Systems Library V1.3 or higher is used as the F-library in the S7 project.
- If custom F-block types are used in your project, you must re-create these with S7 F Systems Library V1.3 SP3 beforehand. To do this, follow the procedure outlined in section "Updating custom F-block types (Page 45)".

Consequences

- Change of the collective signature of the safety program
- Change the safety program
- Complete download with STOP of F-CPU required
- Compilation and download of the OS required

You can find additional information on the possible consequences in the section "Acceptance test following system upgrade (Page 227)".

Procedure

1. Create a backup copy of the entire S7 project for comparison purposes before you install S7 F Systems V6.3.
2. Start the S7 F Systems V6.3 installation program on the ES.

3. Select a program package in the setup.
   - "Engineering AS OS" if you are using ES and OS on this computer.
   - "Engineering AS" if you are using only the ES on this computer. Refer to step 4.
   - "Engineering OS", if the computer is used for the configuration of AS and OS and only the OS is to be updated.

   Detailed information on the options/program packages is available in the section "Installing the S7 F Systems optional package (Page 31)" in the "Installation options" table.
4. If you are using an OS standalone system or an OS server for the OS, then start the installation program on the corresponding computer.
   Select the program package in the setup:
   - "Runtime"
5. Prior to the initial compilation, save the current version of your safety program as a reference ("Save reference" in the "Safety program" dialog) so that it will be available for future comparisons.
6. Select the "S7 F Systems Lib V1.3" F-library in the "Safety Program" dialog.
   To do so, click the "Library Version" button in the "Edit safety program" dialog.
7. In the S7 program, update the existing F-block types. See section "Updating custom F-block types (Page 45)" for more on this.
8. Update all block types in the CFC Editor by selecting **Options > Block Types** and clicking "New Version".
9. In the CFC Editor under **Options > Block Types**, click "Clean Up".
10. Compile and download your hardware configuration.
11. Compile and load your S7 program.

Take the following steps to use the new S7 F Systems HMI faceplates in a project already existing.

1. Launch the WinCC Explorer for the OS assigned to the S7 F Systems project.
2. Open the OS Project Editor and click OK.
   The project is reconfigured and the new block icons are applied.
3. Open the Global Script C Editor and select the menu command "**Options > Regenerate Header**".

Authorizations at the block icons (e.g. LevelInitiate, LevelBypass) may need to be configured again.

Result

ES and OS are upgraded to S7 F Systems V6.3 with the S7 F Systems Library V1.3 SP3.

In order to use the OS functions, you must compile and download the OS for the relevant project.

4.3.6 Updating custom F-block types

If F-block types are used in your project, you must recreate them with the S7 F Systems Library V1.3 SP3. To do this, you need the project (source project) in which the F-block type was created as a block type in the CFC Editor via the menu command **Chart > Compile > Chart as block type**.

Proceed as follows:

1. Install S7 F Systems V6.3 with S7 F Systems Library V1.3 SP3.
2. In the "Safety Program" dialog, select the "S7 F Systems Lib V1.3" F-library.
3. Update all block types in the CFC Editor by selecting **Options > Block Types** and clicking "New Version".
4. In the CFC Editor under **Options > Block Types**, click "Clean Up".
5. Open the CFC chart to be compiled and compile it in the CFC Editor using the menu command **Chart > Compile > Chart as block type**.
6. Now you can copy the compiled F-block type into the S7 programs in which you want to use it.

See also

Creating F-Block types (Page 101)

4.3.7 Updating a multiproject master data library

Introduction

The following describes how you apply the F-blocks from S7 F Systems Library V1.3 SP3 to the master data library of your multiproject.

Requirement

The user projects are already updated.

Note

You update the user projects in your multiproject as described in the section "Overview of upgrading (Page 36)".

If you are using F-block types that you have created in your master data library, you must update these F-block types as described in section "Updating custom F-block types (Page 45)".

All attributes of the F blocks must be applied. Do not perform an update of the old F-block attributes.

Procedure

Proceed as follows to continue using the master data library with fail-safe blocks as usual in the multiproject:

1. Open the block folder in the master data library of your multiproject and select the "Details" view option.
2. Delete all blocks with the author "F_SAFE11" or "F_SAFE12".
   Important: Select the "Also delete symbolic block names" option.
3. In SIMATIC Manager, select **File > Open** and switch to the "Libraries" tab.
4. Select the "S7 F Systems Lib V1.3" library and acknowledge with "OK".
   Result: The library opens.
5. Select the "F-User Blocks" library component to be copied.
6. Select the **Edit > Copy** menu command.
7. Select the folder in the master data library (destination) in which the copied library component is to be placed.
8. Select the menu command **Edit > Paste**. The copied library component is placed into the master data library.
9. Repeat Steps 6 to 8 for the "F-Control Blocks" library component.
10. Repeat Steps 6 to 8 for the block folder containing the F-block types that you created.
11. In SIMATIC Manager, select **Options > Charts > Update Block Types** for the master data library. This will update all blocks in your sample solutions and process tag types in the master data library.

Configuration 5

5.1 Configuration overview

Introduction

The following section lists the main points in which the configuration of a fail-safe system differs from that of an S7 standard system.

Fail-safe components that you must configure

The following hardware components must be configured for S7 F Systems V6.3:

1. F-CPU, e.g. CPU 410-5H
2. F-I/O, such as:
   - ET 200S fail-safe I/O modules
   - ET 200SP fail-safe I/O modules
   - ET 200SP HA fail-safe I/O modules
   - S7-300 fail-safe signal modules in ET 200M (distributed configuration)
   - ET 200eco fail-safe I/O modules
   - ET 200pro fail-safe I/O modules
   - ET 200iSP fail-safe I/O modules
   - Fail-safe DP standard slaves
   - Fail-safe IO standard devices
   - Fail-safe PA field devices

Note

F-I/O for PCS 7

For information on the F-I/O released for PCS 7, please refer to the "Process Control System PCS 7 Released Modules" manual for the respective PCS 7 version.

5.2 Particularities for configuring an F-System

Configuring same as in standard system

You configure an S7 F/FH Systems fail-safe system the same as a standard S7 system. That is, you configure and assign parameters for the hardware in HW Config as a centralized configuration (F-CPU) and as a distributed configuration (F-CPU, F-SMs in ET 200M, F-modules in ET 200S, ET 200SP, ET 200SP HA, ET 200pro, ET 200iSP and ET 200eco, fail-safe DP standard slaves / IO standard devices, fail-safe PA field devices).

For a detailed description of the configuration variants, refer to the "Safety Engineering in SIMATIC S7 (http://support.automation.siemens.com/WW/view/en/12490443)" system manual.

Special F-relevant tabs

There are a few special tabs for the fail-safe functionality in the object properties of the fail-safe I/O. These tabs are described in the following sections.

Assigning symbols for fail-safe inputs/outputs of the fail-safe I/O

For convenience when programming S7 F/FH systems, it is especially important that you assign symbols for the fail-safe inputs and outputs of the F-I/O in HW Config.

Saving and compiling the hardware configuration

You must save and compile the hardware configuration of S7 F/FH systems in HW Config. This is required for subsequent programming of the safety program.

Changing safety-related parameters

Note

If you change a safety-related parameter for an F-I/O or an F-CPU, you must recompile the S7 program.

The same applies to changes in S7 connections for safety-related communication via S7 connections.

Rules for F-systems

In addition to the rules that are generally applicable for the arrangement of modules in an S7-400, you must also comply with the following conditions for an F-system:

- Prior to downloading the safety program, you must download the hardware configuration to the F-CPU.
- If you have changed the configuration of an F-I/O or the F-CPU (cycle times of the cyclic-interrupt OB), you must recompile the S7 program and download it to the F-CPU.

5.3 Configuring the F-CPU

Rules for configuring an F-CPU

> ⚠ WARNING
>
> **An F-CPU containing a safety program must have a password.**
>
> You must ensure that the following conditions are met:
>
> - The "CPU contains safety program" option must be selected.
> - A password must always be assigned.
>
> You make these settings in the object properties of the F-CPU in HW Config.
>
> FSW-003

> ⚠ WARNING
>
> **Configuring a protection level**
>
> In safety mode, access authorization by means of the F-CPU password must not be active when changes are made to the standard user program, because the safety program can then also be changed. To rule out this possibility, you must configure protection level "1".
> If only one person is authorized to change the standard user program and the safety program, protection level "2" or "3" should be configured to ensure that other persons have only limited access or no access to the standard user program and safety program.
>
> FSW-004

Procedure for configuring the protection level

To configure the protection level 1, follow the steps below:

1. Select the desired F-CPU in HW Config, e.g. CPU 410-5H, and then the menu command **Edit > Object properties**.
2. Open the "Protection" tab.
3. Set the protection level to "1: Access protection for F-CPU or keyswitch setting" and "Can be bypassed with password".
   Enter a password for the F-CPU in the fields provided for that purpose and activate the "CPU contains safety program" option.
   You can find information on the password for the F-CPU in section "Overview of access protection (Page 75)". In particular, observe the warning in section "Setting up / changing access permission for the F-CPU (Page 78)":
   Furthermore, it is recommended that the increased password security option be used. The increased password security is only relevant for the engineering system. When this option is activated, the entered password is stored encrypted in the data management. That increases the security of the password. Setting this option does not affect the response to a password operation. Refer to the information on increased password security in section ""Password for Safety Program Creation" dialog (Page 197)".

Important parameters for the F-CPU in S7 FH Systems

To prevent the time monitoring from responding at a master-standby switchover (e.g. H-CiR), you must configure the OB 3x(s) designated for safety programs with a priority > 15 in the "Cyclic interrupts" tab of the F-CPU. You should not place standard blocks in these OBs.

The cyclic interrupt OB of the safety program must be configured as "Cyclic interrupt OB with special handling". Only then will this cyclic interrupt be called just before the start of the disabling time for priority classes > 15 when the standby CPU is updated. For this purpose, you enter the number of the highest priority cyclic interrupt OB to which F-blocks of the safety program are assigned in the CFC Editor in the "Cyclic interrupt OB with special handling" field on the "H Parameters" tab of the CPU properties.

- Ensure that the correction factor is set to 0 ms in the "Clock" group on the "Diagnostics/ Clock" tab.

Note

For S7 FH Systems, only settings up to 12 hours are allowed.

For S7 FH Systems, you are not permitted to modify safety-related self-tests via SFC 90 "H_CTRL". Otherwise, the safety program goes to F-STOP after 24 hours at the latest. Test components are not permitted to be switched on or off (submode 0 to 5 of mode 20, 21 and 22).

For the same reason, you must not disable the updating via SFC 90 "H_CTRL" too long.

Failure to observe this will trigger an F-STOP. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error detected" (event ID 16#75E1)

Changing the OB3x cycle time

After a change of the OB 3x cycle times, you must recompile the S7 program.

5.4 Configuring the F-I/O

5.4.1 Overview of configuring the F-I/O

Overview

You can find general information on the configuration of the F-I/O in the section "General information on configuring the F-I/O (Page 51)".

The configuring of the F-I/O differs in the following options:

- The F_destination_address is set on the fail-safe module via a DIP switch. This option applies to F-modules such as ET 200iSP and S7-300 F-SMs.
  You can find additional information on this in section "Configuration of the F-modules with assignment of the F_destination_address via DIL switches (Page 54)".
- For F-modules such as ET 200SP HA, the PROFIsafe address (F-source and F-destination address) is assigned directly from the engineering system in STEP 7.
  These fail-safe modules do not have a DIP switch for setting the F-destination address.
  You can find additional information on this in section "Configuring fail-safe modules with assignment of F_destination_address in the Engineering System (Page 56)".

Note

Requirement for redundant interface modules and system redundancy of the type R1

For system redundancy of the type R1 for distributed I/Os, e.g. ET 200SP HA, for redundant interface modules (IM) the left IM must be plugged in and the power supply must be switched on so that the F-destination addresses can be assigned to the I/O modules.

If only the right IM is plugged in and the corresponding power supply is switched on, then no F_destination_address can be assigned to the I/O modules.

5.4.2 General information on configuring the F-I/O

Configuring same as in standard system

F-modules such as ET 200S, ET 200eco, ET 200pro, ET 200iSP, ET 200SP, ET 200SP HA and the S7-300 F-SMs are always configured in the same way:

Once the F-I/O have been inserted into the station window of HW Config, you can access the configuration dialog by selecting **Edit > Object Properties** or by double-clicking the F-I/O.

When changes are made to fail-safe I/O in HW Config, you are prompted to enter the password for the safety program.

The values in the shaded fields are automatically assigned by S7 F Systems in the F-relevant tab. You can change the values in the non-shaded fields.

Additional Information

For a description of the parameters, refer to the context-sensitive online help for the tab and the relevant F-I/O manual.

For information on what you must consider when configuring the F-monitoring time for fail-safe I/O, refer to the "Safety Engineering in SIMATIC S7 (http://support.automation.siemens.com/WW/view/en/12490443)" system manual.

Assigning symbols for fail-safe inputs/outputs of the fail-safe I/O

For convenience when programming S7 F/FH systems, it is important that you assign symbols for the fail-safe inputs and outputs of the F-I/O in HW Config.

Note that for certain fail-safe I/O (such as S7-300 F-SMs and ET 200S F-modules), a 1oo2 evaluation can be set for the sensor. In this case, only one of the two combined channels is available.

We recommend that you identify the unavailable channel as reserved in the symbol table. To find out which of the channels combined by the 1oo2 sensor evaluation you can access in the safety program, refer to the relevant manuals for the F-I/O.

Operating mode

For S7-300 fail-safe signal modules, you can distinguish on the basis of the "Operating mode" parameter whether the modules are being used in standard mode (used as standard S7-300 signal modules SM 326; DO 8 × DC 24V/2A, SM 326 F DO 10xDC24V/2A PP (6ES7326-2BF10-0AB0) and SM 336 F AI6x0/4..20mA HART (6ES7336-4GE00-0AB0)) or in safety mode.

ET 200S, ET 200pro, ET 200iSP and ET 200eco fail-safe modules can only be used in safety mode.

Group diagnostics for fail-safe S7-300 signal modules

The "Group diagnostics" parameter is used to activate and deactivate the transmission of channel-specific diagnostic alarms of F-SMs (such as wire break and short-circuit) to the F-CPU. For availability reasons, you should shut down the group diagnostics on unused input or output channels of the following F-SMs:

- SM 326; DI 8 x NAMUR
- SM 326; DO 10 x DC 24V/2A
- SM 336; AI 6 x 13Bit

⚠ WARNING

"Group diagnostics" for fail-safe F-SMs in safety mode

"Group diagnostics" must be activated on all connected channels of fail-safe F-SMs in safety mode.

Check to verify that you have shutdown group diagnostics only for unused input and output channels.

(FSW-005)

You can optionally enable diagnostic interrupts.

The following applies to modules:

- SM 326; DI 24 x DC 24V (as of article no. 6ES7326-1BK01-0AB0)
- SM 326, F-DO10 x DC24V/2A PP (6ES7326-2BF10-0AB0)
- SM 326; DO 8 x DC 24V/2A PM (as of article no. 6ES7326-2BF40-0AB0)
- The following applies to SM 336, F-AI 6 x 0/4 ... 20mA HART (6ES7336-4GE00-0AB0):

By deactivating a channel in HW Config, you also deactivate its group diagnostics function.

PROFIsafe addresses

The F-source address "F_source_address" together with the F-destination address "F_destination_address" forms the PROFIsafe address. The PROFIsafe address is used for the unique identification of the PROFIsafe destination, i.e. the F-I/O.

F_destination_address

The F_Destination_Address is a unique identification of the PROFIsafe destination, i.e. the F-I/O. Therefore, the F_destination_address must be unique network-wide and station-wide (see section "Rules for address assignment").

To prevent incorrect parameter assignment, a "station-wide unique" F_destination_address is automatically assigned when the F-I/O are placed in HW Config.

In S7 F/FH Systems, you must ensure that the F_destination_address is "unique network-wide" when multiple stations are present in a network by manually changing the F_destination_addresses.

If you change the F_destination_address, the uniqueness of the F_destination_address within the station is checked automatically. You yourself must make sure that the F_destination_address is unique network-wide.

F_source_address

The F_source_address is automatically assigned in S7 F Systems and is preset with the value "1".

See also

S7 Distributed Safety - Configuration and Programming (http://support.automation.siemens.com/WW/view/en/54110126)

5.4.3 Configuration of the F-modules with assignment of the F_destination_address via DIL switches

F_destination_address

Fail-safe modules, for example in the ET 200iSP, have a DIP switch with which you can assign the unique F-destination address for each module.

You must set the F_destination_address on the F-I/O via the DIP switch before installing the F-I/O.

Note

For the following S7-300 F-SMs, the F_destination_address is the same as the start address of the F-SM/8:

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

Assign low start addresses for these F-SMs if you are also using other F-I/O.

Rules for address assignment

⚠ WARNING

Address assignment in subnets only and in mixed configurations

The following applies to PROFIBUS DP subnets only:

The PROFIsafe destination address and, thus, the switch setting on the address switch of the F-I/O must be unique network-wide* and station-wide** (system-wide).

For S7-300 F-SMs and ET 200S, ET 200eco, ET 200iSP and ET 200pro F-modules, you can assign a maximum of 1022 different PROFIsafe destination addresses.

The following applies to PROFINET IO subnets only and to mixed configurations of PROFIBUS DP and PROFINET IO:

The PROFIsafe destination address and, thus, the address switch setting on the F-I/O must be unique only*** within the PROFINET IO subnet, including all lower-level PROFIBUS DP subnets, and station-wide** (system-wide).

For S7-300 F-SMs and ET 200S, ET 200eco, ET 200iSP and ET 200pro F-modules, you can assign a maximum of 1022 different PROFIsafe destination addresses.

A PROFINET IO subnet is characterized by the fact that the IP addresses of all networked nodes have the same subnet address, i.e. the IP addresses match in the positions that have the value "1" in the subnet mask.

Example:

IP address: 140.80.0.2.

Subnet mask: 255.255.0.0 = 11111111.11111111.00000000.00000000

Meaning: The first 2 bytes of the IP address define the subnet; subnet address = 140.80.

* A network consists of one or more subnets. "Network-wide" means across subnet boundaries.

** "Station-wide" means for one station in HW Config (e.g. an S7-400H station).

*** Across Ethernet subnets, excluding cyclic PROFINET IO communication (RT communication)

(FSW-006)

5.4.4 Configuring fail-safe modules with assignment of F_destination_address in the Engineering System

Note that the rules for address assignment of the PROFIsafe destination addresses also apply to F-modules, such as in ET 200 SP or ET 200SP HA.

⚠ WARNING

Uniqueness of PROFIsafe addresses across stations required

- Uniqueness across stations:
  F-I/O modules, e.g. the ET 200 SP or ET 200SP HA, are uniquely addressed station-wide by a combination of F-source address (PROFIsafe base address of the assigned F-CPU) and F-destination address. The F-system itself ensures that the F-destination addresses of all F-I/O modules are unique within the assigned F-CPU.
- Uniqueness across stations:
  To also ensure uniqueness across stations, you must check that the PROFIsafe addresses ("F_source_address" + "F_destination_address") of the F-I/O modules are unique across stations.
- Check for a change:
  Since the F-source address "F_source_address" of the PROFIsafe address of the F-CPU is automatically set to "1", you can only change the default address "F_destination_address" for F-I/O modules, e.g. the ET 200 SP or ET 200SP HA.
  Note that the PROFIsafe address of the F-I/O module must be unique across all stations.

For Ethernet subnets and mixed configurations of PROFIBUS and Ethernet subnets, the following also applies:

The combination of F-source address and F-destination address of each F-I/O must only** be unique in the overall Ethernet subnet including all subordinate PROFIBUS subnets.

An Ethernet subnet is characterized by the fact that the IP addresses of all networked stations have the same subnet address. This means that the IP addresses match in the places that have the value "1" in the subnet mask.

Example:

IP address: 140.80.0.2.

Subnet mask: 255.255.0.0 = 11111111.11111111.00000000.00000000

Meaning: The first 2 bytes of the IP address define the subnet; subnet address = 140.80.

(FSW-007)

** When cyclic PROFINET IO communication between Ethernet subnets is excluded

Introduction

Fail-safe modules, for example in the ET 200 SP or ET 200SP HA, do not have a DIP switch with which you can assign the unique F-destination address for each module.

Instead, you assign the PROFIsafe address (F-source address and F-destination address) directly from the Engineering System in STEP 7. Before you use a fail-safe module, you must assign it the associated F-destination address together with the F-source address.

A new assignment is required for fail-safe modules in the following situations:

- Subsequent insertion of an F-module during first commissioning
- Deliberate change to the F-destination address
- Replacement of the terminal block

A reassignment is not necessary in the following cases:

- Power OFF/ON
- Replacement of an F-module (repair case) without PG/PC
- Change to the configuration when a new terminal block is inserted in front of or behind an F-module
- Repair/replacement of the interface module

Basic procedure

1. Configure the F-destination address in HW Config.
2. Identify the F-modules in the distributed I/O to which you want to assign the configured F-destination addresses (together with the F-source address).
   You can find additional information on this in section "Identification of F-modules (address assignment in the engineering system) (Page 57)".
3. Assign the F-destination address (together with the F-source address) to the F-modules.
   You can find additional information on this in section "Assigning the F-destination address and F-source address (address assignment in the engineering system) (Page 59)".

5.4.4.1 Identification of F-modules (address assignment in the engineering system)

Requirements

The following requirements must be met:

- The interface module and the F-I/O modules (F-modules) are configured.
- The configuration was downloaded to the F-CPU.
- The interface module and the F-I/O modules (F modules) can be reached online.
  For type R1 system redundancy for distributed I/Os, e.g. ET 200SP HA, at least the left interface module (IM) must be accessible online for redundant interface modules.

⚠ WARNING

Identification and acknowledgment of the F-I/O

Press the "Identification" button to confirm the fail-safe correctness of the PROFIsafe addresses for the F-modules.

Therefore, proceed cautiously when confirming the F-I/O by LED flashing or by the serial number of the interface module.

Assigning the PROFIsafe addresses with the serial number of the interface module is only permitted if the assignment is to be performed for all F-I/Os of a station. If individual F-I/Os are selected, the flashing of each individual F-I/O must be checked and confirmed.

FSW-008

Procedure

To identify F-modules, follow these steps:

1. Establish an online connection to the F-CPU on which this F-module will be operated.
2. In HW-Config, select the F-module to which you want to assign the F-destination address.
3. Select "Name F-addresses..." from the shortcut menu:
4. Select the method for identification of the F-modules under "Assign F-destination address by".
   – "Identify LED flashing"
   This is the default setting. During the identification, the DIAG and STATUS LEDs of the F-modules to be identified flash.
   – "Identification with the serial number"
   If you do not have direct sight of the F-modules, you can identify the F-modules using the serial number of the interface module.

   Note

   Unlike the serial number printed on the interface module, the displayed serial number may be supplemented to include the year date. The serial numbers are identical despite that.

5. In the "Assign" column, select all F-modules to which you want to assign the F-destination address.
   If you select the check box "Assign F-destination address for all reachable F-modules", all F-modules of the station are selected.
6. Click the "Identification" button.
   If you selected the "Identify LED flashing" option: Observe whether the DIAG LEDs and status LEDs of the F-modules whose F-destination address you want to assign are flashing. The DIAG LED should flash "Red" and the status LED "Green".
   If you selected the "Identify with serial number" option: Compare the displayed serial number with the serial number of the interface module.

See also

Configuring fail-safe modules with assignment of F_destination_address in the Engineering System (Page 56)

Assigning the F-destination address and F-source address (address assignment in the engineering system) (Page 59)

5.4.4.2 Assigning the F-destination address and F-source address (address assignment in the engineering system)

Requirement

The F-modules have been successfully identified as described in the "Identification of F-modules (address assignment in the engineering system) (Page 57)" section.

Procedure

To assign the F-destination address and F-source address, follow these steps:

1. After identification in section "Identification of F-modules (address assignment in the engineering system) (Page 57)", check the reaction of the F-modules.
   - If you selected the "Identify LED flashing" option: Observe whether the DIAG LEDs and status LEDs of the F-modules whose F-destination address you want to assign are flashing. The DIAG LED should flash "Red" and the status LED "Green".
   - If you selected the "Identify with serial number" option: Compare the displayed serial number with the serial number of the interface module.
2. For each F-module selected in the "Assign" column, a query is displayed in the "Identification" column.
   Confirm the identification of an F-module by activating the corresponding check box in the "Identification" column.
   Only then will the "Assign F-destination address" button be activated.
3. Assign the F-destination address (together with the F-source address) to the selected F-modules using the "Assign F-destination address" button. You must enter the password of the F-CPU if necessary.
4. To assign the F-destination address (together with the F-source address), you must confirm the "Confirm assignment" dialog within 60 seconds.

See also

Configuring fail-safe modules with assignment of F_destination_address in the Engineering System (Page 56)

5.4.4.3 Changing the F-destination address or F-source address (address assignment in the engineering system)

Procedure

1. Change the F-destination address or F-source address in the hardware configuration.
2. Compile the hardware configuration.
3. Download the hardware configuration to the F-CPU.
4. Establish an online connection to the F-CPU on which this F-module is operated.
5. Select "Name F-addresses" from the shortcut menu:
6. Repeat the steps described in sections "Identification of F-modules (address assignment in the engineering system) (Page 57)" and "Assigning the F-destination address and F-source address (address assignment in the engineering system) (Page 59)".
7. Compile the user program and download it to the F-CPU.

5.5 Configuring fail-safe DP standard slaves/IO standard devices

Requirement

In order to use fail-safe DP standard slaves/IO standard devices, these standard devices must be on PROFIBUS DP or PROFINET IO and support the PROFIsafe bus profile.

Configuring with GSD/GSDML file

As is the case in a standard system, the fail-safe standard slaves are configured based on the device specification in the so-called GSD file (generic station description).

- In the GSD file for DP standard slaves.
- In der GSDML file for IO standard devices.

For these fail-safe standard devices, portions of the specification are protected by a cyclic redundancy check (CRC).

The GSD/GSDML files are supplied by the device manufacturers. To operate fail-safe standard devices with S7 F Systems, the supplied GSD/GSDML file must meet the following PROFIsafe specification:

- For fail-safe DP standard slaves: PROFIsafe Specification V1.0 or higher
- For fail-safe IO standard devices: PROFIsafe Specification as of V2.0 to V2.6.1

Ask for confirmation of this from the device manufacturer.

Import the GSD/GSDML files into your project (see STEP 7 online help). After the import, the corresponding fail-safe standard devices can be selected in the hardware catalog of HW Config.

Protection of the data structure of the device in GSD/GSDML files

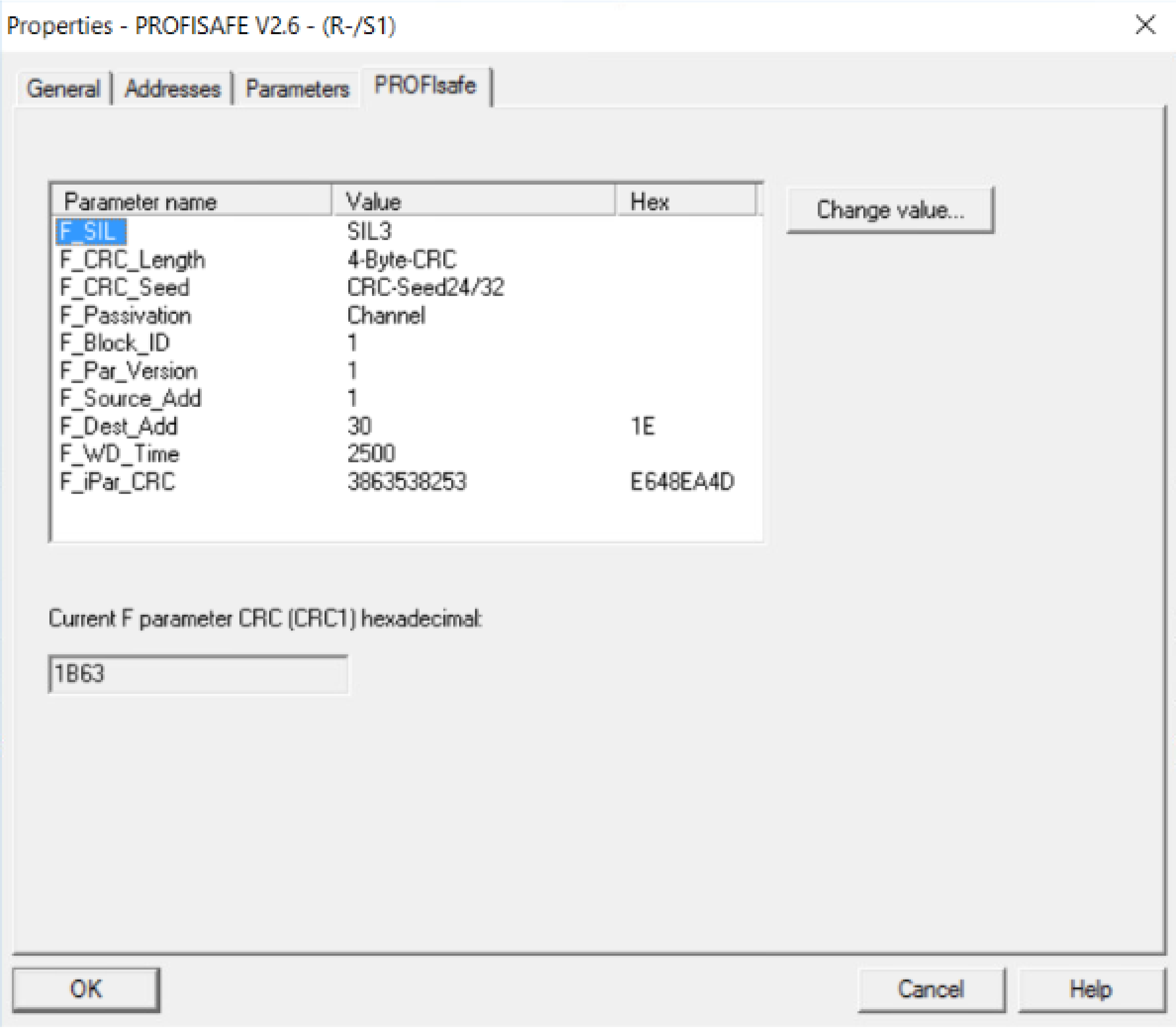
Starting with PROFIsafe Specification V2.0, the data structure of the device described in the GSD or GSDML file must be protected with a CRC stored in this file ("setpoint" for F_IO_StructureDescCRC).

Procedure for configuring with GSD/GSDML file

Import the GSD/GSDML file into your project (see online help for STEP 7).

1. Select the corresponding fail-safe standard device, e.g. a DP standard slave, in the hardware catalog of HW Config and insert it into your DP master system / PROFINET IO system.
2. Select the fail-safe DP or IO master.
3. Open the object properties dialog using the **Edit > Object Properties** menu command or by double-clicking the slot of the fail-safe component.

The figure below shows the properties of a DP standard slave as an example.



Parameter name	Value	Hex
F_SIL	SIL3	
F_CRC_Length	4-Byte-CRC	
F_CRC_Seed	CRC-Seed24/32	
F_Passivation	Channel	
F_Block_ID	1	
F_Par_Version	1	
F_Source_Add	1	
F_Dest_Add	30	1E
F_WD_Time	2500	
F_iPar_CRC	3863538253	E648EA4D

Current F parameter CRC (CRC1) hexadecimal:

1B63

"PROFIsafe" tab

The parameter texts specified in the GSD/GSDML file are contained on the "PROFIsafe" tab under "Parameter name". The associated current value is shown under "Value". You can modify this value using the "Change value" button.

The parameters are explained below.

"F_Check_SeqNr" parameter

This parameter defines whether the sequence number is to be incorporated in the consistency check (CRC calculation) of the F-User data frame.

The "F_Check_SeqNr" parameter must be set to "No check" in the PROFIsafe V1 MODE. Only fail-safe DP standard slaves/PA field devices that behave accordingly are supported.

"F_CHECK_SeqNr" is irrelevant in PROFIsafe V2 MODE.

"F_SIL" parameter

This parameter defines the safety class of the fail-safe DP standard slave/IO standard device/PA field device. The parameter is device-dependent. The "F_SIL" parameter can be set between "No SIL" and "SIL 3" depending on the GSD/GSDML file.

"F_CRC_Length" parameter

A cyclic redundancy check with a length of 2 bytes, 3 bytes or 4 bytes is required, depending on the length of the F-user data (process data) and the PROFIsafe mode. This parameter provides information to the F-CPU on the size of the CRC2 key in the safety message frame.

In PROFIsafe V1 MODE:

S7 F Systems only supports a user data length up to and including 12 bytes and "2-byte CRC". The fail-safe DP standard slave/PA field device must behave accordingly.

In PROFIsafe V2 MODE:

S7 F Systems supports the following user data length:

- With F_CRC_Seed = 0: Up to and including 12 bytes and "3-byte CRC".
- With F_CRC_Seed = 1 (PROFIsafe V2.6.1 XP): Up to and including 13 bytes and "4-byte CRC".

The fail-safe DP standard slave/IO standard device/PA field device must behave accordingly.

"F_CRC_Seed" parameter

In principle, the parameter specifies which value is to be taken as the start value ("seed value") for the CRC2 calculation and which values are included in the cyclic calculation.

- If F_CRC_Seed = 0, the CRC_FP is taken as start value and a counter (sequence number) is cyclically incremented.
  This is the previous behavior, i.e. prior to PROFIsafe V2.6.1.
- If F_CRC_Seed = 1, a 1 is taken as the start value and a monitoring number based on a 32-bit CRC value is added via F-parameter and code name (source/destination address).
  This is the behavior for PROFIsafe V2.6.1 XP.

The "F_CRC_Seed" parameter influences the "F_CRC_Length" parameter.

You can find additional information about these parameters in the PROFIsafe Specification V2.6.1.

Table 5-1 Combinations of the F-parameters "F_CRC_Seed" and "F_Passivation"

F_CRC_Seed	F_Passivation	
0	1	Not permitted
1	0/1	Allowed

The F-parameters "F_CRC_Seed" and "F_Passivation" influence the behavior of a fail-safe IO standard device. They enable configuration according to PROFIsafe version V2.4 or V2.6.1. The combination of the F-parameters cannot be adjusted. Instead, it is determined by selecting an appropriate safety-related (sub)module.

If these two parameters are not available, the safety-related data is transferred with the PROFIsafe Loop-back Extension Protocol (LP) V2.4, otherwise with the PROFIsafe Expanded Protocol (XP) V2.6.1. The default setting for the parameter F_CRC_Seed = CRC-Seed32 and for the parameter F_Passivation = Device/Module.

"F_Passivation" parameter

The parameter is used for passivation:

- F_Passivation = 0: F-(sub)module passivation
- F_Passivation = 1: Channel-level passivation

You can find additional information about these parameters in the PROFIsafe Specification V2.6.1.

"F_Block_ID" parameter

The F_Block_ID parameter has the value 1 if the F_iPar_CRC parameter exists, otherwise it has the value 0.

The value 1 of the F_Block_ID parameter indicates that the data record for the value of F_iPar_CRC has been extended by 4 bytes. You must not change the parameter.

"F_Par_Version" parameter

This parameter identifies the PROFIsafe operating mode. You can identify the operating modes supported by the device from the value range offered.

For fail-safe IO standard devices, this parameter is set to "1" (PROFIsafe V2 MODE) and cannot be changed.

For fail-safe DP standard slaves/PA field devices, you can set this parameter to the following:

- Set "F_Par_Version" to "1" (PROFIsafe V2 MODE) for a homogenous PROFIBUS DP network, if the device and the F-CPU support this. Otherwise, set it to "0" (PROFIsafe V1 MODE).
- For a network that consists of PROFIBUS DP and PROFINET IO subnets, "F_Par_Version" must be set to "1" (PROFIsafe V2 MODE).

Note

The following F-CPUs support V2 MODE:

- As of CPU 410-5H (article no. 6ES7410-5HX08-0AB0)
- As of CPU 410E (article no. 6ES7410-5HM08-0AB0)
- As of CPU 410SIS (article no. 6ES7410-5FM08-0AB0)
- As of CPU 412-5H PN/DP (article no. 6ES7412-5HK06-0AB0)
- As of CPU 414-5H PN/DP (article no. 6ES7414-5HM06-0AB0)
- As of CPU 416-5H PN/DP (article no. 6ES7 416-5HS06-0AB0)
- As of CPU 417-5H PN/DP (article no. 6ES7417-5HT06-0AB0)

If you set "F_Par_Version" to "1" for F-CPUs that do not support PROFIsafe V2 MODE, this will result in a communication error during safety-related communication with the device. One of the following diagnostics events is then entered in the diagnostics buffer of the F-CPU:

- "F-I/O passivated": Check value error (CRC)/Sequence number error ...
- "F-I/O passivated": F-Monitoring time exceeded at the safety message frame detected in the F-CPU ...

⚠ **WARNING**

Devices and "F_Par_Version" parameter for a mixed configuration

For a network that consists of PROFIBUS DP and PROFINET IO subnets, "F_Par_Version" must be set to "1" (PROFIsafe V2 MODE).

Devices that do not support PROFIsafe V2 MODE must not be used on a PROFINET IO network only or with mixed configurations of PROFIBUS DP and PROFINET IO.

FSW-009

"F_Source_Add" and "F_Dest_Add" parameters

The PROFIsafe addresses ("F_Source_Add" and "F_Dest_Add" parameters) uniquely identify the source and destination.

The "F_Source_Add" and "F_Dest_Add" parameters for fail-safe DP standard slaves/IO standard devices/PA field devices correspond to the "F_source_address" and "F_destination_address" parameters of other F-I/O. Exception: The value range is specified by the GSD/GSDML file and is not limited to 1 to 1022 for the PROFIsafe destination address.

Therefore, the information about PROFIsafe address assignment provided in section "General information on configuring the F-I/O (Page 51)" is generally applicable to fail-safe DP standard slaves/IO standard devices.

"F_WD_Time" parameter

This parameter defines the F-monitoring time in the fail-safe DP standard slave/IO standard device/PA field device.

A valid current safety message frame must come from the F-CPU within the monitoring time period. This ensures that failures and faults are detected and appropriate reactions are triggered to maintain the fail-safe system in a safe state or bring it to a safe state.

On the one hand, you should set the monitoring time so high that message frame delays due to communication are tolerated. On the other hand, it should be low enough for the fault reaction function to be quick enough in case of a fault (interruption of the communication connection, for example). (See "Safety Engineering in SIMATIC S7" system manual).

The "F_WD_Time" parameter can be set in 1 ms increments. The value range of the "F_WD_Time" parameter is specified by the GSD/GSDML file.

You can find additional information on the F-monitoring time in the section "Run times, F-Monitoring times, and response times (Page 482)".

"F_iPar_CRC" parameter

CRC via individual device parameters (i-parameter).

The individual device parameters (i-parameters) of a fail-safe DP standard slave/IO standard device/PA field device are configured using the device manufacturer's own parameterization tool.

Enter the CRC calculated by the parameterization tool of the device manufacturer (CPD Tool) for protection of the i-parameters. S7 F Systems takes the value into account when calculating the F-parameter CRC (CRC1).

FB24 serves as an iPar server for fail-safe DP standard slaves / IO standard devices / PA field devices with iPar functionality.

You can find additional information in theIndustry Online Support; entry ID 45841087 (http://support.automation.siemens.com/WW/view/en/45841087).

See also

Safety engineering in SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/12490443)

5.6 Configuring fail-safe PA field devices

Fail-safe PA field devices are configured in the same way as fail-safe DP standard slaves.

When configuring PA field devices, follow the procedure described in the chapter entitled "Configuring fail-safe DP standard slaves/IO standard devices (Page 61)".

5.7 Configuring redundant F-I/O

Introduction

To increase availability of your automation system and, thus, to prevent process failures due to faults in the fail-safe system, you can optionally equip S7 F/FH Systems fail-safe systems as fault-tolerant systems (S7 FH Systems). This increased availability can be achieved by component redundancy (F-CPU, communication connection and F-I/O).

For S7 F Systems, availability can be increased without fault-tolerant configuration.

- You can use S7-300 fail-safe signal modules (F-SMs) redundantly in one ET 200M or in several ET 200Ms.
- Fail-safe I/O modules of the ET 200SP HA can also be used redundantly.

Procedure for fail-safe I/O modules of the ET 200SP HA

Note

You must observe the following for redundantly configured F-I/O modules:

- Both F-I/O modules have the same type, product status and firmware.
- The two input/output modules of the same type must be placed directly next to each other on a terminal block for IO redundancy of the ET 200SP HA.
  The left F-module must be inserted in a slot with even slot number so that the "Redundancy" tab is displayed in the properties dialog of the two modules. Both of the F-modules can thus be used.
  The F-module with the even slot number is then the master module. The F-module of the same type placed to the right of it is always the slave module.
  This assignment of the synchronization role cannot be changed.

For example, to configure two fail-safe I/O modules (F-modules) of the ET 200SP HA redundantly, proceed as follows:

1. Configure the two F-modules of the ET 200SP HA in HW Config.
2. Open the properties dialog at one of the two redundant F-modules.
   Select the option "2 modules" in the "Redundancy" selection field.
   The "Master" setting is then automatically displayed in the "Synchronization role" selection field for the F-module with the even slot number placed on the left. If the F-Module is placed on the right, "Slave" is displayed.
   The "Module overview" table shows the address properties of the two redundant F-modules in this case.
3. Check the uniqueness of the "F_Destination_Address" in the properties of the F-module configured as "Slave".

4. Set additional parameters, if necessary.
   Changes can only be made on the master module for redundant F-Modules, except for the "F_destination_address". These changes are automatically adopted by the slave module.
5. For redundant F-modules, the F-channel driver, e.g. F_CH_DI, can perform a discrepancy analysis to increase availability. To do this, you must set the "Discrepancy time (ms)" parameter in the "Redundancy" tab. If you set the discrepancy time to "0", the discrepancy analysis is deactivated.
   You can find additional information in the online help for the "Redundancy" tab.

Procedure for fail-safe signal modules of the S7-300 (in ET 200M)

Note

In the case of redundantly configured F-SMs, you must ensure the following:

- Both F-SMs have the same type, product status and firmware.
- For both F-SMs of an S7-300, the "Safety mode" is activated in the "Parameters" tab of the object properties dialog.

For example, to configure two fail-safe S7-300 signal modules redundantly when used in the ET 200M, proceed as follows:

1. Configure the two F-SMs in the ET 200M(s) in HW Config.
2. Configure the first F-SM:
   Activate the "Safety mode" operating mode on the "Parameters" tab
3. Configure the second F-SM:
   Activate the "Safety mode" operating mode on the "Parameters" tab
4. For the second F-SM, set the "2 modules" operating mode on the "Redundancy" tab.
5. Select the first F-SM for the F-SM in the "Find redundant module" dialog.
6. Set additional parameters, if necessary. The settings are applied automatically for the first F-SM. As soon as two F-SMs are redundant, changes in the parameter assignment for one of the F-SMs are applied automatically for the other F-SM.
7. For redundant fail-safe digital input modules, the F-channel driver F_CH_DI can perform a discrepancy analysis for increased availability. You must set the "Discrepancy time" parameter for this. If you set discrepancy time "0", the discrepancy analysis is deactivated. You can find additional information in the online help for the "Redundancy" tab.
8. For redundant fail-safe analog input modules, the F-channel driver F_CH_AI can perform a discrepancy analysis for increased availability. You must activate the "DISC_ON" parameter for this. This setting must be made in the CFC. You can find additional information in the online help for the "Redundancy" tab.

See also

F_CH_DI: F-channel driver for digital inputs of F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices) (Page 358)

F_CH_AI: F-channel driver for analog inputs of F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices) (Page 366)

5.8 System modifications during operation

Introduction

Some systems for process control must not be switched off during operation. Reasons for this are, for example, the complex nature of the automation systems or the excessive costs of a restart. Sometimes, however, changes or extensions to these systems are required for process control. This allows you to configure in RUN mode (CiR for short). The program sequence is then stopped for a maximum of 2500 ms. During this time, the process outputs retain their current values. This has no effect on the actual process, especially in process control systems.

Plant modification during operation via CiR is based on precautions in the master system of the output configuration for subsequent hardware expansion of your automation system. You define suitable CiR elements, which you can later replace step-by-step with real elements in the RUN operating state. You can download such a modified configuration into the F-CPU while the process is running.

Before you perform the procedures described below, read the CiR instructions in the "Modifying the System during Operation via CiR (https://support.industry.siemens.com/cs/en/en/view/45531308)" manual.

Calculating the F-monitoring times

Consider the CiR synchronization time when calculating the minimum F-monitoring times. Refer to section "Run times, F-Monitoring times, and response times (Page 482)".

Reducing the F-monitoring times

If the calculated values are not acceptable for the process, you can re-calculate the F-monitoring time by reducing the CiR synchronization time. You have the following options:

- Reduce the number of input and output bytes of the master system.
- Reduce the number of guaranteed slaves of the master systems you intend to change.
- Reduce the number of master systems you intend to change in a CiR.

Extending the maximum cycle time via CiR

If you use CiR, the maximum cycle time is extended by the *lesser* of the two following values:

- CiR synchronization time of the F-CPU
  The CiR synchronization time of the F-CPU is the sum of the CiR synchronization times of all DP master systems that are to be changed simultaneously. The CiR synchronization time of a DP master system is displayed in HW Config in the properties dialog of the corresponding CiR object.
- High limit of the CiR synchronization time
  The default value of this high limit is 1 second. You can reduce or increase it by calling the SFC 104 "CiR" according to your requirements.

You can find information on determining the maximum cycle time in the manual for the F-CPU you are using.

Limiting the CiR synchronization time:

The F-CPU compares the concretely calculated CiR synchronization time with the current high limit value for the CiR synchronization time. If the calculated value is lower than the current high limit, CiR is activated. The default value for the high limit of the CiR synchronization time in the F-CPU is 1 second. The SFC 104 allows you to change the value. This allows you to increase or decrease the high limit within the range 200 ms to 2500 ms. You can find a detailed description of the SFC 104 in the "System software for S7 300/400 system and standard functions (http://support.automation.siemens.com/WW/view/en/1214574)" manual.

5.8.1 Configuring F-I/O with CiR

Introduction

CiR allows you to add new fail-safe I/O to your system or delete existing fail-safe I/O from your system. The following two sections explain the procedure.

Adding fail-safe I/O with CiR

Add fail-safe I/O to your system as follows:

1. Configure the new F-I/O in HW Config. Follow the procedure as described in the "Modifying the System during Operation via CIR (https://support.industry.siemens.com/cs/en/en/view/45531308)" manual. Handle the fail-safe I/O the same as standard I/O.

   Note

   After adding F-I/O modules in HW Config, the message "Caution, This change requires a complete download of the configuration in the stop state of the AS". This message can be ignored when adding/removing F-I/O modules with CiR/H-CiR. A complete download in the stop state is only required when changing the configuration of F-I/O modules that have already been downloaded.

2. Extend your S7 program and compile it with the "Changes" scope and activated "Generate module drivers" option.
3. Download your safety program.

4. When safety mode is activated, you are prompted whether you want to disable safety mode. Confirm this prompt. Safety mode is deactivated and the download operation is carried out.

   Note

   A user acknowledgment at the ACK_REI input is required to activate the fail-safe I/O.

5. After completion of the download operation, you are prompted whether you want to activate safety mode. Confirm this prompt.
   Safety mode is activated.

   Note

   Parameter reassignment of fail-safe I/O is not supported. Additional information can be found in the "Fault-Tolerant Systems S7-400H (http://support.automation.siemens.com/WW/view/en/82478488)" system manual.

Deleting fail-safe I/O with CiR

Delete fail-safe I/O from your system as follows:

1. Delete the F-I/O s in HW Config. Follow the procedure as described in the "Modifying the System during Operation via CiR (https://support.industry.siemens.com/cs/en/en/view/45531308)" manual. Handle the fail-safe I/O the same as standard I/O.

   Note

   After deleting F-I/O modules in HW Config, the message "Caution, This change requires a complete download of the configuration in the stop state of the AS". This message can be ignored when adding/removing F-I/O modules with CiR/H-CiR. A complete download in the stop state is only required when changing the configuration of F-I/O modules that have already been downloaded.

2. Change your S7 program and compile it with the "Changes" scope and activated "Generate module drivers" option.
3. Download your safety program.
4. When safety mode is activated, you are prompted whether you want to disable safety mode. Confirm this prompt. Safety mode is deactivated and the download operation is carried out.
5. Download your configuration using CiR.
6. After completion of the download operation, you are prompted whether you want to activate safety mode.
   Confirm this prompt. Safety mode is activated.

See also

Deactivating safety mode (Page 211)

Activating safety mode (Page 212)

5.8.2 Configuration in RUN im H-System (H-CiR)

H-CiR allows you to add new fail-safe I/O to your fault-tolerant system or delete existing fail-safe I/O from your system.

The procedure is similar to that described in section "Configuring F-I/O with CiR (Page 71)". Follow the instructions in the manual "Fault-Tolerant Systems S7-400H (http://support.automation.siemens.com/WW/view/en/82478488)".

Note

Parameter reassignment of fail-safe I/O is not supported.

Access Protection 6

6.1 Overview of access protection

Purpose and mode of operation

Access protection protects S7 F/FH Systems from unauthorized access, such as undesirable downloads to the F-CPU from the engineering system. In addition to the password for the F-CPU, you need an additional password for the safety program for S7 F/FH Systems.

The table below provides information about the password for the F-CPU and the password for the safety program.

Password for F-CPU	
Assignment/modification of the password	In HW Config during configuration of the F-CPU in the "Protection" tab of the "Properties" dialog box
Password request when	• Downloading the entire S7-program from the CFC Editor or SIMATIC Manager • Downloading safety program changes from the CFC Editor • Performing a memory reset from the CFC Editor or SIMATIC Manager • Changing non-interconnected inputs in CFC test mode
Password validity	Access permission is valid without restriction until it is explicitly canceled using the corresponding function of SIMATIC Manager (**PLC > Access Rights > Cancel** menu command) or you close the last STEP 7 application. Access permission can become invalid if the hardware configuration of the CPU is changed and downloaded.

Password for safety program	
Assignment/modification of the password	In SIMATIC Manager, **Options > Edit Safety Program** menu command The password of the safety program is required if at least one CFC with built-in F-blocks is available: • For the safety program of a configured CPU • To do this, select the program folder of a CPU, e.g. "S7 Program" and then the menu command **Options > Edit Safety Program**. • For F-libraries or projects without a configured CPU To do this, select the corresponding directory of the CFCs with the built-in F-blocks, e.g. within the F-library, and then the menu command **Options > Edit Safety Program**. In these cases, it is possible to assign and change the password.
Password request when	• Compiling changes to the safety program • Downloading changes to the safety program • Disabling and enabling safety mode • Changing non-interconnected inputs in CFC test mode • Saving the safety program as a reference • Changing the shutdown behavior in the "Safety Program" dialog • Adding F-I/Os for which safety mode has been activated or which support safety mode. • Opening the Properties dialog for F-I/O in HW Config. • Making changes in the PROFIsafe tab in HW Config. • Making changes in the "F-Configuration" tab for a fail-safe i-Slave. In addition, as of PCS 7 V7.1: • Opening an F-Chart • With an open F-Chart – Editing object properties of an F-block – Assigning parameters to an input/output on an F block – Instantiating an F-block – Inserting an F block or CFC chart • With F-Runtime groups – Opening a CFC – Opening an F-Runtime group in the runtime view – Moving an F-Runtime group in the runtime view – Modifying the properties of an F-Runtime group As of PCS 7 V8.2 (CFC 8.2), the following applies: • The password prompt is omitted when the CFC chart with fail-safe component is opened. • The password prompt occurs only in the case of safety-related changes, i.e. when the signature of the safety program changes. For this reason, changes can now be made in the standard program of a CFC chart with fail-safe components without a password prompt. • The password prompt occurs independent of whether the user creates or changes an F-block explicitly or this happens implicitly, e.g. by a copy operation.

Password for safety program	
Password validity	The access permission lasts for one hour after correct password entry, during which time it is reset to another hour after each action requiring a password, or until access permission is explicitly revoked in SIMATIC Manager (**Options > Edit Safety Program** menu command, then click the **Password** button followed by the **Revoke** button).

6.2 Setting up / changing access permission for the F-CPU

Procedure

1. Select the F-CPU or its S7 program in SIMATIC Manager.
2. Select the **PLC > Access Rights > Setup** menu command. On the "Protection" tab of the displayed dialog, enter the password that was assigned during parameter assignment of the F-CPU.

Access permission is always valid until you revoke it (**PLC > Access Rights > Cancel**) or until you end the last STEP 7 application.

⚠ WARNING

Limiting accessing using the engineering system

If you have not activated access protection to limit access to the engineering system to persons authorized to modify safety programs, you must use the following organizational measures in the engineering system to ensure the effectiveness of the password protection:

- Only authorized persons may have access to the password.
- Authorized persons must explicitly revoke the access permission for the F-CPU before leaving the engineering system. If you do not implement this measure consistently, you must additionally use a screen saver whose password can only be accessed by authorized persons.

In safety mode, access permission by means of the F-CPU password must not be active when changes are made to the standard user program, because the safety program can then also be changed. To rule out this possibility, you must configure protection level "1".

If only one person is authorized to change the standard user program and the safety program, protection level "2" or "3" should be configured to ensure that other persons have only limited access or no access to the standard user program and safety program.

If safety mode is active after access permission is revoked, check to determine whether

- the collective signature of the safety program online
  and
- the collective signature of the accepted safety program are identical.

If not, download the correct safety program to the F-CPU again.

FSW-010

Note

Automatic downloading of safety programs is not supported in multiprojects. The passwords must be entered at the time of downloading to the respective F-CPU.

Transferring the safety program to multiple F-CPUs

⚠ WARNING

Transferring the safety program to multiple F-CPUs

If multiple F-CPUs can be reached from an ES via a network (e.g. MPI), you must take the following additional measures to ensure that the safety program is downloaded to the correct F-CPU.

Use F-CPU-specific passwords, e.g. a password for the F-CPUs with appended MPI address "FCPUPW_8". The password has a maximum of 8 characters, including at least one special character. In STEP 7 V5.5.4 HF9 and higher, the password must contain 8 characters for new projects.

Note the following:

- Before a safety program for which access permission by means of an F-CPU password does not yet exist is downloaded to an F-CPU, any existing access permission for another F-CPU must first be canceled.

FSW-011

Changing the password

A password can only be changed by reconfiguring.

In the S7 F System, you must switch the F-CPU to STOP for this.

In the S7 FH-System, a password change (configuration change) is possible without a process interruption (in RUN).

⚠ WARNING

Password protection

After a cold restart, the current password is deleted from the RAM load memory and the old password from the flash EPROM memory card becomes valid again. To prevent too many people form knowing the old password on the flash EPROM memory card, you should take organizational measures.

FSW-012

6.3 Setting up/changing an access permission for the safety program

Setting up/changing an access permission for the safety program

Criteria for a secure password

To ensure a secure password, it must meet the following criteria when created for the first time or changed:

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

These criteria apply when the "Increased password security" option is activated in the "Create password for safety program" dialog.

Requirement

To set up an access permission for the safety program, a safety program (F-chart) must exist.

Procedure

To set up or change the password for the safety program, follow these steps:

1. Select the F-CPU or its S7 program in SIMATIC Manager.
2. For an F-library or a project without a configured CPU, select the corresponding directory of the CFCs with the built-in F-blocks.

3. Select the menu command **Options > Edit safety program**.
4. Click the "Password" button in the displayed "Safety Program" dialog. Perform the step required for your situation:
   – During the initial setup of a new password, select the password in conformance with the criteria described below and enter it in the "New password" and "Reenter password" fields. In this case, the "Old password" field is deactivated.
   By selecting the "Increased password security" check box, you can use a more secure password that conforms to the description "Criteria for a secure password" above. Refer to the information on increased password security in section ""Password for Safety Program Creation" dialog (Page 197)".
   – To change a password, you must enter the old password in the "Old password" field. Then, choose the new password and enter it in the "New password" and "Reenter password" fields.
   When the "Increased password security" check box is selected, the description "Criteria for a secure password" above applies to the password selection.
   – You can use the "Logout" button in the "Access permission" area to revoke the 1-hour access permission period since the last time the password was entered. Any user who then wants to perform an action that requires entry of a password must now enter the password for the safety program again.

⚠ WARNING

Limiting accessing using the engineering system

If you have not activated access protection to limit access to the engineering system to persons authorized to modify safety programs, you must use the following organizational measures in the engineering system to ensure the effectiveness of the password protection:

- Only authorized persons may have access to the password.
- Authorized persons must explicitly revoke the access permission for the safety program before leaving the engineering system. If you do not implement this measure consistently, you must additionally use a screen saver whose password can only be accessed by authorized persons.

FSW-013

Note

The access permission relates to the safety program itself and not the persons that work on the ES. This must be taken into consideration, particularly in relation to multi-user engineering projects.

Note

Automatic editing and compiling of safety programs is not supported.

The password must be valid during the respective action.

Assigning a new password for the safety program

If no password has yet been set for the safety program, but a password is required for the desired configuration, you will be prompted to enter the password. The password entry may be needed, for example, when inserting an F-block in the CFC or when inserting F-modules in HW Config.

You can find additional information on the password prompt in section "Overview of access protection (Page 75)" in the "Password for safety program" table.

⚠ WARNING

Passwords must be unique

To improve access protection, use different passwords for the F-CPU and the safety program.

The passwords of various safety programs must also be different.

FSW-014

Changing the password for the safety program

You change the password by entering the old password and then entering the new password twice.

Canceling access permission for the safety program

You can revoke the access permission at any time using the password for the safety program. Follow the procedure below:

1. Select the F-CPU or its S7 program in SIMATIC Manager.
2. Select the menu command **Options > Edit safety program**.
3. Click the "Password" button in the displayed dialog.
4. In the "Create password for safety program" dialog, click the "Logout" button in the "Access permission" area.

Programming

7

7.1 Overview of programming

7.1.1 Overview of the safety program

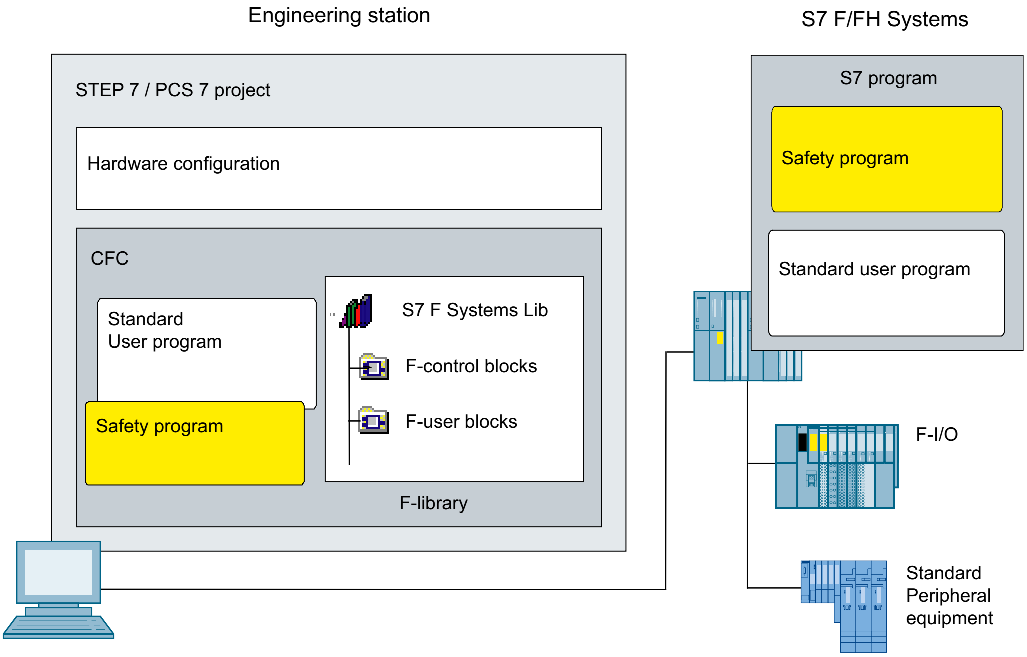
Introduction

A safety program consists of F-blocks that you select from the F-library and interconnect in the "CFC Editor" and F-blocks that are automatically added when the safety program is generated.

When the safety program is generated, fault-control measures are automatically added to the safety program you created and additional safety-related checks are performed.

Schematic structure of a project with standard user program and safety program

The following figure shows the schematic structure of an S7 program on the engineering station (ES) and in the F-CPU:



The S7 program typically consists of a standard user program in which you program the parts of the program not required for the safety function and a safety program for the safety function.

7.1.2 Structure of the safety program

Representation of the program structure

The following figure shows the schematic structure of a safety program for S7 F Systems. A safety program consists of CFC charts with F-blocks that are assigned to F-runtime groups.

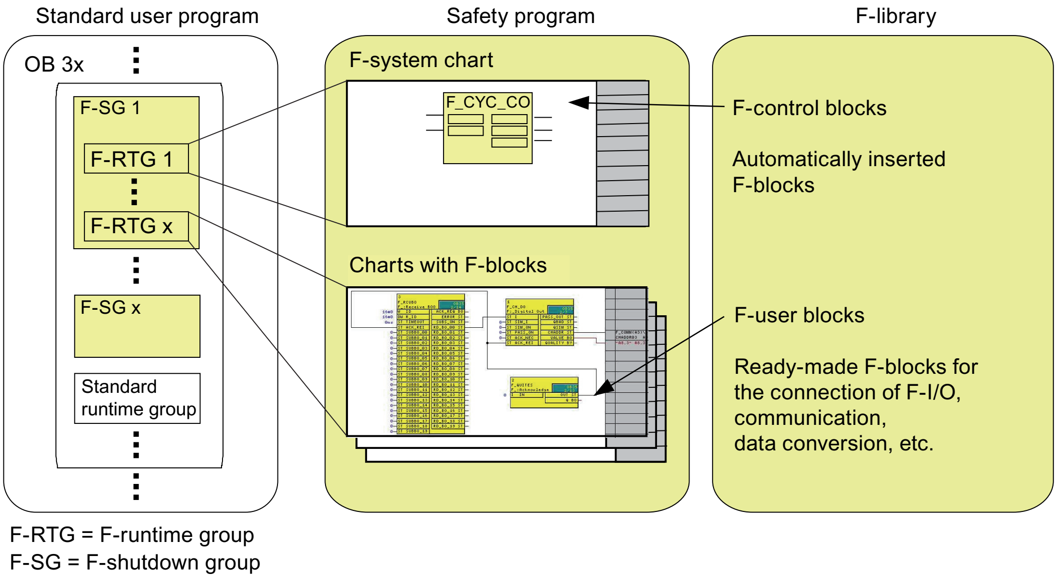


Figure 7-1 Components of the safety program in S7 F Systems

Explanation of the program structure

The safety program contains F-runtime groups and charts assigned to them. The charts contain F-blocks including their parameter assignment and interconnection.

F-runtime groups are combined into F-shutdown groups.

The F-shutdown groups are inserted at the start of a cyclic interrupt OB (OB 30 to OB 38).

The cyclic interrupt OB can also contain standard runtime groups.

Support for creating the program structure

In CFC V8.2 and higher, there is the so-called chart-based runtime group management in which the blocks of a CFC chart are automatically managed in a chart-oriented manner in their own runtime groups. The "Chart-based insertion" option must be activated in the properties of the chart folder or the CFC chart for this.

If a CFC with F-blocks is integrated in CFC in chart-based runtime group management, a runtime group for blocks is not only created automatically in the standard program. A runtime group is then also created for the contained F-blocks, the safety program.

- In this case, it is no longer necessary to manually move the F-blocks to their own runtime group.
- The name of the runtime group for the F-blocks contains the name of the CFC chart with the addition of "_F".

You will find further information on this in the Process Control System PCS 7, CFC for SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/90683154) manual, "Special features of F-blocks in CFC charts".

F-runtime groups

You are not permitted to insert F-blocks directly in tasks (OBs) when programming the safety program.

A runtime group becomes an F-runtime group only when it is called in its F-blocks. If no F-blocks are contained in the runtime group, it is regarded as a standard runtime group.

Your safety program consists of multiple F-runtime groups.

In CFC V8.2 and higher, the creation of F-runtime groups by CFC is supported. Note the paragraph "Support in creating the program structure" regarding this.

F-shutdown groups

An F-shutdown group is a self-contained unit of your safety program. An F-shutdown group contains the user logic which is simultaneously executed or shut down.

The F-shutdown group contains one or more F-runtime groups that are assigned to a common task. You can select whether a fault during execution of the safety program is to trigger a full shutdown of the entire safety program or a partial shutdown, that is, shutdown only of the F-runtime group in which the fault occurred.

F-blocks can exchange data between F-shutdown groups only via special F-blocks. All F-channel drivers belonging to an F-I/O must be located in the same F-shutdown group.

See also

F-STOP (Page 99)

Creating the Safety Program (Page 86)

7.2 Creating the Safety Program

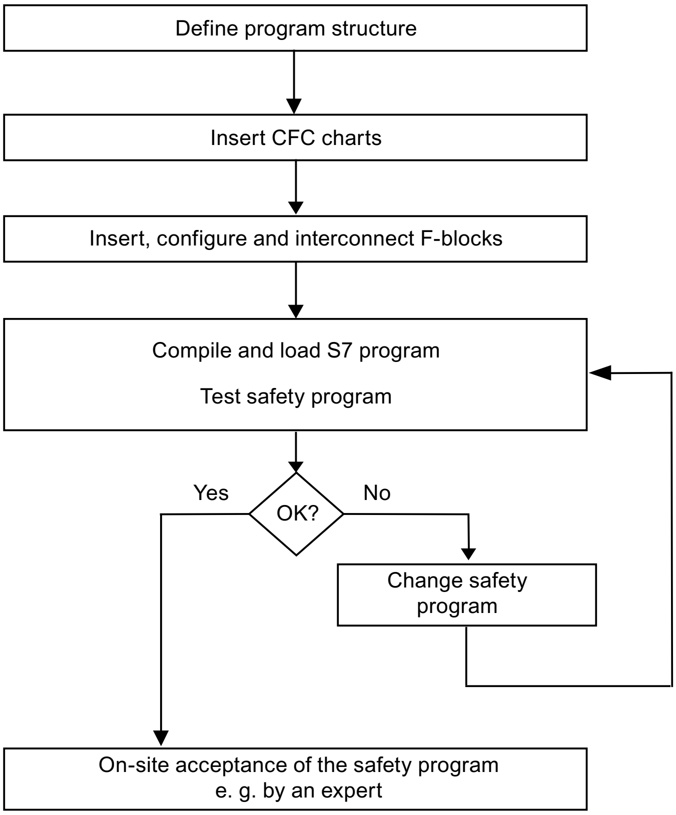
7.2.1 Basic procedure for creating the safety program

Requirements

- You must have created a project structure in SIMATIC Manager.
- You must already have configured the hardware components of your project - in particular, the F-CPU and the F-I/O - prior to programming the safety mode.
- You must have assigned your safety program to an F-capable central processing unit, such as a CPU 410-5H.

Basic procedure

Proceed as follows to create a safety program:


Define program structure
Insert CFC charts
Insert, configure and interconnect F-blocks
Compile and load S7 program
Test safety program
Yes
OK?
No
Change safety program
On-site acceptance of the safety program e. g. by an expert

7.2.2 Defining the program structure

Introduction

When designing an S7 program for S7 F/FH Systems, you must answer the following additional questions as compared to a standard program:

- Which components of the S7 program must be fail-safe?
- What response times do you want to achieve?
  Based on this, you must divide your S7 program into different OB 3x cyclic interrupts.

Note

You can improve performance by writing sections of the program that are not required for the safety functions in the standard user program.

When determining which elements to include in the standard user program and which to include in the safety program, keep in mind that the standard user program can be modified and downloaded to the F-CPU more easily. In general, changes in the standard user program do not require an acceptance test.

Rules for the program structure

You must keep the following rules in mind when designing a safety program for S7 F/FH Systems:

- You can only assign F-Shutdown groups with F-Blocks to the OB 3x (OB 30 to OB 38) cyclic interrupts.
- A chart can contain both F-Blocks and standard blocks. You cannot compile these charts as F-Block types.
- The F-I/O can only be accessed in the safety program via the F-Channel drivers.

7.2.3 Assigning parameters for the maximum F-cycle monitoring

The F-CPU monitors the F-cycle time for each cyclic interrupt OB 3x in which there are F-runtime groups. When compiling the S7 program for the first time, you are prompted to enter a value for the maximum cycle time "MAX_CYC" which may elapse between two calls of this OB. For information on setting the F-monitoring times, see section "Run times, F-Monitoring times, and response times (Page 482)".

If you have to change the maximum F-cycle time, configure the F-cycle time at MAX_CYC parameter of the F_CYC_CO-OB3x block in the @F_CycCo-OB3x chart.

⚠ WARNING

Default setting of the maximum MAX_CYC

The default setting for the maximum F-cycle time is 3000 milliseconds. Check whether this setting is suitable for your process. Change the defaults, if required.

FSW-015

Note

For changes to the F-cycle time in the RUN operating state, refer to section " Changing the time ratios or F-Monitoring times (Page 223) ".

7.2.4 Rules for programming

⚠ WARNING

Do not change values created during compilation

You must not change the automatic placement, interconnections and parameter assignment of F-blocks during compiling!

- In particular, you must not manipulate the structure components COMPLEM and PAR_ID of F-data types.
- You must not change the F-control blocks (except parameter MAX_CYC at F_CYC_CO) that are automatically inserted into the safety program (in F-system charts).
- In F-blocks, you may only interconnect or configure the parameters that are described in the online help or in the manual.

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

FSW-016

⚠ WARNING

Call interval of cyclic interrupt OB 3x is monitored for the maximum value

The call interval of the cyclic interrupt OB 3x is monitored for maximum value, i.e. it is monitored whether the call is performed often enough, but not too often.

Fail-safe times must therefore be implemented via F-blocks, e.g. F_TON, F_TOF, F_TP, and not via counters (OB calls).

FSW-017

7.2.5 Notes for working with CFC

⚠ WARNING

Compression changes the signature

The collective signature of your safety program may change if you compress a CFC program (menu command in the CFC Editor **Options > Settings > Compile/Download**).

Therefore, check the collective signature after compression.

Perform this before the acceptance.

FSW-018

F-blocks are identified by color in the CFC chart. They are colored yellow to draw your attention to the fact that this is a safety program.

CFCs and F-runtime groups with F-blocks are yellow and marked with an "**F**" to distinguish them from the charts and runtime groups of the standard user program.

7.2.6 Inserting CFC charts

Procedure

You insert individual CFCs as for standard user programs in the chart folder:

- In the SIMATIC Manager with the menu command **Insert > S7 Software > CFC**
- Directly in the CFC Editor with the menu command **Chart > New**

Note

To ensure that the newly inserted CFCs are installed immediately in the planned cyclic interrupt OB 3x, you must position the CFC installation pointer accordingly.

Nested charts

You must not connect chart outputs of a lower-level chart that are not internally connected to each other in the higher-level chart.

7.2.7 Inserting F-Runtime groups

Rules for F-runtime groups of the safety program

- To achieve F-cycles whose length are as equal as possible, we recommend the following procedure:
  If you mix F-and standard runtime groups in a cyclic interrupt OB, execute the F-runtime groups before the standard runtime groups, otherwise you will unnecessarily extend the run time of the F-shutdown group and thus influence the response time.
- An F-runtime group must retain the presetting for the reduction ratio and phase offset runtime properties as follows:
  - Reduction ratio = 1
  - Phase offset = 0

  You are not permitted to change these values.
- You are not permitted to move the automatically generated F-runtime groups. You are also not permitted to make any changes within this F-runtime group.

> ⚠ WARNING
>
> **Effect of optimizing the runtime sequence in the CFC**
>
> Optimizing the run sequence in CFC can lead to a change in the collective signature and a deterioration in the response times of the safety program.
>
> It is therefore not possible to optimize the run sequence.
>
> FSW-019

Procedure

As for standard user programs, you insert F-runtime groups in the runtime editor of the CFC Editor.

7.2.8 F-Shutdown groups

Rules for F-Shutdown groups of the safety program

- You must not directly interconnect F-blocks that belong to different F-shutdown groups. For more information, refer to section "Programming data exchange between F-Shutdown groups in an F-CPU (Page 107)".
- All F-channel drivers belonging to an F-I/O must be located in the same F-shutdown group.

Specifying F-shutdown groups

As soon as you position F-blocks in the CFC editor for the first time, all F-runtime groups in an OB form an F-shutdown group, 3x each.

Splitting/combining F-shutdown groups by manually positioning F_PSG_M

Adding or deleting one or more F_PSG_M blocks to/from your project will change the order of your F-shutdown groups. If you make a change to the layout of your F-shutdown groups, you must ensure that the F-module drivers and all associated F-channel drivers are located in the same F-shutdown group.

You have the option of dividing one F-shutdown group into two F-shutdown groups. To do this, place the block F_PSG_M in the runtime editor of the CFC editor, in the last F-runtime group which should belong to the first F-shutdown group. All subsequent F-runtime groups will then form the second F-shutdown group. The F_PSG_M block is not an F-block. You may nevertheless place it in F-runtime groups. For more information, refer to section "Determining the runtime sequence (Page 93)".

The number of F-shutdown groups in all tasks is limited to 110. The number of F-runtime groups in a task is unlimited.

You have the option to combine two F-shutdown groups. To do this, delete the F_PSG_M block between the F-shutdown groups in the runtime editor of the CFC editor. If you combine F-shutdown groups, which exchange data with one another via F-system blocks, to form a shared F-shutdown group, you must remove these F-system blocks and replace them with direct interconnections.

7.3 Inserting and interconnecting F-Blocks

7.3.1 Inserting F-Blocks

Procedure

Insert the F-blocks into your chart as usual in CFC.

Note

All F-blocks are displayed in yellow in the CFC Editor and in the SIMATIC manager. Only these blocks are part of your safety program. There are also standard blocks in the F-library in the F-User Blocks folder, for example, for converting F-data types into standard data types.

Rules for F blocks

- The blocks of the **F-Control Blocks** folder are inserted automatically when compiling the S7 program. You must not insert these blocks yourself.
- You may not place an instance of an F-block in multiple F-runtime groups. This can happen, for example, by copying and pasting an F-runtime group into another task.

Note

F-libraries in different versions

Several versions of the F-library may be present on your engineering system at the same time. However, a safety program may only contain F-blocks of one version.

⚠ **WARNING**

Entries for F-blocks in the symbol table must not be changed

You may not change or delete the names of the F-blocks in the "Symbol" column of the symbol table of your S7 program. This also applies to changes in the symbol table assigned to the F-library.

FSW-020

7.3.2 Parameter assignment and interconnection of F-Blocks

Procedure

Configure and interconnect the inputs and outputs of the F-blocks as usual in CFC.

Rules for parameter assignment and interconnection of F-blocks

- Only the parameters that are documented in the section "F-libraries (Page 245)" may be configured or connected.
- EN/ENO I/Os of the F-blocks and F-runtime groups must not be interconnected. EN must also not be configured with the value 0 (FALSE).
- The F-data types are implemented programmatically as structures in which only the first component **DATA is relevant for you**.
  If you do not observe this, the safety program / F-runtime group goes into F-STOP, i.e. an F-startup is required.

⚠ WARNING

Illegal changes to input parameters of F-blocks can cause a shutdown of the safety program and its outputs

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

- Offline using the CFC Editor
  or
- Online using CFC test mode when safety mode is disabled.

If you do not change F-data types online using CFC test mode when safety mode is enabled, this may cause the outputs involved to shut down or trigger an F-STOP.

FSW-021

Recommendation: Meaningful names for placed F-blocks

Assign a meaningful name to each placed F-block. You can freely choose the names.

7.3.3 Determining the runtime sequence

Correct run sequence of F-blocks

The relevant sequence is the sequence of the F-blocks within the F-shutdown group. It is irrelevant in how many F-runtime groups the F-shutdown group is subdivided.

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

1. Automatically positioned:
   – F-module drivers for fail-safe I/Os with inputs or with inputs and outputs
   – F-communication blocks and F-system blocks for receiving
   – F-block for data conversion
2. F-channel drivers for inputs
3. F-blocks for user logic

4. F-channel drivers for outputs
5. Automatically positioned:
   - F-block F_PLK
   - F-block F_PSG_M
   - F-module drivers for fail-safe I/Os with outputs or with inputs and outputs
   - F-communication blocks and F-system blocks for sending
   - F-block F_PLK_O
   - F-block F_DIAG

The run sequence of the F-blocks listed in 1 and 5 is automatically corrected when the S7 program is compiled. However, you must always pay attention to the careful placement of the F-channel drivers and F-blocks for user logic, and adhere to the sequence described above.

This is to ensure that all inputs are read first and the respective processing steps are initiated. Thereafter, the result of the processing steps is written to all outputs.

Setting the run sequence

The run sequence is defined in the CFC editor, in the same way as for a standard user program.

Note

Changing the run sequence also changes the collective signature.

7.4 Automatically inserted F-Blocks

F-control blocks

When compiling a CFC with F-blocks, the following F-control blocks are automatically inserted into the safety program:

- F_DIAG
- F_CYC_CO
- F_MNR_H
- F_PLK
- F_PLK_O
- F_PS_12
- F_PS_13
- F_PS_MIX
- F_PSG_M
- F_TEST
- F_TESTC
- F_TESTM

When compiling a CFC with F-blocks, the following blocks are automatically inserted into the standard user program:

- DB_INIT
- DB_RES
- F_SHUTDN
- RTGLOGIC
- F_VFSTP1
- F_VFSTP2
- F_MOVRWS *
- F_CHG_WS *

*) The insertion of the F_MOVRWS and F_CHG_WS blocks depends on your programmed user logic.

⚠ WARNING

Do not change automatically inserted F-Control blocks.

The automatically inserted F-control blocks are visible after compiling. You must not delete these F-blocks and must not make any changes to them, since this can lead to errors during the next compiling. Exceptions can be found in the description of the F-blocks in the appendix "F-libraries (Page 245)".

FSW-022

Note

When compiling the S7 program, additional blocks (DB_RES) and calls are automatically inserted at the beginning of the sequence in OB 100.

7.5 F-Startup and reprogramming restart/startup protection

F-startup

S7 F Systems does not distinguish between CPU cold start and CPU warm start. Exception: F-blocks F_CHG_BO, F_CHG_R, F_MOV_R, F_SWC_CB and F_SWC_CR. For more information, refer to sections "Blocks and F-Blocks for data conversion (Page 292)" and "Multiplex blocks (Page 441)". Both a cold restart and a warm restart of the CPU results in an F-startup.

Note

Startup type "Cold restart"

In PCS 7 and when blocks from PCS 7 libraries are used, the startup type "Cold restart" is not permitted.

After an F-startup, the safety program starts up automatically with the initial values.

An F-startup takes place:

- After a CPU STOP when you perform a warm restart or a cold restart of the F-CPU.
- After an F-STOP when you perform the following steps:
  - Set the value "1" at the "Restart" input for the restart.
  - After you accept the value, reset it back to the original value "0".

After a partial shutdown of the safety program, only the F-shutdown groups that were in F-STOP perform an F-startup.

F-shutdown groups that are not fault-free remain in F-STOP.

⚠ **WARNING**

Saved error information is lost following an F-startup.

After a STOP of the F-CPU, the F-system automatically reintegrates the F-I/O following an F-startup.

A data handling error or an internal fault can also trigger a safety program restart with the initial values of the F-blocks. If your process does not allow such a startup, you must program a restart/startup protection in the safety program: Process data outputs must be blocked until manually enabled. Enabling of the process data output must not occur until it is safe to do so and faults have been corrected.

FSW-023

One of the following actions is required after troubleshooting:

- User acknowledgment at the F-channel driver
- User acknowledgment at F-block F_RCVBO or F_RCVR, or F_RDS_BO

For F-blocks F_R_BO and F_R_R, which are used for data exchange between F-runtime groups, the reintegration of the receive data occurs automatically.

Restart/startup protection

If the process does not permit automatic startup of the safety program with initial values, you must program a reaction to the F-startup. The F-block F_START is available for signaling an F-startup of the safety program with initial values.

The COLDSTRT output parameter signals the occurrence of an F-startup.

Examples

You can use the following measures to react to a startup of the safety program with initial values:

- Programming of an **interlock** of the outputs after startup using the PASS_ON passivation inputs at the channel drivers for outputs. To do this, interconnect the COLDSTRT output of the F-block F_START with the S input of an SR-Flip-Flop (F_SR_FF) and the Q output of the F_SR_FF with PASS_ON of the F-channel driver for outputs. You can then enable the interlock manually:
  - Using a button that is queried via an F-I/O.
    or
  - By input at the ES/OS via the F-block F_QUITES. As of S7 F Systems V6.2 also via SWC_QOS (F_SWC_BO).
    You must interconnect the Q output of the F-channel driver belonging to the button or the OUT output of F_QUITES or F_SWC_BO with the R input of F_SR_FF.
- Programming of an **idle loop** so that the internal states of the safety program correspond to the process state again.
- Programming using multiplexers: The output of a multiplexer F_MUX2_R is controlled by the COLDSTRT output of the F-block F_START. As a result, a different program branch can be executed after a startup than in cyclic operation.

7.6 F-STOP

Introduction

If the safety program detects a safety-related fault, a fault reaction is triggered. If no fail-safe values can be output, the fault reaction that is then carried out is called an F-STOP.

Types of F-STOP

There are two types of F-STOP:

- **Full shutdown**
  All F-shutdown groups of the F-CPU are shut down. The shutdown is carried out in the following order:
  - Initially, the F-shutdown group in which the fault was detected is shut down.
  - All other F-shutdown groups are then shut down within a period of time equal to twice the F-monitoring time you assigned for the slowest OB.
- **Partial shutdown**
  Only the F-blocks of the F-shutdown group in which a fault was detected are shut down.

A shutdown of F-shutdown groups means:

- The outputs of the F-I/O controlled by the F-shutdown group are passivated.
- The F-channel drivers of the F-shutdown group set the outputs QBAD to "1" and QUALITY to "0".
- The safety-related communication of the F-shutdown group with other F-CPUs is interrupted.
- The data exchange of the F-shutdown group with other F-shutdown groups is interrupted.
- In the case of data exchange from the safety program to the standard user program, the last valid values are provided to the standard user program.
- The F_SHUTDN block generates a message you can display on an OS.
- Diagnostic events are entered in the diagnostics buffer of the F-CPU.

The standard user program of the F-CPU continues running even after an F-STOP.

In order to assign the F-STOP parameters, use the "Shutdown behavior" button in the "Safety Program" dialog. See also ""Shutdown Behavior" dialog box (Page 196)".

Faults that trigger an F-STOP

- Falsification of
  - Data
  - Program flow
  - Code
- CPU fault

Faults that always trigger a full shutdown

A full shutdown is triggered following an OB request error (e.g. due to an OB overload), regardless of the F-STOP parameter assignment.

Manual triggering of an F-STOP

You can manually trigger an F-STOP by creating a positive edge at the RQ_FULL input of the F-block "F_SHUTDN".

Sequence of an F-STOP in S7 FH Systems

Before a safety program on a redundant F-CPU goes to F-STOP, it performs the following steps:

- The fault occurs in the master:
  - The S7 FH-System performs a master/standby changeover.
  - The F-CPU that was previously the master then switches to TROUBLESHOOTING operating state.
    If a fault is not subsequently found, the F-CPU is reconnected. You can find additional information in the manual "Fault-tolerant System, S7-400H (http://support.automation.siemens.com/WW/view/en/82478488)".
    If a fault was found, the F-CPU that was previously the master switches to DEFECT operating state.
    In the case of redundant F-CPUs, faults on one side do not trigger a shutdown of the program execution.
- The fault occurs in both F-CPUs:
  - The safety program goes to F-STOP immediately.

Ending an F-STOP

Perform an F-startup as described in the section "F-Startup and reprogramming restart/startup protection (Page 97)".

See also

Initial run and startup characteristics (Page 225)

Group passivation (Page 120)

7.7 Creating F-Block types

7.7.1 Introduction

S7 F Systems allows you to generate an F-block type from the CFC of a safety program. You can reuse F-block types in other safety programs.

7.7.2 Rules for F-Block types

Rules for F block types

When creating a new F block type with F blocks, you follow the same basic procedure as for the standard user program. The same rules apply as for creating block types in CFC. In addition, you must also keep the following in mind:

- The new F block type can only contain F blocks from the F-Library, except for:
  - F-Channel driver
  - F blocks for F-Communication
  - F blocks F_CHG_BO, F_CHG_R, F_MOV_R or F_SWC_x
  - All F-Control blocks
    For more information, refer to the section "F-Control blocks S7 F Systems Library V1.3 SP3 (Page 456)".
  - All F-System blocks, except for F_START
    For more information, refer to the section "F-System blocks (Page 409)".
- The F blocks that are called in the new F block type and the F blocks of the entire safety program in which the F block type is used must originate from the same library version. F blocks from different versions of the F-Library are not permitted.
- You are not permitted to connect an output of the F block with two chart inputs/outputs.
- The runtime sequence within one F block type is not automatically corrected during compilation. The sequence determined during creation is retained.

  Note

  If the runtime sequence is different from the data flow, for example, due to feedback, compilation of the F block type is canceled with an error.

- The chart inputs/outputs of the new F block type can have both F-Data types and standard data types.

- You are not permitted to use names of F blocks in the F-Library as the names of F block types.
- For instances of F blocks that are called in an F block type, we recommend that you assign names as follows:
  - Numbers only, as specified in the CFC Editor
    or
    Alphanumeric names, but that must begin with "F_"
  - Upper-case letters only
  - No "_" at the end

⚠ WARNING

Outputs of F blocks always use the predefined initial values

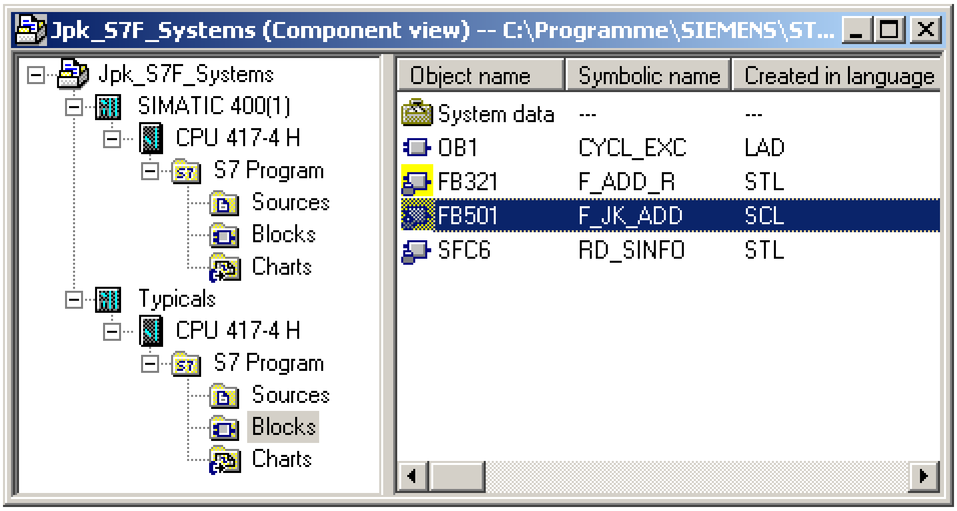
When creating F block types, you are not permitted to change any initial values at F block outputs. CFC allows this and shows you the change. However, S7 F Systems always uses the initial values described in the F block description under "Default".

FSW-024

7.7.3 Creating F-Block types with "Compile Chart as F-Block Type"

Procedure

1. Create the CFC chart in a separate S7 program that is assigned to an F-CPU. The S7 program can be located in the same project.



Jpk_S7F_Systems (Component view) -- C:\Programme\SIEMENS\ST...

- Jpk_S7F_Systems
  - SIMATIC 400(1)
    - CPU 417-4 H
      - S7 Program
        - Sources
        - Blocks
        - Charts
  - Typicals
    - CPU 417-4 H
      - S7 Program
        - Sources
        - Blocks
        - Charts

Object name	Symbolic name	Created in language
System data	---	---
OB1	CYCL_EXC	LAD
FB321	F_ADD_R	STL
FB501	F_JK_ADD	SCL
SFC6	RD_SINFO	STL

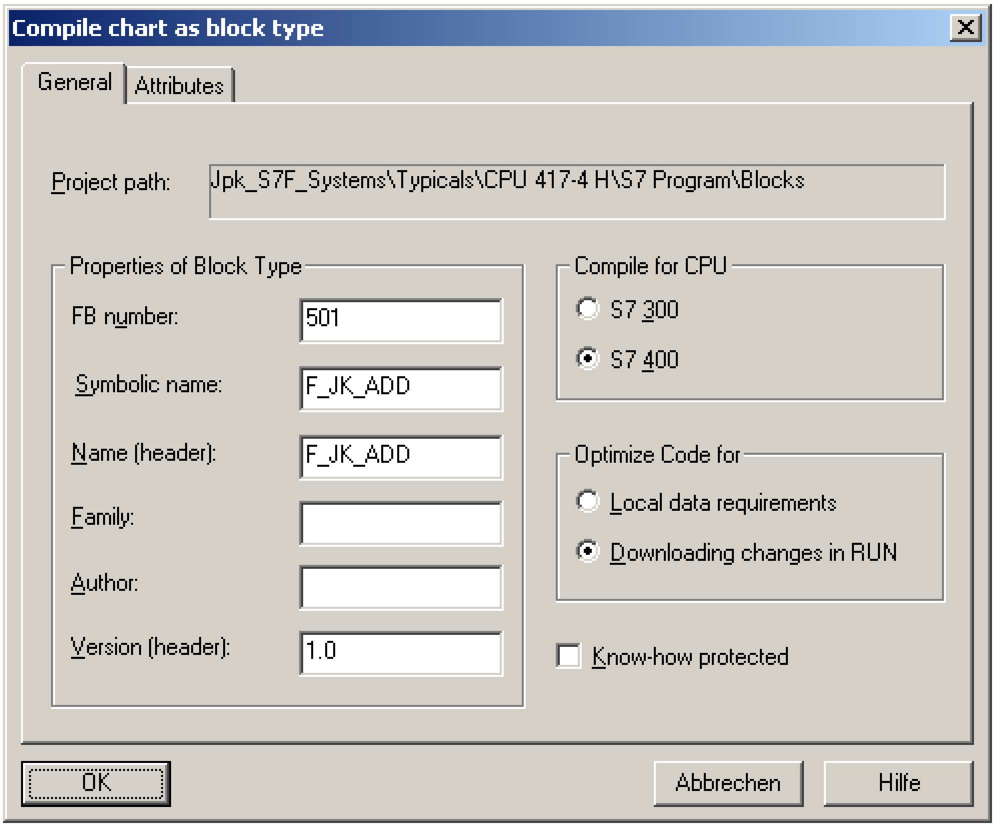
Note

Use a separate AS station to create an F-block type!

Always use a separate AS station that contains only the safety program of the F-block type to create an F-block type.

2. Open the desired chart.

3. Select the menu command **Chart > Compile > Chart as block type**. A dialog for entering the block properties is displayed.



Compile chart as block type

General | Attributes

Project path: Jpk_S7F_Systems\Typicals\CPU 417-4 H\S7 Program\Blocks

Properties of Block Type

FB number: 501

Symbolic name: F_JK_ADD

Name (header): F_JK_ADD

Family:

Author:

Version (header): 1.0

Compile for CPU

○ S7 300

● S7 400

Optimize Code for

○ Local data requirements

● Downloading changes in RUN

□ Know-how protected

4. Open the properties of the new F-block type.
   Ensure that the names under "Symbolic name" and "Name (Header)" are identical.
   When the FB number is assigned, it must be ensured that the selected number does not fall within a number range of the libraries used in the project. This is necessary to prevent conflicts.
5. Activate the "Compile for CPU - S7 400" and "Optimize code for - Download changes in RUN" options and confirm with OK.
   The know-how protection is always activated independent of the setting of the option.
   Result: A new F-block is generated that you can use in a safety program.
6. Insert the new F-block type together with the F-blocks that it calls in a safety program and test it there.

Note

Attributes

Attributes whose name begins with "F_" are managed by S7 F Systems. Assign other names for your own attributes to prevent them from being deleted or overwritten during compiling.

7.7.4 Modifying F-Block types

Changing F-block types

Like all other block types, you must update changed F-block types in the CFC Editor. For this, open the "Block types" dialog with the menu command **Options > Blocks types** and confirm with the "New Version" button.

Changes to F-block types already used can result in you having to compile and download the complete S7 program afterwards.

If you want to use a new version of the F-library, you must compile the F-block types with this new version of the F-library. For more information, refer to section "Updating custom F-block types (Page 45)".

See also

Downloading changes (Page 220)

System Acceptance Test (Page 229)

7.7.5 Integrating F-parameters of custom F-block types in the printout of the safety program

Requirement

You have already created an F-block type and opened it as a CFC chart.

Procedure

1. Select the chart I/O that you want to include in the safety-related printout.
2. Select "Object properties" in the shortcut menu to open the object properties of the tag. Make sure that you open the object properties of the structure and not the subordinate elements.
3. Open the "Attributes" tab and enter the "F_PrintTypParam" attribute in an empty row.
   Set the value of the attribute to "TRUE".
4. Repeat this process for all chart I/Os you want to include in the safety-related printout.
5. Select the menu command **Chart > Compile > Chart as Block Type** and compile the F-block type.

Result

The I/Os with the "F_PrintTypParam" attribute appear in a printout of the F-program with the "Print safety-relevant parameters" option.

See also

Creating F-Block types with "Compile Chart as F-Block Type" (Page 103)

7.8 Programming data exchange between F-Shutdown groups in an F-CPU

Rules for the data exchange between F-shutdown groups

- If you want to exchange data between two F-shutdown groups, you are not permitted to directly interconnect the inputs and outputs. You must use special F-blocks for this.
- Information about the run sequence can be found in section " Determining the runtime sequence (Page 93) ".

Available F-blocks

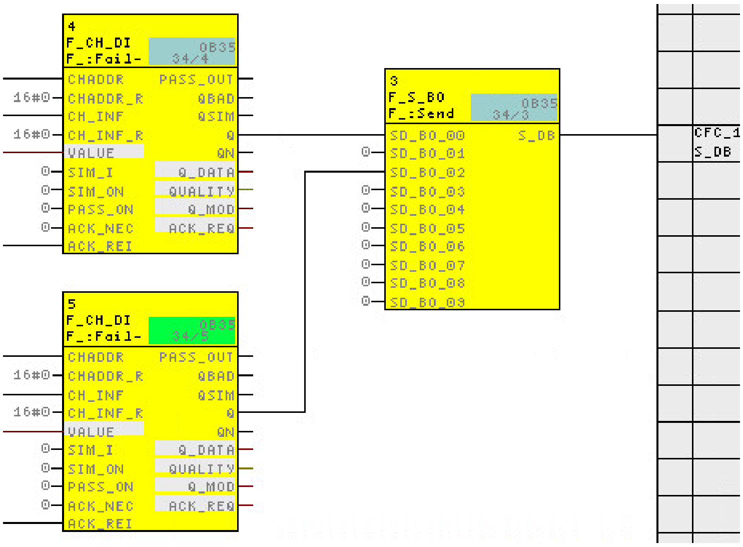
You must use the following F-system blocks for the data exchange between F-blocks in different F-shutdown groups:

F-block	Description
F_S_R / F_R_R	Safe transmission of 5 data elements of F-data type F_REAL.
F_S_BO / F_R_BO	Safe transmission of 10 data elements of F-data type F_BOOL.

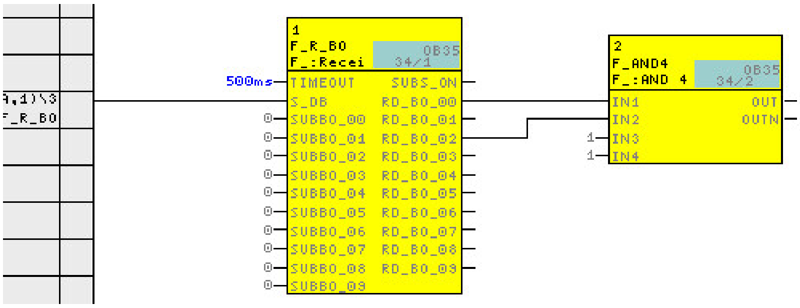
Procedure

1. Insert an F-block of type F_S_R or F_S_BO into the F-shutdown group, from which data is to be transferred.
2. Insert an F-block of type F_R_R or F_R_BO into the F-shutdown group, from which data is to be transferred.
3. Interconnect inputs SD_R_xx of F_S_R or SD_BO_xx of F_S_BO with the data to be transmitted.
4. Interconnect outputs RD_R_xx of F_R_R or RD_BO_xx of F_R_BO with the inputs of the F-blocks for further processing of the received data.
5. Interconnect the S_DB output of the send block with the S_DB input of the associated receive block.
6. Set the desired F-monitoring time for the TIMEOUT inputs of the F_R_R and F_R_BO receive blocks.
   For information regarding calculation of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

Examples: Excerpt from the chart of the F-shutdown group *from* which data will be transmitted



Example: Excerpt from the chart of the F-shutdown group *to* which data will be transmitted



Note

If you interconnect F-blocks in different F-shutdown groups directly (without the above-indicated F-system blocks), a compilation error will be generated at the next compilation.

If you interconnect F-blocks within a F-shutdown group with the above-indicated F-system blocks, an error message will be generated.

7.9 Data exchange between safety program and standard user program

Overview

Safety programs and standard user programs use different data formats. Safety-related F-data types are used in safety programs. Standard data types are used in the standard user program.

You must therefore use special conversion blocks for data exchange.

Parameters are transferred as safety-related F-data types in the safety program.

Data transfer from the safety program to the standard user program

If the standard user program is to further process data from the safety program, for example, for monitoring, you need to insert a data conversion block (F_data type) in the CFC Editor that converts the F-data types to standard data types. You can find these blocks in the F-library.

Data transfer from the standard user program to the safety program

Data from the standard user program cannot be processed in the safety program until a validity check is performed. You need to use additional process-specific plausibility checks in the safety program to ensure that no dangerous states can occur.

If you want to further process data from the standard user program in the safety program, you must use F-blocks for data conversion (F_data type) in order to generate safety-related F-data types from the standard data types. If necessary, you must then subject the converted data to a programmed plausibility check. You can find these F-blocks in the F-library.

7.9.1 Programming data exchange from the safety program to the standard user program

Available conversion blocks

The following blocks are available for conversion:

Block	Description
F_FBO_BO	Converts F_BOOL to standard BOOL
F_FR_R	Converts F_REAL to standard REAL
F_FI_I	Converts F_INT in standard INT
F_FTI_TI	Converts F_TIME to standard TIME

Procedure

Proceed as follows:

1. Insert blocks of the F_FBO_BO, F_FR_R, F_FI_I or F_FTI_TI type into the charts of the standard user program. You can find these blocks in the F-library.
2. Interconnect the inputs of the F_data type to similar signals from the safety program.
3. Interconnect the outputs of the standard data type with similar signals from the standard user program.

7.9.2 Programming data exchange from the standard user program to the safety program

Available F-conversion blocks

The following F-blocks are available for conversion:

F-block	Description
F_BO_FBO	Converts standard BOOL to F_BOOL
F_I_FI	Coverts standard INT in F_INT
F_R_FR	Converts standard REAL to F_REAL
F_TI_FTI	Converts standard TIME to F_TIME

Procedure

Proceed as follows:

1. Insert F-blocks of F_BO_FBO, F_I_FI, F_TI_FTI or F_R_FR the type into the charts of the safety program.
2. Interconnect the inputs of standard data types with similar signals from the standard user program.
3. Use a plausibility check to interconnect the outputs of F-data types with signals of the same type in the safety program.

Note

Adding, changing and deleting the connections from the standard user program to the F-conversion blocks is a change to the safety program, even if these are connections of a standard data type. This means that access authorization is required for compiling (see "Access Protection (Page 75)").

WARNING

Validity check

The F-blocks F_BO_FBO, F_I_FI, F_TI_FTI and F_R_FR only perform a data conversion. You must therefore program additional measures for plausibility checks in the safety program.

FSW-025

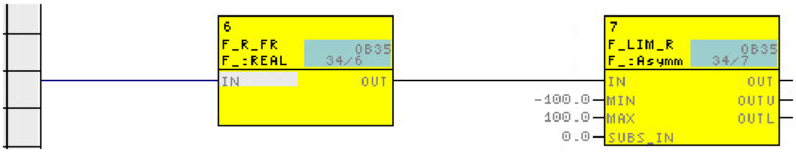
Validity check

The simplest type of plausibility check is an area specification with a fixed high and low limit, for example, with F_LIM_R.

Not all input parameters can be checked for plausibility in a sufficiently simple way.

Example: Converting standard to F-data types

Section of an F-chart for converting from REAL to F_REAL:



7.10 Implementation of user acknowledgment

Options for user acknowledgment

You can implement a user acknowledgment by means of the following:

- An acknowledgment button that you connect to an F-I/O with inputs
- A manual input via the OS

User acknowledgment via acknowledgment button

Note

When a user acknowledgment is implemented using an acknowledgment button and a communication error, F-I/O fault or channel fault occurs on the F-I/O to which the acknowledgment button is connected, an acknowledgment for reintegration of these F-I/O is also no longer possible. This "blocking" can only be canceled by a STOP/RUN transition of the F-CPU. For this reason, provision for an additional acknowledgment via an OS is recommended for the acknowledgment for reintegration of an F-I/O to which an acknowledgment button is connected.

User acknowledgment via an OS

For user acknowledgment via the OS, the "Fail-safe acknowledgment" operator function based on "Secure Write Command++" can be configured and executed as of S7 F Systems V6.2 and S7 F Systems Library as of V1.3 SP2. You can find additional information on this in section "Application case: Fail-safe acknowledgment (Page 148)".

The following description shows the configuration prior to S7 F Systems V6.2. Existing configurations of this type can continue to be used.

User acknowledgment via OS with the F-block F_QUITES

For implementation of a user acknowledgment via an OS, the F-block F_QUITES is required.

Procedure for programming the user acknowledgment via an OS

1. Insert the F-block F_QUITES in your safety program. The acknowledgment signal is available for the user acknowledgments at the OUT output of F_QUITES for evaluation.
2. Set up a field on your OS for manual input of the "Acknowledgment value" "6" (1st acknowledgment step) and "Acknowledgment value" "9" (2nd acknowledgment step) at the IN input of F_QUITES.
3. Optional: Evaluate the Q output of the F_QUITES on your OS to display the time window within which the second acknowledgment step must take place, or to indicate that the first acknowledgment step has already taken place.

⚠ WARNING

The two acknowledgment steps must not be triggered with a single operation.

The two acknowledgment steps must not be triggered by a single operation, e.g. by entering the acknowledgment steps including time conditions automatically in a program and triggering by a single operation! The two separate acknowledgment steps will also prevent erroneous tripping of an acknowledgment by your non-fail-safe OS.

FSW-026

⚠ WARNING

Execution of the two acknowledgment steps, if access to several F-CPUs is possible.

If access to multiple F-CPUs that use F_QUITES for fail-safe acknowledgment is possible from your OS, or if you have internetworked operator control and monitoring systems and F-CPUs (with F_QUITES F-blocks), you must be confident that the intended F-CPU is actually being referenced before executing the two acknowledgment steps:

- For this purpose, store a designation that is unique network-wide for the F-CPU in a DB of your standard user program in every F-CPU.
- Set up a field on your OS from which you can read out the designation of the F-CPU online from the DB before executing the two acknowledgment steps.
- Optional: Set up a field on your OS in which the designation of the F-CPU is additionally permanently stored. Then, a simple comparison of the designation of the F-CPU that is read out online with the permanently stored designation allows you to see whether the intended F-CPU is being referenced.

FSW-027

See also

F-Blocks for F-Communication between F-CPUs (Page 253)

F-Channel drivers for F-I/O (Page 330)

F-I/O access

8

Access via F-driver blocks

The following are required for each F-I/O:

- One F-module driver (to be generated by the compiler)
- One F-channel driver for each utilized input/output channel of the F-I/O

In S7 F/FH Systems, the F-I/O is accessed via F-module drivers. These F-module drivers communicate with the F-modules via direct I/O access. For this reason, a process image partition for the F-module does not have to be configured.

Cyclic updating of the process image is not required.

Note

When a process image partition is configured for the F-module, insertion of the F-module and call-up of the F-driver block in different cyclic interrupt OBs are not permitted!

Failure to observe this may cause sporadic data falsifications during communication with the F-module.

F-module drivers

The F-module driver undertakes the PROFIsafe communication between the safety program and the F-I/O. The F-module driver is automatically placed and interconnected in the safety program by the CFC driver generator.

F-channel drivers

The F-channel drivers in your safety program form the interface to a channel of an F-I/O and perform signal processing. There are different F-channel drivers depending on the F-I/O (see section F-Channel drivers for F-I/O (Page 330)).

You must place and interconnect F-channel drivers in the safety program.

For redundantly configured F-I/O, you need only one F-channel driver for two redundant channels

8.1 Positioning, interconnecting, and assigning parameters to F-Channel drivers

Requirement: Symbolic names

Enter a symbolic name (symbol) for each utilized channel in the symbol table. You must assign this symbol to the VALUE or I_OUT_D I/O of the associated F-channel driver. For more clarity, you should also comment the unused channels as reserved channels or unused channels in the symbol table.

Procedure

1. Place the suitable F-channel driver for each utilized input/output channel.
2. For each F-channel driver, interconnect the VALUE or I_OUT_D I/O with the symbol of the associated channel. This step is required for all placed F-channel drivers. For redundantly configured F-I/O, interconnect the VALUE I/O with the symbol of the channel with the lower channel address.
3. Interconnect the following inputs/outputs with your user logic:
   - The inputs I of the F-channel drivers F_CH_DO, F_CH_BO, F_CH_QBO, F_CH_QIO
   - The outputs Q or QN of the F-channel drivers F_CH_DI, F_PA_DI, F_CH_BI, F_CH_QBI, F_CH_QII
   - The outputs V of the F-channel drivers F_CH_AI, F_PA_AI
4. Optional: Interconnect the simulation I/O.
5. Optional: Connect the PASS_ON input if you want to activate passivation of the channel, e.g. depending on certain states in your safety program.
6. Check the parameter assignment at the respective ACK_NEC input. Assign the value "1" to the respective ACK_NEC input if a user acknowledgment is required for reintegration of the channel.
7. Interconnect the respective ACK_REI input with the signal for acknowledgment of reintegration (see section "Group passivation (Page 120)").
8. Optional: Interconnect the PASS_OUT or QBAD output in order to observe whether a fail-safe value or a valid process value is being output.
9. Optional: Evaluate the QUALITY output in the standard user program or on the OS if you want to query or observe the value status (quality code) of the process value.
10. Optional: Evaluate the ACK_REQ output in the standard user program or on the OS in order to determine whether a user acknowledgment is required.
11. Optional: Connect the QBIT output with F-channel drivers for PROFIsafe profile 2.6.1 XP, e.g. F_CH_QBI, F_CH_QBO, to evaluate the validity of the corresponding process value at the input/output channel.

Depending on the F-channel driver, there are other inputs and outputs you can or must interconnect (see appendix "F-Channel drivers for F-I/O (Page 330)")

8.2 Generating F-Module drivers

Generating F-module drivers

Use the driver generator of the CFC for this purpose.

When the S7 program is compiled in the "Compile program" dialog, the "Generate module drivers" option is activated by default. Check the setting of the option, and activate the option if it is not activated.

The driver generator thus places all automatically generated F-module drivers in custom CFCs named @F_(1), @F_(2), etc. The instances of the F-module drivers automatically obtain the name that you have entered in HW Config for the corresponding F-I/O devices (F_Name_x). The F-channel drivers are interconnected with the associated F-module drivers.

If you use PCS 7, the driver generator inserts additional blocks (see PCS 7 documentation).

8.3 Process data or fail-safe values

When are substitute values used?

The safety function requires that when passivating the entire F-I/O or individual channels of an F-I/O, substitute values are used instead of the process values in the following cases:

- For an F-startup
- When there are errors in safety-related communication (communication errors) between F-CPU and F-I/Os via the safety protocol according to PROFIsafe
- When F-I/O or channel faults are detected (for example, wire-break, short-circuit, or discrepancy error)
- As long as you activate a passivation of the F-I/O at the F-channel driver at PASS_ON input.

Substitute value output for F-I/O/channels of a F-I/O

For an F-I/O with inputs, the F-system provides substitute values at the F-channel driver instead of the process values at the fail-safe inputs during passivation.

The substitute value 0 is provided for (digital) channels of the BOOL data type.

For analog channels, you must configure the substitute values at the SUBS_V input of the F-channel driver and enable it by configuring the SUBS_ON input with 1 or select the last valid value as the substitute value by configuring the SUBS_ON input with 0 (= preset).

WARNING

F-I/O with digital inputs of the BOOL data type

For F-I/O with inputs, the substitute value "0" provided at the F-channel driver must be further processed for (digital) channels of data type BOOL in the safety program.

FSW-028

For an F-I/O with outputs, substitute values are transferred from the F-system to the fail-safe outputs instead of the output values provided on the F-channel driver during passivation.

Reintegration

The changeover from the substitute values to process values (reintegration of a F-I/O devices) takes place automatically or only after a user acknowledgment at the fail-safe channel driver.

The type of reintegration depends on:

- Cause of passivation of the F-I/O or channels of the F-I/O
- Configuration to be performed by you on the F-channel driver

Note

For F-I/Os with outputs, an acknowledgment may only be possible in the minute range after error correction due to required test signal connections after F-I/O/channel errors (see manuals for F-I/Os).

See also

F-Channel drivers for F-I/O (Page 330)

8.4 Group passivation

Description

If you want to enable passivation of additional F-I/O when an F-I/O or a channel of an F-I/O is passivated by the F-System, you can use the PASS_OUT output or PASS_ON input to perform a group passivation of associated F-I/O.

Group passivation by means of PASS_OUT/PASS_ON can, for example, be used to force simultaneous reintegration of all F-I/O after startup of the F-System.

For group passivation, you must OR all PASS_OUT outputs of the F-Channel drivers in the group with F_OR4 F-Blocks and interconnect the result at the OUT output of F_OR4 with all PASS_ON inputs of the F-Channel drivers in the group.

See also

F-Channel drivers for F-I/O (Page 330)

Programming communication 9

9.1 Safety-related communication between F-CPUs

9.1.1 Configuring safety-related communication via S7 connections

Introduction

Safety-related communication between the safety programs of F-CPUs via S7 connections takes place using connection tables in NetPro, in the same way as with standard programs.

Note

In S7 F/FH Systems, safety-related communication via S7 connections is possible to and from the following F-CPUs:

- CPU 315F-2 and higher
- CPU 317F-2 and higher
- CPU 319F-3 and higher
- CPU 412-4H and higher
- CPU 414-4H and higher
- CPU 414F-3 and higher
- CPU 416F-x and higher
- CPU 416-5H and higher
- CPU 417-4H and higher
- CPU 410-5H and higher

Note

⚠ WARNING

CPU-CPU communication and public networks

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

FSW-029

Creating an S7 connection in the connection table

For each communication connection between two F-CPUs, you need to create an S7 connection in the connection table in NetPro.

STEP 7 assigns a local ID and a partner ID for each connection end-point. You can change the local ID in NetPro if necessary. You assign the local ID to the ID parameter of the appropriate F-blocks in the safety programs.

Note

Safety-related communication via S7 connections to unspecified partners is not possible.

Procedure for configuring S7 connections

You configure the S7 connections for safety-related CPU-to-CPU communication the same way as for standard systems, or even as a fault-tolerant S7 connection, if necessary.

Note

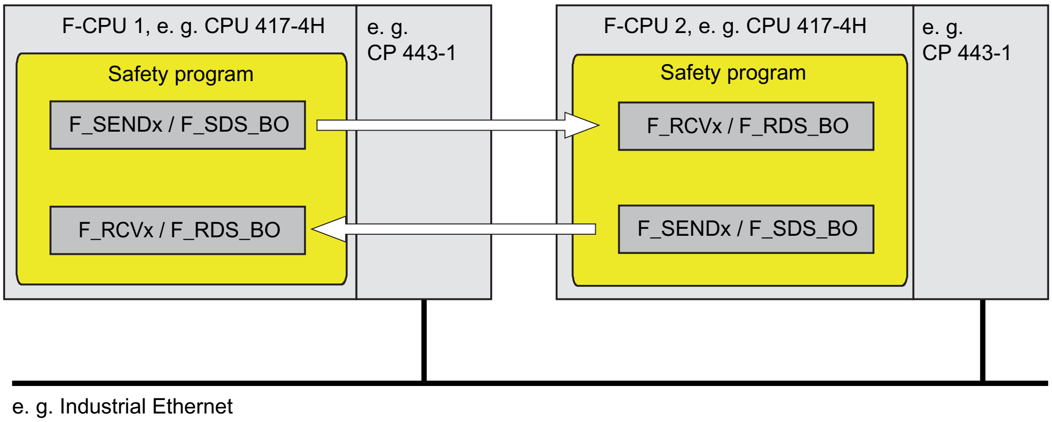
If you modify the configuration of S7 connections for safety-related communication, you must recompile the relevant S7 programs and download them to the F-CPUs.

Additional information

You will find a description of how to configure S7 connections in the following sources:

- In the manual "Configuring hardware and configure connections with STEP 7 V 5.5 (https://support.industry.siemens.com/cs/ww/en/view/109751824)"
- In the manual "Automation System S7-400H Fault-Tolerant Systems (http://support.automation.siemens.com/WW/view/en/82478488)" and
- STEP 7 online help.

9.1.2 Communication via F_SENDBO/F_RCVBO, F_SENDR/F_RCVR, and F_SDS_BO/F_RDS_BO



The **F_SENDBO / F_RCVBO, F_SENDR / F_RCVR and F_SDS_BO / F_RDS_BO** F-communication blocks are used for fail-safe sending and receiving of data via S7 connections.

This enables you to securely transfer a fixed number of up to 20 data of the F-data type F_REAL and up to 20/32 data of the F-data type F_BOOL.

9.1.3 Programming safety-related CPU-to-CPU communication via S7 connections

Requirements for programming

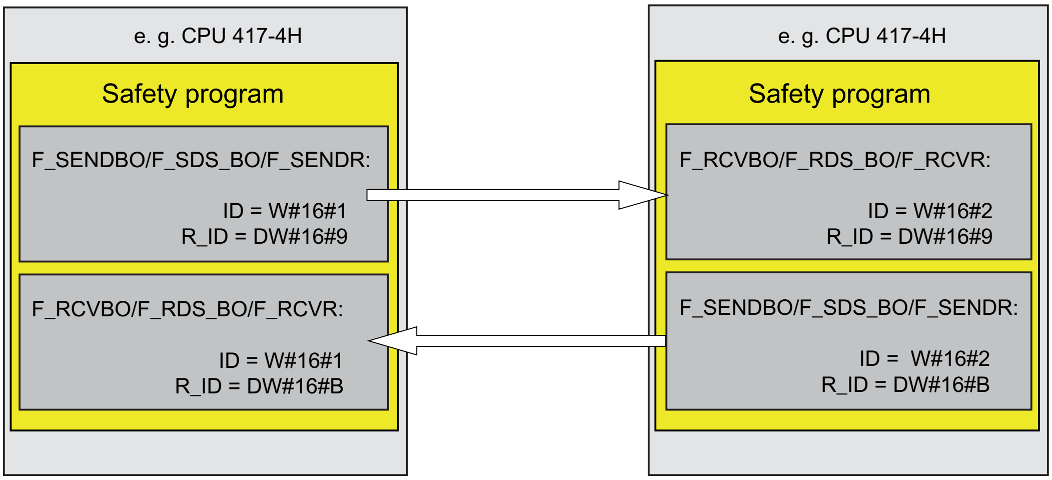
The following requirements must be met prior to programming:

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

Programming procedure

1. In the safety program that is to send data, insert the F-block F_SENDBO/F_SDS_BO/ F_SENDR for sending.
2. In the safety program that is to receive data, insert the F-block F_RCVBO/F_RDS_BO/ F_RCVR for receiving.
3. Configure the ID input of the F_SENDBO/F_SDS_BO/F_SENDR with the local ID of the S7 connection configured in NetPro (data type: WORD).
4. Configure the ID input of F_RCVBO/F_RDS_BO/F_RCVR with the local ID of the S7 connection configured in NetPro (data type: WORD).

5. Assign the R_ID inputs of F_SENDBO/F_SDS_BO/F_SENDR and F_RCVBO/F_RDS_BO/F_RCVR an odd number (data type: DWORD). In this way, you determine the association between an F_SENDBO/F_SDS_BO/F_SENDR and an F_RCVBO/F_RDS_BO/F_RCVR. The F-blocks that belong together receive the same value for R_ID.



⚠ **WARNING**

Value for the relevance address reference

The value for the respective address relationship (input parameter R_ID; data type: DWORD) can be selected by the user but must be an odd number and unique network-wide for all safety-related communication connections. The value R_ID + 1 is internally assigned and must not be used.

FSW-030

6. Connect the SD_BO_xx or SD_R_xx inputs of the F_SENDBO/F_SDS_BO/F_SENDR F-blocks with the transmit signals.
7. Connect the RD_BO_xx or RD_R_xx outputs of the F_RCVBO/F_RDS_BO/F_RCVR F-blocks with the F-blocks for further processing of the received signals.
8. Configure the SUBBO_xx or SUBR_xx inputs of the F-blocks F_RCVBO/F_RDS_BO/F_RCVR with the substitute values that are to be made available at the RD_BO_xx or RD_R_xx outputs,
   - During the initial connection setup between the communication partners after an F-startup of the F-systems,
   - When a communication error has occurred.

9. Configure the TIMEOUT inputs of F_SENDBO/F_SDS_BO/F_SENDR and F_RCVBO/F_RDS_BO/F_RCVR with the required F-monitoring time.

⚠ **WARNING**

Duration of the signal level to be transmitted

It can only be ensured (from a fail-safe standpoint) that a signal level to be transmitted will be detected on the sender side and transmitted to the receiver if the signal level is present for at least as long as the assigned F-monitoring time (TIMEOUT).

For information regarding the calculation of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

FSW-031

Note

For safety reasons, the parameters at the TIMEOUT inputs must be set with the minimum F-monitoring time. TIMEOUT must not be used to increase availability.

10. At the EN_SEND input of the F_SENDBO/F_SDS_BO/F_SENDR, you can temporarily switch off communication between the F-CPUs to reduce the bus load by supplying input EN_SEND (default setting = "1") with "0". Then no more send data is sent to the corresponding F_RCVBO/F_RDS_BO/F_RCVR and the receiver F_RCVBO/F_RDS_BO/F_RCVR provides the configured substitute values for this period. If communication between the connection partners has already been established, a communication error is detected.
11. Optional: Evaluate the ACK_REQ output of the F_RCVBO/F_RDS_BO/F_RCVR, for example, in the standard user program, to query or display whether a user acknowledgment is required.
12. Interconnect the ACK_REI input of F_RCVBO/F_RDS_BO/F_RCVR with the signal for acknowledgment for reintegration.
13. Optional: Evaluate the SUBS_ON output of F_RCVBO/F_RDS_BO/F_RCVR or F_SENDBO/F_SDS_BO/F_SENDR to query whether F_RCVBO/F_RDS_BO/F_RCVR outputs the substitute values that you configured at the SUBBO_xx/SUBR_xx inputs.

14. Optional: Evaluate the ERROR output of F_RCVBO/F_RDS_BO/F_RCVR or F_SENDBO/F_SDS_BO/F_SENDR in the standard user program, for example, to query or display whether a communication error has occurred.

15. Optional: Evaluate the SENDMODE output of F_RCVBO/F_RDS_BO/F_RCVR to query whether the F-CPU with the associated F_SENDBO/F_SDS_BO/F_SENDR is in deactivated safety mode.

⚠ WARNING

Data reception when safety mode is deactivated

If the F-CPU with the associated F_SENDBO/F_SDS_BO/F_SENDR is in deactivated safety mode, you can no longer assume that the data received from this F-CPU were generated safely. You must then also ensure the safety of the plant units that are influenced by the received data by organizational measures, such as monitored operation and manual safety shutdown, or output of safe substitute values in the F-CPU with F_RCVBO/F_RDS_BO/F_RCVR by evaluating SENDMODE instead of the received data.

FSW-032

⚠ WARNING

The S7 program must be recompiled if the S7 connections for communication between F-CPUs have been changed.

If the safety program contains F-blocks for safety-related CPU-CPU communication, the S7 program involved in the communication must be recompiled after the following actions so that the connection data is updated:

- Copying an F-CPU
- Copying a safety program or chart to another F-CPU
- Changing a communication partner of an S7 connection
- Removing/inserting a project containing the communication partner of an S7 connection from/to the multiproject

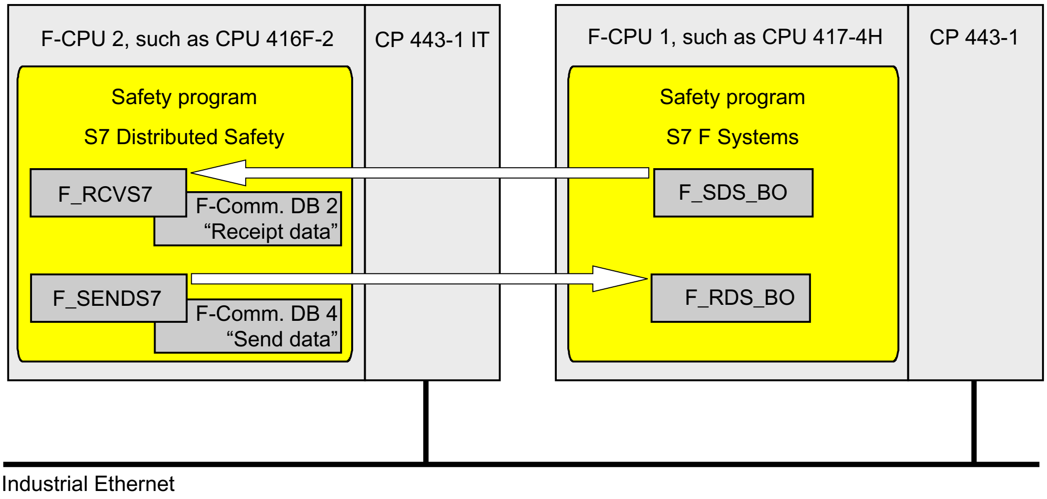
FSW-033

See also

Determining the runtime sequence (Page 93)

Safety engineering in SIMATIC S7 System Manual (http://support.automation.siemens.com/WW/view/en/12490443)

9.2 Safety-related communication between S7 F Systems and S7 Distributed Safety



Procedure on the S7 F Systems side

On the S7 F Systems side, proceed as described in section "Safety-related communication between F-CPUs (Page 121)".

Particularity:

Communication between S7 F Systems and S7 Distributed Safety is only possible on the S7 F Systems side with the F blocks F_SDS_BO/F_RDS_BO.

Procedure on the S7 Distributed Safety side

On the S7 Distributed Safety side, proceed as described in section "Safety-related communication via S7 communications" in manual "S7 Distributed Safety - Configuring and Programming (http://support.automation.siemens.com/WW/view/en/22099875)".

Particularity:

For communication between S7 F Systems and S7 Distributed Safety, you must create the F-DB with exactly 32 data elements of data type BOOL on the S7 Distributed Safety side.

Operations with "Secure Write Command++" 10

10.1 Concept of "Secure Write Command++"

Function

The "Secure Write Command++" functionality (SWC++) enables safety-related changes to be made to F-parameters in the safety program of an F-CPU from an operation station (OS).

The safety-related changes are executed by the following operator functions based on "SWC++":

- Maintenance Override
- Change process values
- Fail-safe acknowledgment

You can find additional information on the operator functions in section "Operator functions based on "Secure Write Command++" (Page 132)".

Note

The operator functions based on "SWC++" are available only under SIMATIC PCS 7.

With "SWC++" the actions for changing parameters in the F-CPU from the WinCC OS are separated into:

Component in the F-CPU	• Transaction of the protocol • Receipt of parameters
Component in the OS	• Object that calculates the checksum • Check interface for confirming the transaction

Each of these actions is carried out either in individual F-blocks in the F-CPU or individual objects in the OS.

Blocks for operator function based on "Secure Write Command++"

Block type	Function	Name	Use [*1)]	Version
Protocol block	Centralized control of operator input via the OS	F_SWC_P	CHG, MOS, QOS	S7 F Systems as of V6.1 and S7 F Systems Library as of V1.3
Parameter assignment block	Value change for data type F_BOOL	F_SWC_BO	MOS, QOS	S7 F Systems as of V6.1 and S7 F Systems Library as of V1.3
	Value change for data type F_REAL	F_SWC_R	MOS	S7 F Systems as of V6.1 and S7 F Systems Library as of V1.3
	Value change for data type F_BOOL	F_SWC_CB	CHG	S7 F Systems as of V6.2 and S7 F Systems Library as of V1.3 SP2
	Value change for data type F_REAL	F_SWC_CR	CHG	S7 F Systems as of V6.2 and S7 F Systems Library as of V1.3 SP2
Operator control block	Establishes the connection to the WinCC faceplate.	SWC_MOS	MOS	S7 F Systems as of V6.1 and S7 F Systems Library as of V1.3
	Establishes the connection to the WinCC faceplate.	SWC_CHG	CHG	S7 F Systems as of V6.2 and S7 F Systems Library as of V1.3 SP2
	Establishes the connection to the WinCC faceplate.	SWC_QOS	QOS	S7 F Systems as of V6.2 and S7 F Systems Library as of V1.3 SP2

[1)] Meaning of the abbreviations:
"CHG" = Function "Change process values"
"MOS" = Function "Maintenance Override"
"QOS" = Function "Fail-safe acknowledgment"

Other components for operator functions based on "Secure Write Command++"

Type	Description	Name	Use [*1)]	Version
"Chart-in-Chart"	Used for a time-controlled Maintenance Override	SWC_TR	MOS	S7 F Systems as of V6.1 and S7 F Systems Library as of V1.3
Faceplates	Faceplates for the OS	-	MOS CHG, QOS	Starting from S7 F Systems V6.1 Starting from S7 F Systems V6.2

[*1)] Meaning of the abbreviations:
"CHG" = Function "Change process values"
"MOS" = Function "Maintenance Override"
"QOS" = Function "Fail-safe acknowledgment"

Note

When used with PCS 7, one PO license is used for each instance of an operator control block in the safety program.

Operator input types

The action for safety-related changing of F-parameters in the safety program is referred to as an "operator input".

You perform an operator input in the OS via a faceplate. The operator input consists of a sequence of operations that can be performed by one or two operators.

See also

Blocks and F-Blocks for data conversion (Page 292)

10.2 Operator functions based on "Secure Write Command++"

Overview

The following operator functions are based on "Secure Write Command++" (SWC++):

- "Maintenance Override"
  "Maintenance Override" allows you to set bypasses in the safety program from the OS. Starting from S7 F Systems V6.1, you can create a bypass for up to three process signals for F_BOOL or F_REAL. The bypasses can be mutually interlocked, if required. In addition, you can use Maintenance Override to change fail-safe values for process signals and assign a reset time in order to reset the set bypasses automatically after this time.
- "Change process values"
  "Change process values" allows you to change F-parameters in the safety program from the OS.
  Starting from S7 F Systems V6.2 with S7 F Systems Lib as of V1.3 SP2, you can change an F-parameter of data type F_BOOL or F_REAL with "SWC++" (F_SWC_CB / F_SWC_CR and SWC_CHG).
- "Fail-safe acknowledgment"
  "Fail-safe acknowledgment" allows you to implement a fail-safe acknowledgment from the OS.
  As of S7 F Systems V6.2 with S7 F Systems Lib as of V1.3 SP2, you can control reintegration of F-I/O via the ES/OS with "SWC++" (F_SWC_BO and SWC_QOS).

Note

Possible combinations of blocks

- The F_SWC_CB and F_SWC_CR blocks may only be used with SWC_CHG. It is not possible to use these blocks for SWC_MOS or SWC_QOS.
- The F_SWC_BO block may only be used with SWC_MOS and SWC_QOS. It is not possible to use this block with SWC_CHG.
- The F_SWC_R block may only be used with SWC_MOS. It is not possible to use this block with SWC_CHG.

10.3 "SWC++" operator control functions via "Web Option for OS"

Overview

As of S7 F Systems V6.3, you can operate and monitor the following operator control functions based on "SWC++" over the intranet/Internet on a PCS 7 Web client with the help of the "PCS 7 Web Option for OS".

- "Maintenance override" allows you to set bypasses in the safety program from the OS.
- "Change process values" allows you to change F-parameters in the safety program from the OS.
- "Fail-safe acknowledgment" for fail-safe acknowledgment from the OS

Configuration steps on the ES

- Faceplates, e.g. SWC_QOS, were placed in the CFCs during configuration.
- Faceplates were configured for the operator control blocks.

You can find additional information on this in section "Basic procedure for configuring operator control functions with "SWC++". (Page 135)".

Note

No operations based on the "Safety Data Write" functionality are possible via "PCS 7 Web Option for OS".

You can find a detailed description of the "Web Option for OS" in the Function Manual *"Process Control System PCS 7 Web Option for OS"*. Additional information on this document is available in the preface in the section "Scope of information".

When using "Web Option for OS" in an OS single-user system or OS multi-user system, note the following:

- The notes in the foreword to "Safety concepts and communication".
- The conditions and notes in the Function Manual *"Process Control System PCS 7 Web Option for OS"* in the section "Overview of the Web Option for OS".
  - An OS client that is configured as Web server, for example, can no longer be utilized as an operator station (OS client, SIMATIC BATCH client, etc.) within the PCS 7 system.
  - The Web client cannot be used as an additional PCS 7 station.

Requirements:

- OS:
  - S7 F Systems HMI must be installed on the OS.
  - "PCS 7 Web Option for OS" must be installed and set up on the OS.
  - "Web Option for OS" requires PCS 7 V9.0.2 or higher.
- Web client
  - The required plug-ins must be installed on the Web client.
    The plug-in is available for download and installation after the Web client has logged onto the Web Navigator Server.
  - VC++ redist 2010 must be installed.
    This software is available from the product DVD.
  - No S7 F Systems HMI must be installed on the Web client.

10.4 Programming operator functions

10.4.1 Basic procedure for configuring operator control functions with "SWC++".

Basic procedure

To perform an operator function via an OS, follow these steps:

On the engineering station (ES)

1. Place an operator control block, e.g. SWC_QOS, one or more parameter assignment blocks, e.g. F_SWC_BO, and one or more protocol blocks F_SWC_P in your CFC chart and interconnect them.
   For more information, refer to section "Placement, parameter assignment and interconnection of F-blocks in the CFC (Page 135)".
2. Configure the faceplate for the operator control block.
   For more information, refer to section "Configuring the faceplate of the operator functions (Page 149)".

On the operator station (OS)

- Perform a value change with "Change process values" on an F-parameter.
- Create a bypass with "Maintenance Override" at the F-channel drivers and change the fail-safe value, if necessary.
- Perform a fail-safe acknowledgment with "Fail-safe acknowledgment".

You can find further information about these operator inputs on the OS in section "Executing operator functions (Page 155)".

10.4.2 Placement, parameter assignment and interconnection of F-blocks in the CFC

10.4.2.1 Introduction

Introduction

The following sections show you typical application cases for the individual operator functions.

You will be given information on the procedure for placement, parameter assignment and interconnection of blocks and F-blocks for the operator functions in CFC charts.

- "Change process values"
  - Application case: "Change process values" with logic blocks (Page 137)
  - Application case: "Change process values" with arithmetic block (Page 139)
- "Maintenance Override"
  - Application case: Simulating a F-channel driver (Page 141)
  - Application case: Grouped maintenance override with mutual interlock (Page 143)
  - Application case: Time-triggered maintenance override (Page 145)
- "Fail-safe acknowledgment"
  - Application case: Fail-safe acknowledgment (Page 148)

Note

The creation of F-block types based on the "Secure Write Command++" function is not supported.

Use of a keyswitch

To ensure that only authorized persons can perform operator inputs, you can connect the EN_SWC input of the F-block F_SWC_P to a keyswitch.

Input EN_SWC = 1 must be set during an operator input. When EN_SWC = 0 after an operator input, all existing bypasses are deactivated. However, set fail-safe values are retained.

⚠ WARNING

The "Secure Write Command++" functionality allows changes to the safety program to be made during RUN mode

As a result, the following additional safety measures are required:

- Ensure that operator inputs that could compromise plant safety cannot be carried out. You can use the EN_SWC input of the F-block F_SWC_P for this purpose, for example, by controlling it with a keyswitch or on a process-dependent basis via the safety program.
- Ensure that only authorized persons can carry out operator inputs.

Examples:

- Control the EN_SWC input of the F-block F_SWC_P with a keyswitch.
- Set up access protection for the operator stations where an operator function based on "Secure Write Command++" can be performed.

FSW-034

Multiple protocol blocks in a shutdown group

Starting from S7 F Systems V6.2 with S7 F Systems Lib as of V1.3 SP2, it is possible to place multiple protocol blocks for each shutdown group and to thus enable multiple simultaneous operator inputs from the OS.

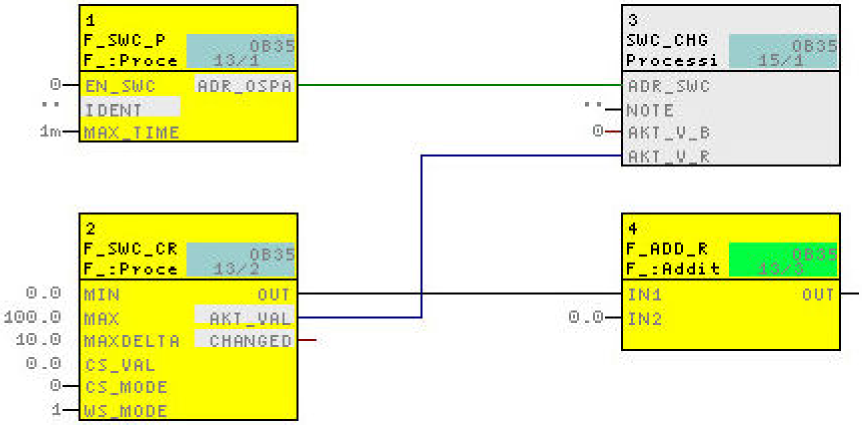
This requires an interconnection between the ADR_OSPA output of the F_SWC_P protocol block and the ADR_SWC input of the corresponding operator control block.

If multiple F_SWC_P blocks per shutdown group are present, the ADR_OSPA output of each F_SWC_P must be interconnected.

This interconnection is not required when simultaneous operator inputs per shutdown group are not needed.

Principle of configuration

1. Place the protocol block F_SWC_P and an operator control block, e.g. SWC_CHG, in a CFC chart.
2. Connect the ADR_OSPA output of F_SWC_P to the ADR_SWC input of the operator control block, e.g. SWC_CHG.
   The following figure shows a possible configuration of the blocks and this interconnection.



The remaining configuration steps are described in the following application cases.

10.4.2.2 Application case: "Change process values" with logic blocks

Application

This application case shows you how to control a signal in your plant with the "Change process values" function dependent on a control signal from your plant.

Procedure

⚠ WARNING

Warnings in the descriptions of the F-blocks

Observe the warnings in the descriptions of the following F-blocks.

F_SWC_CB

F_SWC_CR

F_SWC_BO

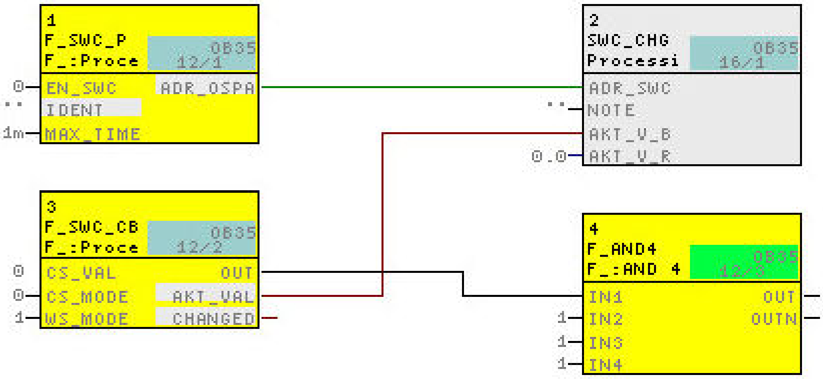
F_SWC_R

FSW-035

1. Place the SWC_CHG block in your CFC chart.
   Observe the information on assigning names in section "SWC_CHG: Operator function for Change process values (Page 325)".
2. Place the F-block F_SWC_P, if necessary.
   Optional:
   If you place multiple protocol blocks F_SWC_P per shutdown group so that multiple simultaneous operator inputs are possible from the OS, connect the ADR_OSPA output of F_SWC_P to the ADR_SWC input of the associated operator control block SWC_CHG. This interconnection is not required when simultaneous operator inputs per shutdown group are not needed. You can find additional information on this in section "Introduction (Page 135)".
3. Place one F-block F_SWC_CB and F_AND4 each.
4. Connect the EN_SWC input of the F-block F_SWC_P to a keyswitch.
5. Assign the maximum duration of the operator input (default setting is 1 minute) at the MAX_TIME input of the F-block F_SWC_P.
6. Interconnect the inputs and outputs of the F-block F_SWC_CB:
   Outputs:
   - OUT with the INx input of the F-block F_AND4
   - AKT_VAL with the AKT_V_B input of the SWC_CHG block

   Inputs:
   - Assign the initial value to the CS_VAL input that is to be transferred to the OUT output following a cold restart.
   - Optional: Assign the value "0" to the WS_MODE input if the value at the CS_VAL input is also to be transferred to the OUT output following a warm restart. The WS_MODE input is set to "1" by default.
7. Interconnect the INy input of the F-block F_AND4 with the controlling signal from your plant.
8. Interconnect the OUT output of the F-block F_AND4 with the signal of your plant to be controlled.
9. Before compiling, check the assignment of the SWC_CHG block. The block must be assigned to a standard runtime group.

10. Compile your CFC chart.
    Additional connections between the SWC_CHG block, the F-blocks F_SWC_CB and F_SWC_P are created during compilation.



11. Follow the procedure as described in section "Configuring the faceplate of the operator functions (Page 149)".

10.4.2.3 Application case: "Change process values" with arithmetic block

Application

This application case shows you how to control a signal in your plant with the "Change process values" function dependent on a control signal from your plant.

Procedure

WARNING

Warnings in the descriptions of the F-blocks

Observe the warnings in the descriptions of the following F-blocks.

F_SWC_CB

F_SWC_CR

F_SWC_BO

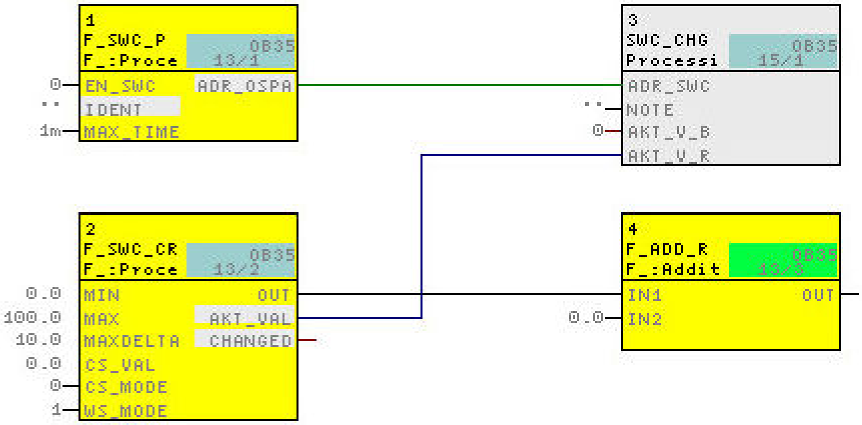
F_SWC_R

FSW-035

1. Place the SWC_CHG block in your CFC chart.
   Observe the information on assigning names in section "SWC_CHG: Operator function for Change process values (Page 325)".
2. Place the F-block F_SWC_P, if necessary.
   Optional:
   If you place multiple protocol blocks F_SWC_P per shutdown group so that multiple simultaneous operator inputs are possible from the OS, connect the ADR_OSPA output of F_SWC_P to the ADR_SWC input of the associated operator control block SWC_CHG. This interconnection is not required when simultaneous operator inputs per shutdown group are not needed. You can find additional information on this in section "Introduction (Page 135)".
3. Place one F-block F_SWC_CR and F_ADD_R each.
4. Connect the EN_SWC input of the F-block F_SWC_P to a keyswitch.
5. Assign the maximum duration of the operator input (default setting is 1 minute) at the MAX_TIME input of the F-block F_SWC_P.
6. Interconnect the inputs and outputs of the F-block F_SWC_CR:
   Outputs:
   - Interconnect OUT with the INx input of the F-block F_ADD_R
   - Interconnect AKT_VAL with the AKT_V_R input of the SWC_CHG block

   Inputs:
   - Assign limits to the MIN and MAX inputs to specify the time during which the OUT output may be changed.
   - Assign the value of the maximum permissible increment of the change to the MAXDELTA input to specify the amount (+/-) by which the OUT output can change relative to the current value.
   - Assign the initial value to the CS_VAL input that is to be transferred to the OUT output following a cold restart.
   - Optional: Assign the value "0" to the WS_MODE input if the value at the CS_VAL input is also to be transferred to the OUT output following a warm restart. The WS_MODE input is set to "1" by default.
7. Interconnect the INy input of the F-block F_ADD_R with the controlling signal from your plant.
8. Interconnect the OUT output of the F-block F_ADD_R with the signal of your plant to be controlled.
9. Before compiling, check the assignment of the SWC_CHG block. The block must be assigned to a standard runtime group.

10. Compile your CFC chart.
    Additional connections between the SWC_CHG block, the F-blocks F_SWC_CR and F_SWC_P are created during compilation.



11. Follow the procedure as described in section "Configuring the faceplate of the operator functions (Page 149)".

10.4.2.4 Application case: Simulating a F-channel driver

Application

This application case shows you how to simulate an F-channel driver with "Maintenance Override".

Procedure

⚠ **WARNING**

Warnings in the descriptions of the F-blocks

Observe the warnings in the descriptions of the following F-blocks.

F_SWC_CB

F_SWC_CR

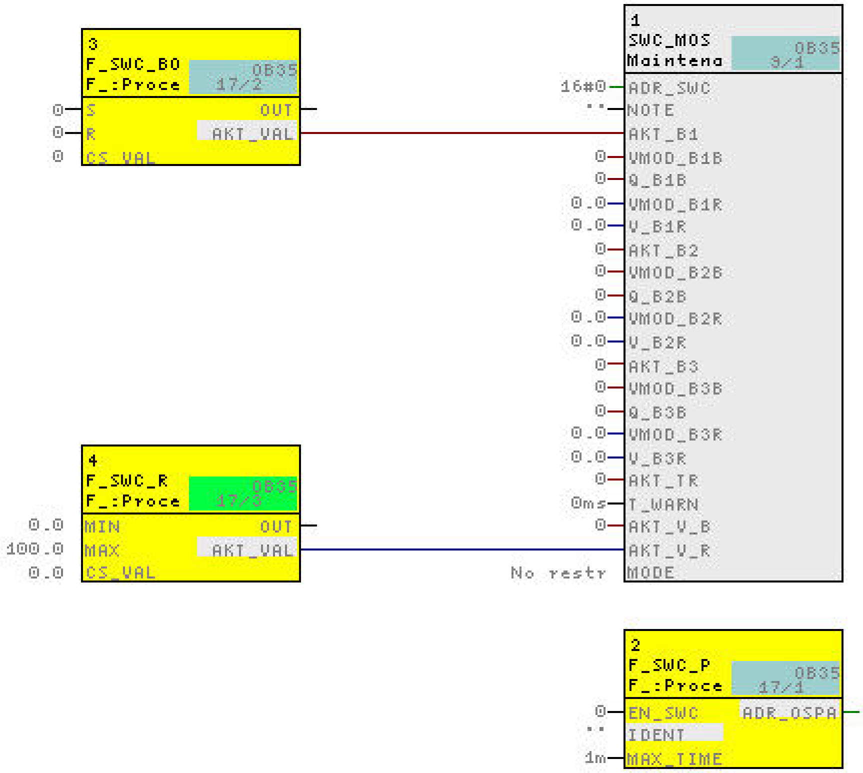
F_SWC_BO

F_SWC_R

FSW-035

1. Place the SWC_MOS block in your CFC chart.
   Observe the information on assigning names in section "SWC_MOS: Command function for Maintenance Override (Page 326)".
2. Place the F-block F_SWC_P, if necessary.
   Optional:
   If you place multiple protocol blocks F_SWC_P per shutdown group so that multiple simultaneous operator inputs are possible from the OS, connect the ADR_OSPA output of F_SWC_P to the ADR_SWC input of the associated operator control block SWC_MOS. This interconnection is not required when simultaneous operator inputs per shutdown group are not needed. You can find additional information on this in section "Introduction (Page 135)".
3. Place an F-block F_SWC_BO that will start and stop the simulation.
4. Place an F-block F_SWC_BO or F_SWC_R that will change the simulation value, if such a change is desired.
5. Connect the EN_SWC input of the F-block F_SWC_P to a keyswitch.
6. Assign the maximum duration of the operator input (default setting is 1 minute) at the MAX_TIME input of the F-block F_SWC_P.
7. Connect the outputs of the F-block F_SWC_BO that will start and stop the simulation:
   – Connect OUT to the SIM_ON input of the F-channel driver
   – Connect AKT_VAL to the AKT_B1 input of the SWC_MOS block
8. Connect the outputs of the F-block F_SWC_BO or F_SWC_R that will change the simulation value:
   – Connect OUT to the SIM_I or SIM_V input of the F-channel driver
   – Connect AKT_VAL to the AKT_V_B or AKT_V_R input of the SWC_MOS block
9. Optional:
   Assign a low limit and high limit for the fail-safe value (default setting 0.00 and 100.0, respectively) for the MIN and MAX inputs of the F-block F_SWC_R. Assign the CS_VAL input of the F-block F_SWC_R, if necessary.
10. Optional:
    If you want to have the current value of an F-I/O displayed in the faceplate when a bypass is activated, connect the Q_MOD or V_MOD output of the F-channel driver to the V_MOD_B1B or V_MOD_B1R input of the SWC_MOS block.
11. Optional:
    If you want to have the process value and its QUALITY displayed for the F-channel driver in the faceplate, connect the following outputs of the F-channel driver:
    – Q_DATA or V_DATA output to the Q_BxB or V_BxR input of the SWC_MOS block.
    – QUALITY output to the QUAL_Bx input of the SWC_MOS block
12. Before compiling, check the assignment of the SWC_MOS block. The block must be assigned to a standard runtime group.

13. Compile your CFC chart.
    Additional connections between the SWC_MOS block, the F-blocks F_SWC_BO or F_SWC_R, F_SWC_P and the F-channel drivers are created during compilation.



14. Follow the procedure as described in section "Configuring the faceplate of the operator functions (Page 149)".

10.4.2.5 Application case: Grouped maintenance override with mutual interlock

Application

This application case shows you how to create a grouped "Maintenance Override".

Procedure

⚠ WARNING

Warnings in the descriptions of the F-blocks

Observe the warnings in the descriptions of the following F-blocks.

F_SWC_CB

F_SWC_CR

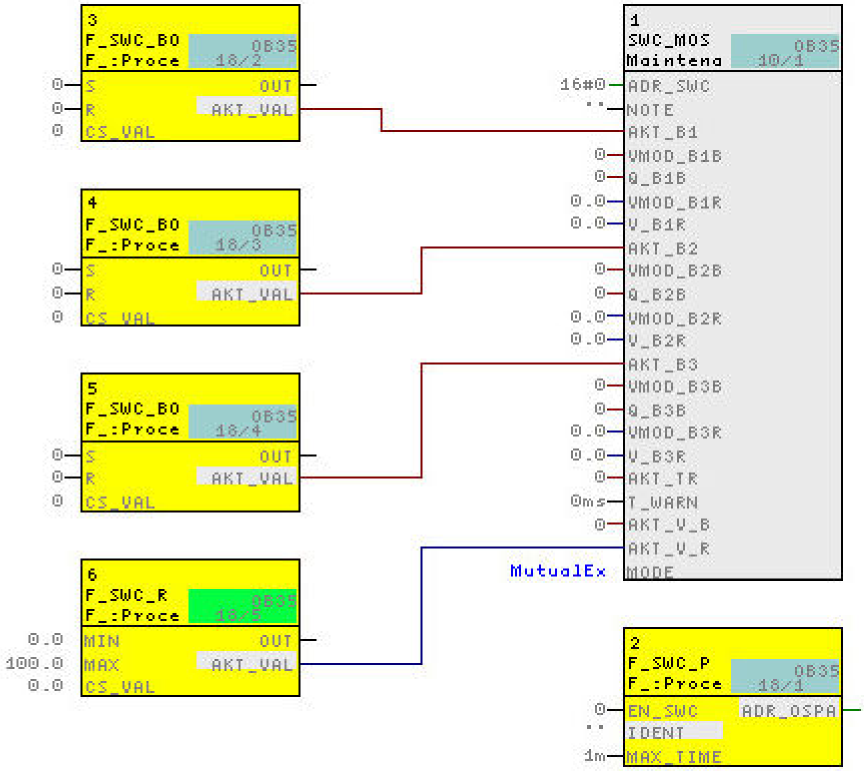
F_SWC_BO

F_SWC_R

FSW-035

1. Place the SWC_MOS block in your CFC chart.
   Observe the information on assigning names in section "SWC_MOS: Command function for Maintenance Override (Page 326)".
2. Place the F-block F_SWC_P, if necessary.
   Optional:
   If you place multiple protocol blocks F_SWC_P per shutdown group so that multiple simultaneous operator inputs are possible from the OS, connect the ADR_OSPA output of F_SWC_P to the ADR_SWC input of the associated operator control block SWC_MOS. This interconnection is not required when simultaneous operator inputs per shutdown group are not needed. You can find additional information on this in section "Introduction (Page 135)".
3. Place 2 or 3 F-blocks F_SWC_BO that will start and stop the simulation.
4. If required, place an F-block F_SWC_BO or F_SWC_R that will change the simulation value.
5. Connect the EN_SWC input of the F-block F_SWC_P to a keyswitch.
6. Assign the maximum duration of the operator input (default setting is 1 minute) at the MAX_TIME input of the F-block F_SWC_P.
7. Connect the outputs of the F-blocks F_SWC_BO that will start and stop the simulation:
   – Connect OUT to the SIM_ON inputs of the associated F-channel drivers
   – Connect AKT_VAL to the AKT_Bx inputs of the SWC_MOS block
8. Connect the outputs of the F-block F_SWC_BO or F_SWC_R that will change the simulation value:
   – Connect OUT to the SIM_I and SIM_V inputs of the F-channel drivers
   – Connect AKT_VAL to the AKT_V_B or AKT_V_R input of the SWC_MOS block
9. Assign the MODE = 'MutualExclBypass' input of the SWC_MOS block in order to activate the mutual interlock.
10. Optional:
    Assign a low limit and high limit for the fail-safe value (default setting 0.00 and 100.0, respectively) for the MIN and MAX inputs of the F-block F_SWC_R. Assign the CS_VAL input of the F-block F_SWC_R, if necessary.

11. Optional:
    If you want to display the current value of an F-I/O in the faceplate when the bypass is activated, connect the following outputs to the F-channel driver:
    – Output Q_MOD or V_MOD on the F-channel driver with the V_MOD_BxB or V_MOD_BxR input on the SWC_MOS block
12. Optional:
    If you want to have the process value and its QUALITY displayed for the F-channel driver in the faceplate, connect the following outputs of the F-channel driver:
    – Q_DATA or V_DATA output to the Q_BxB or V_BxR input of the SWC_MOS block.
    – QUALITY output to the QUAL_Bx input of the SWC_MOS block
13. Compile your CFC chart.
    Additional connections between the SWC_MOS block, the F-blocks F_SWC_BO or F_SWC_R, F_SWC_P and the F-channel drivers are created during compilation.



14. Follow the procedure as described in section "Configuring the faceplate of the operator functions (Page 149)".

10.4.2.6 Application case: Time-triggered maintenance override

Application

This application case shows you how to create a time-controlled "Maintenance Override".

Procedure

⚠ WARNING

Warnings in the descriptions of the F-blocks

Observe the warnings in the descriptions of the following F-blocks.

F_SWC_CB

F_SWC_CR

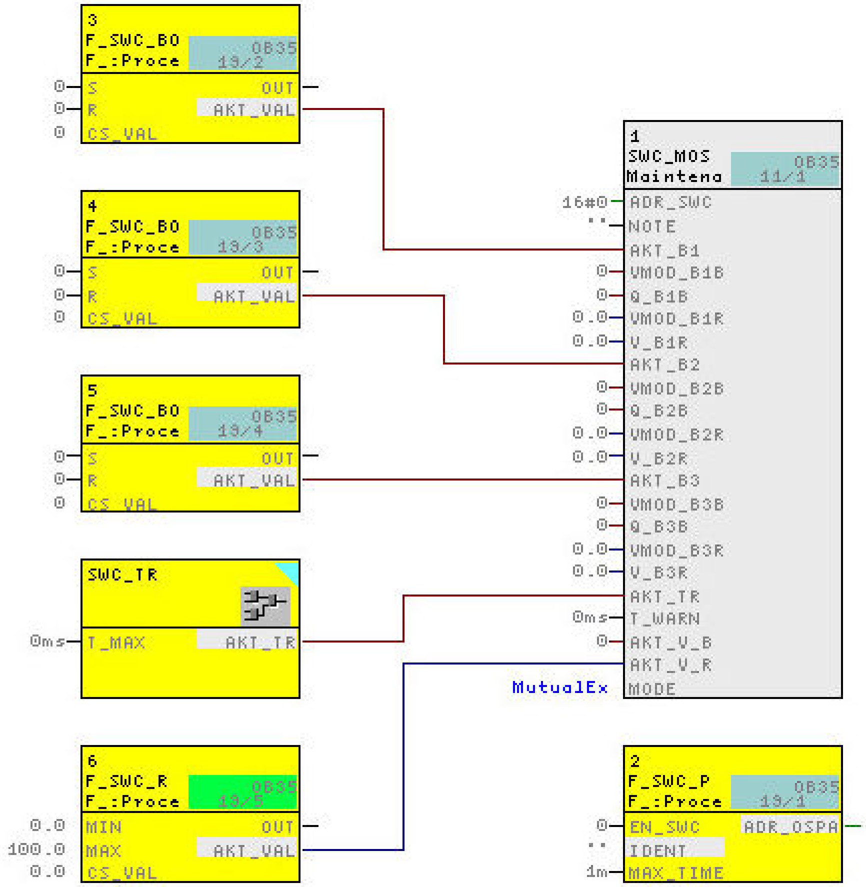
F_SWC_BO

F_SWC_R

FSW-035

1. Place the SWC_MOS block in your CFC chart.
   Observe the information on assigning names in section "SWC_MOS: Command function for Maintenance Override (Page 326)".
2. Place the F-block F_SWC_P, if necessary.
   Optional:
   If you place multiple protocol blocks F_SWC_P per shutdown group so that multiple simultaneous operator inputs are possible from the OS, connect the ADR_OSPA output of F_SWC_P to the ADR_SWC input of the associated operator control block SWC_MOS. This interconnection is not required when simultaneous operator inputs per shutdown group are not needed. You can find additional information on this in section "Introduction (Page 135)".
3. Place one or more F-blocks F_SWC_BO that will start and stop the simulation.
4. Place an F-block F_SWC_BO or F_SWC_R that will change the simulation value.
5. Place the Chart-in-Chart SWC_TR.
   Assign the "reset time" (default setting = 0 ms) at the T_MAX input.
6. Connect the EN_SWC input of the F-block F_SWC_P to a keyswitch.
7. Assign the maximum duration of the operator input (default setting is 1 minute) at the MAX_TIME input of the F-block F_SWC_P.
8. Connect the outputs of the F-blocks F_SWC_BO that will start and stop the simulation:
   – Connect OUT to the SIM_ON inputs of the associated F-channel drivers
   – Connect AKT_VAL to the AKT_Bx inputs of the SWC_MOS block
9. Connect the outputs of the F-block F_SWC_BO or F_SWC_R that will change the simulation value:
   – Connect OUT to the SIM_I and SIM_V inputs of the F-channel drivers
   – Connect AKT_VAL to the AKT_V_B or AKT_V_R input of the SWC_MOS block
10. Connect the AKT_TR output of the "Chart-in-Chart" block SWC_TR to the AKT_TR input of the SWC_MOS block.
11. Optional:
    Assign a low limit and high limit for the fail-safe value (default setting 0.00 and 100.0, respectively) for the MIN and MAX inputs of the F-block F_SWC_R. Assign the CS_VAL input of the F-block F_SWC_R, if necessary.

12. Optional:
    Assign the prewarning time for the automatic reset of the active bypasses (default setting = 0 ms) at the T_WARN input of the SWC_MOS block.
13. Optional:
    Set the MODE = 'MutualExclBypass' input of the SWC_MOS block in order to activate the mutual interlock.
14. Optional:
    If you want to have the current value of an F-I/O displayed in the faceplate when a bypass is activated, connect the Q_MOD or V_MOD output of the F-channel driver to the V_MOD_BxB or V_MOD_BxR input of the SWC_MOS block.
15. Optional:
    If you want to have the process value and its QUALITY displayed for the F-channel driver in the faceplate, connect the following outputs of the F-channel driver:
    – Q_DATA or V_DATA output to the Q_BxB or V_BxR input of the SWC_MOS block.
    – QUALITY output to the QUAL_Bx input of the SWC_MOS block
16. Compile your CFC chart.
    Additional connections between the SWC_MOS block, the F-blocks F_SWC_BO or F_SWC_R, F_SWC_P and the F-channel drivers are created during compilation.



17. Follow the procedure as described in section "Configuring the faceplate of the operator functions (Page 149)".

10.4.2.7 Application case: Fail-safe acknowledgment

Application

This application case shows you how to perform a "Fail-safe acknowledgement" for a channel driver with the SWC_QOS block.

Core statement

⚠ WARNING

Warnings in the descriptions of the F-blocks

Observe the warnings in the descriptions of the following F-blocks.

F_SWC_CB

F_SWC_CR

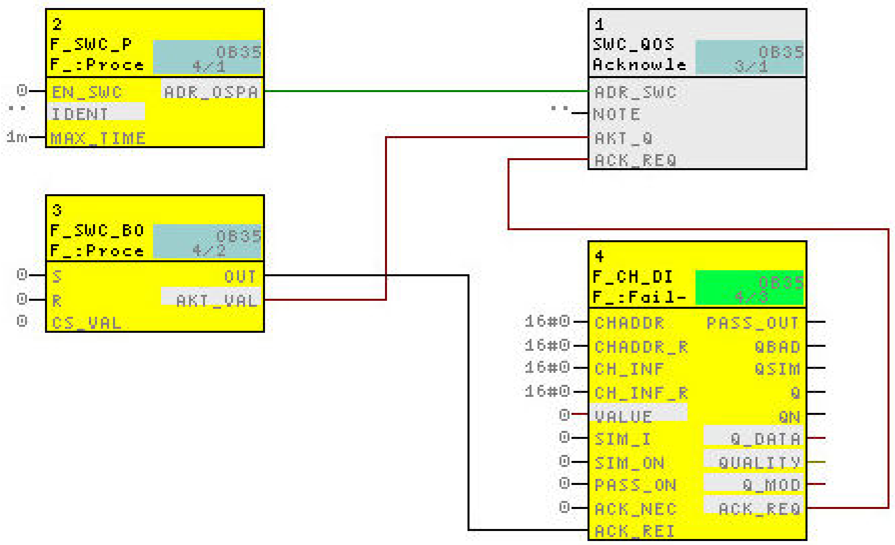
F_SWC_BO

F_SWC_R

FSW-035

1. Place the SWC_QOS block in your CFC chart.
   Observe the information on assigning names in section "SWC_QOS: Operator function for fail-safe acknowledgment (Page 328)".
2. Place the F-block F_SWC_P, if necessary.
   Optional:
   If you place multiple protocol blocks F_SWC_P per shutdown group so that multiple simultaneous operator inputs are possible from the OS, connect the ADR_OSPA output of F_SWC_P to the ADR_SWC input of the associated operator control block SWC_QOS. This interconnection is not required when simultaneous operator inputs per shutdown group are not needed. You can find additional information on this in section "Introduction (Page 135)".
3. Place one F-block F_SWC_BO and F_CH_DI each.
4. Connect the EN_SWC input of the F-block F_SWC_P to a keyswitch.
5. Assign the maximum duration of the operator input (default setting is 1 minute) at the MAX_TIME input of the F-block F_SWC_P.
6. Connect the outputs of the F-block F_SWC_BO:
   - Connect OUT to the ACK_REI input of the F-block F_CH_DI
   - Connect AKT_VAL to the AKT_Q input of the SWC_QOS block
7. Connect the ACK_REQ output of F-block F_CH_DI to the ACK_REQ input of block SWC_QOS.
8. Before compiling, check the assignment of the SWC_QOS block. The block must be assigned to a standard runtime group.

9. Compile your CFC chart.
   Additional connections between the SWC_QOS block, the F-blocks F_SWC_BO and F_SWC_P are created during compilation.



10. Follow the procedure as described in section "Configuring the faceplate of the operator functions (Page 149)".

10.4.3 Configuring the faceplate of the operator functions

A faceplate is created in the OS for each instance of an operator control block, e.g. SWC_MOS, in the safety program. The operator steps for "Secure Write Command++" are performed in the required sequence by one or two operators on the faceplate. The corresponding faceplate is called up in the OS via the associated block icon.

Requirements

- Placement, parameter assignment and interconnection of all required F-blocks, such as F_SWC_R, F_SWC_BO, in the CFCs is complete.
  For more information, refer to section "Placement, parameter assignment and interconnection of F-blocks in the CFC (Page 135)".
- The CFCs with F-blocks for the desired operator function are located in the plant hierarchy.

Overview configuration of the faceplates

Configure the faceplates for the required operating function, e.g. "Maintenance Override", in the engineering system with the following steps:

1. Creating block icons
2. Initializing properties of the block icons

3. Setting up authorizations for operators
4. Transferring configuration to the OS

The individual steps are described below.

Creating block icons

1. Open the PCS 7 project in SIMATIC Manager.
2. Create a new picture object in the level of the plant hierarchy containing the CFC charts with the F-blocks of the desired operator function.
3. Select the OS object in the project and select "Compile" from the shortcut menu to compile the OS.
   Press the "Compile" button in the last dialog.

Result: When the OS is compiled, the block icons are automatically inserted in the new picture.

Initializing properties of the block icons

1. Double-click the picture file in the plant view of the PCS 7 project.
   Result: WinCC Explorer is started and the picture file is displayed in the Graphics Designer. The name is displayed in the header of each block icon. The name of the block icon is formed from the name of the CFC chart and the name of the associated F-block instance.
2. Select a block icon and open the object properties.
3. Select the "Configurations" entry in the "Properties" tab.
4. Assign the desired authorizations to the "LevelInitiate", "LevelConfirm", "LevelBypass" and "LevelBypassValue attributes.
   - The "LevelInitiate" and "LevelConfirm" attributes apply to the operator functions “Change process values", "Maintenance Override" and "Fail-safe acknowledgment".
   - The "LevelBypass" and "LevelBypassValue" attributes apply to the operator function "Maintenance Override".

   Alternatively, you can accept the default authorizations for operators. For more information on this, refer to the "Setting up user authorizations for operators" section below.
   Default authorizations (correspond to the user hierarchies from PCS 7):
   - For the operator that initiates a bypass or fail-safe value change with Maintenance Override (Initiator): No. 5, "Process controlling"
   - For the operator that initiates only a bypass with Maintenance Override (Bypass): No. 5, "Process controlling"
   - For the operator that initiates a fail-safe value change with Maintenance Override (BypassValue): No. 5, "Process controlling"
   - For the operator that confirms the bypass and a fail-safe value change with Maintenance Override (Confirmer): No. 6, "Higher process controlling"
5. Repeat Steps 2 and 4 for all block icons present.
6. Save the picture file.

Setting up user authorizations for operators

An operator function is performed by two operators. For this purpose, create two users.

- The "Initiator" initiates the operator input, e.g. the bypass and/or the setting of bypass values in the case of "Maintenance Override".
- The "Confirmer" confirms this operator input.

Alternatively, the two steps can also be performed by only one operator. For this, create a user that has both "Initiator" and "Confirmer" authorizations.

Create the users with the following authorizations in WinCC Explorer using the "User Administrator" editor.

- For the "Maintenance Override" function

User	Action	Required authorizations			
		Initiate	Confirm	Bypass	BypassValue
Initiator	Set bypasses	X	—	X	—
	Set bypass values	X	—	—	X
	Set bypasses and bypass values	X	—	X	X
Confirmer	Confirm bypasses	—	X	X	—
	Confirm bypass values	—	X	—	X
	Confirm bypasses and bypass values	—	X	X	X
Initiator & Confirmer	Set and confirm bypasses	X	X	X	—
	Set and confirm bypass values	X	X	—	X
	Set and confirm bypasses and bypass values	X	X	X	X

- For the "Change process values" function

User	Action	Required authorizations	
		Initiate	Confirm
Initiator	Change value	X	—
Confirmer	Confirm value change	—	X

- For the "Fail-safe acknowledgment" function

User	Action	Required authorizations	
		Initiate	Confirm
Initiator	Change value	X	—
Confirmer	Confirm value change	—	X

Activating the OS

Activate the WinCC Runtime system of the OS, e.g. by selecting **File > Activate** in WinCC Explorer.

Result

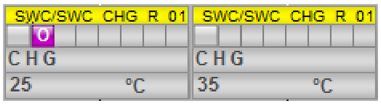
After activation, the hierarchy levels appear as buttons in the runtime system of the OS. Click the button to display the block icons for this level.

Example

The following figures show two block icons in the runtime system of the OS, dependent on the operator function.

Clicking a block icon opens the faceplate.

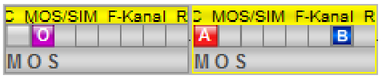
- Operator function "Change process values"

  You can change F-parameters in the safety program. The successful change is visible from the changes in the last line.
  The following symbol in the block icon indicates "Acknowledgment request is active".

  O

- Operator function "Maintenance Override"

  You can use "Maintenance Override" to establish a bypass of the F-channel drivers for maintenance work.
  The following symbols appear in the block icon:

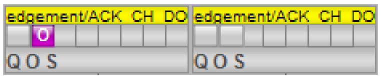
  – "Acknowledgment request is active"

    O

  – "Bypass active"

    B

- Operator function "Fail-safe acknowledgment"

  In the block icon, the following symbol signals "Acknowledgment request is active".

  O

Note

The "Acknowledgment request is active" function ("O" symbol) is only supported as of F Systems Library V1.3 SP3.

Detailed information

For detailed information on the described steps, refer to:

- "PCS 7 Operator Station (https://support.industry.siemens.com/cs/ww/en/view/90682677)" configuration manual
- Online help for the WinCC Editors, e.g. Graphics Designer and User Administrator

10.4.4 Integrating an operator function in an existing project

Introduction

You can also integrate an operator function such as "Maintenance Override" in an existing project.

Requirement

In order to integrate the operator function in an existing project, you must update your project.

Updating an existing project

1. Launch WinCC Explorer for the OS contained in the project.
2. Open the OS Project Editor.
3. Select the "Basic Data" tab.
   If pictures from S7 F Systems HMI (picture "@PCS7Typicals_S7F_SDW.PDL" and all pictures "@PG_SWC_x.PDL") are already present in the project in the "Accept picture modules from the libraries" area, select these.
   User-specific changes in these screens are lost.
4. Make sure that all other settings in the OS Project Editor conform to your specifications.
5. Then click the "OK" button.
   The project is reconfigured and, as a result, the new block icons and the new pictures are applied.
6. Open the Global Script C Editor and select the menu command "Options > Regenerate Header".

Integrating an operator function

In order to introduce the new block icons into existing plant pictures, you must re-compile the relevant project.

1. Start the SIMATIC Manager, navigate to the desired OS object and then continue in the hierarchy until the corresponding picture objects are displayed.
2. Make sure that the "Derive block icons from the plant hierarchy" option is selected in the "Block icons" tab of the object properties for the relevant picture object. (This is the default setting with PCS 7.)
3. Select the OS object in the navigation window and select the menu command "Compile" from the shortcut menu. The "Wizard: Compile OS" dialog box opens.
4. Click the "Compile" button in the last step of the wizard.

Result

Once you have performed these steps, your project will contain the new block icons of the operator functions and the necessary pictures.

Note

If user settings for the block icon of an operator function are to be retained during a subsequent OS compilation of an existing picture, you must clear the "Derive block icons from the plant hierarchy" option for this WinCC picture.

10.5 Executing operator functions

10.5.1 Requirements and general notes

You carry out an operator input for a parameter in the OS by means of a faceplate. The operator input consists of a sequence of operations that can be performed by one or two operators.

Requirements

- The S7 program is compiled and downloaded to the F-CPU.
- The user(s) with the relevant authorizations are set up.
- The configuration of the faceplates is compiled and downloaded to the OS.
- When using OS clients, make sure that no default server is set for tags (in WinCC Explorer select "Server Data," in the shortcut menu select "Default Server" and in the "Configure Default Server" dialog for the "Tags" component select "No Default Server").

General information

WARNING

Initiator and confirmer must not accept an invalid value

Before starting the transaction, you must verify the following values in the faceplate:

- The technological name in the header of the faceplate.
- The name contained in the "ID" field (HID of the CPU or value of the "IDENT" parameter of the F_SWC_P).
- The "Tag name".

As the initiator or confirmer, you must not accept an invalid value. If there are inconsistencies, you must cancel the operation. As an operator, you must not rely on individual display fields of the faceplate; rather, you must check the values and compare them with each other.

FSW-037

WARNING

Technological assignment must be appropriate for the environment

When opening the faceplate, make sure that the technological assignment in the top line is appropriate for the environment in which the block icon was placed.

FSW-038

⚠ WARNING

Transaction for changing an F-Parameter

You can only perform one transaction for changing an F-Parameter at a time. You must use organizational measures to ensure that multiple transactions are not performed simultaneously for the same F-parameter. Otherwise, the transaction cannot be performed correctly, resulting in unexpected results, such as:

- Display of incorrect values in the faceplate fields
  Or
- Unexpected cancellation of the transaction

FSW-039

If an operation is already active

If an operation for another faceplate is already in progress, the message "Other command function active" appears when opening the faceplate in WinCC Runtime.

Note

The message "Other operator function active" appears when two operator control blocks are assigned to the same protocol block and both want to perform an operator input at the same time.

Starting from S7 F Systems V6.2, multiple operator functions can be executed simultaneously. You can find additional information in section "Introduction (Page 135)" in paragraph "Multiple protocol blocks in a shutdown group".

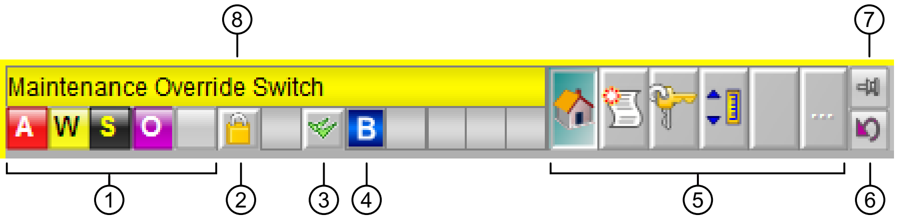
10.5.2 Operating and display bar of the faceplates

Introduction

In faceplates used for SWC++, the so-called operating and display bar is located at the top.

Display and operator controls

The figure below shows an example of an operator control bar and display bar for a faceplate: The display of the symbols depends on the current status and the function.



The faceplate provides the following display and operator controls:

(1) Group display

(2) Lock/unlock messages

(3) Acknowledge messages

(4) Status of bypass

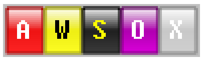
(5) Open views of the block

(6) Back to block icon

(7) Pin faceplate

(8) Name of the faceplate

(1) Group display



The group display shows the following information:

- Alarms (A)
- Warnings (W)
- Faults (F)
- Operator requests (O)

(2) Lock/unlock messages

The "Lock/unlock messages" button is used to lock or release the triggering of messages directly in the automation system.

- "Enable messages"

- "Lock messages"

(3) Acknowledge messages

You can acknowledge all messages for the block instance using this button.

✓

(4) Status of bypass

This symbol shows the status for a bypass.

- "Bypass active"

  B

- "Bypass inactive"

  □

(5) Calling the views of a block

Use this area to open the various views of the faceplate.

Left-clicking shows the view in the same window. A right-click opens a new window.

You can select the following views here:

Symbol	Identifier
🏠	Standard view This view shows the operations for the functions of SWC++, e.g. initialization, acknowledgment
📜	Alarm view This view displays the current messages.
🔑	Operator authorization levels This view displays information about the operating authorizations of the current user.
↕	Limit view This view displays information about the current limits.
...	Additional views If other views are available, the button can be selected.

Note

If views are not selectable, the buttons are disabled.

(6) Back to block icon

Use this button to return to the block icon in the process picture of the corresponding faceplate. You can use this function when you have pinned a faceplate and then switched to a process picture, for example.

(7) Pin faceplate

You can pin a faceplate on top of the user interface using this button. This allows you to change to another picture or area without closing the faceplate.

(8) Name of the faceplate

This area displays the name of the faceplate.

10.5.3 Use of operator function "Change process value" with two operators

Operator authorizations

To change a process value, two operators having different authorizations are required.

- The Initiator initiates the process value change. The authorization corresponds to the "InitiatorAuthorization" attribute in the properties of the block icon. The default setting is No. 5, "Process controlling".
- The Confirmer verifies and confirms the change. This operator must have the necessary authorization for confirming the change but not for initiating it. The authorization corresponds to the "ConfirmerAuthorization" attribute in the properties for the block icon. The default setting is No. 6, "Higher process controlling".

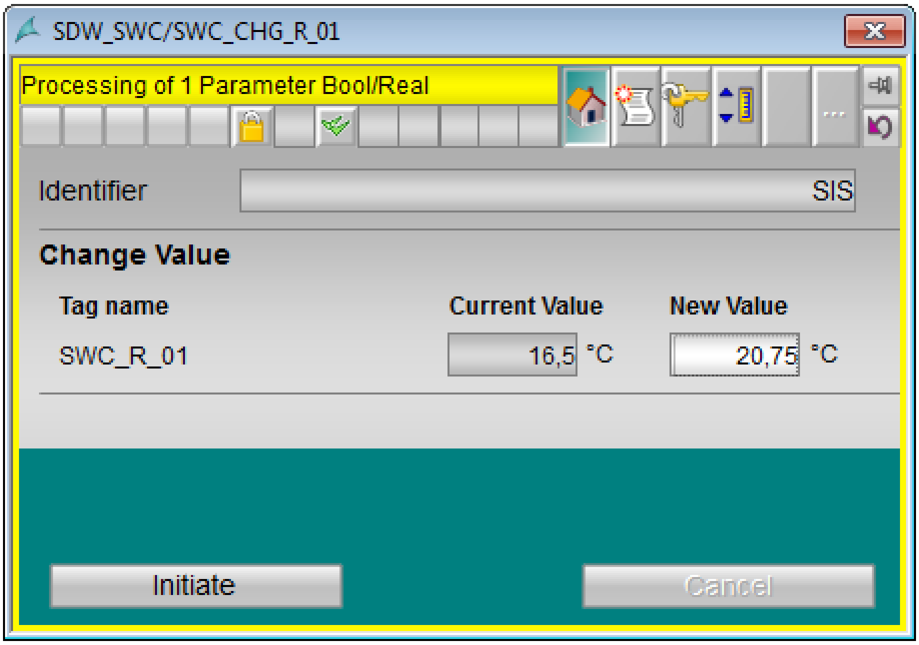
Note

The sections below describe the necessary operator input steps for the two operators. The figures show the example of an F_REAL parameter with the operator identifiers (Login):

- level5 – Initiator
- level6 – Confirmer

Initiator: Initiate value change

1. Log on to the OS as a user with "Initiator" authorization.
2. Click the desired block icon to open the faceplate.



SDW_SWC/SWC_CHG_R_01

Processing of 1 Parameter Bool/Real

Identifier SIS

Change Value

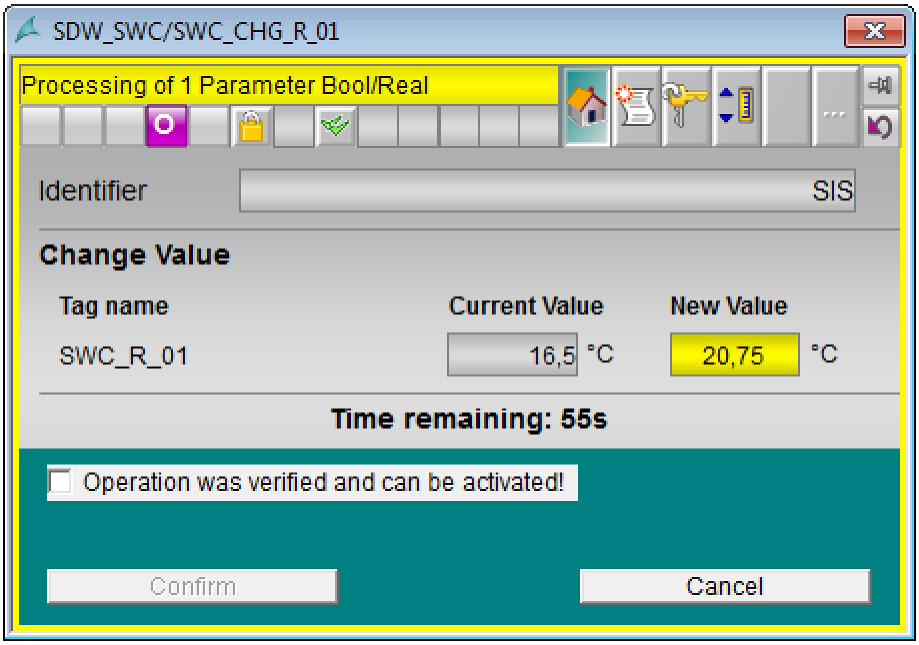
Tag name	Current Value	New Value
SWC_R_01	16,5 °C	20,75 °C

   You can check the authorization of the logged on operator in the "User rights" view of the faceplate, which is opened by the button of the same name in the toolbar.

3. To perform a value change, enter the desired value in the "New value" text box and confirm the input by pressing the <Enter> key. If you are changing an F_REAL value, the configured "MIN", "MAX" and "MAXDELTA" values are evaluated.
   You can check the current limits in the "Limits" view of the faceplate, which is opened by the button of the same name in the toolbar.
4. Click the "Initiate" button.
   The Confirmer must then continue the operator input. If you cancel the operator input after pressing the "Initiate" key, check whether the previously valid value is displayed in the "Current value" field.

Confirmer: Confirm value change

1. Log on to the OS as a user with "Confirmer" authorization.
   You can log on to a second OS or on the same OS as the Initiator.
2. Click the desired block icon to open the faceplate.



SDW_SWC/SWC_CHG_R_01

Processing of 1 Parameter Bool/Real

Identifier: SIS

Change Value

Tag name	Current Value	New Value
SWC_R_01	16,5 °C	20,75 °C

Time remaining: 55s

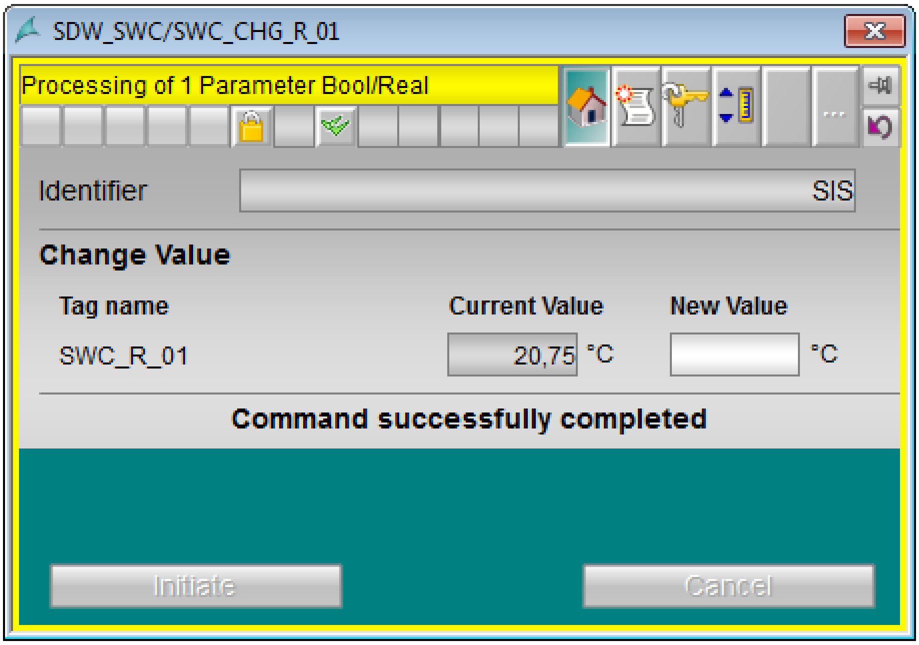
□ Operation was verified and can be activated!

   The faceplate has the "O" symbol to indicate that acknowledgment is required.
   You can check the authorization of the logged on operator in the "User rights" view of the faceplate.

3. Verify that:
   – The right operator control block was selected (technological name in the header of the faceplate).
   – The right F-CPU was selected (for identifier, refer to section "F_SWC_P: Centralized control of operator input via the OS (Page 299)").
   – The right parameter is to be changed (tag name).
   – The change (modified value) is displayed correctly.
   – New values of the changed parameters are highlighted in yellow under "New value".
4. Confirm the change with "Operation was verified and can be activated!" or cancel the operator input with the "Cancel" button.
5. Press the "Confirm" button to activate the value change. Click "Cancel" to cancel the operation.

Result

The successful value change is signaled. The entry in the "New value" text box has been applied to the field under "Current value".



Processing of 1 Parameter Bool/Real

Identifier: SIS

Change Value

Tag name	Current Value	New Value
SWC_R_01	20,75 °C	°C

Command successfully completed

See also

Operating and display bar of the faceplates (Page 156)

10.5.4 Use of operator function "Change process value" with one operator

Authorization for the operator

If the "Change process value" operator input is performed by only one operator, this operator must have the "Initiator" and "Confirmer" authorizations.

For this purpose, create an operator assigned the "LevelInitiate" and "LevelConfirm" levels in the properties of the block icon. Further information on this can be found in section "Configuring the faceplate of the operator functions (Page 149)".

Changing process values with only one operator

The sequence is the same as when the operation is carried out with two operators, but one operator can perform all the steps (see also section "Use of operator function "Change process value" with two operators (Page 159)").

The difference is that there is no longer a wait for the Confirmer. Instead, the operator can verify and confirm the operator input immediately after pressing the "Initiate" button.

All other steps remain the same.

10.5.5 Use of operator function "Maintenance Override" with two operators

Operator authorizations

The "Maintenance Override" operator function allows you to set bypasses in the safety program from the OS.

Two operators having different authorizations are required to create a bypass.

- The Initiator initiates the bypass of the F-channel driver. This operator must have the "LevelInitiate", "LevelBypass" and "LevelBypassValue" authorizations for initiating the bypass but not for confirming it.
- The Confirmer verifies and confirms the change. This operator must have the required "LevelConfirm", "LevelBypass" and "LevelBypassValue" authorizations for confirming the change but not for initiating it.

Reset time

If you have configured a retrigger function in the CFC chart, the simulation is only active for the time configured at the T_MAX input of the chart-in-chart block SWC_TR. As the Initiator, if you click the "Retrigger" button while the configured reset time is running, the reset time restarts with the configured time after the change is confirmed by the Confirmer.

Quality of the process value on the F-Channel driver

The quality of the process value on the F-Channel driver is indicated in the faceplate by the following symbols:

Symbol	State	Quality code
No symbol	Valid value	16#80
🖐	Simulation	16#60
🔧	SUBSTITUTION VALUE Last valid value Invalid value (F-STOP)	16#48 16#44 16#00

See also section "F-Channel drivers for F-I/O (Page 330)".

Value on the F-Channel driver

If the V_MOD_Bx inputs are interconnected on the SWC_MOS block, the values on the F-Channel drivers are displayed under V_MOD.

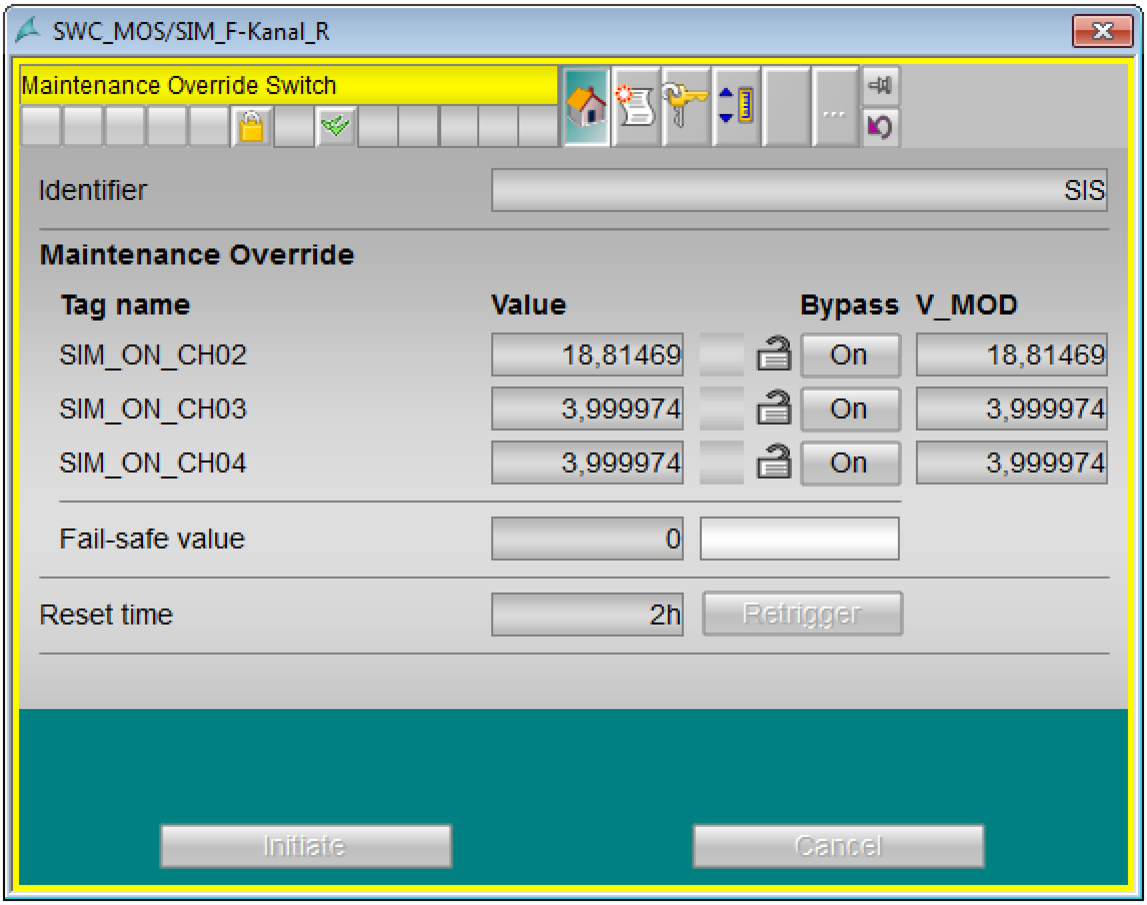
Note

The sections below describe the necessary transaction steps for the two operators. The figures show the example of an F_REAL parameter with the operator identifiers (Login):

- level5 – Initiator
- level6 – Confirmer

Initiator: Initiating a bypass

1. Log on to the OS as a user with "Initiator" authorization.
2. Click the desired block icon to open the faceplate.



SWC_MOS/SIM_F-Kanal_R

Maintenance Override Switch

Identifier: SIS

Maintenance Override

Tag name	Value	Bypass	V_MOD
SIM_ON_CH02	18,81469	🔓 On	18,81469
SIM_ON_CH03	3,999974	🔓 On	3,999974
SIM_ON_CH04	3,999974	🔓 On	3,999974

Fail-safe value: 0

Reset time: 2h Retrigger

You can check the authorization of the logged on operator in the "User rights" view of the faceplate, which is opened by the button of the same name in the toolbar.
Under "Value" on the Maintenance Override faceplate, you can see the current process value of the F-I/O and the current fail-safe value setting. The values on the F-Channel drivers are displayed in the V_MOD column.
The symbols under "Bypass" show you the current status of the bypass (SIM_ON) on the F-channel drivers:

Symbol	Meaning
□	Bypass not active
B	Bypass active
🔓	A bypass can be created for this F-Channel driver.
🔒	For this F-Channel driver, either a bypass cannot be created (mutually exclusive interlock) or the user authorization is insufficient.

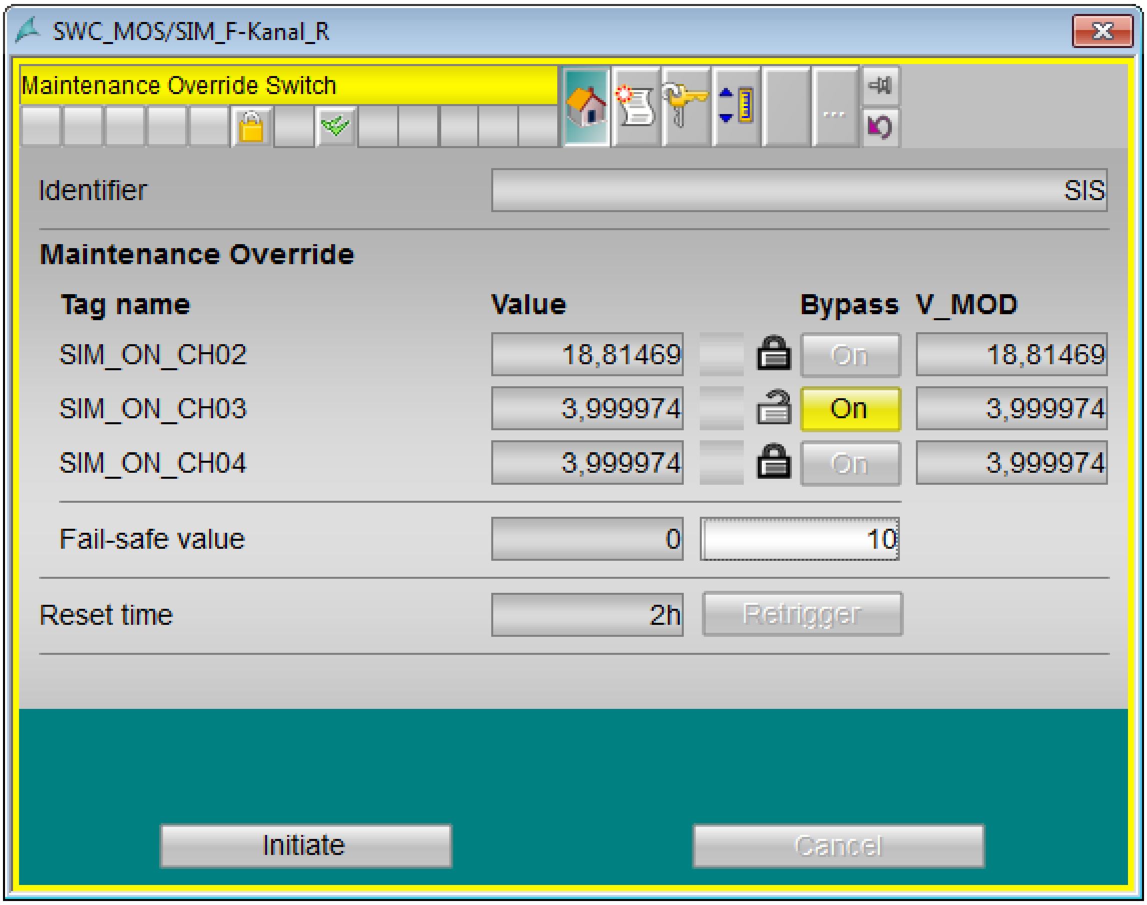
3. To enable a bypass for one or more F-channel drivers, press the corresponding button under "Bypass".

4. If the input setting MODE = 'MutualExclBypass' has been assigned on the SWC_MOS block, the remaining F-Channel drivers are interlocked when a bypass is enabled. The interlocked F-channel drivers are indicated by the following symbol.

   🔒

5. If you want to change the current fail-safe value on F-channel drivers for F_BOOL, press the button under "Bypass".
   If you are using F-channel drivers for F_REAL and want to change the fail-safe value, enter the new fail-safe value in the text box and confirm your input with the <Enter> key. The configured "MIN" and "MAX" limits are evaluated in the process.
   You can check the current limits in the "Limits" view of the faceplate, which is opened by the button of the same name in the toolbar.

6. If you want to reset the reset time to the configured initial value, click the "Retrigger" button.



SWC_MOS/SIM_F-Kanal_R

Maintenance Override Switch

Identifier: SIS

Maintenance Override

Tag name	Value		Bypass	V_MOD
SIM_ON_CH02	18,81469	🔒	On	18,81469
SIM_ON_CH03	3,999974	🔓	On	3,999974
SIM_ON_CH04	3,999974	🔒	On	3,999974

Fail-safe value: 0 | 10

Reset time: 2h

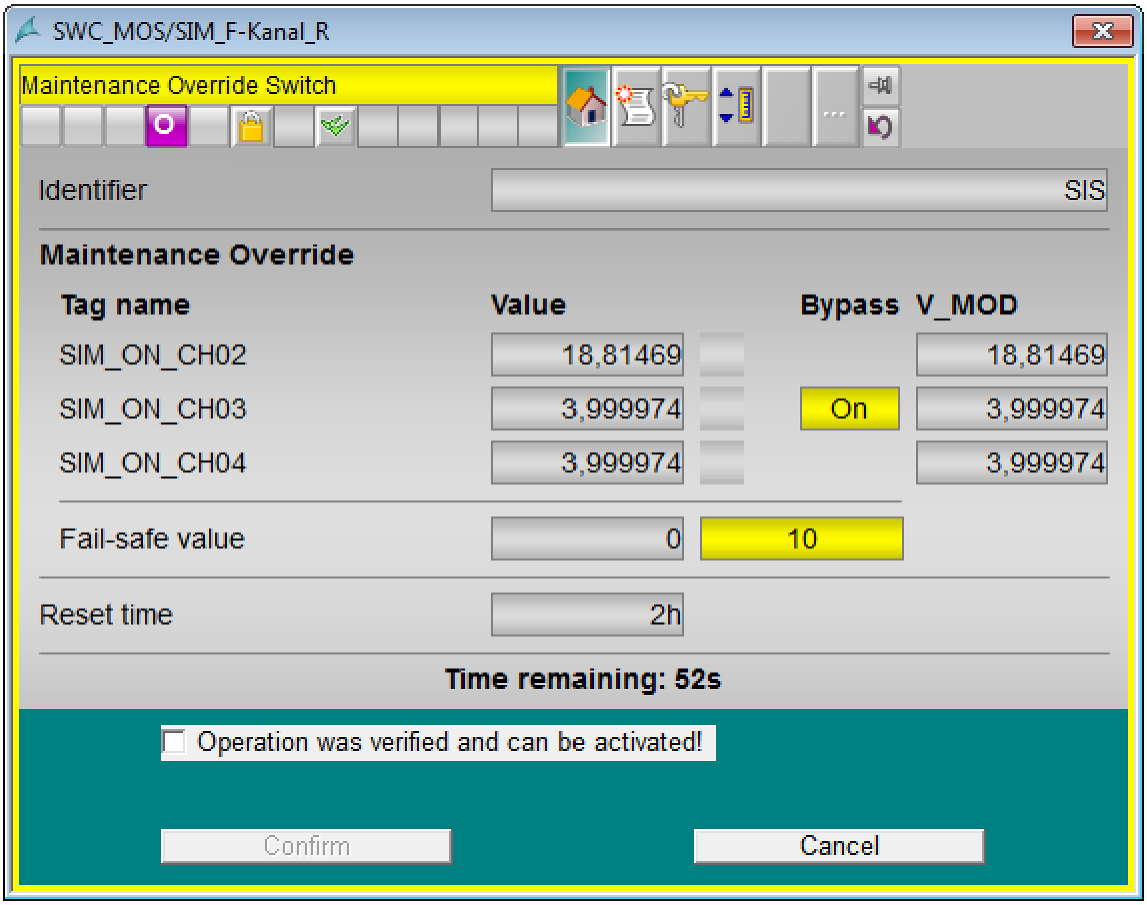
7. Click the "Initiate" button.

The Confirmer must then continue the operator input.

If you cancel the operator input after pressing the "Initiate" button, check whether the previously valid value is displayed in the "Value" field.

Confirmer: Confirming a bypass

1. Log on to the OS as a user with "Confirmer" authorization.
   You can log on to a second OS or on the same OS as the Initiator.
2. Click the desired block icon to open the faceplate.



SWC_MOS/SIM_F-Kanal_R

Maintenance Override Switch

Identifier: SIS

Maintenance Override

Tag name	Value	Bypass	V_MOD
SIM_ON_CH02	18,81469		18,81469
SIM_ON_CH03	3,999974	On	3,999974
SIM_ON_CH04	3,999974		3,999974

Fail-safe value: 0 | 10

Reset time: 2h

Time remaining: 52s

□ Operation was verified and can be activated!

The faceplate has the "O" symbol to indicate that acknowledgment is required.
You can check the authorization of the logged on operator in the "User rights" view of the faceplate.

3. Verify that:
   - The right operator control block was selected (technological name in the header of the faceplate).
   - The right F-CPU was selected (for identifier, refer to section "F_SWC_P: Centralized control of operator input via the OS (Page 299)").
   - The right parameter is to be changed (tag name).
   - The change (modified value) is displayed correctly.
   - New values of the changed parameters are highlighted in yellow under "Bypass".
   - No other fields for new values are highlighted in yellow.

4. Confirm the change with "Operation was verified and can be activated!" or cancel the operator input with the "Cancel" button.
5. Click "Confirm" to enable the bypass. Click "Cancel" to cancel the operation.

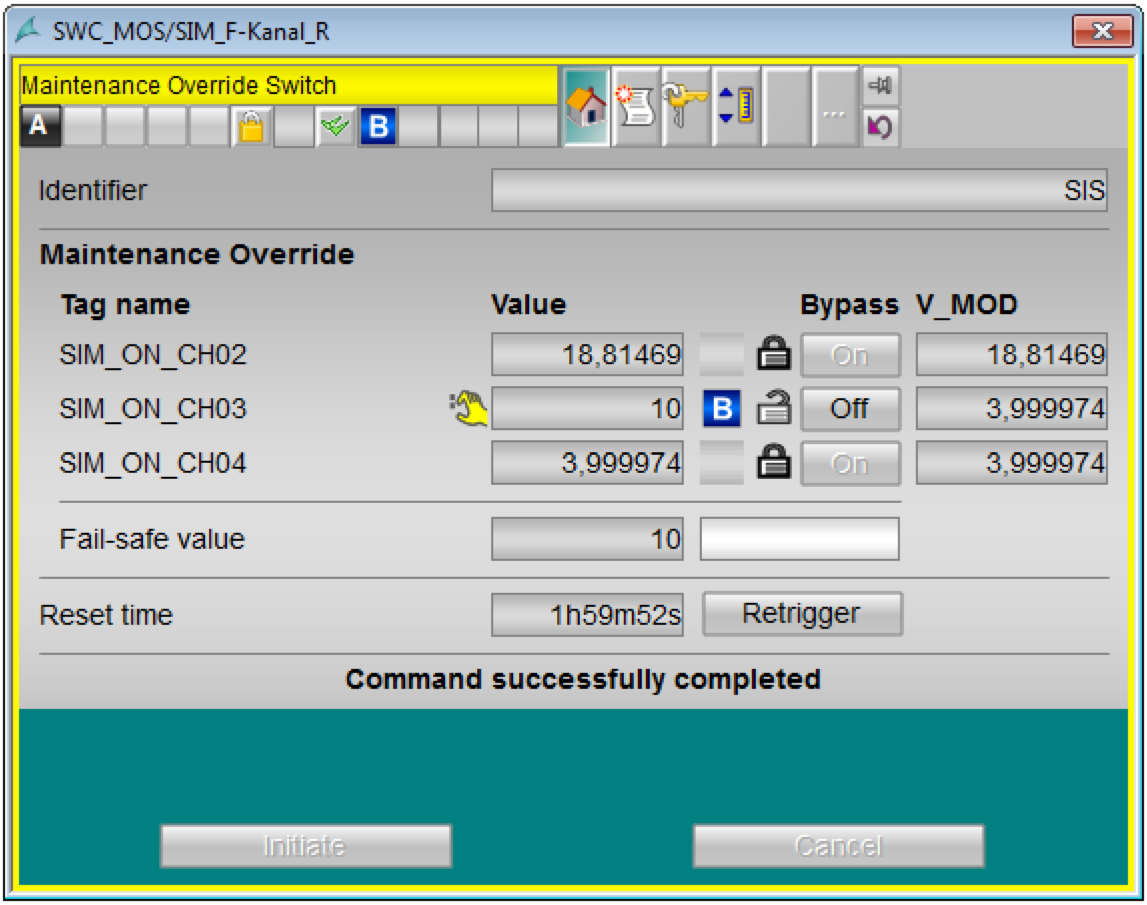
Result

The successful change on the F-Channel drivers is signaled. The F-channel driver for which the bypass was activated is indicated with the following symbol.

B

Depending on the interconnection on SWC_MOS, additional status displays become visible (see section "SWC_MOS: Command function for Maintenance Override (Page 326)").

If you have configured a reset time, the countdown for this time begins. Bypasses are automatically canceled when the reset time has elapsed.



Identifier: SIS

Maintenance Override

Tag name	Value		Bypass	V_MOD
SIM_ON_CH02	18,81469		On	18,81469
SIM_ON_CH03	10	B	Off	3,999974
SIM_ON_CH04	3,999974		On	3,999974

Fail-safe value: 10

Reset time: 1h59m52s

Command successfully completed

See also

Operating and display bar of the faceplates (Page 156)

10.5.6 Use of operator function "Maintenance Override" with one operator

Authorization for the operator

The "Maintenance Override" operator function allows you to set bypasses in the safety program from the OS.

If the bypass of the F-channel driver is implemented by only one operator, this operator must be authorized to both initiate and confirm the bypass.

For this purpose, create an operator assigned the "LevelInitiate", "LevelConfirm", "LevelBypass" and "LevelBypassValue" levels in the properties of the block icon. Further information on this can be found in section "Configuring the faceplate of the operator functions (Page 149)".

Creating a bypass with only one operator

The sequence is the same as when the operation is carried out with two operators, but one operator can perform all the steps (see also section "Use of operator function "Maintenance Override" with two operators (Page 163)").

The difference is that there is no longer a wait for the Confirmer. Instead, the operator can verify and confirm the operator input immediately after pressing the "Initiate" button.

All other steps remain the same.

10.5.7 Use of operator function "Fail-safe acknowledgment" with two operators

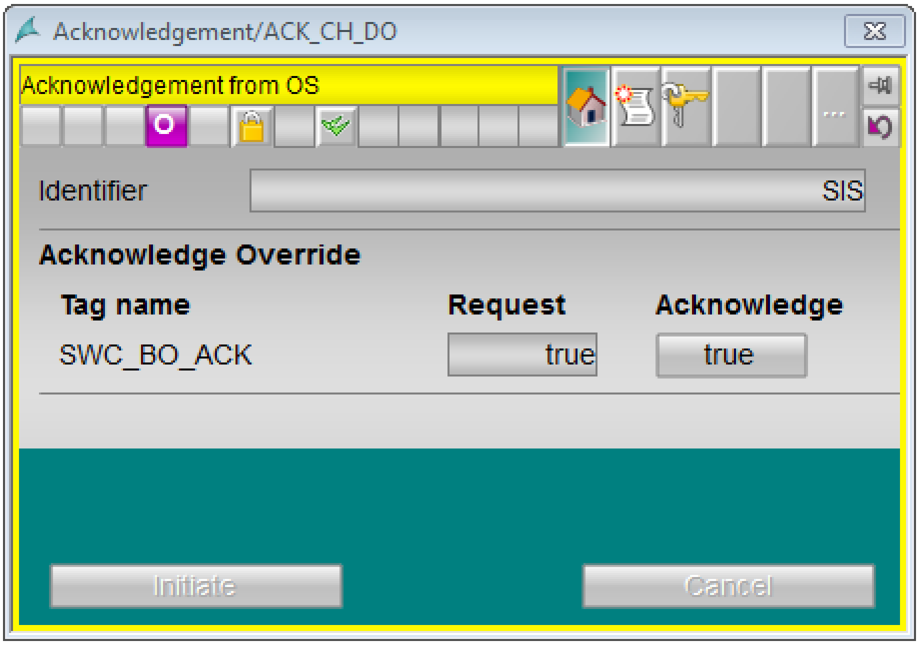
Operator authorizations

The fail-safe acknowledgment requires two operators having different authorizations.

- The Initiator initiates the fail-safe acknowledgment. The authorization corresponds to the "InitiatorAuthorization" attribute in the properties of the block icon. The default setting is No. 5, "Process controlling".
- The Confirmer verifies and confirms the acknowledgment. This operator must have the necessary authorization for confirming the change but not for initiating it. The authorization corresponds to the "ConfirmerAuthorization" attribute in the properties for the block icon. The default setting is No. 6, "Higher process controlling".

Initiator: Initiating a fail-safe acknowledgment

1. Log on to the OS as a user with "Initiator" authorization.
2. Click the desired block icon to open the faceplate.



Acknowledgement/ACK_CH_DO

Acknowledgement from OS

Identifier: SIS

Acknowledge Override

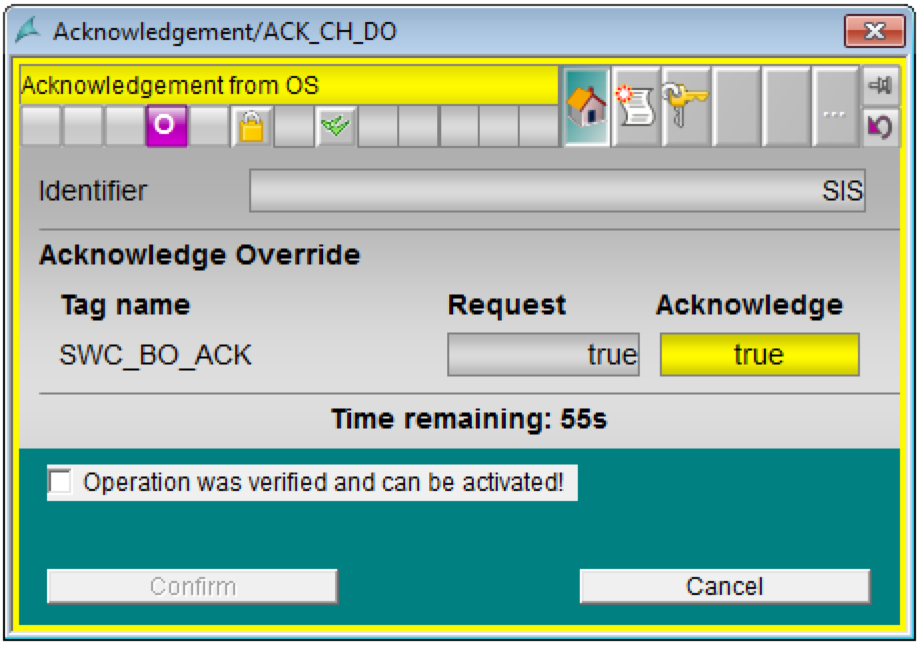
Tag name	Request	Acknowledge
SWC_BO_ACK	true	true

You can check the authorization of the logged on operator in the "User rights" view of the faceplate, which is opened by the button of the same name in the toolbar.

3. To perform a fail-safe acknowledgment, click the button below "Acknowledge". The button background turns yellow.
4. Click the "Initiate" button.
   The Confirmer must then continue the acknowledgment.

Confirmer: Confirming the fail-safe acknowledgment

1. Log on to the OS as a user with "Confirmer" authorization.
   You can log on to a second OS or on the same OS as the Initiator.
2. Click the desired block icon to open the faceplate.



Acknowledgement from OS

Identifier: SIS

Acknowledge Override

Tag name	Request	Acknowledge
SWC_BO_ACK	true	true

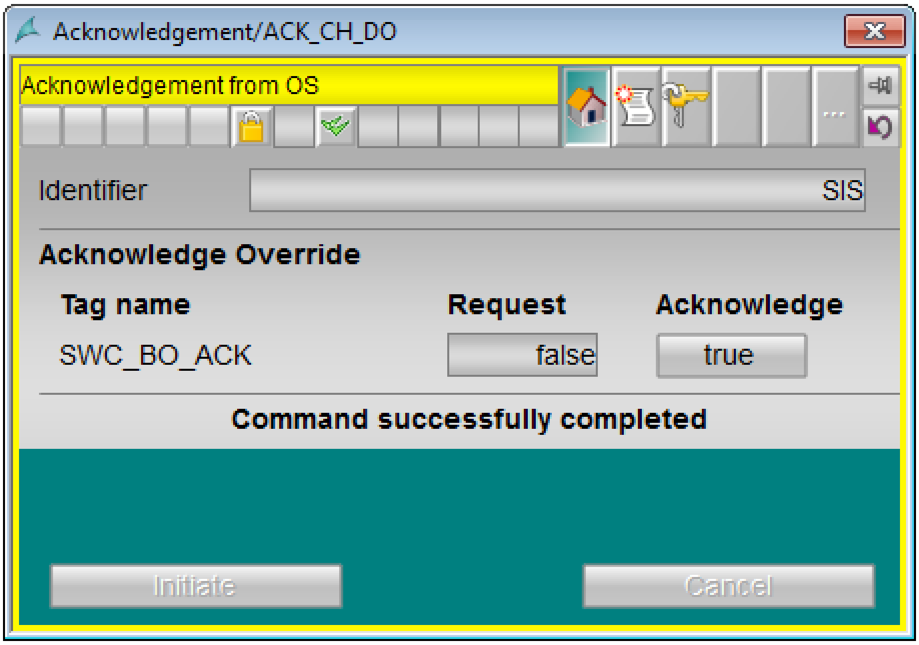
Time remaining: 55s

□ Operation was verified and can be activated!

   You can check the authorization of the logged on operator in the "User rights" view of the faceplate.
3. Verify that:
   - The right operator control block was selected (technological name in the header of the faceplate).
   - The right F-CPU was selected (for identifier, refer to section "F_SWC_P: Centralized control of operator input via the OS (Page 299)").
   - The right parameter is to be changed (tag name).
   - The new value of the changed parameter is highlighted in yellow under "Acknowledge".
4. Confirm the change with "Operation was verified and can be activated!" or cancel the operator input with the "Cancel" button.
5. Press the "Confirm" button to confirm the fail-safe acknowledgment. Click "Cancel" to cancel the operation.

Result

The successful operator input is signaled.



Acknowledgement/ACK_CH_DO

Acknowledgement from OS

Identifier: SIS

Acknowledge Override

Tag name	Request	Acknowledge
SWC_BO_ACK	false	true

Command successfully completed

See also

Configuring the faceplate of the operator functions (Page 149)

Operating and display bar of the faceplates (Page 156)

10.5.8 Use of operator function "Fail-safe acknowledgment" with one operator

Authorization for the operator

If the fail-safe acknowledgment is performed by only one operator, this operator must have the "Initiator" and "Confirmer" authorizations.

For this purpose, create an operator assigned the "LevelInitiate" and "LevelConfirm" levels in the properties of the block icon. Further information on this can be found in section "Configuring the faceplate of the operator functions (Page 149)".

Fail-safe acknowledgment with only one operator

The sequence is the same as when the operation is carried out with two operators, but one operator can perform all the steps (see also section "Use of operator function "Fail-safe acknowledgment" with two operators (Page 169)").

The difference is that there is no longer a wait for the Confirmer. Instead, the operator can verify and confirm the operator input immediately after pressing the "Initiate" button.

All other steps remain the same.

"Safety Data Write": Changing F-parameters from the OS 11

11.1 Safety Data Write concept

Function

The "Safety Data Write" functionality enables safety-related changes to be made to F-parameters in the safety program of an F-CPU from an operator station (OS).

A special safety protocol is used for changing F-parameters during safety mode operation. This ensures compliance with the safety requirements of Safety Integrity Level up to SIL3 in accordance with IEC 61508:2010. The modified F-parameter values can be retained even after a warm restart of S7 F/FH systems.

Note

Use and availability

- Use:
  Instead of the "Safety Data Write" functionality, it is recommended that from S7 F Systems V6.2 and S7 F Systems Lib from V1.3 SP2 onward, the safety-related changing of F parameters in the safety program via the "Change Process Values" operating function of "Secure Write Command++" is used.
  You can find additional information in the section "Concept of "Secure Write Command++" (Page 129)".
- Availability:
  The "Safety Data Write" functionality is available only under SIMATIC PCS 7.

The S7 F Systems optional software offers the following for Safety Data Write:

- Two F-blocks that you must integrate in the CFC charts of your safety program
  - F_CHG_R: Safety Data Write for F-parameters of data type F_REAL
  - F_CHG_BO: Safety Data Write for F-parameters of data type F_BOOL
- The associated faceplates that you must integrate in your OS

Transaction for Safety Data Write

Safety Data Write allows an F-parameter in the safety program of an F-CPU to be changed, provided a certain operating sequence is carried out in the OS within a certain time. The entire change operation is referred to as a "transaction".

Operator Types for Safety Data Write

A transaction can be performed by an individual operator who initiates, verifies, and confirms the change. However, a transaction can also be performed by two operators. One operator (the initiator) initiates the change, and the second (the confirmer) re-enters, verifies, and confirms this value.

11.2 Programming Safety Data Write

11.2.1 Basic procedure

Basic procedure

To perform Safety Data Write via an OS, proceed as follows:

On the engineering station (ES)

1. Insert the blocks F_CHG_R / F_CHG_BO into the CFC and interconnect them.
2. Configure the faceplate for Safety Data Write.

On the operator station (OS)

- Change the F-parameters with Safety Data Write.

The individual steps are described in detail in the sections below.

11.2.2 Positioning, interconnecting, and assigning parameters to F-Blocks in the CFC chart

Application

The F_CHG_R and F_CHG_BO F-blocks allow you to change F-parameters of the safety program using Safety Data Write.

Procedure

⚠ WARNING

Warnings in the descriptions of the F-blocks

Observe the warnings in the descriptions of the F_CHG_R/F_CHG_BO F-blocks.

FSW-040

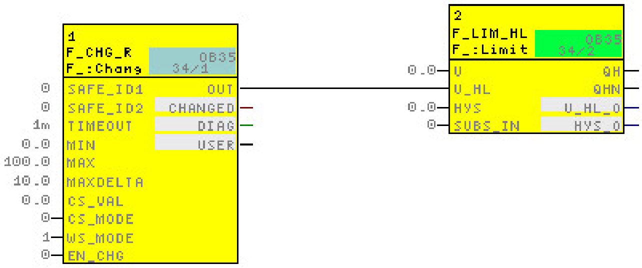
1. Insert one F_CHG_R or F_CHG_BO F-block for each input with the F_BOOL data type that you want to change using Safety Data Write (see Example 1: F_CHG_R (Page 179) or Example 2: F_CHG_BO (Page 179)).
2. Interconnect the OUT output to the input whose value you want to change using Safety Data Write.

3. Assign a pair of numbers to the SAFE_ID1 and SAFE_ID2 inputs. This ensures the association between the instance of F_CHG_R/F_CHG_BO and the corresponding faceplate. SAFE_ID1 must be unique from all others in the program. The pair of numbers for SAFE_ID1 and SAFE_ID2 must be unique from all others in the system. You must configure the same pair of numbers on the block icon of the associated faceplate.
4. Interconnect the EN_CHG input to the enable signal for Safety Data Write.
5. Assign the maximum permissible time for the duration of the transaction to the TIMEOUT input. The transaction starts as soon as the initiator has accepted his entry.
   All steps for verifying the transaction must be taken into account when configuring this time. For example, if two operators are required to enable the change, an appropriate amount of time must be allotted for both operators to log on and perform the necessary steps.
6. For F_CHG_R only: Assign limits to the MIN and MAX inputs to specify the time during which the F-parameters (output OUT) can be changed.
7. For F_CHG_R only: Assign the value of the maximum permissible increment of the change to the MAXDELTA input to specify the amount (+/-) by which the F-parameter (output OUT) can change relative to the current existing value.
8. Assign the initial value to the CS_VAL input that is to be transferred to the OUT output following a cold restart.
   For F_CHG_R only: When a cold restart occurs, CS_VAL is applied at output OUT irrespective of the values for MIN and MAX. The configured value at input CS_VAL must be between the MIN and MAX values.
9. Optional: Assign the value "0" to the WS_MODE input if the value at the CS_VAL input is also to be transferred to the OUT output following a warm restart. The WS_MODE input is set to 1 by default.
10. Optional: Evaluate the CS_USED output in the safety program if you have to react differently in your safety program after an F-start, depending on whether the CS_VAL value or the last valid value was made available at the OUT output.
11. For F_CHG_R only: Set the unit of measurement for the F-parameter to be changed.
    To do this, open the properties of the F-block and select the CURR_R output in the "Outputs" tab. In the "Unit" field, select the desired unit (e.g. kg/min) from the drop-down list.
    The unit is displayed on the faceplate in the OS.

11.2.3 Examples: Safety Data Write

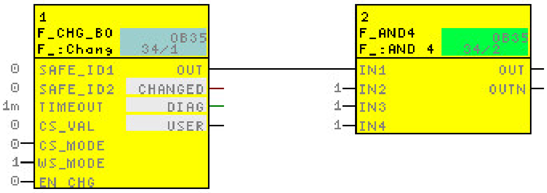
11.2.3.1 Example 1: F_CHG_R

The following figure shows an instance of F_CHG_R. The OUT output is interconnected to the "U_HL" input of F_LIM_HL whose value is to be changed in a fail-safe manner using Safety Data Write.



11.2.3.2 Example 2: F_CHG_BO

The following figure shows an instance of F_CHG_BO. The OUT output is interconnected to the "IN1" input of F_AND4 whose value is to be changed in a fail-safe manner using Safety Data Write.



11.2.4 Configuring the Faceplate for Safety Data Write.

A faceplate must be created in the OS for each instance of an F-block F_CHG_R and F_CHG_BO in the safety program. The operator steps for the Safety Data Write transaction are performed on the faceplate in the required sequence by one or two operators. The corresponding faceplate is called up in the OS via the associated block icon.

Requirements

- Placement, parameter assignment and interconnection of all required F-blocks F_CHG_R and F_CHG_BO in the CFC charts is complete.
- The CFC charts with the F_CHG_R and F_CHG_BO F-blocks are located in the plant hierarchy.
- The safety program is compiled.

Configuring faceplates

Configure the faceplates for Safety Data Write in the engineering system with the following steps:

1. Creating block icons
2. Initializing properties of the block icons
3. Setting up authorizations for operators
4. Transferring configuration to the OS

The individual steps are described below.

Creating block icons

1. Open the PCS 7 project in SIMATIC Manager.
2. Create a new picture object in the level of the plant hierarchy containing the CFC charts with the F-blocks F_CHG_R and F_CHG_BO.
3. Select the picture object and open the object properties.
4. In the "Block Icons" tab, activate the "Derive block icons from the plant hierarchy" option.
5. Click "OK" or "Apply" to confirm the revised properties.
6. Select the OS object and select "Compile" from the shortcut menu to compile the OS.
7. If necessary, select the "Create/update block icons" option in the "Compile OS" wizard when selecting the data you want to compile and the scope of the compilation. Press the "Compile" button in the last dialog.

Result: When the OS is compiled, the block icons are automatically inserted in the new picture.

Note

To prevent overwriting SAFE_ID1 and SAFE_ID2, deactivate the "Derive block icons from the plant hierarchy" option in the object properties for the WinCC picture before recompiling the OS.

Initializing properties of the block icons

1. Double-click the picture file in the plant view of the PCS 7 project.
   Result: WinCC Explorer is started and the picture file is displayed in the Graphics Designer. The name is displayed in the header of each block icon. The name of the block icon is formed from the name of the CFC chart and the name of the associated F-block instance.
2. Select a block icon and open the object properties.
3. Select "User configuration" on the "Properties" tab.

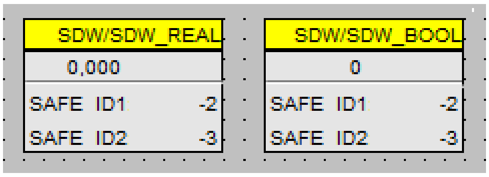
4. Assign the exact static values to the SAFE_ID1 and SAFE_ID2 attributes that are configured for the SAFE_ID1 and SAFE_ID2 inputs of the associated F-block instance.

> ⚠ WARNING
>
> **Static values of the SAFE_ID1 and SAFE_ID2 attributes**
>
> The static values of the SAFE_ID1 and SAFE_ID2 attributes must be identical to the F-parameters that are configured for the SAFE_ID1 and SAFE_ID2 inputs of the associated F-block instance.
>
> Note that you must enter these values independently and separately at the F-blocks in the CFC Editor and at the block icons in WinCC.
>
> FSW-041

5. Assign the desired authorizations to the "InitiatorAuthorization" and "ConfirmerAuthorization" attributes. Alternatively, you can accept the default authorizations for operators. See also "Setting up authorizations for operators".
   Default authorizations (correspond to the user hierarchies from PCS 7):
   - For the operator who initiates the change to an F-parameter using Safety Data Write (Initiator): No. 5, Process controlling
   - For the operator who confirms the change to an F-parameter using Safety Data Write (Confirmer): No. 6, Higher process controlling
6. Repeat Steps 2 and 5 for all block icons present.
7. Save the picture file.

Examples

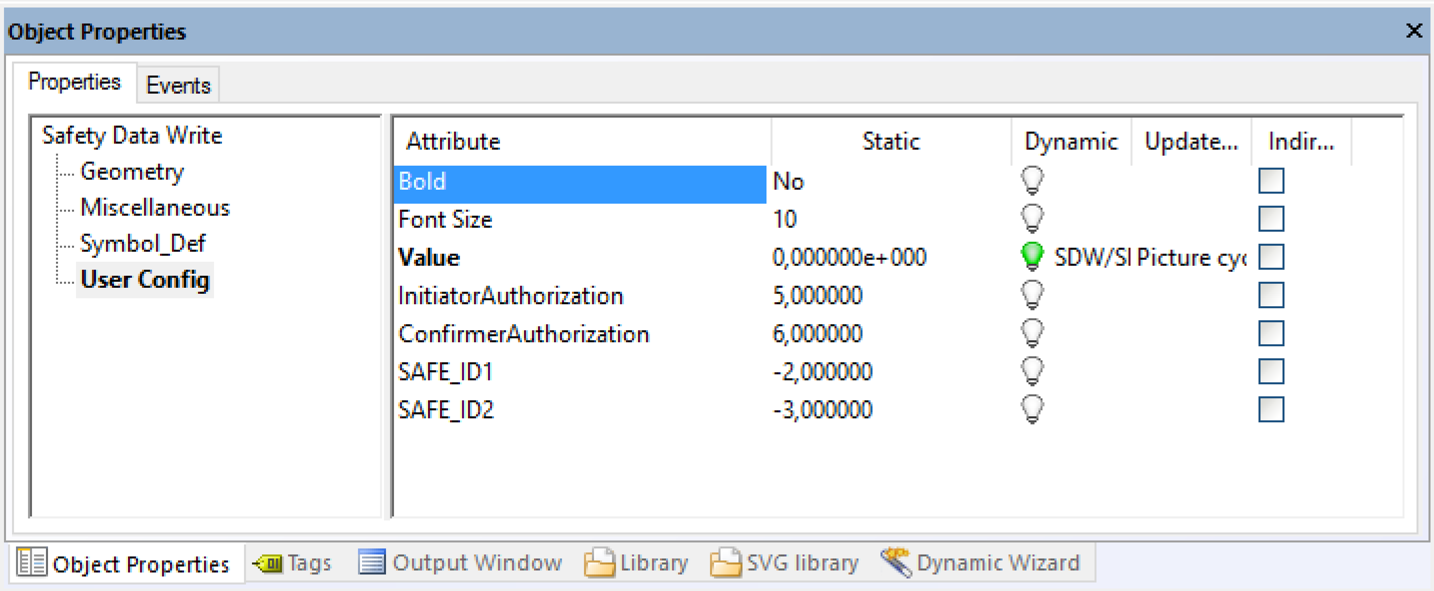
- Example: Block icons in a picture file



SDW/SDW_REAL	
0,000	
SAFE ID1	-2
SAFE ID2	-3

SDW/SDW_BOOL	
0	
SAFE ID1	-2
SAFE ID2	-3

- Example: Properties of a block icon



Object Properties

Properties | Events

Safety Data Write
- Geometry
- Miscellaneous
- Symbol_Def
- **User Config**

Attribute	Static	Dynamic	Update...	Indir...
Bold	No	○		□
Font Size	10	○		□
Value	0,000000e+000	● SDW/SI Picture cyc		□
InitiatorAuthorization	5,000000	○		□
ConfirmerAuthorization	6,000000	○		□
SAFE_ID1	-2,000000	○		□
SAFE_ID2	-3,000000	○		□

Setting up user authorizations for operators

Create the following users based on whether the transaction is to be performed by two operators or by one operator only:

- If the transaction for an F-parameter is to be performed by two operators, create two users:
  - The Initiator initiates the change to an F-parameter using Safety Data Write. This user must have the authorization assigned to the "InitiatorAuthorization" attribute in the properties for the block icon. However, the Initiator is not authorized to confirm the change.
  - The Confirmer verifies and confirms the change. This user must have the authorization assigned to the "ConfirmerAuthorization" attribute in the properties for the block icon. However, the "Confirmer" is not authorized to initiate the change.
- If only one operator is to perform all of the transaction steps, create a user who has both authorizations assigned to the "InitiatorAuthorization" and "ConfirmerAuthorization" attributes in the properties for the block icon.

Create the users in WinCC Explorer using the "User Administrator" editor.

Activating the OS

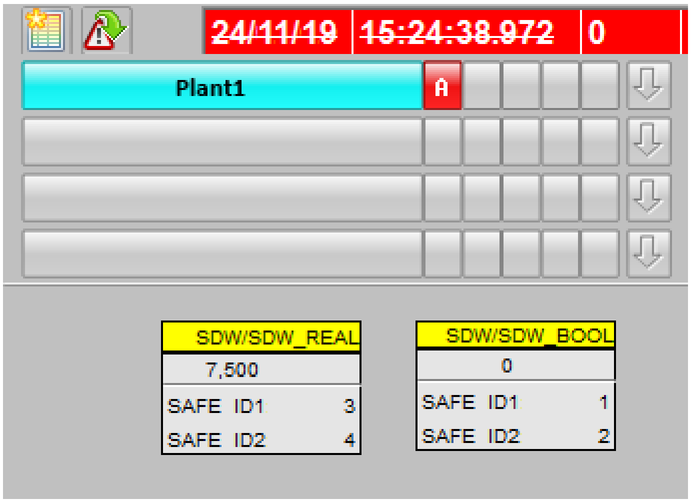
Activate the WinCC Runtime system of the OS, e.g. by selecting **File > Activate** in WinCC Explorer.

Result

After activation and login, the hierarchy levels appear as buttons in the runtime system of the OS. Click the button to display the block icons for this level.

Example

The following figure shows two block icons in the runtime system of the OS.



SDW/SDW_REAL
7,500
SAFE ID1 3
SAFE ID2 4

SDW/SDW_BOOL
0
SAFE ID1 1
SAFE ID2 2

Clicking a block icon opens the faceplate that you can use to change an F-parameter by means of Safety Data Write.

Detailed information

For detailed information on the described steps, refer to:

- "PCS 7 Operator Station (https://support.industry.siemens.com/cs/ww/en/view/90682677)" configuration manual
- Online help for the WinCC editors (e.g. Graphics Designer and User Administrator)

11.3 Changing F-Parameters with Safety Data Write

11.3.1 Requirements and General Instructions

You perform a transaction for changing an F-parameter using Safety Data Write using a faceplate in the OS. The transaction consists of a sequence of operations that can be performed by one or two operators.

Requirements

- The S7 program is compiled and downloaded to the F-CPU.
- The user(s) with the relevant authorizations are set up.
- The configuration of the faceplates is downloaded to the OS.
- The AS/OS connection is OK. The operator can test the AS/OS connection using the "OS Test" button (see "Testing AS/OS Connection" section below).
- The EN_CHG input of the F-block instance of F_CHG_R or F_CHG_BO for enabling Safety Data Write is set to TRUE.
- When using OS clients, make sure that no default server is set for tags (in WinCC Explorer select "Server Data," in the shortcut menu select "Default Server" and in the "Configure Default Server" dialog for the "Tags" component select "No Default Server").

Specifications for changing an F-parameter using Safety Data Write

To change an F-parameter via Safety Data Write, the following information is required for the operator(s):

- Name of the block icon
- New value for the F-parameter

General Information

The transaction must be completed within a specified time interval (Timeout). If the transaction is not finished before the Timeout interval elapses, the transaction is automatically canceled once the Timeout interval expires.

⚠ WARNING

Initiator and confirmer must not accept an invalid value

As the initiator or confirmer, you must not accept an invalid value. If there are inconsistencies, you must cancel the transaction.

As an operator, you must not rely on individual display fields of the faceplate; rather, you must check the values and compare them with each other.

Before starting the transaction, you must verify the plant name in the header of the faceplate.

FSW-042

⚠ WARNING

Technological assignment must be appropriate for the environment

When opening the faceplate, make sure that the technological assignment in the top line is appropriate for the environment in which the block icon was placed.

FSW-043

⚠ WARNING

Transaction for changing an F-parameter

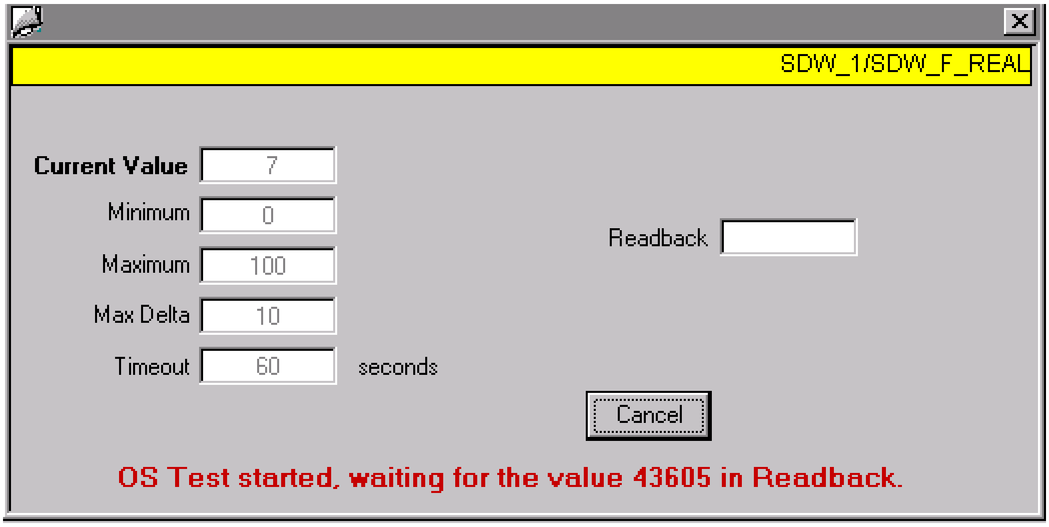
You can only perform one transaction for changing an F-parameter at a time. You must use organizational measures to ensure that multiple transactions are not performed simultaneously for the same F-parameter. Otherwise, the transaction cannot be performed correctly, resulting in unexpected results, such as:

- Display of incorrect values in the faceplate fields
  or
- Unexpected cancellation of the transaction

FSW-044

Testing the AS/OS connection

Before starting the transaction, you can test the AS/OS connection by clicking the "OS Test" button.



SDW_1/SDW_F_REAL

Current Value: 7

Minimum: 0

Maximum: 100

Max Delta: 10

Timeout: 60 seconds

Readback:

OS Test started, waiting for the value 43605 in Readback.

If the AS/OS connection is OK, a message to that effect is output and the expected value is displayed in the "Readback" field.

If the AS/OS connection is not OK, the following error message is displayed: "OS test failed".

If the F-block is busy...

If a transaction for a faceplate has been started already, the following message appears when opening the faceplate in WinCC Runtime:

"Function Block Busy. Please wait..."

To start a new transaction, click "Cancel" and the faceplate again.

11.3.2 Changing an F-Parameter with Two Operators

Operator authorizations

The transaction requires two operators having different authorizations.

- The initiator initiates a change to an F-Parameter using Safety Data Write. This user must have the authorization for initiating the change but not for confirming it. The authorization corresponds to the "InitiatorAuthorization" attribute in the properties for the block icon. The default setting is no. 5, process controlling.
- The confirmer enters the modified value again, verifies it, and confirms the change. This user must have the necessary authorization for confirming the change but not for initiating it. The authorization corresponds to the "ConfirmerAuthorization" attribute in the properties for the block icon. The default setting is No. 6, Higher-level operator-process communications.

Note

The sections below describe the necessary transaction steps for the two operators. The figures illustrate the example of an F_REAL parameter with the login:

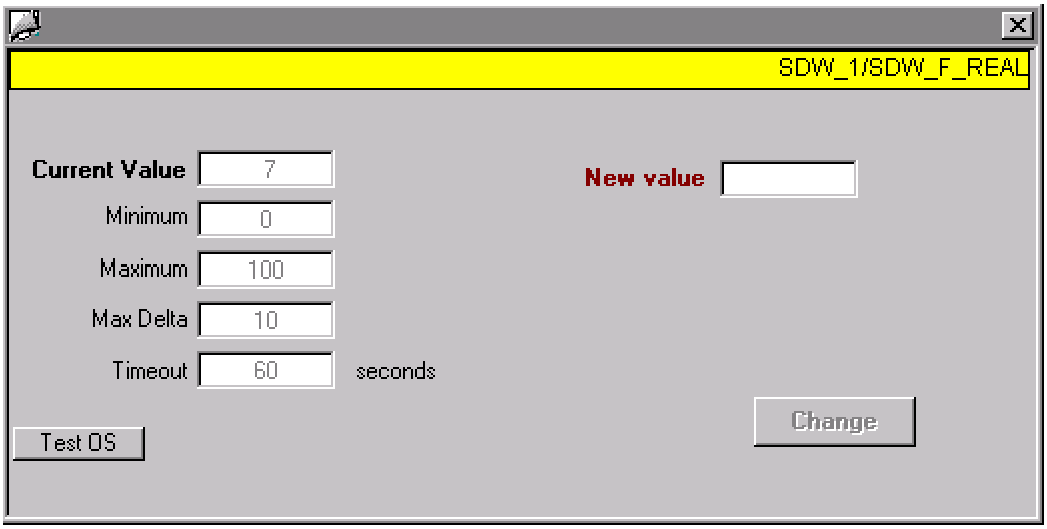
- level5 – Initiator
- level6 – Confirmer

Note

When changing F_BOOL parameters using Safety Data Write, you must enter the value "true" or "false" and not "1" or "0". This entry is not case-sensitive.

Initiator: Initiating a change

1. Log on to the OS as a user with initiator authorization.
2. Click the desired block icon to open the faceplate.



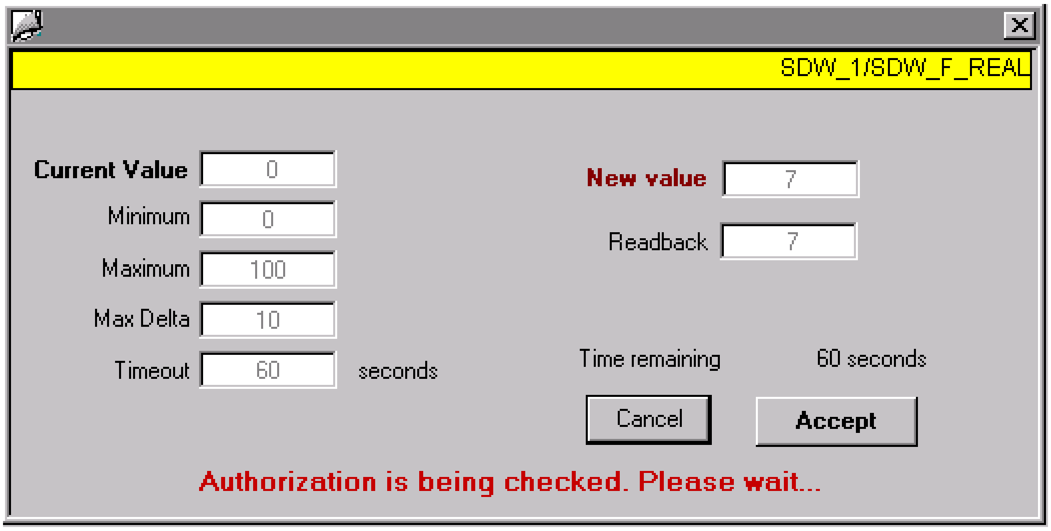
SDW_1/SDW_F_REAL

Current Value: 7
Minimum: 0
Maximum: 100
Max Delta: 10
Timeout: 60 seconds
New value:

The Safety Data Write dialog indicates the current value, the Timeout value in seconds, and, in the case of F_CHG_R, the values for the change limits (Minimum, Maximum, and MaxDelta) as well as the unit of measurement, where applicable.

3. Enter the new value in the "New value" field (using a maximum of 10 characters including decimal separators and plus or minus signs).
In the case of an F_REAL value, verify that the change limits (Minimum, Maximum, and MaxDelta) are not violated. If the new value violates one of the limit values, an error message is displayed and the "Change" button cannot be activated.

4. Click "Change". The modified value is also displayed in the "Readback" field.
5. Compare the values in the "New value" and "Readback" fields. If they are identical, click the "Accept" button.
   Note: If the block input EN_CHG changes to FALSE before you click the "Accept" button, this is indicated by a message, and the "Accept" button is disabled (see also the description of the F-blocks "F_CHG_R: Safety Data Write for F_REAL (Page 311)" and "F_CHG_BO: Safety Data Write for F_BOOL (Page 317)").



SDW_1/SDW_F_REAL

Current Value 0

Minimum 0

Maximum 100

Max Delta 10

Timeout 60 seconds

New value 7

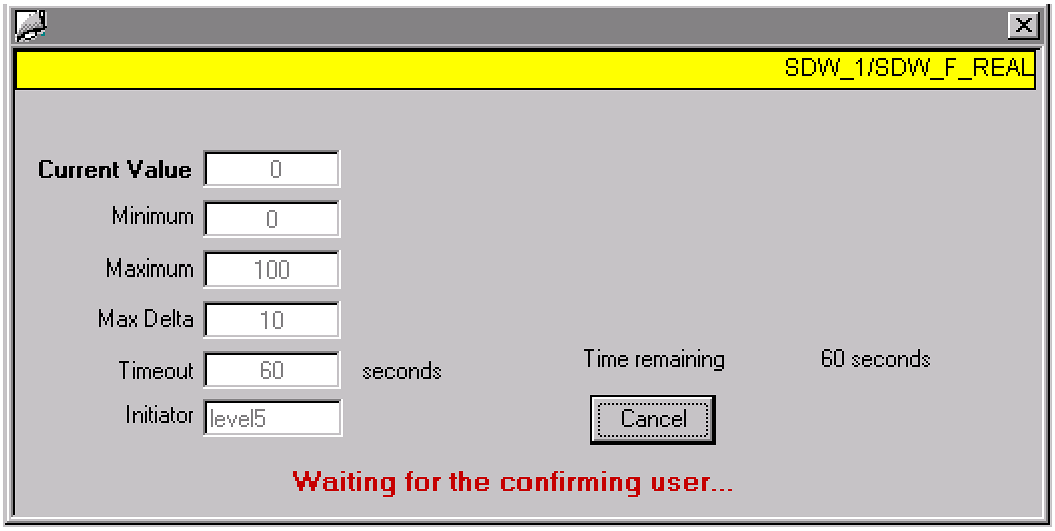
Readback 7

Time remaining 60 seconds

Authorization is being checked. Please wait...

Result

The timeout counter is started and you are informed that the change must be confirmed by a second operator.



SDW_1/SDW_F_REAL

Current Value 0

Minimum 0

Maximum 100

Max Delta 10

Timeout 60 seconds

Initiator level5

Time remaining 60 seconds

Waiting for the confirming user...

The confirmer must then continue the transaction.

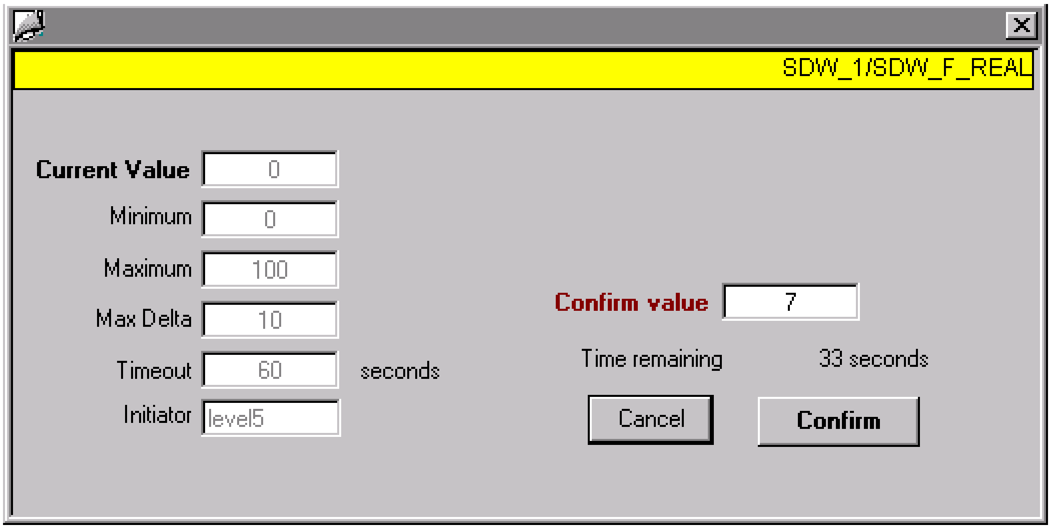
If you cancel the transaction after clicking "Accept," check whether the previously valid value is displayed in the "Current value" field.

Confirmer: Confirming the change

Note

The confirmation must take place before the remaining time expires.

1. Log on to the OS as a user with "confirmer authorization".
   You can log on to a second OS or on the same OS as the initiator.
2. Click the desired block icon to open the faceplate.



SDW_1/SDW_F_REAL

Current Value 0
Minimum 0
Maximum 100
Max Delta 10
Timeout 60 seconds
Initiator level5

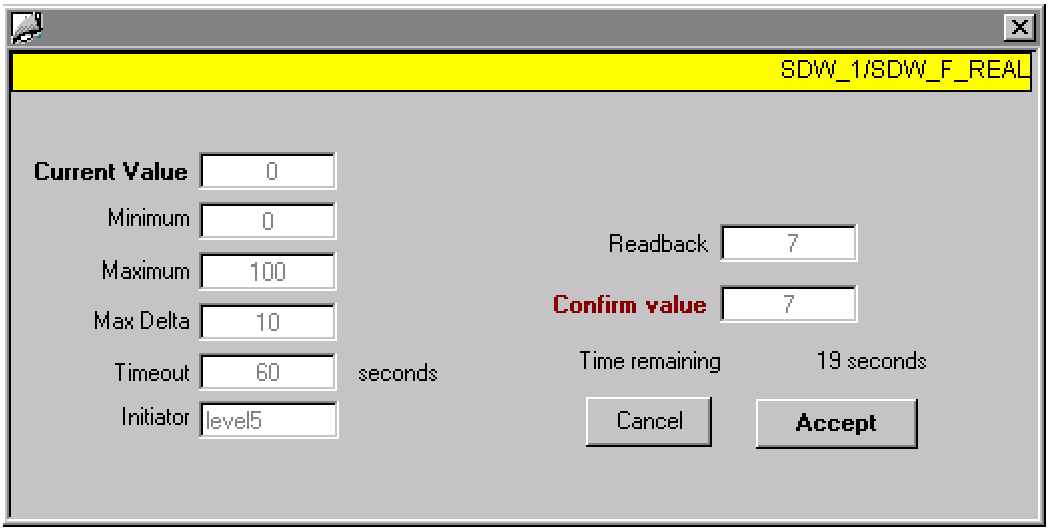
Confirm value 7
Time remaining 33 seconds

3. Enter the new value in the "Confirm value" field. If the confirm value differs from the new value that was entered by the initiator, an error message is displayed and the "Confirm" button cannot be activated.

   Note

   You must confirm the change by entering the new value separately. The value is deliberately not displayed since an unbiased confirmation by the second operator is required.

4. Click "Confirm".
   The value entered by the initiator is displayed in the "Readback" field.
   Note: If the block input EN_CHG is changed to FALSE, this is indicated by a message, and the input is canceled. Values can be re-entered once EN_CHG changes back to TRUE (see the description of the F-blocks "F_CHG_R: Safety Data Write for F_REAL (Page 311)" and "F_CHG_BO: Safety Data Write for F_BOOL (Page 317)").
5. Compare the values in the "Confirm value" and "Readback" fields. If they are identical, click the "Accept" button to permanently save the change. If the values do not match, you must click "Cancel".
   Note: If the block input EN_CHG changes to FALSE before you click the "Accept" button, this is indicated by a message, and the "Accept" button is disabled (see also the description of the F blocks "F_CHG_R: Safety Data Write for F_REAL (Page 311)" and "F_CHG_BO: Safety Data Write for F_BOOL (Page 317)").



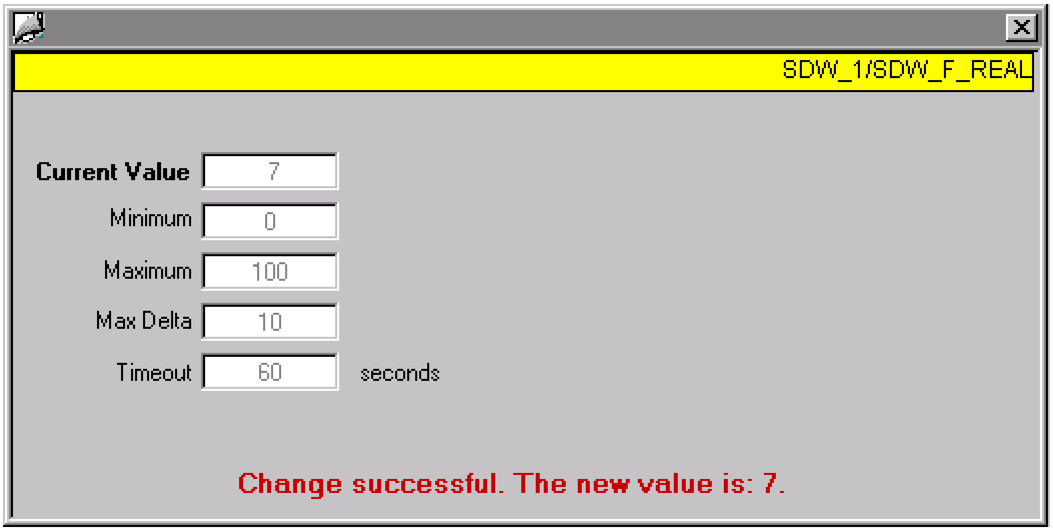
SDW_1/SDW_F_REAL

Current Value 0
Minimum 0
Maximum 100
Max Delta 10
Timeout 60 seconds
Initiator level5

Readback 7
Confirm value 7
Time remaining 19 seconds

Result

If the transaction is finished within the remaining time, a successful F-Parameter change is signaled.



SDW_1/SDW_F_REAL

Current Value 7

Minimum 0

Maximum 100

Max Delta 10

Timeout 60 seconds

Change successful. The new value is: 7.

11.3.3 Changing an F-Parameter with One Operator

Operator Authorization

If only one operator is to perform the transaction, this operator must be authorized to both initiate and confirm changes using Safety Data Write. The authorization must include the values of both the "InitiatorAuthorization" and "ConfirmerAuthorization" attributes. Default is No. 5, Operator-process communications and No. 6, Higher-level operator-process communications.

Transaction Sequence with Only One Operator

The procedure is the same as for operation with two operators, except that one operator is able to perform all of the steps (see also the section entitled "Changing an F-Parameter with Two Operators (Page 187)").

The difference is there is no waiting period for the confirmer. Rather, the operator is prompted immediately to enter the confirm value.

All other steps remain the same.

Compiling and commissioning an S7 program 12

12.1 Compiling an S7 program

Introduction

You compile a safety program by compiling the entire S7 program as usual in the CFC Editor.

Procedure

If an S7 program contains a safety program, this is automatically also compiled when the CFC charts are compiled. At the same time, fault-control measures are automatically added and additional safety-related checks are performed.

Read the documentation on CFC: "SIMATIC Process Control System PCS 7 CFC for SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/90683154)".

If you have changed the safety program since it was last compiled, you will be prompted for the password of your safety program during the compilation operation. You must enter the password of your safety program to continue compiling.

12.2 "Safety Program" dialog

This dialog displays information about the safety program and provides buttons for editing the safety program.

In SIMATIC Manager, open the "Safety Program" dialog by selecting the "**Options > Edit safety program**" menu command.

Starting from S7 F Systems V6.2, the size of the "Safety Program" dialog can be changed.

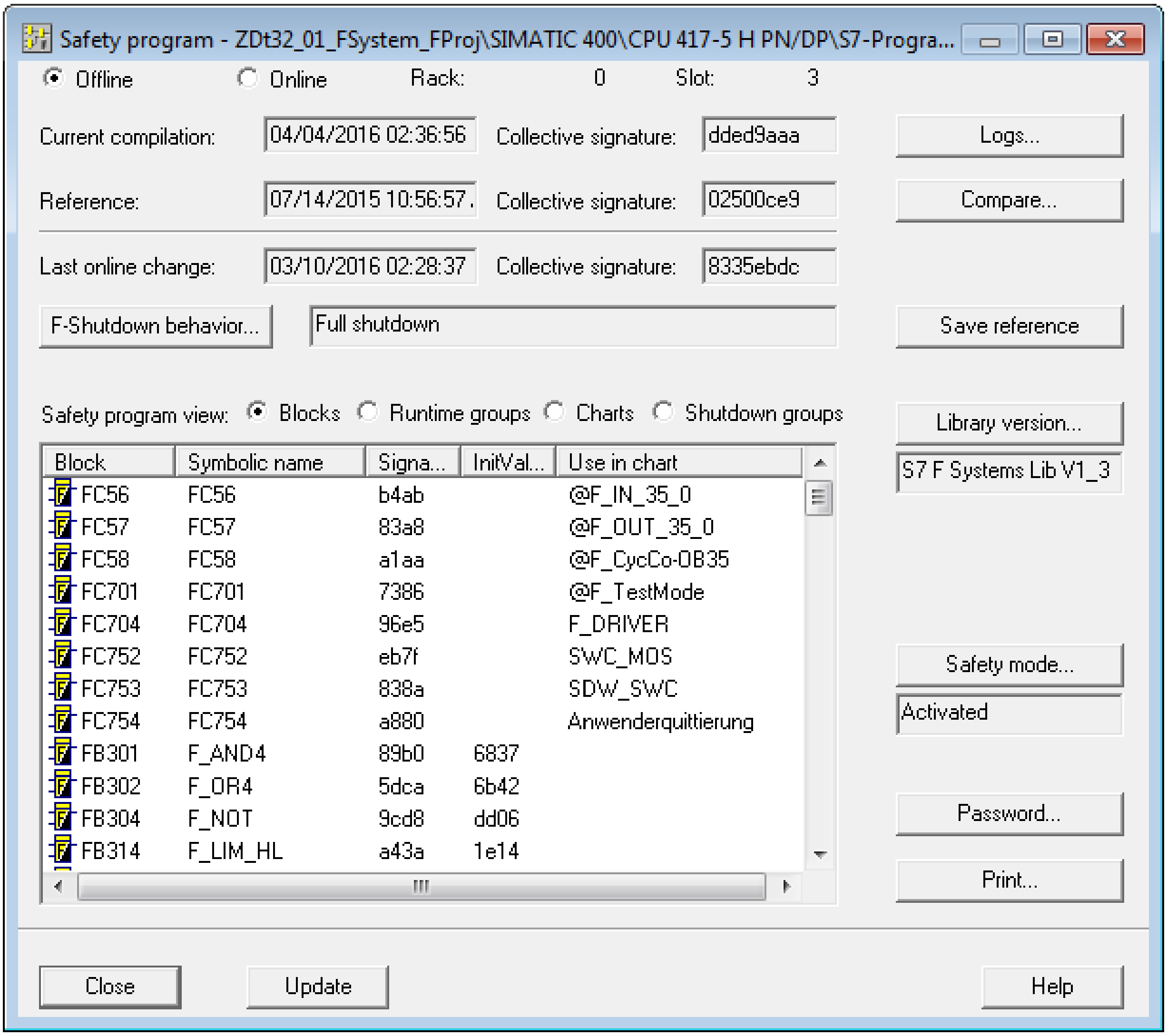
Available operating options and displays in the dialog

The operating options in the dialog depend on the desired function.

- If you want to assign or change the password for the safety program of a configured CPU, all operator controls are available and the display fields show the corresponding values. This requires selection of the program folder of a CPU, e.g. "S7 Program" before the menu command **Options > Edit Safety Program**.
- If you want to assign or change the password for an F-library or a project without a configured CPU, you can only use the "Password..." button.
  This requires selection of the corresponding directory of the CFCs with the built-in F blocks, e.g. within the F-library, before the menu command **Options > Edit Safety Program**.

Example

The following figure shows the dialog with all display elements and operator control functions for assigning/changing the password for the safety program of a configured CPU.



Safety program - ZDt32_01_FSystem_FProj\SIMATIC 400\CPU 417-5 H PN/DP\S7-Progra...

● Offline ○ Online Rack: 0 Slot: 3

Current compilation: 04/04/2016 02:36:56 Collective signature: dded9aaa

Reference: 07/14/2015 10:56:57. Collective signature: 02500ce9

Last online change: 03/10/2016 02:28:37 Collective signature: 8335ebdc

F-Shutdown behavior...: Full shutdown

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

Block	Symbolic name	Signa...	InitVal...	Use in chart
FC56	FC56	b4ab		@F_IN_35_0
FC57	FC57	83a8		@F_OUT_35_0
FC58	FC58	a1aa		@F_CycCo-OB35
FC701	FC701	7386		@F_TestMode
FC704	FC704	96e5		F_DRIVER
FC752	FC752	eb7f		SWC_MOS
FC753	FC753	838a		SDW_SWC
FC754	FC754	a880		Anwenderquittierung
FB301	F_AND4	89b0	6837	
FB302	F_OR4	5dca	6b42	
FB304	F_NOT	9cd8	dd06	
FB314	F_LIM_HL	a43a	1e14	

Library version...: S7 F Systems Lib V1_3

Safety mode...: Activated

The following information about the safety program located online on the F-CPU or offline in the engineering system will be displayed in the "Safety Program" dialog box:

- A list of all included F-blocks with signatures and initial value signatures
- Current compilation: Date and collective signature
- Reference: Date and collective signature
- Last online change: Date and collective signature
  This data is provided for information purposes only and is not relevant for acceptance.

Buttons in the "Safety Program" dialog box

The dialogs you can access and the actions you can perform using the buttons in the "Safety Program" dialog box are described in the sections below.

Not all operator controls are available, depending on the desired function. Refer to the section above, "Available operating options and displays in the dialog".

Button	Description
F-Shutdown behavior	""Shutdown Behavior" dialog box (Page 196)"
Logs	""Logs..." button (Page 197)"
Compare	"Comparing safety programs (Page 200)"
Save Reference	""Save Reference" button (Page 197)"
Library version	""Library Version" button (Page 197)"
Safety mode	"Safety mode (Page 210)"
Password	""Password for Safety Program Creation" dialog (Page 197)"
Print	"Printing project data of the safety program (Page 207)"
Refresh	""Update" button (Page 199)"

See also

Testing a safety program (Page 216)

12.2.1 "Shutdown Behavior" dialog box

Description

Using the "Shutdown behavior" dialog, you can select how the safety program should react to a detected error, i.e. an F-STOP:

- "Complete shutdown": All F-shutdown groups of a safety program are switched off in an F-shutdown group when the first error is detected.
- "According to the configuration of F_SHUTDN":
  - The faulty F-shutdown group(s) are switched off in an F-shutdown group (partial shutdown) when the first error is detected.
    or
  - All F-shutdown groups of a safety program are switched off in an F-shutdown group when the first error is detected.

After changing the shutdown behavior, you must compile the S7 program again.

You must also enter the password for the safety program if you change the shutdown behavior.

See also

F-STOP (Page 99)

12.2.2 "Logs..." button

You can use the "Logs..." button to open the "Logs" dialog of the CFC Editor. The "Compile" and "Download" logs are relevant for the acceptance of the safety program. You can find more detailed information on acceptance in the section "System Acceptance Test (Page 229)".

12.2.3 "Save Reference" button

You can save all data of a safety program (charts, parameters, etc.) as a reference to be used as necessary for comparisons.

12.2.4 "Library Version" button

Description

You can use the "Library version..." button to upgrade the version of the F-library used in the project to the current version of the F-library.

The window below the button displays the version of the F-library currently used in the project.

12.2.5 "Password for Safety Program Creation" dialog

Description

In the "Create password for safety program" dialog, you can create a new password or change an existing password for the safety program.

Target system and program name:

The upper part of the dialog shows the target system and program name for the safety program for which the password is being created or changed.

If the password for an F-library or a project without a configured CPU is to be changed, no entry is displayed under "CPU".

Overview

You must create a password for each safety program. You must enter this password using the "Password..." button in the "Safety program" dialog before you can perform the actions described in section "Overview of access protection (Page 75)".

When the password for the safety program is entered for one of these actions, the user obtains access permission. This access permission is valid for one hour. After this time elapses, the user is prompted to enter the password again when he wants to perform one of the above-named actions.

The access permission is reset to 1 hour following each safety-related action.

The access permission can also be canceled in this dialog.

"Increased password security" check box

With this option you can activate the "Increased password security" in order to use a more secure password.

- If you activate the option, the rules corresponding to the description "Criteria for a secure password" below apply to the password.
- If you clear the option, the previous rules apply to the assignment of the password.

Note

This option is activated by default as of S7 F Systems V6.3.

When using Safety Matrix with version V6.2.2 or earlier, the option "Increased password safety" must not be activated.

Criteria for a secure password

To ensure a secure password, it must meet the following criteria when created for the first time or changed:

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

These criteria apply when the "Increased password security" option is activated in the "Create password for safety program" dialog.

Creating a new password

During the initial setup of a new password, select the password in conformance with the criteria described below and enter it in the "New password" and "Reenter password" fields. In this case, the "Old password" field is deactivated.

By selecting the "Increased password security" check box, you can use a more secure password that conforms to the description "Criteria for a secure password" above.

If a password has not yet been created for the safety program, you will be prompted to do so if a password is required for the desired configuring task, e.g. when inserting an F-block in a CFC chart or when inserting fail-safe modules in HW Config.

You can find additional information on the password prompt in section "Overview of access protection (Page 75)" in the "Password for safety program" table.

Changing a password

To change a password, you must enter the old password in the "Old password" field.

As of S7 F Systems V6.3, this dialog can also be used to change the password for a project without a configured CPU (e.g. an F-library).

Then, choose the new password based on whether or not the "Increased password security" check box is selected and enter it in the "New password" and "Reenter password" fields.

Revoking access permission

You can use the "Logout" button in the "Access permission" area to revoke the 1-hour access permission period since the last time the password was entered.

Any user who then wants to perform an action that requires entry of a password must now enter the password for the safety program again.

12.2.6 "Update" button

Description

You can use this button to update all displayed information. This may be necessary, for example, if changes have been made in other applications, such as the CFC Editor, since the dialog was opened.

12.3 Comparing safety programs

Introduction

The "Compare Programs" dialog box enables you to compare safety programs and display and print out differences.

You can compare the following safety programs:

- Online safety program in the F-CPU
- Current offline safety program
- Last compilation of the current S7 program
- Saved reference program
- Other project

The result of the comparison shows you whether the following are the same or different:

- Collective signature
- Individual signatures
- Parameter values
- Differences in the safety program and control structures
- Modified or deleted F-Blocks and interconnections, etc.

With the "Compare Programs" dialog, you can also tell if a safety program was not modified. For this purpose, compare the safety program with the reference program.

As of S7 F Systems V6.2, the dialog can be resized to improve the readability of the table.

In S7 F/FH Systems V6.1 and later, system-related changes are shown in a combined display, making it easy for you to identify changes that are relevant for checks. This facilitates the acceptance test for changes.

System-related changes are primarily found:

- In system charts beginning with @F_x
- In runtime groups beginning with @F_x
- On driver blocks

Program/reference

Select one of these option boxes to specify whether you want to compare the current program or the reference program.

Compare with:

Use this drop-down list box to specify the second safety program to which you want to compare the safety program you just selected.

Program	**Compare with ...**	
	Reference	Last saved reference for this safety program
	Last compilation	The last compilation of this S7 program during which safety-related changes were detected.
	Online	Currently downloaded safety program in the F-CPU
	Other project	Any offline program. Use the "Browse" button to select the offline program.
Reference	**Compare with ...**	
	Current safety program	Current offline program
	Last compilation	The last compilation of this S7 program during which safety-related changes were detected.
	Online	Currently downloaded safety program in the F-CPU
	Other project	Any offline program. Use the "Browse" button to select the offline program.

"Browse" button

Use this button and the "Open" dialog to select the offline program of any project to be compared.

"Start" button

Click this button to start the comparison.

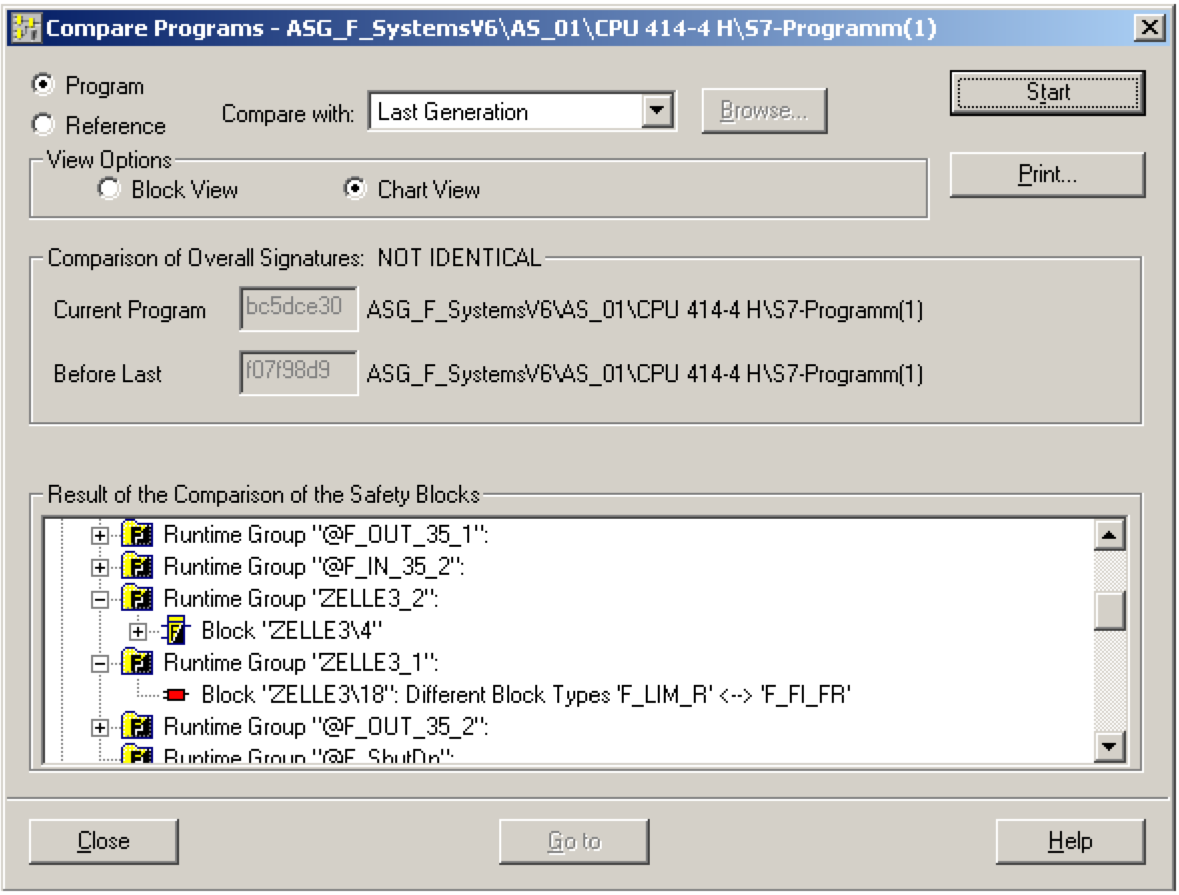
View options

If you want to compare two offline programs, you can switch back and forth between the following options by clicking the relevant option buttons:

- **Block view**:
  Shows you a list with the differing blocks (different block signatures).
- **Chart view**:
  Shows you a hierarchy of all differences in the:
  - Task
  - F-Runtime group
  - F-Block
  - Parameters

  In this view, the "Go to" button is available.

Result of the comparison (both safety programs offline)



Compare Programs - ASG_F_SystemsV6\AS_01\CPU 414-4 H\S7-Programm(1)

● Program
○ Reference

Compare with: Last Generation

View Options
○ Block View ● Chart View

Comparison of Overall Signatures: NOT IDENTICAL

Current Program bc5dce30 ASG_F_SystemsV6\AS_01\CPU 414-4 H\S7-Programm(1)

Before Last f07f98d9 ASG_F_SystemsV6\AS_01\CPU 414-4 H\S7-Programm(1)

Result of the Comparison of the Safety Blocks

```
⊞ Runtime Group "@F_OUT_35_1":
⊞ Runtime Group "@F_IN_35_2":
⊟ Runtime Group 'ZELLE3_2':
    ⊞ Block 'ZELLE3\4"
⊟ Runtime Group 'ZELLE3_1':
    Block 'ZELLE3\18": Different Block Types 'F_LIM_R' <--> 'F_FI_FR'
⊞ Runtime Group "@F_OUT_35_2":
  Runtime Group "@F_ShutDn":
```

A note is displayed indicating whether or not the collective signatures of all F-Blocks are identical.

Display of differences in the block view

In the block view, all F-blocks whose signatures have changed are displayed with the relevant signature, but the F-Runtime group and task are not displayed.

Display of differences in the chart view

The differences between charts are displayed in a hierarchical format similar to Explorer. In this view, all F-Blocks are shown under the relevant task and F-Runtime group. Information about the possible changes are shown individually for each F-Block. This information relates to the task, the F-Runtime group, and the sequence within the F-Runtime group, as well as the parameter assignment and interconnections of the F-Blocks.

Only tasks, F-Runtime groups, F-Blocks, and parameters in which changes were found are displayed.

Changes are described as follows:

Text	Meaning
Deleted	F-Block only present in source
Added	F-Block only present in comparison program
Runtime position changed	F-Block is located in a different runtime position in the F-Runtime group
Interface changed	• Additional parameters • Removed parameters • Modified data type (e.g. F-Bool <- Bool)
Signature changed	Signature of F-Block type (FB) changed
Value: "new" <- "old"	The parameter assignment of an input or output or the interconnection source of an input has been changed from "old" to "new". "Not-interconnected" can also be specified as the interconnection source if an interconnection has been deleted or newly created.

Note

If "Different versions of F-Reference data" appears in the chart view when comparing the safety program to a reference, this means that you created the reference with an older version of S7 F Systems and did not overwrite it with the current version during migration.

Instead, use the old project version that you archived prior to migration.

Displayed changes

Note the following when changing names:

The S7 F Systems comparator references the elements according to their names. If an element name is changed, the element can no longer be assigned.

- Chart names
- Name of a runtime group
- Block name (instance in a chart)
- Parameter name (for F-Block types)

Although chart names are not relevant for runtime, changes still affect the "Chart view":

- Each time a chart name is changed, the chart is displayed with the old name as "Deleted" and with the new name as "Added".
- With a CFC, an F-runtime group with the same name is renamed at the same time. Therefore, this F-Runtime group is also displayed with the old name as "Deleted" and with the new name as "Added".

- All interconnects of F-Blocks outside of this chart to F-Blocks within this chart as displayed as changed. The reason for this is that the chart name is also used as the name component of an interconnection peer to identify the interconnection.
- The block view correctly returns no difference in this case. The collective signature of the safety program does not change. In order to prevent such unnecessary entries in the chart view, we recommend that you do not rename any F-Charts or shift between F-Charts after performing the acceptance test.

Note the following:

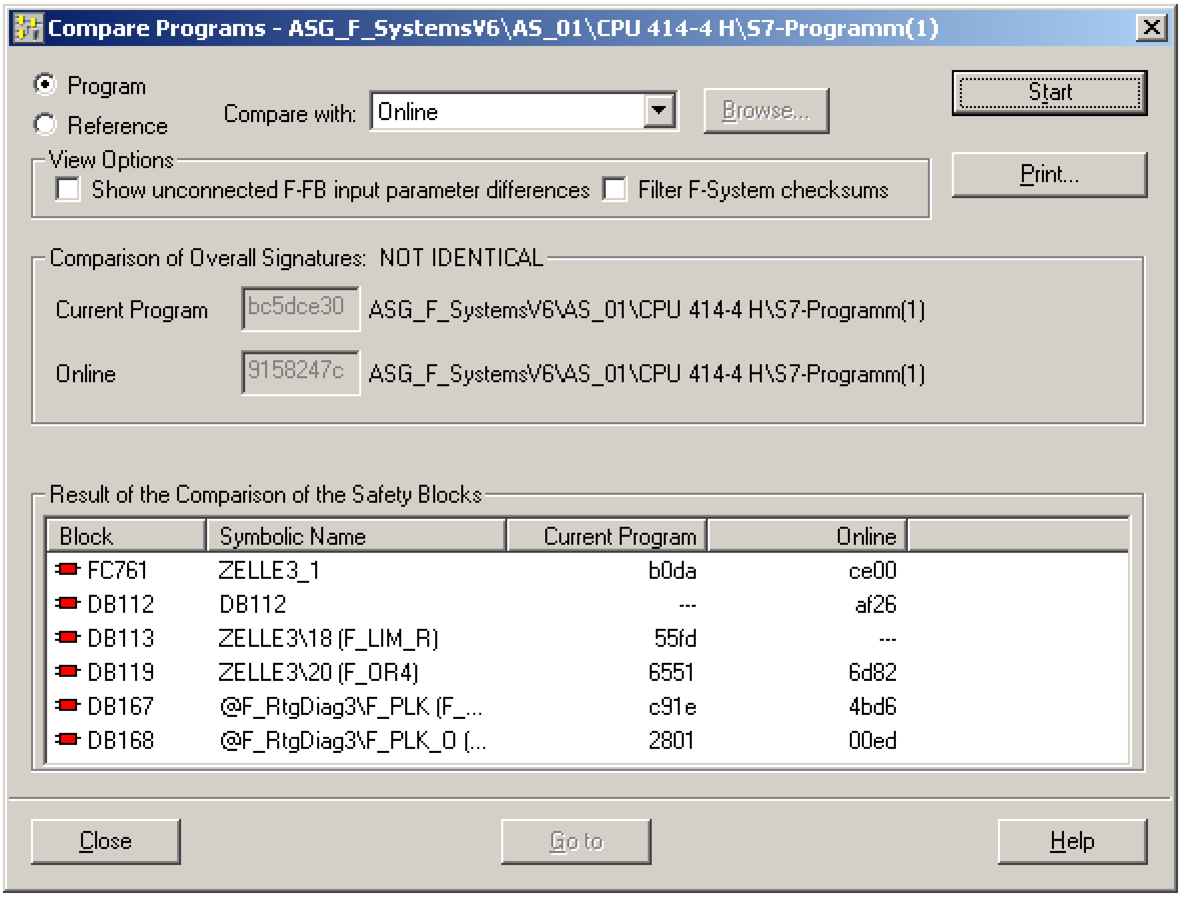
- In the chart view of the comparison, only differences pertaining to the safety program are generally displayed. In particular, changes in interconnections between the safety program and the standard program or global addresses are not displayed.
- If an interconnection of an output is changed at the same time as the initial value of this output, the modified interconnection will be displayed, but not the modified initial value.

Result of the comparison (online safety programs with offline)

When a comparison to the online program is made, an indication is given as to whether the source, load memory, and work memory match (this allows you to detect non-permissible data manipulations on non-interconnected, fail-safe input parameters in the work memory).

If you have selected the online program in the "Compare with" drop-down list box, only the block view is available. In this case, the following two view options are available:

- Show unconnected F-FB input parameter differences
- Filter F-System checksums



Compare Programs - ASG_F_SystemsV6\AS_01\CPU 414-4 H\S7-Programm(1)

● Program
○ Reference

Compare with: Online

View Options
□ Show unconnected F-FB input parameter differences □ Filter F-System checksums

Comparison of Overall Signatures: NOT IDENTICAL

Current Program	bc5dce30	ASG_F_SystemsV6\AS_01\CPU 414-4 H\S7-Programm(1)
Online	9158247c	ASG_F_SystemsV6\AS_01\CPU 414-4 H\S7-Programm(1)

Result of the Comparison of the Safety Blocks

Block	Symbolic Name	Current Program	Online
FC761	ZELLE3_1	b0da	ce00
DB112	DB112	---	af26
DB113	ZELLE3\18 (F_LIM_R)	55fd	---
DB119	ZELLE3\20 (F_OR4)	6551	6d82
DB167	@F_RtgDiag3\F_PLK (F_...	c91e	4bd6
DB168	@F_RtgDiag3\F_PLK_O (...	2801	00ed

Just as in the offline block view, the window shows you all F-blocks whose signatures differ.

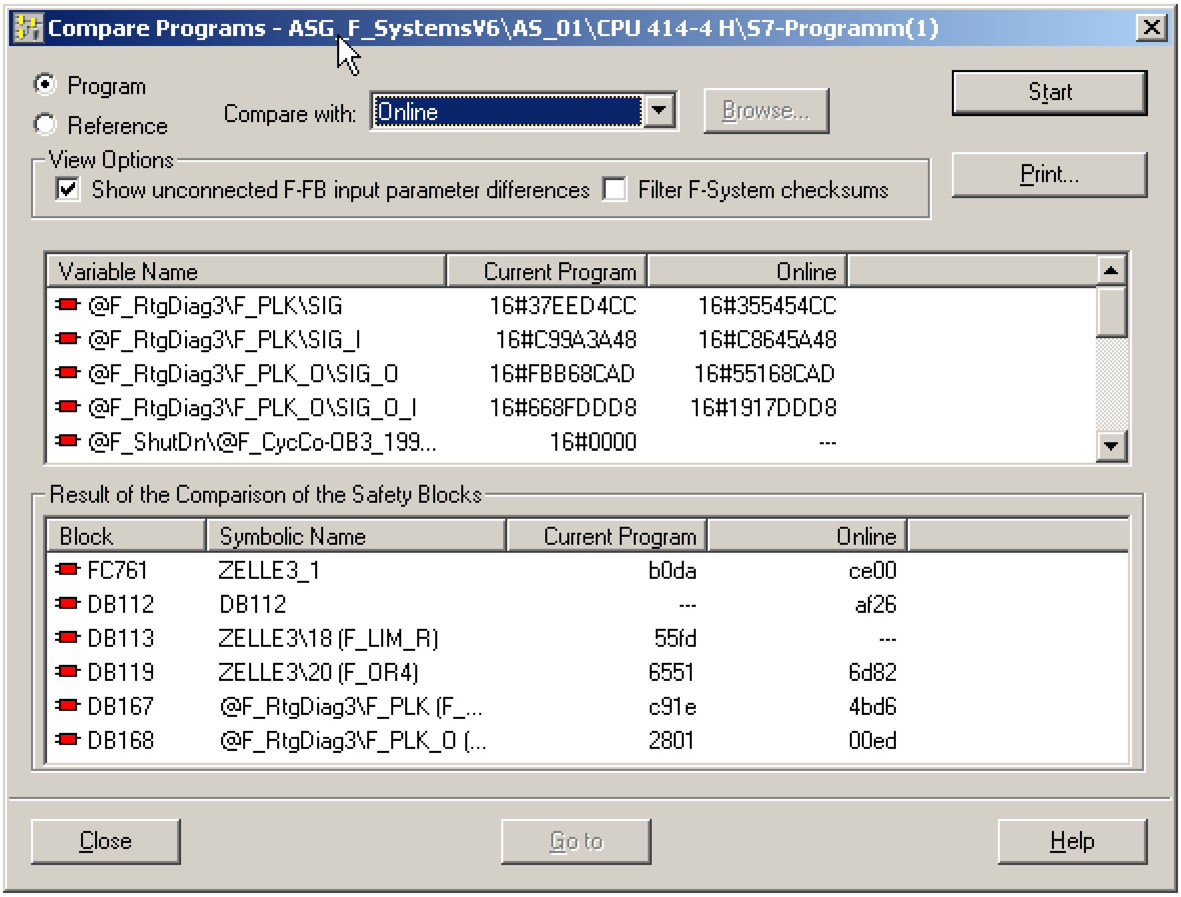
"Show unconnected F-FB input parameter differences" view option

This option compares the assigned parameter values of all non-interconnected inputs. It compares the online program to the offline program.

The differences are displayed in the list at the top of the dialog box.

This view option is normally selected only if the collective signatures already match. This indicates that the offline program has not been changed since the last time it was downloaded to the F-CPU.

This option enables you to perform a thorough search for parameters that have been changed online, but not through compilation or download.



Compare Programs - ASG_F_SystemsV6\AS_01\CPU 414-4 H\S7-Programm(1)

● Program
○ Reference

Compare with: Online

View Options
☑ Show unconnected F-FB input parameter differences ☐ Filter F-System checksums

Variable Name	Current Program	Online
@F_RtgDiag3\F_PLK\SIG	16#37EED4CC	16#355454CC
@F_RtgDiag3\F_PLK\SIG_I	16#C99A3A48	16#C8645A48
@F_RtgDiag3\F_PLK_O\SIG_O	16#FBB68CAD	16#55168CAD
@F_RtgDiag3\F_PLK_O\SIG_O_I	16#668FDDD8	16#1917DDD8
@F_ShutDn\@F_CycCo-OB3_199...	16#0000	---

Result of the Comparison of the Safety Blocks

Block	Symbolic Name	Current Program	Online
FC761	ZELLE3_1	b0da	ce00
DB112	DB112	---	af26
DB113	ZELLE3\18 (F_LIM_R)	55fd	---
DB119	ZELLE3\20 (F_OR4)	6551	6d82
DB167	@F_RtgDiag3\F_PLK (F_...	c91e	4bd6
DB168	@F_RtgDiag3\F_PLK_O (...	2801	00ed

"Filter F-System checksums" view option:

This option suppresses expected differences that can occur when the F-CPU writes to specific F-Blocks (for example, input signature values of F_PLK and F_PLK_O). You can only use this view option in connection with the "Show unconnected F-FB input parameter differences..." option.

"Print" button

Click this button to print out the result of the comparison.

"Go to" button

In the chart view, you can select any F-Block or parameter in the differences display and then click this button to access the relevant block in the *CFC Editor*.

See also

Upgrade to S7 F Systems V6.3 (Page 36)

12.4 Printing project data of the safety program

Requirement

The safety protocol can be printed in landscape format.

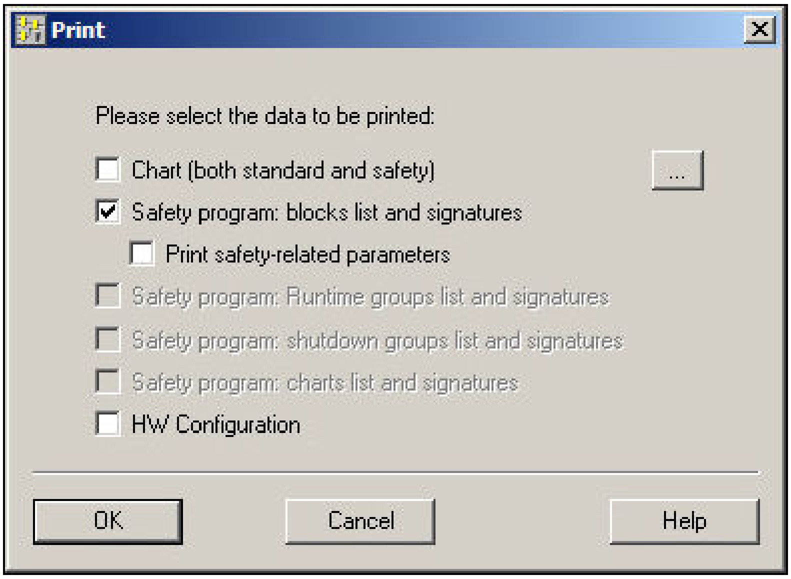
To ensure that all columns are printed, make the following settings:

1. In SIMATIC Manager, select the menu command **File > Page Setup...**. In the following dialog, select landscape format in the "Paper Size" tab.
2. Also select landscape in the format settings of the printer or the PDF generator.

Procedure:

You receive a printout of all important project data as follows.

1. Select the program folder (e.g., "S7 Program").
2. Select the menu command **Options > Edit Safety Program**.
   The "Safety Program" dialog will appear.
3. Click "Print". In the "Print" dialog, you can select the parts of the project you want to print:



Print

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

The selectable print options in this dialog depend on the selected option "Blocks", "Runtime groups", "Charts" or "Shutdown groups" in the "Safety Program" dialog.

– **Chart (both standard and safety):**
  Prints all or selected charts of the standard program and safety program in a graphical representation.
  A selection dialog for selecting the charts to be printed can be opened using the "..." button. Additional information can be found in the next section "Selecting the charts for printing".
  If not all charts were selected in the selection dialog, the "Chart (both standard and safety)" check box is shown partially activated.

– **Safety program: Block list and signatures**
  Offline/online status log
  Name of the safety program
  Date of the last compile operation and the collective signature of the safety program
  Date of the last compile operation and collective signature of the reference program
  F-blocks in the safety program
  Print safety-related parameters
  The footer on each page of the printout shows you the version of S7 F Systems used to generate the printout along with the collective signature.

– **HW configuration:**
  Printout of the complete hardware configuration or portions thereof. The "Print" dialog will appear so that you can specify what information is to be printed for the F-I/O.

The printout of the safety program also contains the collective signature and the date of the last compilation, which are relevant to the on-site acceptance of the safety program (e.g. by experts). The collective signature of the compiled S7 program appears twice in the printout:

1. In the program information section as a value of the block container
2. In the footer as a value from the chart container

(See also section "Checking the signatures").

Selecting the charts for printing

In the "Select charts" dialog, you can select charts for printing.

To open this dialog, open the "Print" dialog using the "Print" button in the "Safety program" dialog and then click the "..." button of the "Chart (both standard and safety)" option.

Structure of the dialog:

- "Target system"
  The output field shows the target system from which the charts are selected.
- "Program name"
  The output field shows the path and the name of the S7 program from which the charts are selected.
- "Filter" drop-down list
  A variety of options are available in the drop-down list for filtering the charts.
- "Display" entry field
  In this field, you can enter one or more characters to be searched for in the currently displayed chart names in the table. The filter result is immediately displayed in the table.
- Table:
  The table shows the charts available for selection. The content of the table is influenced by the "Filter" drop-down list and the "Display" entry field.
  - Only the selected charts are printed, i.e. the charts for which the check box in front of the chart name is selected.
  - Functions in the shortcut menu of a table row, e.g. "Invert selection", and the shortcut "<Ctrl>+<A>" are available for selection.
  - The width of the table columns can be changed in the table header.

12.5 Safety mode

12.5.1 Overview of safety mode

Introduction

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

Description

All the safety mechanisms for fault detection and fault reaction are activated in safety mode. The safety program cannot be modified during operation (in RUN mode) in safety mode.

You can activate or deactivate safety mode in the F-CPU in RUN mode using the "Safety Mode..." button in the "Safety Program" dialog. Downloading safety program changes in RUN mode is only made possible by temporarily switching the safety mode to "deactivated" using this button.

The window below this button indicates whether safety mode is "activated" or "deactivated". It will indicate "Unknown" if the safety program does not correspond to the safety program in the F-CPU or if no communication is taking place with the F-CPU.

You can also determine whether or not safety mode is enabled from the SAFE_M output of the F_SHUTDN block (located in the @F_ShutDn chart).

See also

Overview of downloading the safety program (Page 213)

12.5.2 Deactivating safety mode

Introduction

Deactivation of safety mode enables changes to be made to the safety program during operation (RUN). For this purpose, mechanisms for detecting changes to the safety program that would trigger shutdown of the safety program and its outputs in activated safety mode are deactivated. The safety program and thus the programmed safety functions continue to be executed. "Incidental hardware faults" will continue to be detected and the diagnostics of the modules remain active.

⚠ WARNING

Deactivating safety mode

Because changes can be made to the safety program in RUN mode when safety mode is deactivated, you must observe the following:

- Deactivation of safety mode is intended for test purposes, commissioning, etc. Whenever safety mode is deactivated, the safety of the plant must be ensured by other organizational measures, such as operation monitoring and manual safety shutdown.
- Deactivation of safety mode must be verifiable. Logging is required and can, for example, be guaranteed by using an OS. The automatically placed F_SHUTDN block generates corresponding messages for this. Otherwise, you must log the deactivation of safety mode through organizational measures.
- Furthermore, we recommend that deactivation of safety mode be displayed, e.g. on the OS. For this purpose, the automatically placed F-block F_SHUTDN sets the SAFE_M output to "0" when safety mode is deactivated (or F-block F_TESTM sets the TEST output to 1).
- Safety mode is deactivated only F-CPU-wide. You must observe the following for safety-related CPU-CPU communication:
  If the F-CPU with the F_SENDBO, F_SENDR or F_SDS_BO is in deactivated safety mode, you can no longer assume that the data sent by this F-CPU were generated safely. To ensure the safety of the parts of the plant influenced by the sent data, you must then also take organizational measures, e.g. monitored operation and manual safety shutdown, or output safe fail-safe values instead of the received data in the F-CPU with the F_RCVBO, F_RCVR or F_RDS_BO through evaluation of SENDMODE.

FSW-045

Requirements

The F-CPU is in RUN mode and safety mode is activated.

Procedure

1. Select the F-CPU or its S7 program in SIMATIC Manager.
2. Select the menu command **Options > Edit Safety Program**.
3. Select the "Safety mode" button.

You can then download changes in the safety program to the F-CPU during operation (in RUN mode).

12.5.3 Activating safety mode

Introduction

After changes in the safety program are downloaded, you must reactivate safety mode in order to guarantee safe execution of the safety program.

Requirements

The F-CPU is in RUN mode and safety mode is deactivated.

Procedure

1. Select the F-CPU or its S7 program in SIMATIC Manager.
2. Select the menu command **Options > Edit Safety Program** .
3. Select the "Safety mode" button.

Note

If the safety program detects a safety-related error during deactivated safety mode, it is no longer possible to activate safety mode. You then receive a corresponding message with corrective actions.

See also

Downloading changes (Page 220)

12.6 Downloading the safety program

12.6.1 Overview of downloading the safety program

Introduction

After compiling, you can load the CFC program into the target system. Depending on whether Safety mode is enabled or disabled, you can load the entire Safety program or changes to the Safety program as follows

Download ...	F-CPU in STOP	F-CPU in RUN, safety mode activated	F-CPU in RUN, safety mode deactivated
Entire S7 program	Possible	F-CPU is automatically set to STOP by the CFC Editor	F-CPU is automatically set to STOP by the CFC Editor
Changes in the standard user program	Possible	Possible	Possible
Changes in the entire S7 program	Possible	Not possible	Possible

Requirements

- The hardware configuration data of the station is downloaded to the F-CPU
- The S7 program was compiled without error.
- You have access rights to the target system.
- There is an online connection between the F-CPU and your ES.

Rules for downloading

- You can only download the safety program from the CFC Editor or from the SIMATIC Manager via the chart folder.
- When an accepted safety program is downloaded, you must check the collective signature after downloading the same as for acceptance.
(See also the section "Collective signature" in section "Downloading the S7 program to the F-CPU (Page 235)").

⚠ WARNING

Do not copy F-Blocks with SIMATIC Manager

As is usual in PCS 7, you must not copy individual blocks between the block containers online and offline. To do this, use the downloading in the CFC Editor or download the chart folder.

You can find more detailed information in the "SIMATIC Process Control System PCS 7 CFC for SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/90683154)" manual, section "Downloading" and "Reading back charts".

FSW-046

12.6.2 Downloading the S7 program

Procedure

To load the safety program to the PLC, use the menu command **PLC > Download > Entire program** in the CFC Editor. The F-CPU is thereby set to STOP.

Note

Before the safety program is downloaded, a prompt for the password of the F-CPU is displayed when changes in the safety program are detected.

Working with safety programs on memory card

⚠ WARNING

Safety program on a memory card

If you are using the safety program on a memory card, you must observe the following:

- Before you switch the S7 F System to RUN mode, compare the collective signature of the safety program on the Flash EPROM memory card with the collective signature of the reference data. If necessary, mark the memory card with the collective signature.
- For a fault-tolerant S7 FH System, you ensure that the memory cards of the redundant F-CPUs are of the same type (RAM or Flash EPROM) and redundant Flash EPROM memory cards contain the same safety program.
- You ensure access protection with regard to removal and insertion of memory cards.
- Online parameter changes must not be performed when using Flash EPROM memory cards, since the values changed online are lost during a transition from STOP to RUN. If it is not possible or desired to block the online change, e.g. for commissioning, the program must be read back after the online change and then the entire program must be downloaded so that the changes are transferred to the Flash EPROM memory card.

FSW-047

⚠ WARNING

Downloading the safety program with multiple F-CPUs

If multiple F-CPUs can be reached from an ES via a network (e.g. MPI), you must take the following additional measures to ensure that the safety program is downloaded to the correct F-CPU.

Use F-CPU-specific passwords, e.g. a password for the F-CPUs with appended MPI address "FCPUPW_8". The password has a maximum of 8 characters, including at least one special character. In STEP 7 V5.5.4 HF9 and higher, the password must contain 8 characters for new projects.

Note the following:

- Before a safety program for which access permission by means of an F-CPU password does not yet exist is downloaded to an F-CPU, any existing access permission for another F-CPU must first be canceled.

FSW-048

12.7 Testing a safety program

Introduction

Testing is performed as usual in CFC by switching to test mode.

Switching to test mode

After compiling and downloading, you have the opportunity to test the safety program. You can test safety programs by switching to test mode with the menu command **Test > Test mode** in the CFC Editor. In Test mode, you are connected online with the automation system (F-CPU).

Rules for testing

⚠ **WARNING**

Shutdown of the safety program following changes to the fail-safe outputs

In test mode of the CFC Editor, you can monitor safety programs and change unconnected inputs of F-blocks. Changes made online to fail-safe outputs and automatically supplied connections are not permitted; they cause the safety program to shut down.

FSW-049

12.7.1 Testing with S7-PLCSIM

Procedure

The S7-PLCSIM software package enables you to simulate a Safety program on your ES.

To simulate your safety program with S7-PLCSIM, proceed as in the standard scenario.

When you download the safety program in S7-PLCSIM, the "Set Up Access Rights" dialog box appears. You will be prompted for the password for the F-CPU.

You can only download changes in the safety program with the complete safety program.

Note

If an F-STOP is triggered for the safety program, you must then follow the procedure below:

- Memory reset of the virtual F-CPU (S7-PLCSIM).
- Download the configuration data and the S7 program again.

⚠ WARNING

A simulation is no substitute for a function test!

If the simulation takes place on an engineering system with an online connection to the F-CPU, you must not deactivate safety mode. In addition, you are not permitted to have access permission through the password for the F-CPU.

FSW-050

12.8 Modifying a safety program

12.8.1 Overview for changing the safety program

Introduction

Changes in the safety program can be made offline as well as online. Online changes are made by means of the CFC test mode and take effect immediately. You must then download offline changes to the F-CPU.

Note

Safety program changes made otherwise, for example, by means of the "Monitor/Modify Variables" function, can lead to an F-STOP.

12.8.2 Online changes in CFC test mode

Introduction

In test mode of the CFC Editor, you have the option of changing the values of non-interconnected inputs of F-blocks during operation.

Rules

- For inputs in safety data format, you may only change the DATA component and not the COMPLEM or PAR_ID component.
- You are not permitted to change outputs or any inputs not documented in the block description.

Requirements

Ensure that the following requirements are met before you switch on test mode of the CFC Editor:

- The F-CPU must be in RUN mode.
- Safety mode of the safety program must be deactivated. Otherwise, you will be prompted to deactivate safety mode when you attempt to change the first parameter.

WARNING

Change of the collective signature following changes in CFC test mode

Changing the safety program in CFC test mode causes the collective signature to change. This means that the safety program must undergo acceptance again, if necessary.

FSW-051

Procedure

For changing the fail-safe block I/O, follow the usual procedure in the CFC Editor.

The collective signature at the F_SIG_OUT output of the F_SHUTDN F-block is set to 0 at the first change in CFC test mode and updated after CFC test mode is ended.

WARNING

Do not change values created during compilation

When safety mode is activated, direct operator control of safety programs is not permitted! You may input safety parameters for non-interconnected inputs:

- from the standard user program via F-conversion blocks with additional validity check
  or
- in test mode of the CFC Editor and with deactivated safety mode
  or
- with the "Safety Data Write" or "Secure Write Command++" function

Failure to observe this warning will trigger an F-STOP. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error detected" (event ID 16#75E1)

FSW-052

12.8.3 Downloading the changes

12.8.3.1 Downloading changes

Requirements

- Safety mode must be deactivated.
- S7 FH Systems must be in redundant system state.

Procedure

1. To download changes in the safety program, follow the usual procedure for downloading changes in CFC. For more information, refer to the "SIMATIC Process Control System PCS 7 CFC for SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/90683154)" manual.
2. Activate safety mode again by responding to the prompt that appears.
3. If necessary, repeat Steps 1 and 2 to download incremental changes, for example.
4. In the SIMATIC Manager select the menu command **Options > Edit safety program**.
5. Follow the procedure described in Section "Acceptance test of safety program changes (Page 237)".

⚠ WARNING

Abort of download operation

If the download operation is aborted, you must repeat the download and the check of the collective signature online and offline. In this way, you ensure the consistency of data in the load memory and work memory.

FSW-053

Note

Undoing changes

If you undo a change and download it nevertheless, it is possible that a different collective signature will be generated than before the change.

⚠ WARNING

Moving F-blocks or F-runtime groups

Note that

- F-blocks that were moved to another F-runtime group
  or
- F-runtime groups that were moved to another task

while downloading changes over multiple processing cycles may be processed multiple times or not at all.

FSW-054

⚠ WARNING

Modifying the safety program in RUN mode

- When changes are made to the safety program in RUN mode when safety mode is deactivated, switchover effects may occur. Take additional organization measures to ensure that this does not impair the safety of the plant.
- Whenever possible, the standard user program and the safety program should be changed separately and the changes downloaded. Otherwise, an error may be downloaded to the standard user program while the required protection function in the safety program is not yet effective or switchover effects may occur in both programs.

FSW-055

Note

- Note also the corresponding FAQs (http://support.automation.siemens.com/WW/view/en/13711209/133000) on the Internet regarding downloading changes.
- Changes to the automatically generated charts and F-runtime groups are generally forbidden and may trigger an F-STOP. Exceptions:
  - The MAX_CYC parameter of the F_CYC_CO blocks for which you assign the F-monitoring time for a cyclic interrupt OB
  - Parameter assignments for the F_SHUTDN block for the F-shutdown behavior

Note

Splitting or combining F-runtime groups when safety programs are running represents an essential change in the run sequence. Before downloading changes with the "Compare safety programs" dialog, check for moved F-module drivers.

This can lead to the following unintended behavior when changes are downloaded in RUN mode:

- Passivation of output channels
- Processing of outdated input data at the input channels

The change in the run sequence causes the associated F-module drivers to be moved to other F-runtime groups.

12.8.3.2 Changes that can be transferred by downloading changes

You can transfer the following changes to the F-CPU by downloading changes.

If you do not observe the information in Chapter "Downloading changes (Page 220)" and the boundary conditions listed below, an F-STOP can be triggered for the safety program.

- Inserting new F-Runtime groups with new instances of F-Blocks/F-Block types.
- Inserting, modifying, and deleting interconnections of F-Blocks.
- Deleting and reinserting F-Blocks or moving F-Blocks in the runtime sequence within the F-Runtime group.
- Changing values of inputs and outputs of F-Blocks.
  Exception: Changes in safety-related communication between F-CPUs (see " Change in the safety-related communication between F-CPUs (Page 224) ")
- Moving of instances of F-Blocks/F-Block types between F-Runtime groups within an F-Shutdown group.
- Moving of instances of F-Blocks between F-Runtime groups of different F-Shutdown groups.
  Boundary condition: Note that all fail-safe channel drivers of an F-I/O must be contained in a common F-Shutdown group.
- Inserting/deleting F-Shutdown groups by means of F_PSG_M
  Boundary condition:
  - The must be no instances of F-Block types prior to the position in the F-Shutdown group where you insert or delete the F_PSG_M.
  - Note that all fail-safe channel drivers of an F-I/O must be contained in a common F-Shutdown group.
- Moving the F-Runtime groups that do not contain instances of F-Block types to another task.
  Boundary conditions:
  - Note that all fail-safe channel drivers of an F-I/O must be contained in a common F-Shutdown group.
- Adding F-I/O by means of CiR
  Boundary condition: Note the information about CIR in Chapter " System modifications during operation (Page 70) ".

12.8.3.3 Changes requiring an F-Startup

The following changes require an F-startup of the safety program. You cannot download these changes to the F-CPU without triggering an F-STOP, see section "F-STOP (Page 99)". These changes may only be transferred with a complete download.

- Splitting/merging F-shutdown groups using F_PSG_M
  - There are instances of F-block types before the position within the F-shutdown group where you insert or delete F_PSG_M.
- Moving instances of F-block types between different F-shutdown groups
- Moving F-runtime groups with instances of F-block types to another task.

12.8.3.4 Changes that require a cold restart or warm restart (restart) of the F-CPU

The following changes take effect only after a cold restart or warm restart of the F-CPU:

- Changes in values of the ID or R_ID parameter of the F-blocks F_SENDR/BO, F_RCVR/BO, F_SDS_BO and F_RDS_BO. (See also section " Change in the safety-related communication between F-CPUs (Page 224) ".)

Note

In the PCS 7 process control system and when blocks from PCS 7 libraries are used, the startup type "Cold restart" is not permitted.

12.8.3.5 Changes that require an F-CPU STOP in a single CPU

In an S7 FH system you can make changes to the hardware configuration in the same way as in an S7 H system, see manual "Automation System S7-400H Fault-Tolerant Systems (http://support.automation.siemens.com/WW/view/en/82478488)".

If you operate a non-redundant F-CPU, these changes can only be downloaded via a STOP of the F-CPU.

Special features for S7 FH systems:

- In an S7 FH system, the F-I/Os can only receive a changed configuration after pulling and plugging. The F-I/Os detect a communication error after loading the first change.

12.8.3.6 Changing the time ratios or F-Monitoring times

Make sure that time monitoring is not triggered when changing the time conditions or F-monitoring times.

- Changing the OB cycle time

Procedure for changing the OB cycle time

1. Calculate the minimum F-monitoring times for the OB cycle time using the new desired value:
   - F-cycle time monitoring at input MAX_CYC at F-control block F_CYC_CO
   - TIMEOUT inputs of the F-blocks for safety-related communication between F-CPUs
   - TIMEOUT inputs of the F-blocks for data exchange between F-shutdown groups
   - F-I/Os

   For more information about the F-Monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".
2. If the previously configured values are less than the newly calculated values, you must increase the F-monitoring times before changing the OB cycle time. Compile the S7 program and download the changes.
3. Change the OB cycle time.

   Note

   Changing the OB cycle time also changes the hardware configuration. Read also section "Changes that require an F-CPU STOP in a single CPU (Page 223)".

- Moving F-runtime group to another task
  Corresponds to changing the OB cycle times of the affected tasks (see above).
- Changing F-monitoring times on F-blocks for safety-related communication between F CPUs and for data exchange between F-shutdown groups.
- Changing the F-monitoring times of an F-I/O.

  Note

  Changing the F-monitoring times of an F-I/O also changes the hardware configuration. Read also section "Changes that require an F-CPU STOP in a single CPU (Page 223)".

When changing these F-monitoring times, make sure that the calculated minimum F-monitoring times do not fall below the limits. For more information about the F-Monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

12.8.3.7 Change in the safety-related communication between F-CPUs

Introduction

If safety-related communication between F-CPUs is to continue in all phases, you need to proceed in several steps.

Rule

Never change the interconnection for the send data at F_SENDBO/F_SDS_BO/F_SENDR and for the corresponding receive data at F_RCVBO/F_RDS_BO/F_RCVR at the same time. Otherwise, the simultaneous activation of the new interconnections is not ensured.

Procedure for changing the interconnections

To change an interconnection to the send data of the F_SENDBO/F_SDS_BO/F_SENDR F-blocks or the receive data of the F_RCVBO/F_RDS_BO/F_RCVR, you must adhere to the following sequence:

1. Interconnect the new data to be sent with a previously unused SD_BO_xx/SD_R_xx input of F_SENDBO/F_SDS_BO/F_SENDR. Compile the S7 program and download the change.
   Result: The new data is then available at the corresponding RD_BO_xx/RD_R_xx output of F_RCVBO/F_RDS_BO/F_RCVR.
2. Interconnect the blocks for further processing of the received signal to the new RD_BO_xx/RD_R_xx output. Compile the S7 program and download the change.
   Result: This results in a consistent switchover to the new data path.
3. Delete the superfluous connection at F_SENDBO/F_SDS_BO/F_SENDR.
4. Compile the S7 program and download the change.

Procedure for exchanging the communication partner

When exchanging a communication partner, you need to adhere to the following sequence:

1. Configure the new S7 connection in NetPro. Download the connection data in RUN.
2. Place a new instance of F_SENDBO/F_SDS_BO/F_SENDR on the send page. Configure the ID and R_ID inputs with the data of the new S7 connection. Interconnect the new data to be sent with the SD_BO_xx/SD_R_xx inputs of the F_SENDBO/F_SDS_BO/F_SENDR. Compile the S7 program and download the change.
3. Place a new instance of F_RCVBO/F_RDS_BO/F_RCVR on the receive page. Configure the ID and R_ID inputs with the data of the new S7 connection.
   Compile the S7 program and download the change.
   Result: This makes the data of the old and new communication partner available to you on the receiver side.
4. Interconnect the blocks for further processing of the received signals to the RD_BO_xx/RD_R_xx outputs of the new F_RCVBO/F_RDS_BO/F_RCVR.
   Delete the superfluous F_RCVBO/F_RDS_BO/F_RCVR. Compile the S7 program and download the change.
   Result: This ensures a consistent switchover to the new communication partner.
5. Delete the superfluous F_SENDBO/F_SDS_BO/F_SENDR. Compile the S7 program and download the change.
6. If necessary, delete the superfluous connection from *NetPro*. Download the connection data in RUN.

12.8.3.8 Initial run and startup characteristics

Newly inserted F-Blocks execute an initial run after online changes. In this regard, note the startup characteristics described in the block descriptions. In cases where the initial run is not specifically mentioned, the behavior described after an F-Startup also applies to the initial run.

12.9 Deleting the safety program

Procedure

To delete a safety program from an F-CPU, proceed as follows:

1. Delete all F-charts from the chart folder. The symbols of these charts are located in the SIMATIC Manager and are highlighted in yellow.
2. Delete all charts whose name begins with "@F_".
3. Compile the S7 program with the option "Generate module drivers" selected.
4. In HW Config, open the properties dialog of the associated F-CPU from which you want to delete the safety program. Remove the check mark at "CPU contains safety program" under "Protection".
5. Compile and load the hardware configuration.
6. Compile and download the S7 program.

12.10 Acceptance test following system upgrade

Acceptance after a system upgrade

The following tables show whether an upgrade to S7 F Systems V6.3 changes the signature and necessitates a STOP of the F-CPU or a new acceptance.

Upgrade from	Change of signature	STOP of F-CPU required	New acceptance required
S7 F Systems V6.0 (or higher) without update of the F-library (starting from S7 F Systems Lib V1.3)	No	No	No

Upgrading from S7 F Systems Library V1.3 to S7 F Systems Library V1.3 SP1	Change of signature	STOP of F-CPU required	New acceptance required
• With use of the new F-blocks	Yes	No	Changes
• With use of the changed F_CH_DO	Yes	Yes [1]	Changes
• With use of the changed F_CH_BI	Yes	No	Changes
• With use of the changed F_QUITES	Yes	No	Changes
• With use of the changed F_CH_AI	Yes	No	Changes
• With use of the changed F_PA_AI	Yes	No	Changes
• With use of the changed F_SQRT	Yes	No	Changes
• With use of the changed F_CHG_BO	No	No	Changes
• With use of the changed F_CHG_R	No	No	Changes

1): The change is not safety-related and does not influence the usability of the existing project.

You can find additional information on this in section "Differences between the F-libraries S7 F Systems Library V1.3 and V1.3 SP1 (Page 478)".

Upgrading from S7 F Systems Library V1.3 SP1 to SP2	Change of signature	STOP of F-CPU required	New acceptance required
• When the new F-blocks are used (F_SWC_CB, F_SWC_CR, F_CH_RI)	Yes	Yes	Changes
• With use of the changed F_XOUTY	Yes	Yes	Changes
• With use of the changed F_2oo3AI	Yes	Yes	Changes
• With use of the changed F_CH_AI	Yes	Yes	Changes
• With use of the changed F_TESTC / F_PLK	Yes	Yes	Changes
• With use of the changed F-blocks for F-communication: F_SDS_BO, F_SENDBO and F_SENDR	Yes	No	Changes
• With use of the changed F-blocks for F-communication: F_RDS_BO, F_RCVBO und F_RCVR	Yes	Yes	Changes
• When the changed F-block F_SWC_BO for Maintenance Override (MOS) is used	Yes	No	Changes
S7 F Systems Library V1.3 SP2 to SP3			

You can find additional information on this in section "Differences between the F-libraries S7 F Systems Library V1.3 SP1 and SP2 (Page 479)".

Upgrading from S7 F Systems Library V1.3 SP2 to SP3	Change of signature	STOP of F-CPU required	New acceptance required
• With use of the new F-block F_PS_13	Yes	No	Changes
• With use of the new F-block F_CH_QBI	Yes	No	Changes
• With use of the new F-block F_CH_QBO	Yes	No	Changes
• With use of the new F-block F_CH_QII	Yes	No	Changes
• With use of the new F-block F_CH_QIO	Yes	No	Changes
• With use of the changed F-block F_PS_12	Yes	Yes	Changes
• With use of the changed F-block F_PS_MIX	Yes	No	Changes
• With use of the changed F-block F_SWC_BO	Yes	Yes	Changes
• With use of the changed F-blocks for F-communication: F_SDS_BO, F_SENDBO, F_SENDR, F_RDS_BO, F_RCVBO, F_RCVR	Yes	No	Changes
• With use of the changed F-block F_CH_DO	Yes	Yes	Changes
• With use of the changed F-block F_CH_AI	Yes	Yes	Changes

1): The change is not safety-related and does not influence the usability of the existing project.

You can find additional information on this in section "Differences between the F-libraries S7 F Systems Library V1.3 SP2 and SP3 (Page 480)".

System Acceptance Test 13

13.1 Overview of system acceptance test

Introduction

During the system acceptance, all relevant application-specific standards must be adhered to as well as the following procedures. This also applies to plants that are not subject to acceptance. For the acceptance, you must observe the requirements subject to approval in the report for the certificate.

As a general rule, the acceptance of an F-system is performed by an independent expert.

Special functions in the SIMATIC Manager support you during the acceptance of an F-system. This allows you to:

- Compare safety programs
- Log the safety program
- Print out the safety program

All data relevant for the acceptance of the S7 F system can be archived in the SIMATIC Manager (**File > Archive**) and printed out if required.

You can find more information on these topics in the sections "Comparing safety programs (Page 200)", ""Logs..." button (Page 197)" and "Printing project data of the safety program (Page 207)".

13.2 Commissioning a safety program

13.2.1 Initial acceptance test of a safety program

Basic procedure for the initial acceptance of a safety program

1. Preliminary test of the configuration of the F-CPU and F-I/O (optional)
2. Backup of the STEP 7 project
3. Inspection of the printout
4. Downloading the S7 program to the F-CPU
5. Execution of a complete function test

13.2.2 Checking the configuration of the F-CPU and F-Peripheries

Introduction

After you finish configuring the hardware and assigning parameters for the F-CPU and F-I/O, you can perform an initial acceptance for the F-I/O configuration.

In order to do this, the hardware configuration data must be printed out, checked, and saved together with the overall STEP 7 project.

Printing hardware configuration data

1. Select the correct F-CPU or S7 program assigned to it.
2. In the SIMATIC Manager select the menu command **Options > Edit safety program**.
   The "Safety Program" dialog will appear.
3. Click the "Print" button and select the "HW Configuration" option in the next dialog:
4. Select "All" for the print range, and select the "Module description" and "Address list" options there. In addition, select the "Including parameter description" option to include your parameter descriptions in the printout.

Checking hardware configuration data

1. Check the parameters of the F-CPU in the printout.
In safety mode, access by means of the F-CPU password must not be authorized when making changes to the standard user program, since changes to the safety program can also be made. To rule out this possibility, you must configure **Protection Level 1**. In addition, you must select the "CPU contains safety program" option. The corresponding protection level and "CPU contains safety program" is included in the printout.

2. Check the safety-related parameters of the F-I/O in the printout.
These safety-related parameters can be found in the printout for the respective F-I/O. The data are structured differently according to the F-I/O as follows:
SM 326; DI 24 x DC 24V (article no. 6ES7326-1BK00-0AB0), SM 326; DI 8 x Namur, SM 326 DO 10 x DC 24V/2A and SM 336; AI 6 x13 Bit

   – The PROFIsafe source address does not appear in the printout.

   – You determine the PROFIsafe destination address from the address value under "Addresses – Inputs – Start". Divide this address value by "8".

   – The safety-related parameters are found under "Parameters – Basic Settings" or "Parameters – Input/Output x".

   Fail-safe modules ET 200S, ET 200SP, ET 200SP HA, ET 200pro, ET 200eco, ET 200iSP, SM 326; DI 24 x DC 24V (as of article no. 6ES7326-1BK01-0AB0) and SM 326; DO 8 x DC 24V/2A PM

   – The PROFIsafe source address is found under "Parameters – F-Parameters – F_Source_Address".

   – The PROFIsafe destination address is found under "Parameters – F-Parameters – F_destination_address".

   – The safety-related parameters are found under "Parameters – F-Parameters" and "Parameters – Module parameters".

   Fail-safe DP standard slaves/IO standard devices

   – The PROFIsafe source address is found under "PROFIsafe – F_Source_Add".

   – The PROFIsafe destination address is found under "PROFIsafe – F_Dest_Add".

   – The safety-related parameters are found under "PROFIsafe".
   For information on handling of any technological safety-related parameters, refer to the documentation for the respective DP standard slave/IO standard device.

3. Once the safety-related parameters of an F-I/O module are checked, the parameter CRCs in the printout are sufficient as reference for further acceptance. These parameter CRCs have the following appearance (address/F-address = PROFIsafe address):
   Fail-safe signal modules S7-300 (SM 326; DI 24 x DC 24V, with article no. 6ES7326-1BK00-0AB0; SM 326; DI 8 x NAMUR; SM 326; DO 10 x DC 24V/2A; SM 336; AI 6 x 13-bit)
   Example:

   – Parameters - CRC: 12345

   – Parameters - CRC (without F-addresses): 54321

   Fail-safe modules ET200S, ET 200SP, ET 200SP HA, ET 200pro, ET 200eco, ET 200iSP and S7-300 fail-safe signal modules (SM 326; DI 24 x DC 24 V, as of article no. 6ES7326-1BK01-0AB0; SM 326; DO 8 x DC 24V/2A PM)
   Example:

   – Parameters - CRC: 12345

   – Parameters - CRC (without F-addresses): 54321
   As of PROFIsave profile V2.6.1:

   – Parameters - CRC (CRC_FP): 0x4a22fed8 (1243807448)

   – Parameters - CRC (without F-addresses): 0xD410 (54288)

   Fail-safe DP standard slaves/IO standard devices
   Example:

   – Parameters - CRC: 12345

   – Parameters - CRC (without F-addresses): 54321
   As of PROFIsave profile V2.6.1:

   – F_iPar_CRC 0x59C752D1 (1506235089)

   – F_Par_CRC 0x5D49 (23881)

   – F_Par_CRC (without F addresses): 0x2391 (9105)

   F-I/O that are to be assigned the same safety-related parameters can be copied during configuration. All safety-related parameters for these no longer have to checked individually: It is sufficient to compare every other CRC (for example, "Parameter CRC (excluding address)") of the copied F-I/O to the corresponding CRC of the previously checked F-I/O and to check the PROFIsafe source and destination addresses.

4. Check that the PROFIsafe addresses are unique from one another.
   To determine the PROFIsafe addresses of individual F-I/O, refer to step 1.

⚠ WARNING

Address assignment in subnets only and in mixed configurations

The following applies to PROFIBUS DP subnets only:

The PROFIsafe destination address and, thus, the switch setting on the address switch of the F-I/O must be unique network-wide* and station-wide** (system-wide). You can assign up to 1022 different PROFIsafe destination addresses.

The following applies to PROFINET IO subnets only and mixed configurations of PROFIBUS DP and PROFINET IO:

The PROFIsafe destination address and, thus, the address switch setting on the F-I/O must be unique only*** within the PROFINET IO subnet, including all lower-level PROFIBUS DP subnets, and station-wide** (system-wide).

For S7-300 F-SMs and ET 200S, ET 200eco, ET 200iSP and ET 200pro F-modules, you can assign a maximum of 1022 different PROFIsafe destination addresses. For ET 200SP and ET 200SP HA max. 65534 destination addresses are possible.

A PROFINET IO subnet is characterized by the fact that the IP addresses of all networked nodes have the same subnet address, i.e. the IP addresses match in the positions that have the value "1" in the subnet mask.

Example:

IP address: `140.80.0.2.`

Subnet mask: `255.255.0.0 = 11111111.11111111.00000000.00000000`

Meaning: Bytes 1 and 2 of the IP address define the subnet; subnet address: `140.80.`

* A network consists of one or more subnets. "Network-wide" means across subnet boundaries.

** "Station-wide" means for one station in HW Config (e.g. an S7-400H station).

*** Across Ethernet subnets, excluding cyclic PROFINET IO communication (RT communication)

FSW-056

13.2.3 Backup of the STEP 7 project

Requirement

Before acceptance, compile the safety program to be accepted.

Backup and archiving

The safety program to be approved must be backed up and archived with the entire STEP 7 project. All project data must be printed out unfiltered and archived together with the STEP 7 project:

- Chart (both standard and safety):
- Safety program: Block list and signatures
- Safety-related parameters
- HW configuration
- Compilation log
- Download log

The backup and archiving of STEP 7 projects is described in the basic help of STEP 7.

13.2.4 Inspection of the printout

Introduction

Print the entire project as described in the section "Printing project data of the safety program (Page 207)".

Printout

The printout contains the collective signature as a reference. The collective signature appears in the printout at two positions. All values must match the value in the footer.

- In the program information section as a value of the block container:
  - For the current compilation
  - For the reference
  - For the last online change (optional)
- In the footer as a value from the source

The following relations must be checked depending on an online change:

- If no online change has taken place, the collective signature for the current compilation must match the collective signature in the footer.
- If an online change has taken place, the collective signature in the footer corresponds to the collective signature of the last online change.

If a collective signature is not printed in the footer, this means that the safety program or the configuration (HW Config or NetPro) has changed. In this case, you must recompile the safety program.

The version number of the utilized S7 F Systems optional package appears in the footer of the printout and must be checked by you.

Check of safety-related parameters

Check the values of all safety-related parameters in the corresponding section of the printout for the safety program.

The following will be printed out:

- Values of all non-interconnected, invisible input parameters
- Values of all special input parameters to be checked, such as F-Monitoring times

A marking occurs in the printout:

- Marking "(*)":
  Values of all output parameters for which the runtime sequence does not correspond to the data flow
  This is the case if the F block is first called after the output parameter was already transferred to another F block, for example, in a feedback loop.
- Marking "(!)":
  Inputs or outputs on an F block that have been identified by the system as parameters to be taken into account in the printout

Checking the signatures and initial value signatures of the F-blocks

The signatures and initial value signatures of all F-blocks must match those in Annex 1 of the Certificate Report.

Checking the signatures and initial value signatures of the F-block types

The signatures and initial value signatures of all F-block types must match those in the acceptance documents of the F-block types (see section "Acceptance test of F-Block types (Page 238)").

The acceptance documents of the F-block types also list the signatures and initial value signatures of all called F-blocks. These signatures must also match those in the safety program.

13.2.5 Downloading the S7 program to the F-CPU

Introduction

Download the S7 program to the F-CPU as described in section "Downloading the safety program (Page 213)". Then check the signatures.

Checking the collective signatures

After downloading the S7-program to the F-CPU you have to compare the collective signature of the safety program in the F-CPU with the collective signature in the accepted printout. S7 FH Systems must be in redundant system state and safety mode must be activated.

You can get the collective signature of the safety program and the signatures of the F-blocks in the F-CPU with the menu command **Options > Edit safety program**.

13.2.6 Implementation of a complete function test

Overview

Requirements

For successful initial acceptance of a safety program, a complete function test is required.

For this purpose, corresponding test specifications must be implemented based on documented procedures in order to verify the configured safety functions and rule out unwanted side effects.

The following points must be observed:

- Conformity to the specification of the safety function
- Full coverage of the safety program during the function test

Note

The system charts created by S7 F Systems with prefix "@F_" do not have to be tested.

- Negative tests
- Tests for the time sequence and logic sequence

Results

The results of the function test must be documented, The following information should be present:

- Collective signature of the safety program
- Safety program printout
- Any utilized test tools including version
- Name of responsible persons
- Test description
- Test result

13.3 Acceptance test of safety program changes

Procedure

To perform an acceptance test on your safety program changes, follow these steps:

1. Back up your safety program.
2. Compare your new safety program with your accepted safety program. For more information, refer to Chapter " Comparing safety programs (Page 200) ".
3. Inspect the changes in the printout. You must locate the changes that you made to your safety program on the printout again. Check the signature in the printout (and in the footer). To do so, follow the same procedure as for the initial acceptance test.
4. Download your modified safety program to the F-CPU.
5. Perform a function test of your changes.

13.4 Acceptance test of F-Block types

Initial acceptance

The same process is used for initial acceptance of a newly created F-block type as for initial acceptance of a safety program. The function test of the F-block type must take place in a different safety program than the test environment.

For acceptance of F-block types, the signature and initial value signature of the resulting generated F-block are relevant. You can obtain these signatures from the printout of the safety program. In addition, you must also check the signatures and initial value signatures of the called F-blocks.

The collective signatures in the footers of the printouts of the safety program and the CFC chart of the F-block type must match. Otherwise, you must recompile the F-block type.

All F-blocks called in an F-block type must be compared.

Note

For testing a safety program in which an F-block type is used, you must check the signatures of the F-block type and the signatures of all called F-blocks.

Acceptance of changes

The process for acceptance of changes to an F-block type is the same as for a safety program.

For acceptance of the F-block types, use a printout to document the signature and initial value signature of the new F-block type as well as the signatures and initial value signatures of all F-blocks called in the F-block type.

In addition, you must use a function test to test all points in the test safety program at which the new F-block type is called. Changed signatures of F-blocks are displayed in the chart view when safety programs are compared.

Operation and Maintenance 14

14.1 Notes on safety mode of the safety program

Introduction

Below you will find the rules and safety instructions for the operation of S7 F/FH Systems.

Using simulation devices / simulation programs

⚠ WARNING

Safety of the F-system when using simulation devices / simulation programs

If you operate simulation devices / simulation programs that generate safety telegrams, e.g. according to PROFIsafe, and make them available to the F-system S7 F/FH System via the bus system (e.g. PROFIBUS DP), you must ensure the safety of the F-system using organizational measures, e.g. with observed operation and manual safety shutdown.

If you use the S7-PLCSIM STEP 7 function to simulate safety programs, these measures are not necessary, since S7-PLCSIM cannot establish an online connection to a real S7 component.

Note that, for example, a protocol analyzer is not allowed to execute a function for playback of recorded telegram sequences with correct time behavior.

FSW-057

STOP via ES operation, operating mode switch or communication function

⚠ WARNING

STOP not as a safety condition

Changing from STOP to RUN via ES operation, via operating mode switch or via communication function is not locked. With ES operation, for example, you only need to press a button to change from STOP to RUN. This is why you must not regard the STOP set via ES operation, operating mode switch or communication function as a safety condition.

Therefore, always switch off the F-CPU directly at the device during maintenance work.

FSW-058

Setting the F-CPU to STOP with the SFC 46 "STP".

⚠ WARNING

STOP state, which was initiated with SFC 46 "STP", is not a safety-related STOP

A STOP state that was initiated with the SFC 46 "STP" can easily be canceled via ES operation (even unintentionally). This is why the STOP initiated via the SFC 46 is not a safety-related STOP.

FSW-059

Fiber optic cables between the synchronization modules for S7 F/FH Systems

⚠ WARNING

Two F-CPUs not simultaneously as master system

In S7 F/FH Systems, you need to prevent having both F-CPUs acting as master systems at the same time. Otherwise, dangerous errors may occur.

Such a state (both F-CPUs master at the same time) can occur if the two fiber optic cables for coupling the F-CPUs are pulled or interrupted simultaneously in the Redundant system state of S7 F/FH Systems. This must be prevented by laying the fiber optic cables separately.

After the repair of an F-CPU, this condition (both F-CPUs simultaneously master) can also occur if the F-CPUs have not yet been connected over *both* fiber optic cables before the power supply is switched on.

Organizational measures must be taken to ensure that after an F-CPU has been replaced, both connections are established via fiber optics cables before the power supply is switched on.

FSW-060

Additional information

For information on replacing components in high-availability systems, refer to the manual "SIMATIC Fault-tolerant systems S7-400H (http://support.automation.siemens.com/WW/view/en/82478488) ".

14.2 Replacing software and hardware components

Replacement of software components

When you replace software components on your ES, e.g. in case of a new version of PCS 7 or STEP 7, you must observe the information on upward and downward compatibility in the documentation and in the readme files of these products.

Installing new versions of the software packages

After installing a new version of PCS 7, STEP 7 or the optional packages CFC, SCL etc., do the following:

1. Compile the S7 program in the new environment.
2. Compare the collective signature of the newly compiled S7 program with the collective signature of the accepted safety program (see also "Checking the collective signature" in section "Commissioning a safety program (Page 230)").
3. If the collective signatures are identical, the safety programs match.
4. If the collective signatures are not identical, the safety program has changed. In this case, follow the same procedure as for a change of the safety program.

Replacement of hardware components

You replace hardware components for S7 F/FH Systems (modules, batteries, etc.) the same as in standard mode.

Removal and insertion of F-I/O during operation

F-I/O can be removed and inserted during operation in exactly the same way as standard I/O. Note however that the replacement of an F-I/O during operation may trigger a communication error in the F-CPU.

You must acknowledge the communication error at the ACK_REI input of the F-channel driver in your safety program. Without acknowledgment, the F-I/O remains passivated.

CPU operating system update

- Check of the CPU operating system for F-validity:
  When a new CPU operating system is used (operating system update), you must check whether the utilized CPU operating system is permitted for use in an F-system.
  The annex of the certificate specifies the minimum CPU operating system version that ensures fail-safe compatibility. This specification and any information about the new CPU operating system must be observed.
- Replace the CPU with a CPU with firmware version V6.0 or higher:
  If a CPU with firmware version < V4.5 (only PROFIsafe V1 mode support) is replaced for a CPU with firmware version V6.0 or higher, the PROFIsafe communication is automatically switched to PROFIsafe V2 mode.
  All F-modules in the project must then be configured in HW Config to V2 mode and the CFCs must be created and compiled with the module driver.

Firmware update for interface modules

When using a new firmware for an interface module, e.g. IM155-6 PN (ET 200SP HA) (firmware update, see STEP 7 online help), you must observe the following:

If you have selected the check box "Activate firmware after download" during the firmware update, the IM is automatically reset after successful download and then runs with the new firmware. Once the IM is started, all F-I/O are passivated (not with type R1 system redundancy).

The reintegration of the F-I/O is performed in the same way as after a communication error, i.e. by an acknowledgment at the ACK_REI input of the F-channel driver.

Duration of repair of S7 F/FH Systems

For S7 F/FH Systems, the repair for redundant components should be organized in such a way that the duration of the repair following a failure does not exceed 24 hours if possible. At unmanned plants, a repair duration of 72 hours is permitted on weekends. In general, availability increases as the repair duration decreases.

Fiber-optic cables with S7 F/FH Systems

After repair of an F-CPU, you must not withdraw fiber-optic cables simultaneously from the F-CPU.

Preventive maintenance (Proof Test)

For an ordinary configuration, the probability values for the certified components of the F-system guarantee a service life (proof-test interval) of 20 years.

For detailed information, refer to the F-I/O manuals. Proof test for complex electronic components usually means replacement with unused goods.

A shorter proof-test interval is usually required for sensors and actuators.

Uninstalling S7 F Systems

For information on uninstallation of software, refer to section "Installing the S7 F Systems optional package (Page 31)".

You disassemble and dispose of the hardware of an F-system in the same was as for standard automation systems. You can find additional information in the manuals for the hardware.

14.3 F-Forcing

Introduction

S7 F Systems as of V6.1 with S7 F Systems Library V1.3 as of SP1 supports forcing of F-parameters in deactivated safety mode depending on the CFC version used.

F-Forcing allows you to modify F-Parameters at user interconnections.

- The modification of F-Parameters at system interconnections is not supported.
- Changing force values with activated F-forcing is not supported for F-parameters.

Consult the documentation for CFC or PCS 7 to find out which CFC versions support forcing of F-Parameters, in particular.

⚠ WARNING

Using the "F-Forcing" function

Forcing is only permitted when the safety of the system is ensured by other measures.

FSW-061

Procedure

1. Configure forcing for F-Parameters in CFC using the same procedure as for forcing with standard parameters.
2. If you haven't already done so, you will be prompted to deactivate safety mode.
   – Modify and check the force values for F-Parameters.
   – Enable F-Forcing for F-Parameters.
3. In your CFC program, make changes to F-Parameters of user interconnections by means of F-Forcing.
4. Activate safety mode again when forcing is no longer taking place in the F-Parameters.

Note

F-Forcing is deactivated automatically any time the F-Program starts up. The display in the CFC Editor is not updated after startup, however. The display can be updated by deactivating/activating safety mode again, for example.

The F-Program starts up:

- Each time the CPU restarts (cold/warm restart), e.g., following a brief power outage
- Each time the CPU restarts after a full shutdown

Note

Safety mode cannot be activated if F-Forcing is activated for an F-Parameter.

Note

F-Forcing is a typical commissioning function. The final F-Program should not include F-Forcing of F-Parameters.

Use the Maintenance Override function for the maintenance functions.

See also

Operations with "Secure Write Command++" (Page 129)

F-libraries

A

A.1 Overview of F-library S7 F Systems Library V1.3 SP3

A.1.1 F-Blocks

Overview

You will find the following in the F-library S7 F Systems Library V1.3 SP3:

- In the block container "F-user blocks\blocks": F-blocks
- In the block container "F-Control Blocks\Blocks": F-control blocks

Note

See also section "Differences between the S7 F Systems Lib F-libraries (Page 478)".

Note

You are not permitted to change the name of the F-library.

Note

FB numbers of F-blocks

You are not permitted to change the numbers of the F-blocks.

The following F-blocks available as of the S7 F Systems Library V1.3 SP2 use FBs that are also used in S7 Distributed Safety:

S7 F Systems Library V1.3 SP2 (or higher)	Number of the FB	F-Library "Distributed Safety (V1)"
F_CH_DII	FB 465	F_IGNTR
F_CH_DIO	FB 466	F_TIGHTN
F_POLYG	FB 467	F_GAS_BU
F_INT_P	FB 468	F_OIL_BU
F_PT1_P	FB 469	F_AIRD

A.1.2 F-Data types

Function

Special F-data types in a safety data format are used for fail-safe block interfaces. The safety data format is used to expose data and address errors.

Example

F_BOOL:

	STRUCT
DATA	BOOL
PAR_ID	WORD
COMPLEM	WORD
	END_STRUCT

If you want to change the value (default) of a block IO with an F-data type, you must only change the DATA component.

> ⚠ **WARNING**
>
> **Values of PAR_ID and COMPLEM must not be changed**
>
> You must not change the PAR_ID and COMPLEM components after the S7 program has been compiled since this might result in serious errors remaining undetected. If errors in the safety data format are detected during the execution of the safety program, an F-STOP is triggered. If necessary, you need to compile the S7 program again and download it to the F-CPU.
>
> FSW-101

A.1.3 Block interfaces

Note the following special features regarding the block IOs of F-blocks:

- The EN and ENO connections are neither evaluated nor supplied by the program code of the F-blocks, and must not be interconnected.
- In addition to the documented connections in the block descriptions, all F-blocks have additional connections. These are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

A.1.4 Behavior of F-Blocks with floating-point operations in the event of a number range overflow

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

- Either output at the output and available for further processed by the subsequent F-Blocks *or*
- Signaled at special outputs. If necessary, a fail-safe value is output.

If the floating-point operation yields an invalid floating-point number (NaN) and an invalid floating-point number (NaN) does not already exist as an address, the following diagnostic event is entered in the diagnostic buffer of the F-CPU:

- "Safety program: invalid REAL number in DB" (Event ID 16#75D9)

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

Refer also to the documentation of the F-Blocks.

If you cannot rule out the occurrence of these events in your safety program, you must decide independently of your application whether you have to react to these events in your safety program. With F-Block F_LIM_R, you can check the result of a floating-point operation for overflow (± infinity) and invalid floating-point number (NaN).

A.1.5 Behavior of F-Blocks in the event of safety-related faults

If F-Blocks or F-Control blocks detect a safety-related fault, they trigger a fault reaction. Error information is entered in the diagnostic buffer of the F-CPU. The online help for the diagnostic events provides detailed information and suggests corrective actions.

The respective fault reactions and other diagnostic options can be found in the documentation for the F-Blocks and F-Control blocks.

A.2 F-Blocks S7 F Systems Library V1.3 SP3

A.2.1 Logic blocks with the BOOL data type

A.2.1.1 Logic Blocks of the BOOL Data Type

Overview

Block name	Block number	Description
F_AND4	FB 301	AND logic operation on four inputs
F_OR4	FB 302	OR logic operation on four inputs
F_XOR2	FB 303	XOR logic operation on two inputs
F_NOT	FB 304	NOT logic operation
F_2OUT3	FB 305	2oo3 evaluation of inputs of data type BOOL
F_XOUTY	FB 306	XooY evaluation of inputs of data type BOOL

A.2.1.2 F_AND4: AND logic operation on four inputs

Function

This block links the INx inputs by means of AND. The OUT output is "1" when all INx inputs are "1". Otherwise the OUT output is "0". The OUTN output corresponds to the negated OUT output.

Truth table

IN1	IN2	IN3	IN4	OUT	OUTN
0	0	0	0	0	1
0	0	0	1	0	1
0	0	1	0	0	1
0	0	1	1	0	1
0	1	0	0	0	1
0	1	0	1	0	1
0	1	1	0	0	1
0	1	1	1	0	1
1	0	0	0	0	1
1	0	0	1	0	1
1	0	1	0	0	1
1	0	1	1	0	1
1	1	0	0	0	1
1	1	0	1	0	1

IN1	IN2	IN3	IN4	OUT	OUTN
1	1	1	0	0	1
1	1	1	1	1	0

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_BOOL	Input 1	1
	IN2	F_BOOL	Input 2	1
	IN3	F_BOOL	Input 3	1
	IN4	F_BOOL	Input 4	1
Outputs:	OUT	F_BOOL	Output	1
	OUTN	F_BOOL	Negated output	0

Error handling

None

A.2.1.3 F_OR4: OR logic operation on four inputs

Function

This F-Block combines the INx inputs with a logical OR. The OUT output is "1" when at least one INx input is "1". If all INx inputs are "0", the OUT output is "0". The OUTN output corresponds to the negated OUT output.

Truth table

IN1	IN2	IN3	IN4	OUT	OUTN
0	0	0	0	0	1
0	0	0	1	1	0
0	0	1	0	1	0
0	0	1	1	1	0
0	1	0	0	1	0
0	1	0	1	1	0
0	1	1	0	1	0
0	1	1	1	1	0
1	0	0	0	1	0
1	0	0	1	1	0
1	0	1	0	1	0
1	0	1	1	1	0
1	1	0	0	1	0

IN1	IN2	IN3	IN4	OUT	OUTN
1	1	0	1	1	0
1	1	1	0	1	0
1	1	1	1	1	0

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_BOOL	Input 1	0
	IN2	F_BOOL	Input 2	0
	IN3	F_BOOL	Input 3	0
	IN4	F_BOOL	Input 4	0
Outputs:	OUT	F_BOOL	Output	0
	OUTN	F_BOOL	Negated output	1

Error handling

None

A.2.1.4 F_XOR2: XOR logic operation on two inputs

Function

This F-Block combines the INx inputs with an exclusive OR. The OUT output is "1" if exactly one INx input is "1". The OUTN output corresponds to the negated OUT output.

Truth table

IN1	IN2	OUT	OUTN
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_BOOL	Input 1	0
	IN2	F_BOOL	Input 2	0
Outputs:	OUT	F_BOOL	Output	0
	OUTN	F_BOOL	Negated output	1

Error handling

None

A.2.1.5 F_NOT: NOT logic operation

Function

This F-Block inverts the input.

Truth table

IN	OUT
0	1
1	0

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	F_BOOL	Input	0
Output:	OUT	F_BOOL	Output	1

Error handling

None

A.2.1.6 F_2OUT3: 2oo3 evaluation of inputs of data type BOOL

Function

This F-Block monitors three binary inputs for signal state "1". The OUT output is "1" when at least two INx inputs are "1". Otherwise the OUT output is "0". The OUTN output corresponds to the negated OUT output.

Truth table

IN1	IN2	IN3	OUT	OUTN
0	0	0	0	1
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1

IN1	IN2	IN3	OUT	OUTN
1	0	1	1	0
1	1	0	1	0
1	1	1	1	0

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_BOOL	Input 1	0
	IN2	F_BOOL	Input 2	0
	IN3	F_BOOL	Input 3	0
Outputs:	OUT	F_BOOL	Output	0
	OUTN	F_BOOL	Negated output	1

Error handling

None

A.2.1.7 F_XOUTY: XooY evaluation of inputs of data type BOOL

Function

The F-block monitors up to 16 binary inputs IN1…IN16 for signal state 1. The input signals are monitored for signal state 1 beginning with input IN1 up to an including input INY. The number of binary inputs to be monitored is set with the Y parameter. The OUT output is 1, when at least x inputs IN1…IN16 are 1. Otherwise, output OUT is 0. The OUTN output corresponds to the negated OUT output.

The binary inputs must be assigned consecutively beginning from IN1. When X > Y, X ≤ 0, X > 16, Y ≤ 0, then output OUT is 0. When Y > 16, the OUT output behaves the same as when Y = 16.

The OUT_XA output gives the number of active inputs, enabling larger functions such as "5oo32" with a significantly reduced block count.

I/Os

	Name	Data type	Explanation	Default
Inputs:	IN1	F_BOOL	Input 1	0
	IN2	F_BOOL	Input 2	0
	IN3	F_BOOL	Input 3	0
	…		…	
	IN16	F_BOOL	Input 16	0
	X	F_INT	Minimum number of inputs with signal state 1: 0 < X ≤ 16	0
	Y	F_INT	Number of inputs to be monitored: 0 < Y ≤ 16	0
Outputs:	OUT	F_BOOL	Output	0
	OUTN	F_BOOL	Negated output	1
	OUT_XA	F_REAL	Number of inputs with signal state 1	0

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.2 F-Blocks for F-Communication between F-CPUs

A.2.2.1 F-Blocks for F-Communication between F-CPUs

Overview

F-block name	Block number	Description
F_SENDBO	FB 370	Sending 20 data of the data type F_BOOL in fail-safe manner to other F-CPU
F_RCVBO	FB 371	Receiving 20 data of the data type F_BOOL in fail-safe manner from other F-CPU
F_SENDR	FB 372	Sending 20 data of the data type F_REAL in fail-safe manner to other F-CPU
F_RCVR	FB 373	Receiving 20 data of the data type F_REAL in fail-safe manner from other F-CPU

F-block name	Block number	Description
F_SDS_BO	FB 352	Sending 32 data of the data type F_BOOL in fail-safe manner to other F-CPU
F_RDS_BO	FB 353	Receiving 32 data of the data type F_BOOL in fail-safe manner from other F-CPU

A.2.2.2 F_SENDBO: Sending of 20 data elements of data type F_BOOL in a fail-safe manner to another F-CPU

Function

The F-block F_SENDBO sends the data of data type F_BOOL at the SD_BO_xx inputs in a fail-safe manner to another F-CPU. The data must be received there with the F-block F_RCVBO.

At the EN_SEND input, you can temporarily switch off communication between the F-CPUs in order to reduce the bus load by supplying the EN_SEND input with 0 (default setting = 1). Send data are then no longer sent to the associated F_RCVBO, and F_RCVBO provides the assigned fail-safe values for this time period. If communication was already established between the connection partners, a communication error is detected.

At the ID input you must specify – from the perspective of the F CPU – the local ID of the S7 connection (from connection table in NetPro).

Communication between the F-CPUs is implemented hidden in the background using a special safety protocol. For this purpose, you must define the communication relationship between an F_SENDBO in an F-CPU and an F_RCVBO in the other F-CPU by specifying an odd number at the R_ID input of F_SENDBO and F_RCVBO. Associated F_SENDBO and F_RCVBO are given the same value for R_ID.

⚠ WARNING

Value for the relevance address reference

The value for the respective address relationship (input parameter R_ID; data type: DWORD) can be selected by the user but must be an odd number and unique network-wide for all safety-related communication connections. The value R_ID + 1 is internally assigned and must not be used. You must supply the ID and R_ID inputs with constant values when the F-block is called.

FSW-102

You must assign the desired F-monitoring time at the TIMEOUT input. The TIMEOUT input cannot be interconnected.

WARNING

Detecting and transmitting a signal level

It can only be ensured (from a fail-safe standpoint) that a signal level to be transmitted will be detected on the sender side and transmitted to the receiver if the signal level is present for at least as long as the assigned F-monitoring time (TIMEOUT).

For information regarding the calculation of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

FSW-103

Note

If the data is received with the F-block F_RCVBO of the F-library Fail-safe Blocks (V1.2) or (V1.1), you must configure the input EN_SMODE with 0 (default = 1), otherwise F_RCVBO will detect a CRC error.

Otherwise, you must leave the default value of the EN_SMODE input unchanged, because the operating mode of the F-CPU can otherwise not be evaluated with F_SENDBO at the SENDMODE output of the F-CPU.

I/Os

	Name	Data type	Explanation	Default
Inputs:	EN_SEND	BOOL	1 = Enable sending	1
	ID	WORD	Addressing parameter ID	W#16#0
	R_ID	DWORD	Addressing parameter R_ID	DW#16#0
	SD_BO_00	F_BOOL	Send data 00	0
	…		…	
	SD_BO_19	F_BOOL	Send data 19	0
	CRC_IMP	DWORD	Address relationship CRC	DW#16#0 to be automatically supplied *
	TIMEOUT	F_TIME	F-monitoring time in ms	T#0ms
	EN_SMODE	F_BOOL	1 = SENDMODE	1
Outputs:	ERROR	F_BOOL	1 = Communication error	0
	SUBS_ON	F_BOOL	1 = Receiver outputs fail-safe values	0
	RETVAL	WORD	Error code	W#16#0

*) The CRC_IMP input is automatically supplied when the S7 program is compiled and must not be changed. The CRC_IMP input is indicated as changed during comparison of safety programs if changes were made to the connection configuration in NetPro.

Fail-safe value

Fail-safe values are output by the receiver F_RCVBO in the following cases:

- A communication error (e.g. CRC error, timeout) was detected.
- The communication was disabled using EN_SEND = 0.
- An F-startup is present.

The SUBS_ON output is set to 1.

If the output of the fail-safe value is caused by a communication error, output ERROR = 1 is additionally set.

A "Timeout" communication error is detected for the first time when the communication between the F_SENDBO and F_RCVBO connection partners has already been established once. If communication cannot be established after startup of the sending F-system and receiving F-system, check the configuration of the safety-related CPU-CPU communication, the parameter assignment of the F_SENDBO and F_RCVBO and the bus connection. You can also obtain information on possible error causes by evaluating the RETVAL outputs of F_SENDBO and F_RCVBO. In general, always evaluate RETVAL of F_SENDBO and F_RCVBO as it may be that only one of the two outputs contains error information.

Reintegration

After a communication error, the data active at the SD_BO_xx inputs are only output again when a communication error is no longer detected and acknowledgment is made with a positive edge at the ACK_REI input of the F_RCVBO.

Startup behavior

After start-up of the sending and receiving F-systems, the communication between the connection partners F_SENDBO and F_RCVBO must be established for the first time. The receiver F_RCVBO provides fail-safe values during the time period. The SUBS_ON output is set to 1.

RETVAL output

Non-fail-safe information about the type of communication error that occurred is provided at the RETVAL output for service purposes. You can read out this information on your ES/OS or evaluate it in your standard user program if necessary. The DIAG bits are saved until an acknowledgment is made at the ACK_REI input of the associated F_RCVBO.

Structure of RETVAL

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 0	Reserve	—	—
Bit 1	Receiver outputs fail-safe values	See bits 2-7	Check bits 2-7

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 2	ERROR bit of USEND set	Basic communication problems of the internally called SFB 8 "USEND" detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 3	ERROR bit of USEND set	Basic communication problems of the internally called SFB 8 "USEND" detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 4	ERROR bit of URCV set	Basic communication problems of the internally called SFB 9 "URCV" detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 5	CRC error detected	See description for bit 7	See description for bit 7
Bit 6	Sequence number error detected	See description for bit 7	See description for bit 7
Bit 7	Timeout detected	Connection configuration not correct	Check and reload connection configuration
		The bus connection to the partner F-CPU is faulty.	Check bus connection and ensure that no external sources of disturbance are present.
		F-monitoring time of the F-CPU and of the partner F-CPUs is set too low	Check the assigned F-monitoring time TIMEOUT for F_SENDBO and F_RCVBO of both F-CPUs. Set higher value, if necessary. Compile S7 programs again and download them to the F-CPUs.
		STOP or internal fault of the CP	Switch the CPs to RUN. Check diagnostics buffer of the CPs. Replace the CPs, if necessary.
		STOP, partial shutdown or full shutdown or internal fault of the F-CPU/partner F-CPU	Switch F-CPUs to RUN. Perform F-startup. Check diagnostics buffer of F-CPUs. Replace F-CPUs, if necessary
		Communication was disabled with EN_SEND = 0.	Enable communication again at the associated F_SENDBO with EN_SEND = 1
		S7 connection has changed, e.g. IP address of the CP was changed	Compile S7 programs again and download them to the F-CPUs.
Bit 8 - 15	= "STATUS" error information of the internally called SFB 8 "USEND" or SFB 9 "URCV"	See description of the "STATUS" error information in the online help for the SFB 8/SFB 9 or in the "System Software for S7 300/400 System and Standard Functions (http://support.automation.siemens.com/WW/view/en/1214574)" manual	—

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.2.3 F_RCVBO: Receiving of 20 data elements of data type F_BOOL in a fail-safe manner from another F-CPU

Function

The F-block F_RCVBO receives 20 data elements of data type F_BOOL from another F-CPU and makes it available to the RD_BO_xx outputs. The data must be sent from the other F-CPU with the F-block F_SENDBO.

At the ID input you must specify – from the perspective of the F-CPU – the local ID of the S7 connection (from the connection table in NetPro).

Communication between the F-CPUs is implemented hidden in the background using a special safety protocol. For this purpose, you must define the communication relationship between an F_RCVBO in one F-CPU and an F_SENDBO in the other F-CPU by specifying an odd number at the R_ID input of F_SENDDP and F_RCVDP. Associated F_SENDBO and F_RCVBO receive the same value for R_ID.

⚠ WARNING

Value for the respective address relationship

The value for the respective address relationship (input parameter R_ID; data type: DWORD) can be selected by the user but must be an odd number and unique network-wide for all safety-related communication connections. The value R_ID + 1 is internally assigned and must not be used. You must supply the ID and R_ID inputs with constant values when the F-block is called.

FSW-102

You must assign the desired F-monitoring time at the TIMEOUT input. The TIMEOUT input cannot be interconnected.

⚠ WARNING

Detecting and transmitting the signal level

It can only be ensured (from a fail-safe standpoint) that a signal level to be transmitted will be detected on the sender side and transmitted to the receiver if the signal level is present for at least as long as the assigned F-monitoring time (TIMEOUT).

For information regarding the calculation of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

FSW-103

The operating mode of the F-CPU with F_SENDDP is provided at the SENDMODE output. If the F-CPU with F_SENDDP is in deactivated safety mode, the SENDMODE output becomes = 1.

Note

If the data is received from an F_SENDBO block from older F-libraries, you must assign the COMMVER_USED input with 0. Otherwise, sequence number errors may occur. Default setting is "1".

I/Os

	Name	Data type	Explanation	Default
Inputs:	ID	WORD	Addressing parameter ID	W#16#0
	R_ID	DWORD	Addressing parameter R_ID	DW#16#0
	CRC_IMP	DWORD	Address relationship CRC	DW#16#0 To be automatically supplied*
	TIMEOUT	F_TIME	F-monitoring time in ms	T# 0 ms
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	SUBBO_00	F_BOOL	Substitute value for receive data 00	0
	…		…	
	SUBBO_19	F_BOOL	Substitute value for receive data 19	0
	COMMVER_USED	INT	0 = Communication with blocks from older F-libraries < V1.3 SP2 (compatibility mode) 1 = Communication with blocks of F-Library V1.3 SP2 (or higher)	1
Outputs:	ACK_REQ	BOOL	Acknowledgment for reintegration is required	0
	ERROR	F_BOOL	Communication error	0
	SUBS_ON	F_BOOL	Fail-safe values are output	0
	RD_BO_00	F_BOOL	Receive data 00	0
	…		…	
	RD_BO_19	F_BOOL	Receive data 19	0
	SENDMODE	F_BOOL	1 = F-CPU with F_SENDBO in deactivated safety mode	0
	RETVAL	WORD	Error code	W#16#0

*) The CRC_IMP input is automatically supplied when the S7 program is compiled and must not be changed. The CRC_IMP input is indicated as changed during comparison of safety programs if changes were made to the connection configuration in NetPro.

Fail-safe values

The fail-safe values active at the SUBBO_xx inputs are output in the following cases:

- A communication error (e.g. CRC error, timeout) was detected.
- The communication was disabled at the associated F_SENDBO via EN_SEND = 0.
- An F-startup is present.

The SUBS_ON output is set to 1.

If the output of the fail-safe value is caused by a communication error, output ERROR = 1 is additionally set.

A "Timeout" communication error is detected for the first time when the communication between the F_SENDBO and F_RCVBO connection partners has already been established once. If communication cannot be established after startup of the sending and receiving F-system, check the configuration of the safety-related CPU-CPU communication, the parameter assignment of F_SENDDP and F_RCVDP and the bus connection. You can also obtain information on possible error causes by evaluating the RETVAL outputs of F_SENDBO and F_RCVBO. In general, always evaluate RETVAL of F_SENDBO and F_RCVBO as it may be that only one of the two outputs contains error information.

Reintegration

After a communication error, the data active at the SD_BO_xx inputs of the associated F_SENDBO are only output again at the RD_BO_xx outputs when a communication error is no longer detected and acknowledgment is made with a positive edge at the ACK_REI input.

Output ACK_REQ = 1 is used to signal that a user acknowledgment at the ACK_REI input is required for the acknowledgment.

⚠ WARNING

User acknowledgment is always required for communication errors

For this, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permitted.

FSW-104

Startup characteristics

After start-up of the sending and receiving F-systems, the communication between the connection partners F_SENDBO and F_RCVBO must be established for the first time. The fail-safe values active at the SUBBO_xx inputs are output during this time period. The SUBS_ON output is set to 1.

The SENDMODE output is preset with 0 and is not updated as long as output SUBS_ON = 1.

RETVAL output

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 0	Reserve	—	—
Bit 1	Receiver outputs fail-safe values	See bits 2-7	Check bits 2-7
Bit 2	ERROR bit of USEND is set	Basic communication problems of internally called SFB 8 "USEND" are detected.	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 3	ERROR bit of USEND is set	Basic communication problems of internally called SFB 8 "USEND" are detected.	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 4	ERROR bit of URCV is set	Basic communication problems with the internally called SFB 9 "URCV" are detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 5	CRC error is detected	See description for bit 7	See description for bit 7
Bit 6	Sequence number error is detected	See description for bit 7	See description for bit 7
Bit 7	Timeout is detected	Connection configuration is incorrect	Check connection configuration and download it again
		Bus connection to the partner F-CPU is faulty	Check the bus connection and ensure that no external sources of disturbance are present.
		F-monitoring time of the F-CPU and of the partner F-CPU is set too short	Check the assigned F-monitoring time TIMEOUT for F_SENDDP and F_RCVDP of both F-CPUs. Set a higher value if necessary. Compile S7 programs again and download them to the F-CPUs.
		STOP or internal error of the CPs	Switch CPs to RUN. Check the diagnostics buffer of the CPs. Replace the CPs, if necessary.
		STOP, partial shutdown or full shutdown or internal error of the F-CPU/partner F-CPU	Switch F-CPUs to RUN. Perform F-startup. Check diagnostics buffer of the F-CPUs. Replace F-CPUs, if necessary.
		The communication was disabled with EN_SEND = 0.	Enable communication again at the associated F_SENDBO with EN_SEND = 1
		S7 connection has changed, e.g. the IP address of the CP was changed	Compile S7 programs again and download them to the F-CPUs.
Bits 8 - 15	= "STATUS" error information of the internally called SFB 8 "USEND" or SFB 9 "URCV"	See description of the "STATUS" error information in the online help for the SFB 8/SFB 9 or in the "System Software for S7 300/400 System and Standard Functions (http://support.automation.siemens.com/WW/view/en/1214574)" manual	—

Error handling

An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.2.4 F_SENDR: Sending of 20 data elements of data type F_REAL in a fail-safe manner to another F-CPU

Function

In a fail-safe operation, the F-block F_SENDR sends the data of the data type F_REAL, which is present at the SD_R_xx inputs, to another F-CPU. The data must be received there with the F-block F_RCVR.

At the EN_SEND input, you can temporarily switch off the communication between the F-CPUs to reduce the bus load by supplying the input EN_SEND (default = 1) with 0. No send data is then sent to the associated F_RCVR, and the F_SENDR provides the configured substitute values for this period. If communication between the connection partners has already been established, a communication error is detected.

At the ID input you must specify – from the perspective of the F CPU – the local ID of the S7 connection (from connection table in NetPro).

Communication between the F-CPUs is implemented hidden in the background using a special safety protocol. For this purpose, you must define the communication relationship between an F_SENDR in one F-CPU and an F_RCVR in the other F-CPU by specifying an odd number at the R_ID input of F_SENDR and F_RCVR. Associated F_SENDR and F_RCVR receive the same value for R_ID.

⚠ **WARNING**

Value for the respective address relationship

The value for the respective address relationship (input parameter R_ID; data type: DWORD) can be selected by the user but must be an odd number and unique network-wide for all safety-related communication connections. The value R_ID + 1 is internally assigned and must not be used. You must supply the ID and R_ID inputs with constant values when the F-block is called.

FSW-102

You must assign the desired F-monitoring time at the TIMEOUT input. The TIMEOUT input cannot be interconnected.

⚠ WARNING

Detecting and transmitting a signal level

It can only be ensured (from a fail-safe standpoint) that a signal level to be transmitted will be detected on the sender side and transmitted to the receiver if the signal level is present for at least as long as the assigned F-monitoring time (TIMEOUT).

For information regarding the calculation of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

FSW-103

Note

If the data is received with the F-block F_RCVR of the F-library Fail-safe Blocks (V1.2) or (V1.1), you must configure the input EN_SMODE with 0 (default = 1), otherwise F_RCVR will detect a CRC error.

Otherwise, you must leave the default setting of the EN_SMODE input unchanged, since otherwise the SENDMODE output of the F_RCVR will not be able to evaluate the operating mode of the F-CPU with the F_SENDR.

I/Os

	Name	Data type	Explanation	Default
Inputs:	EN_SEND	BOOL	1 = Enable sending	1
	ID	WORD	Addressing parameter ID	W#16#0
	R_ID	DWORD	Addressing parameter R_ID	DW#16#0
	SD_R_00	F_REAL	Send data 00	0
	…		…	
	SD_R_19	F_REAL	Send data 19	0
	CRC_IMP	DWORD	Address relationship CRC	DW#16#0 Supplied automatically*
	TIMEOUT	F_TIME	F-monitoring time in ms	T#0ms
	EN_SMODE	F_BOOL	1 = SENDMODE	1
Outputs:	ERROR	F_BOOL	1 = Communication error	0
	SUBS_ON	F_BOOL	1 = Receiver outputs substitute values	0
	RETVAL	WORD	Error code	W#16#0

*) The CRC_IMP input is automatically supplied when the S7 program is compiled and must not be changed. The CRC_IMP input is indicated as changed during comparison of safety programs if changes were made to the connection configuration in NetPro.

Substitute value

Substitute values are output by the receiver F_RCVR in the following cases:

- A communication error (e.g. CRC error, timeout) was detected.
- The communication was disabled with EN_SEND = 0.
- An F-startup is present.

The SUBS_ON output is set to 1.

If the output of the fail-safe value is caused by a communication error, output ERROR = 1 is additionally set.

A "Timeout" communication error is detected for the first time when the communication between the F_SENDR and F_RCVR connection partners has already been established once. If communication cannot be established after startup of the sending and receiving F-system, check the configuration of the safety-related CPU-CPU communication, the parameter assignment of F_SENDR and F_RCVR and the bus connection. You can also obtain information on possible error causes by evaluating the RETVAL outputs of F_SENDR and F_RCVR. In general, always evaluate RETVAL of F_SENDR and F_RCVR as it may be that only one of the two outputs contains error information.

Reintegration

After a communication error, the data active at the SD_R_xx inputs are only output again when a communication error is no longer detected and acknowledgment is made with a positive edge at the ACK_REI input of the F_RCVR.

Startup behavior

After start-up of the sending and receiving F-systems, the communication between the connection partners F_SENDR and F_RCVR must be established for the first time. The receiver F_RCVR provides substitute values during this period. The SUBS_ON output is set to 1

RETVAL output

Non fail-safe information about the nature of the communication error that occurred is made available at the RETVAL output for service purposes. You can read out this information on your ES/OS or evaluate it in your standard user program if necessary. The DIAG bits remain stored until you acknowledge at the ACK_REI input of the corresponding F_RCVR.

Structure of RETVAL

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 0	Reserve	—	—
Bit 1	Receiver outputs fail-safe values	See bits 2-7	Check bits 2-7

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 2	ERROR bit of USEND is set	Basic communication problems of internally called SFB 8 "USEND" are detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 3	ERROR bit of USEND is set	Basic communication problems of internally called SFB 8 "USEND" are detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 4	ERROR bit of URCV is set	Basic communication problems of the internally called SFB 9 "USEND" are detected.	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 5	CRC error is detected	See description for bit 7	See description for bit 7
Bit 6	Sequence number error is detected	See description for bit 7	See description for bit 7
Bit 7	Timeout is detected	Connection configuration is incorrect	Check connection configuration and download it again
		Bus connection to the partner F-CPU is faulty	Check the bus connection and ensure that no external sources of disturbance are present.
		F-monitoring time of the F-CPU and of the partner F-CPU is set too short	Check the assigned F-monitoring time TIMEOUT for F_SENDR and F_RCVR of both F-CPUs. Set a higher value if necessary. Compile S7 programs again and download them to the F-CPUs.
		STOP or internal error of the CPs	Switch CPs to RUN. Check the diagnostics buffer of the CPs. Replace the CPs, if necessary.
		STOP, partial shutdown or full shutdown or internal error of the F-CPU/ partner F-CPU	Switch F-CPUs to RUN. Perform F-startup. Check diagnostics buffer of the F-CPUs. Replace F-CPUs, if necessary.
		The communication was disabled with EN_SEND = 0.	Enable communication again at the associated F_SENDR with EN_SEND = 1
		S7 connection has changed, e.g. the IP address of the CP was changed	Compile S7 programs again and download them to the F-CPUs.
Bits 8 - 15	= "STATUS" error information of the internally called SFB 8 "USEND" or SFB 9 "URCV"	See description of the "STATUS" error information in the online help for the SFB 8/SFB 9 or in the "System Software for S7 300/400 System and Standard Functions (http://support.automation.siemens.com/WW/view/en/1214574)" manual	—

Error handling

An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.2.5 F_RCVR: Receiving of 20 data elements of data type F_REAL in a fail-safe manner from another F-CPU

Function

The F-block F_RCVR receives 20 data elements of data type F_REAL from another F-CPU and makes it available to the RD_R_xx outputs. The data must be sent from the other F-CPU with the F-block F_SENDR.

At the ID input you must specify – from the perspective of the F CPU – the local ID of the S7 connection (from connection table in NetPro).

Communication between the F-CPUs is implemented hidden in the background using a special safety protocol. For this purpose, you must define the communication relationship between an F_SENDR in one F-CPU and an F_RCVR in the other F-CPU by specifying an odd number at the R_ID input of F_SENDR and F_RCVR. Associated F_SENDR and F_RCVR receive the same value for R_ID.

⚠ WARNING

Value for the respective address relationship

The value for the respective address relationship (input parameter R_ID; data type: DWORD) can be selected by the user but must be an odd number and unique network-wide for all safety-related communication connections. The value R_ID + 1 is internally assigned and must not be used. You must supply the ID and R_ID inputs with constant values when the F-block is called.

FSW-102

You must assign the desired F-monitoring time at the TIMEOUT input. The TIMEOUT input cannot be interconnected.

⚠ WARNING

Detecting and transmitting the signal level

It can only be ensured (from a fail-safe standpoint) that a signal level to be transmitted will be detected on the sender side and transmitted to the receiver if the signal level is present for at least as long as the assigned F-monitoring time (TIMEOUT).

For information regarding the calculation of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

FSW-103

The operating mode of the F-CPU with F_SENDR is provided at the SENDMODE output. If the F-CPU with F_SENDR is in deactivated safety mode, the SENDMODE output becomes = 1.

Note

If the data is received from an F_SENDR block from older F-libraries, you must assign the COMMVER_USED input with 0. Otherwise, sequence number errors may occur. Default setting is "1".

I/Os

	Name	Data type	Explanation	Default
Inputs:	ID	WORD	Addressing parameter ID	W#16#0
	R_ID	DWORD	Addressing parameter R_ID	W#16#0
	CRC_IMP	DWORD	Address relationship CRC	W#16#0 Is supplied automatically*
	TIMEOUT	F_TIME	F-monitoring time in ms	T#0ms
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	SUBR_00	F_REAL	Substitute value for receive data 00	0
	…		…	
	SUBR_19	F_REAL	Substitute value for receive data 19	0
	COMMVER_USED	INT	0 = Communication with blocks from older F-libraries < V1.3 SP2 (compatibility mode) 1 = Communication with blocks of F-Library V1.3 SP2 (or higher)	1
Outputs:	ACK_REQ	BOOL	Acknowledgment for reintegration is required	0
	ERROR	F_BOOL	1 = Communication error	0
	SUBS_ON	F_BOOL	1 = Fail-safe values are output	0
	RD_R_00	F_REAL	Receive data 00	0
	…		…	
	RD_R_19	F_REAL	Receive data 19	0
	SENDMODE	F_BOOL	1 = F-CPU with F_SENDR in deactivated safety mode	
	RETVAL	WORD	Error code	W#16#0

*) The CRC_IMP input is automatically supplied when the S7 program is compiled and must not be changed. The CRC_IMP input is indicated as changed during comparison of safety programs if changes were made to the connection configuration in NetPro.

Fail-safe values

The fail-safe values active at the SUBR_xx inputs are output in the following cases:

- A communication error (e.g. CRC error, timeout) was detected.
- The communication was disabled at the associated F_SENDR via EN_SEND = 0.
- An F-startup is present.

The SUBS_ON output is set to 1.

While output SUBS_ON = 1, the SENDMODE output is not updated.

If the output of the fail-safe value is caused by a communication error, output ERROR = 1 is additionally set.

A "Timeout" communication error is detected for the first time when the communication between the F_SENDR and F_RCVR connection partners has already been established once. If communication cannot be established after startup of the sending and receiving F-system, check the configuration of the safety-related CPU-CPU communication, the parameter assignment of F_SENDR and F_RCVR and the bus connection. You can also obtain information on possible error causes by evaluating the RETVAL outputs of F_SENDR and F_RCVR. In general, always evaluate RETVAL of F_SENDR and F_RCVR as it may be that only one of the two outputs contains error information.

Reintegration

After a communication error, the data active at the SD_R_xx inputs of the associated F_SENDR are only output again at the RD_R_xx outputs when a communication error is no longer detected and acknowledgment is made with a positive edge at the ACK_REI input.

Output ACK_REQ = 1 is used to signal that a user acknowledgment at the ACK_REI input is required for the acknowledgment.

⚠ WARNING

User acknowledgment is always required for communication errors

For this, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permitted.

FSW-104

Startup characteristics

After start-up of the sending and receiving F-systems, the communication between the connection partners F_SENDR and F_RCVR must be established for the first time. The fail-safe values active at the SUBR_xx inputs are output during this time period. The SUBS_ON output is set to 1.

The SENDMODE output is preset with 0 and is not updated as long as output SUBS_ON = 1.

RETVAL output

Non fail-safe information about the nature of the communication error that occurred is made available at the RETVAL output for service purposes. You can read out this information on your ES/OS or evaluate it in your standard user program if necessary. The DIAG bits remain stored until you acknowledge at the ACK_REI input.

Structure of RETVAL

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 0	Reserve	—	—
Bit 1	Receiver outputs fail-safe values	See bits 2-7	See bits 2-7
Bit 2	ERROR bit of USEND is set	Basic communication problems of internally called SFB 8 "USEND" are detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 3	ERROR bit of USEND is set	Basic communication problems of internally called SFB 8 "USEND" are detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 4	ERROR bit of URCV is set	Basic communication problems of the internally called SFB 9 "USEND" are detected.	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 5	CRC error is detected	See description for bit 7	See description for bit 7
Bit 6	Sequence number error is detected	See description for bit 7	See description for bit 7

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 7	Timeout is detected	Connection configuration is incorrect	Check connection configuration and download it again
		Bus connection to the partner F-CPU is faulty	Check the bus connection and ensure that no external sources of disturbance are present.
		F-monitoring time of the F-CPU and of the partner F-CPU is set too short	Check the assigned F-monitoring time TIMEOUT for F_SENDR and F_RCVR of both F-CPUs. Set a higher value if necessary. Compile S7 programs again and download them to the F-CPUs.
		STOP or internal error of the CPs	Switch CPs to RUN. Check the diagnostics buffer of the CPs. Replace the CPs, if necessary.
		STOP, partial shutdown or full shutdown or internal error of the F-CPU/partner F-CPU	Switch F-CPUs to RUN. Perform F-startup. Check diagnostics buffer of the F-CPUs. Replace F-CPUs, if necessary.
		The communication was disabled with EN_SEND = 0.	Enable communication again at the associated F_SENDR with EN_SEND = 1
		S7 connection has changed, e.g. the IP address of the CP was changed	Compile S7 programs again and download them to the F-CPUs.
Bits 8 - 15	= "STATUS" error information of the internally called SFB 8 "USEND" or SFB 9 "URCV"	See description of the "STATUS" error information in the online help for the SFB 8/SFB 9 or in the "System Software for S7 300/400 System and Standard Functions (http://support.automation.siemens.com/WW/view/en/1214574)" manual	—

Error handling

An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.2.6 F_SDS_BO: Sending of 32 data elements of data type F_BOOL in a fail-safe manner to another F-CPU

Function

The F-block F_SDS_BO sends the data of the data type F_BOOL, that are present at the inputs SD_BO_*xx*, to another F-CPU in a fail-safe operation. The data must be received there with the F-block F_RDS_BO.

Note

The F-block F_SDS_BO can also send the data of the F_BOOL data type, that are present at the SD_BO_xx inputs, to an F-CPU with S7 Distributed Safety in a fail-safe operation. The data must then be received there with the F-block F_RCVS7 and an F-communication DB with exactly 32 data elements of the F_BOOL data type.

At the EN_SEND input, you can temporarily switch off the communication between the F-CPUs to reduce the bus load by supplying the input EN_SEND (default = 1) with 0. No send data is then sent to the associated F_RDS_BO, and the F_RDS_BO provides the configured substitute values for this period. If communication between the connection partners has already been established, a communication error is detected.

At the ID input you must specify – from the perspective of the F-CPU – the local ID of the S7 connection (from connection table in NetPro).

Communication between the F-CPUs is implemented hidden in the background using a special safety protocol. For this purpose, you must define the communication relationship between an F_SDS_BO in one F-CPU and an F_RDS_BO in the other F-CPU by specifying an odd number at the R_ID input of F_SDS_BO and F_RDS_BO. Associated F_SDS_BO and F_RDS_BO receive the same value for R_ID.

⚠ **WARNING**

Value for the respective address relationship

The value for the respective address relationship (input parameter R_ID; data type: DWORD) can be selected by the user but must be an odd number and unique network-wide for all safety-related communication connections. The value R_ID + 1 is internally assigned and must not be used. You must supply the ID and R_ID inputs with constant values when the F-block is called.

FSW-102

You must assign the desired F-monitoring time at the TIMEOUT input. The TIMEOUT input cannot be interconnected.

⚠ WARNING

Detecting and transmitting a signal level

It can only be ensured (from a fail-safe standpoint) that a signal level to be transmitted will be detected on the sender side and transmitted to the receiver if the signal level is present for at least as long as the assigned F-monitoring time (TIMEOUT).

For information regarding the calculation of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

FSW-103

I/Os

	Name	Data type	Explanation	Default
Inputs:	EN_SEND	BOOL	1 = Enable sending	1
	ID	WORD	Addressing parameter ID	W#16#0
	R_ID	DWORD	Addressing parameter R_ID	DW#16#0
	SD_BO_00	F_BOOL	Send data 00	0
	…		…	
	SD_BO_31	F_BOOL	Send data 31	0
	CRC_IMP	DWORD	Address relationship CRC	DW#16#0 Supplied automatically*
	TIMEOUT	F_TIME	F-monitoring time in ms	T#0ms
Outputs:	ERROR	F_BOOL	1 = Communication error	0
	SUBS_ON	F_BOOL	1 = Receiver outputs substitute values	0
	RETVAL	WORD	Error code	W#16#0

*) The CRC_IMP input is automatically supplied when the S7 program is compiled and must not be changed. The CRC_IMP input is indicated as changed during comparison of safety programs if changes were made to the connection configuration in NetPro.

Substitute values

The receiver F_RDS_BO outputs substitute values in the following cases:

- A communication error (e.g. CRC error, timeout) was detected.
- The communication was disabled with EN_SEND = 0.
- An F-startup is present.

The SUBS_ON output is set to 1.

If the output of the fail-safe value is caused by a communication error, output ERROR = 1 is additionally set.

A "Timeout" communication error is detected for the first time when the communication between the F_SDS_BO and F_RDS_BO connection partners has already been established once. If communication cannot be established after startup of the sending and receiving F-system, check the configuration of the safety-related CPU-CPU communication, the parameter assignment of F_SDS_BO and F_RDS_BO, and the bus connection. You can also obtain information on possible error causes by evaluating the RETVAL outputs of F_SDS_BO and F_RDS_BO. In general, always evaluate RETVAL of F_SDS_BO and F_RDS_BO as it may be that only one of the two outputs contains error information.

Reintegration

After a communication error, the data active at the SD_BO_xx inputs are only output again when a communication error is no longer detected and acknowledgment is made with a positive edge at the ACK_REI input of the F_RDS_BO.

Startup behavior

After startup of the sending and receiving F-system, the communication between the connection partners F_SDS_BO and F_RDS_BO must be established for the first time. The receiver F_RDS_BO provides substitute values during this period. The SUBS_ON output is set to 1.

RETVAL output

Non fail-safe information about the nature of the communication error that occurred is made available at the RETVAL output for service purposes. You can read out this information on your ES/OS or evaluate it in your standard user program if necessary. The DIAG bits remain stored until you acknowledge at the ACK_REI input of the corresponding F_RDS_BO.

Structure of RETVAL

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 0	Reserve	—	—
Bit 1	Receiver outputs fail-safe values	See bits 2-7	Check bits 2-7
Bit 2	ERROR bit of USEND is set	Basic communication problems of internally called SFB 8 "USEND" are detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 3	ERROR bit of USEND is set	Basic communication problems of internally called SFB 8 "USEND" are detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 4	ERROR bit of URCV is set	Basic communication problems of the internally called SFB 9 "USEND" are detected.	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 5	CRC error is detected	See description for bit 7	See description for bit 7
Bit 6	Sequence number error is detected	See description for bit 7	See description for bit 7
Bit 7	Timeout is detected	Connection configuration is incorrect	Check connection configuration and download it again
		Bus connection to the partner F-CPU is faulty	Check the bus connection and ensure that no external sources of disturbance are present.
		F-monitoring time of the F-CPU and of the partner F-CPU is set too short	Check the assigned F-monitoring time TIMEOUT for F_SDS_BO and F_RDS_BO of both F-CPUs. Set a higher value if necessary. Compile S7 programs again and download them to the F-CPUs.
		STOP or internal error of the CPs	Switch CPs to RUN. Check the diagnostics buffer of the CPs. Replace the CPs, if necessary.
		STOP, partial shutdown or full shutdown or internal error of the F-CPU/ partner F-CPU	Switch F-CPUs to RUN. Perform F-startup. Check diagnostics buffer of the F-CPUs. Replace F-CPUs, if necessary.
		The communication was disabled with EN_SEND = 0.	Enable communication again at the associated F_SDS_BO with EN_SEND = 1
		S7 connection has changed, e.g. the IP address of the CP was changed	Compile S7 programs again and download them to the F-CPUs.
Bits 8-15	= "STATUS" error information of the internally called SFB 8 "USEND" or SFB 9 "URCV"	See description of the "STATUS" error information in the online help for the SFB 8/SFB 9 or in the "System Software for S7 300/400 System and Standard Functions (http://support.automation.siemens.com/WW/view/en/1214574)" manual	—

Error handling

An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.2.7 F_RDS_BO: Receiving of 32 data elements of data type F_BOOL in a fail-safe manner from another F-CPU

Function

The F-block F_RDS_BO receives 32 data elements of the F_BOOL data type from another F-CPU, and provides them to RD_BO_xx outputs. The data must be sent from the other F-CPU with the F-block F_SDS_BO.

Note

The F-block F_RDS_BO can also receive the 32 data elements of data type F_BOOL in a fail-safe manner from an F-CPU with S7 Distributed Safety. The data must then be sent there with the F-block F_SENDS7 and an F-communication DB with exactly 32 data elements of the F_BOOL data type.

At the ID input you must specify – from the perspective of the F-CPU – the local ID of the S7 connection (from connection table in NetPro).

Communication between the F-CPUs is implemented hidden in the background using a special safety protocol. For this purpose, you must define the communication relationship between an F_SDS_BO in one F-CPU and an F_RDS_BO in the other F-CPU by specifying an odd number at the R_ID input of F_SDS_BO and F_RDS_BO. Associated F_SDS_BO and F_RDS_BO receive the same value for R_ID.

⚠ **WARNING**

Value for the respective address relationship

The value for the respective address relationship (input parameter R_ID; data type: DWORD) can be selected by the user but must be an odd number and unique network-wide for all safety-related communication connections. The value R_ID + 1 is internally assigned and must not be used. You must supply the ID and R_ID inputs with constant values when the F-block is called.

FSW-102

You must assign the desired F-monitoring time at the TIMEOUT input. The TIMEOUT input cannot be interconnected.

⚠ **WARNING**

Detecting and transmitting the signal level

It can only be ensured (from a fail-safe standpoint) that a signal level to be transmitted will be detected on the sender side and transmitted to the receiver if the signal level is present for at least as long as the assigned F-monitoring time (TIMEOUT).

For information regarding the calculation of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

FSW-103

The operating mode of the F-CPU with F_SDS_BO is provided at the SENDMODE output. If the F-CPU with F_SDS_BO is in deactivated safety mode, the SENDMODE output becomes = 1.

Note

If the data is received from an F_SDS_BO block from older F-libraries, you must assign the COMMVER_USED input with 0. Otherwise, sequence number errors may occur. Default setting is "1".

I/Os

	Name	Data type	Explanation	Default
Inputs:	ID	WORD	Addressing parameter ID	W#16#0
	R_ID	DWORD	Addressing parameter R_ID	DW#16#0
	CRC_IMP	DWORD	Address relationship CRC	DW#16#0 To be automatically supplied*
	TIMEOUT	F_TIME	F-monitoring time in ms	T#0ms
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	SUBBO_00	F_BOOL	Substitute value for receive data 00	0
	...		...	
	SUBBO_31	F_BOOL	Substitute value for receive data 31	0
	COMMV-ER_USED	INT	0 = Communication with blocks from older F-libraries < V1.3 SP2 (compatibility mode) 1 = Communication with blocks of F-Library V1.3 SP2 (or higher)	1
Outputs:	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	ERROR	F_BOOL	1 = Communication error	0
	SUBS_ON	F_BOOL	1 = Fail-safe values are output	0
	RD_BO_00	F_BOOL	Receive data 00	0
	...		...	
	RD_BO_31	F_BOOL	Receive data 31	0
	SENDMODE	F_BOOL	1 = F-CPU with F_SDS_BO in de-activated safety mode	0
	RETVAL	WORD	Error code	W#16#0

*) The CRC_IMP input is automatically supplied when the S7 program is compiled and must not be changed. The CRC_IMP input is indicated as changed during comparison of safety programs if changes were made to the connection configuration in NetPro.

Fail-safe values

The fail-safe values active at the SUBBO_*xx* inputs are output in the following cases:

- A communication error (e.g. CRC error, Timeout) was detected.
- The communication was disabled at the associated F_SDS_BO via EN_SEND = 0.
- An F-startup is present.

The SUBS_ON output is set to 1.

While output SUBS_ON = 1, the SENDMODE output is not updated.

If the output of the fail-safe value is caused by a communication error, output ERROR = 1 is additionally set.

A "Timeout" communication error is detected for the first time when the communication between the F_SDS_BO and F_RDS_BO connection partners has already been established once. If communication cannot be established after startup of the sending and receiving F-systems, check the configuration of the safety-related CPU-CPU communication, the parameter assignment of F_SDS_BO and F_RDS_BO and the bus connection. You can also obtain information on possible error causes by evaluating the RETVAL outputs of F_SDS_BO and F_RDS_BO. In general, always evaluate RETVAL of F_SDS_BO and F_RDS_BO as it may be that only one of the two outputs contains error information.

Reintegration

After a communication error, the data active at the SD_BO_xx inputs of the associated F_SDS_BO are only output again at the RD_BO_xx outputs when a communication error is no longer detected and acknowledgment is made with a positive edge at the ACK_REI input.

Output ACK_REQ = 1 is used to signal that a user acknowledgment at the ACK_REI input is required for the acknowledgment.

⚠ WARNING

User acknowledgment is always required for communication errors

For this, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permitted.

FSW-104

Startup characteristics

After start-up of the sending and receiving F-systems, the communication between the connection partners F_SDS_BO and F_RDS_BO must be established for the first time. The fail-safe values active at the SUBBO_xx inputs are output during this time period. The SUBS_ON output is set to 1.

The SENDMODE output is preset with 0 and is not updated as long as output SUBS_ON = 1.

RETVAL output

Non fail-safe information about the nature of the communication error that occurred is made available at the RETVAL output for service purposes. You can read out this information on your ES/OS or evaluate it in your standard user program if necessary. The DIAG bits remain stored until you acknowledge at the ACK_REI input.

Structure of RETVAL

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 0	Reserve	—	—
Bit 1	Receiver outputs fail-safe values	See bits 2-7	Check bits 2-7
Bit 2	ERROR bit of USEND is set	Basic communication problems of internally called SFB 8 "USEND" are detected	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 3	ERROR bit of USEND is set	Basic communication problems of internally called SFB 8 "USEND" are detected.	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 4	ERROR bit of URCV is set	Basic communication problems of the internally called SFB 9 "USEND" are detected.	Bit 8-15 = Evaluate "STATUS" of SFB 8 "USEND" or SFB 9 "URCV"
		See also description for bit 7	See also description for bit 7
Bit 5	CRC error is detected	See description for bit 7	See description for bit 7
Bit 6	Sequence number error is detected	See description for bit 7	See description for bit 7

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 7	Timeout is detected	Connection configuration is incorrect	Check connection configuration and download it again
		Bus connection to the partner F-CPU is faulty	Check the bus connection and ensure that no external sources of disturbance are present.
		F-monitoring time of the F-CPU and of the partner F-CPU is set too short	Check the assigned F-monitoring time TIMEOUT for F_SDS_BO and F_RDS_BO of both F-CPUs. Set a higher value if necessary. Compile S7 programs again and download them to the F-CPUs.
		STOP or internal error of the CPs	Switch CPs to RUN. Check the diagnostics buffer of the CPs. Replace the CPs, if necessary.
		STOP, partial shutdown or full shutdown or internal error of the F-CPU/ partner F-CPU	Switch F-CPUs to RUN. Perform F-startup. Check diagnostics buffer of the F-CPUs. Replace F-CPUs, if necessary.
		The communication was disabled with EN_SEND = 0.	Enable communication again at the associated F_SDS_BO with EN_SEND = 1
		S7 connection has changed, e.g. the IP address of the CP was changed	Compile S7 programs again and download them to the F-CPUs.
Bits 8 - 15	= "STATUS" error information of the internally called SFB 8 "USEND" or SFB 9 "URCV"	See description of the "STATUS" error information in the online help for the SFB 8/SFB 9 or in the "System Software for S7 300/400 System and Standard Functions (http://support.automation.siemens.com/WW/view/en/1214574)" manual	—

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostic buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.3 F-Blocks for comparing two input values of the same type

Overview

Block name	Block number	Description
F_CMP_R	FB 313	Comparator for two REAL values
F_LIM_HL	FB 314	Monitoring of upper limit violation of a REAL value
F_LIM_LL	FB 315	Monitoring of lower limit violation of a REAL value

A.2.3.1 F_CMP_R Comparator for two REAL values

Function

This F-Block compares two inputs of data type F_REAL and sets outputs GT, GE, EQ, LT or LE to "1", whatever the comparator result:

- GT = 1 if IN1 > IN2
- GE = 1 if IN1 ≥ IN2
- EQ = 1 if IN1 = IN2
- LT = 1 if IN1 < IN2
- LE = 1 if IN1 ≤ IN2

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_REAL	Input 1	0
	IN2	F_REAL	Input 2	0
Outputs:	GT	F_BOOL	IN1 > IN2	0
	GE	F_BOOL	IN1 ≥ IN2	0
	EQ	F_BOOL	IN1 = IN2	0
	LT	F_BOOL	IN1 < IN2	0
	LE	F_BOOL	IN1 ≤ IN2	0

Error handling

- If one of the inputs IN1 or IN2 is an invalid floating point number (NaN), outputs GT and LT are set to 1.
- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.3.2 F_LIM_HL: Monitoring of upper limit violation of a REAL value

Function

This F-Block monitors the input variable U for limit violation (U_HL). A hysteresis can also be specified at the HYS input to avoid fluttering of the QH output in the event of fluctuations in the input value.

- U ≥ U_HL: If the upper limit is exceeded, output QH = 1.
- (U_HL – HYS) ≤ U < U_HL: QH remains unchanged in this range.
- U < (U_HL – HYS): If the limit value hysteresis is fallen below, output QH = 0.

The QHN output corresponds to the negated QH output.

The limit value and hysteresis are also available as non-fail-safe data at the U_HL_O and HYS_O outputs for further processing in the standard user program.

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	U	F_REAL	INPUT	0.0
	U_HL	F_REAL	UPPER LIMIT	100.0
	HYS	F_REAL	HYSTERESIS	0.0
	SUBS_IN	F_BOOL	SUBSTITUTE VALUE	0
Outputs:	QH	F_BOOL	1 = UPPER LIMIT VIOLATION	0
	QHN	F_BOOL	NEGATING OUTPUT QH	1
	U_HL_O	REAL	UPPER LIMIT	100.0
	HYS_O	REAL	HYSTERESIS	0.0

Error handling

- If one of the inputs U, U_HL or HYS is an invalid floating point number (NaN) or if invalid floating-point numbers (NaN) arise due to calculations in the F-Block, the fail-safe value at the input SUBS_IN is output at output QH.
  If invalid floating-point numbers (NaNs) arise due to calculations in the F-Block, the following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: invalid REAL number in DB" (Event ID 16#75D9)
- An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.3.3 F_LIM_LL: Monitoring of lower limit violation of a REAL value

Function

This F-Block monitors the input variable U for lower limit violation

(U_LL). A hysteresis can also be specified at the HYS input to avoid fluttering of the QL output in the event of fluctuations in the input value.

- U ≤ U_LL: If the lower limit is violated, output QL = 1.
- U_LL < U ≤ (U_LL + HYS): QL remains unchanged in this range.
- U > (U_LL + HYS): If the upper limit is exceeded violated + hysteresis, output QL = 0.

Output QLN corresponds to the negated QL output.

The limit value and hysteresis are also available as non-fail-safe data at the U_LL_O and HYS_O outputs for evaluation in the standard user program.

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	U	F_REAL	INPUT	0.0
	U_LL	F_REAL	LOWER LIMIT	100.0
	HYS	F_REAL	HYSTERESIS	0.0
	SUBS_IN	F_BOOL	FAIL-SAFE VALUE	0
Outputs:	QL	F_BOOL	1 = LOWER LIMIT VIOLATION	0
	QLN	F_BOOL	NEGATING OUTPUT QL	1
	U_LL_O	REAL	LOWER LIMIT	100.0
	HYS_O	REAL	HYSTERESIS	0.0

Error handling

- If one of the inputs U, U_LL or HYS is an invalid floating point number (NaN) or if invalid floating-point numbers (NaNs) arise due to calculations in the F-Block, the fail-safe value at the input SUBS_IN is output at output QL.
  If invalid floating-point numbers (NaNs) arise due to calculations in the F-Block, the following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  – "Safety program: invalid REAL number in DB" (Event ID 16#75D9)
- An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  – "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.4 Voter blocks for inputs of data type REAL and BOOL

Overview

Block name	Block number	Description
F_2oo3DI	FB 316	2oo3 evaluation of inputs of data type BOOL with discrepancy analysis
F_2oo3AI	FB 318	2oo3 evaluation of inputs of data type REAL with discrepancy analysis
F_1oo2AI	FB 317	1oo2 evaluation of inputs of data type REAL with discrepancy analysis

A.2.4.1 F_2oo3DI: 2oo3 evaluation of inputs of data type BOOL with discrepancy analysis

Function

This F-block monitors three binary inputs for signal state 1. The OUT output is 1 when at least two INx inputs are 1. Otherwise, the OUT output is 0. The OUTN output corresponds to the negated OUT output.

If input DIS_ON = 1 is set, a discrepancy analysis is performed. If one INx input differs from the other two INy inputs longer than the assigned discrepancy time DIS_TIME, a discrepancy error is detected and saved with 1 in the DIS and DIS_D outputs.

If a discrepancy is no longer detected, the discrepancy error is acknowledged according to the parameter assignment of ACK_NEC:

- When ACK_NEC = 0, an automatic acknowledgment is carried out.
- When ACK_NEC = 1, you must acknowledge the discrepancy error with a positive edge at the ACK input.

Output ACK_REQ = 1 is used to signal that user acknowledgment at the ACK input is required for acknowledging the discrepancy error.

I/Os

	Name	Data type	Explanation	Default
Inputs:	IN1	F_BOOL	Input 1	0
	IN2	F_BOOL	Input 2	0
	IN3	F_BOOL	Input 3	0
	DIS_ON	F_BOOL	1 = Discrepancy analysis	0
	DIS_TIME	F_TIME	Discrepancy time in ms	1000
	ACK_NEC	F_BOOL	1 = Acknowledgment required	0
	ACK	F_BOOL	Acknowledgment	0

	Name	Data type	Explanation	Default
Outputs:	OUT	F_BOOL	Output	0
	OUTN	F_BOOL	Output inverted	1
	DIS	F_BOOL	Discrepancy error	0
	DIS_D	BOOL	DATA component of DIS	0
	ACK_REQ	BOOL	Acknowledgment required	0

WARNING

Fail-safe user times

When determining your response times when using an F-block with time monitoring, take into account the following timing uncertainties:

- The timing uncertainty familiar from the standard program that arises due to the cyclic processing
- The tolerance of the internal monitoring of the times in the F-CPU
  - For time values from 10 ms to 50 s: 5 ms
  - For time values from > n × 50 s to (n+1) × 50 s: ± (n+1) × 5 ms

FSW-105

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.4.2 F_2oo3AI: 2oo3 evaluation of inputs of the REAL data type with discrepancy analysis

Function

This F-block performs a 2oo3 evaluation of REAL values with discrepancy analysis.

This block is generally intended for detecting the failure or discrepancy of a sensor.

If a REAL value is invalid, a 1oo2 evaluation is performed. It calculates the average and median or the maximum and minimum of the INx inputs, depending on the QBADx inputs:

- If all INx inputs are valid (QBAD1, QBAD2 and QBAD3 = 0) and no discrepancy error was saved (DIS1CH = 0, DISALL = 0), the average [(IN1+IN2+IN3)/3] is provided at the OUT_AVG output and the median of IN1, IN2 and IN3 is provided at the MED_MAX und MED_MIN outputs.
- If all INx inputs are valid (QBAD1, QBAD2 and QBAD3 = 0) and the assigned tolerance DELTA is exceeded at all INx inputs (DIS1CH = 0, DISALL = 1), the average [(IN1+IN2+IN3)/3] is provided at the OUT_AVG output and the median of IN1, IN2 and IN3 is provided at the MED_MAX und MED_MIN outputs.

- If all INx inputs are valid (QBAD1, QBAD2 and QBAD3 = 0), the assigned tolerance DELTA is exceeded at all INx inputs and a discrepancy error was saved (DIS1CH = 1, DISALL = 1), then the outputs behave as follows:
  - MODE = 0
    OUT_AVG = Average of the INx inputs that were previously discrepancy-free. i.e. when DIS1CH = 1 and DISALL = 0.
    MED_MAX = MED_MIN = Median of IN1, IN2 and IN3
  - MODE = 1
    OUT_AVG = Average of the INx inputs that were previously discrepancy-free. i.e. when DIS1CH = 1 and DISALL = 0.
    MED_MAX = MED_MIN = Median of IN1, IN2 and IN3
  - MODE = 3
    OUT_AVG = Average of the INx inputs that were previously discrepancy-free. i.e. when DIS1CH = 1 and DISALL = 0.
    MED_MAX = Maximum of the INx inputs that were previously discrepancy-free
    MED_MIN = Minimum of the INx inputs that were previously discrepancy-free
- If all INx inputs are valid (QBAD1, QBAD2 and QBAD3 = 0) and a discrepancy error was saved (DIS1CH = 1, DISALL = 0), then the outputs behave as follows:
  - MODE = 0
    OUT_AVG = Average of the INx inputs that were previously discrepancy-free
    MED_MAX = MED_MIN = Median of IN1, IN2 and IN3
  - MODE = 1
    OUT_AVG = Average of the discrepancy-free INx inputs
    MED_MAX = MED_MIN = Median of IN1, IN2 and IN3
  - MODE = 3
    OUT_AVG = Average of the discrepancy-free INx inputs
    MED_MAX = Maximum of the discrepancy-free INx inputs
    MED_MIN = Minimum of the discrepancy-free INx inputs

Note

Change of the MODE parameter

Changes to the MODE parameter are only possible by carrying out a cold restart of the CPU. An online change is not permitted.

A cold restart of the CPU is not allowed under PCS 7. For this reason, the MODE parameter can be changed in PCS 7 by means of a full download with changed parameters.

- If only two inputs INx are valid (QBADx = 0 und QBADy = 1), the average of the valid INx inputs is provided at the OUT_AVG output, the maximum and minimum of the valid INx inputs are provided at the MED_MAX and MED_MIN outputs, respectively, and QBAD_1CH = 1 is set.
- If only one INx input is valid (QBADx = 0 and QBADy = 1), INx is provided at the OUT_AVG, MED_MAX and MED_MIN outputs and QBAD_2CH = 1 is set.
- If no INx input is valid (QBAD1, QBAD2 and QBAD3 = 1), the fail-safe value SUBS_V is provided at the OUT_AVG, MED_MAX and MED_MIN outputs and QBAD_ALL = 1 is set.

A discrepancy analysis is carried out as follows:

- All INx inputs are valid (QBAD1, QBAD2 and QBAD3 = 0)
  - If one INx input differs from the two other INy inputs by more than the assigned tolerance DELTA and for longer than the assigned discrepancy time DIS_TIME, a discrepancy error is detected and saved with 1 in the DIS1CH and DIS1CH_D outputs.
  - If all INx inputs differ by more than the assigned tolerance DELTA and for longer than the assigned discrepancy time DIS_TIME, a discrepancy error is detected and saved with 1 in the DISALL and DISALL_D outputs.
- Two inputs INx are valid (QBADx = 0 and QBADy = 1):
  - If the two valid INx inputs differ by more than the assigned tolerance DELTA and for longer than the assigned discrepancy time DIS_TIME, a discrepancy error is detected and saved with 1 in the DISALL and DISALL_D outputs.
- Only one INX input is valid (QBADx = 0 and QBADy = 1) or all INx inputs are invalid (QBAD1, QBAD2 and QBAD3 = 1):
  - A discrepancy analysis is not carried out.

The absolute value is always used in this case for the DELTA und DIS_TIME inputs.

Note

If the process signals at the inputs fluctuate strongly, you must set the DELTA und DIS_TIME parameters in such a way that regular fluctuations between the process values are not detected as errors.

If the inputs fall within the assigned tolerance again, the discrepancy error is acknowledged depending on the parameter assignment of ACK_NEC:

- When ACK_NEC = 0, an automatic acknowledgment is carried out.
- When ACK_NEC = 1, you must acknowledge the discrepancy error with a positive edge at the ACK input.

Output ACK_REQ = 1 is used to signal that user acknowledgment at the ACK input is required for acknowledging the discrepancy error.

Note

If you want to implement a trigger of your safety function when a limit is exceeded (e.g. with F-block F_LIM_HL), you must use the MED_MAX output for the limit monitoring. If you want to implement a trigger of your safety function when a limit is fallen below (e.g. with F-block F_LIM_LL), you must use the MED_MIN output for the limit monitoring.

You may only then use the OUT_AVG output if it flows into an evaluation in which – dependent on the process situation – the safe direction is represented once by the maximum and once by the minimum. In this case, output DISALL = 1 should also trigger the safety function.

I/Os

	Name	Data type	Explanation	Default
Inputs:	DELTA	F_REAL	Tolerance between INx	0.0
	DIS_TIME	F_TIME	Discrepancy time in ms	1000
	IN1	F_REAL	Input 1	0.0
	IN2	F_REAL	Input 2	0.0
	IN3	F_REAL	Input 3	0.0
	QBAD1	F_BOOL	1 = IN1 input invalid	0
	QBAD2	F_BOOL	1 = IN2 input invalid	0
	QBAD3	F_BOOL	1 = IN3 input invalid	0
	SUBS_V	F_REAL	Fail-safe value	0.0
	ACK_NEC	F_BOOL	1 = Acknowledgment required	0
	ACK	F_BOOL	Acknowledgment	0
	MODE	F_WORD	Operating mode • MODE = 0: Discrepancies that occur are saved and taken into account when calculating OUT_AVG. Detected discrepancy errors are saved until all three process values are within the assigned tolerance DELTA again. Only then does OUT_AVG correspond to the average of all 3 process values again. (Behavior in S7 F Systems Lib <= V1.3 SP1) • MODE = 1: Discrepancy errors that occurred previously are not saved. Only current discrepancies are taken into account when calculating OUT_AVG. (New behavior as of S7 F Systems Lib V1.3 SP2). • MODE = 2: Reserved, not supported • MODE = 3: Discrepancy errors that occurred previously are not saved. Only current discrepancies are taken into account when calculating OUT_AVG. MED_MAX corresponds to the maximum of the discrepancy-free INx inputs. MED_MIN corresponds to the minimum of the discrepancy-free INx inputs. (New behavior as of S7 F Systems Lib V1.3 SP2).	0

	Name	Data type	Explanation	Default
Outputs:	OUT_AVG	F_REAL	Average of INx	0.0
	MED_MAX	F_REAL	Median/maximum of INx	0.0
	MED_MIN	F_REAL	Median/minimum of INx	0.0
	QBAD_1CH	F_BOOL	One INx input invalid	0
	QBAD_2CH	F_BOOL	Two INx inputs invalid	0
	QBAD_ALL	F_BOOL	All INx inputs invalid	0
	DIS1CH	F_BOOL	Discrepancy error at one INx input	0
	DISALL	F_BOOL	Discrepancy error at all INx inputs	0
	DIS1CH_D	BOOL	DATA component of DIS1CH	0
	DISALL_D	BOOL	DATA component of DISALL	0
	ACK_REQ	BOOL	Acknowledgment required	0
	Q_MODE	WORD	Status of MODE input	0

⚠ WARNING

Fail-safe user times

When determining your response times when using an F-block with time monitoring, take into account the following timing uncertainties:

- The timing uncertainty familiar from the standard program that arises due to the cyclic processing
- The tolerance of the internal monitoring of times in the F-CPU
  - For time values from 10 ms to 50 s: 5 ms
  - For time values from > n × 50 s to (n+1) × 50 s: ± (n+1) × 5 ms

FSW-105

Use together with F-channel driver F_CH_AI

If you interconnect the INx input of F_2oo3AI with the V output of F_CH_AI, you must observe the following:

- Interconnect the QBADx input of F_2oo3AI with the QBAD output of the F_CH_AI whose V output you want to interconnect with the INx input of F_2oo3AI.

Error handling

- If an INx input is an invalid floating-point number (NaN), it is handled as an invalid INx input with QBAD = 1.
- If the DELTA input is an invalid floating-point number (NaN), DIS1CH, DISALL, DIS1CH_D and DISALL_D are set to 1.

- If calculations result in invalid floating-point numbers (NaN) in the F-block, the fail-safe value SUBS_V is provided at the OUT_AVG, MED_MAX and MED_MIN outputs, QBAD_1CH, QBAD_2CH and QBAD_ALL = 1 is set, and the following diagnostics event is entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Invalid REAL number in DB" (Event ID 16#75D9).
- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.4.3 F_1oo2AI: 1oo2 evaluation of inputs of data type REAL with discrepancy analysis

Function

This F-block performs a 1oo2 evaluation of REAL values with discrepancy analysis. It calculates the mean value, the maximum and minimum of the IN1 and IN2 inputs, depending on the QBADx inputs:

- If both INx inputs are valid (QBAD1 and QBAD2 = 0), the mean value of IN1 and IN2 [(IN1+IN2)/2] is provided at output OUT_AVG, the maximum at output OUT_MAX, and the minimum at output OUT_MIN.
- If only the INx input is valid (QBADx = 0 and QBADy = 1), INx is provided at the OUT_AVG, OUT_MAX, and OUT_MIN outputs and QBAD_1CH = 1 is set.
- If no INx input is valid (QBAD1 and QBAD2 = 1), the substitute value SUBS_V is provided at the OUT_AVG, OUT_MAX, and OUT_MIN outputs and QBAD_ALL = 1 is set.

If both INx inputs are valid (QBAD1 und QBAD2 = 0), a discrepancy analysis is performed:

If the two INx inputs differ by more than the assigned tolerance DELTA and for longer than the assigned discrepancy time DIS_TIME, a discrepancy error is detected and saved with 1 in the DIS and DIS_D outputs. The absolute value is always used in this case for the DELTA und DIS_TIME inputs.

If the inputs fall within the assigned tolerance again, the discrepancy error is acknowledged depending on the parameter assignment of ACK_NEC:

- When ACK_NEC = 0, an automatic acknowledgment is performed.
- When ACK_NEC = 1, you must acknowledge the discrepancy error with a positive edge at the ACK input.

Output ACK_REQ = 1 is used to signal that user acknowledgment at the ACK input is required for acknowledging the discrepancy error.

Note

If you want to implement a trigger of your safety function when a limit is exceeded (e.g. with F-block F_LIM_HL), you must use the OUT_MAX output for the limit monitoring. If you want to implement a trigger of your safety function when a limit has fallen below (e.g. with F-block F_LIM_LL), you must use the OUT_MIN output for the limit monitoring.

You may only use the OUT_AVG output if it flows into an evaluation in which – depending on the process situation – the safe direction is represented once by the maximum and once by the minimum. In this case, output DIS = 1 should also trigger the safety function.

I/Os

	Name	Data type	Explanation	Default
Inputs:	DELTA	F_REAL	Tolerance between INx	0.0
	DIS_TIME	F_TIME	Discrepancy time in ms	0
	IN1	F_REAL	Input 1	0.0
	IN2	F_REAL	Input 2	0.0
	QBAD1	F_BOOL	1 = IN1 input invalid	0
	QBAD2	F_BOOL	1 = IN2 input invalid	0
	SUBS_V	F_REAL	Substitute value	0.0
	ACK_NEC	F_BOOL	1 = Acknowledgment required	0
	ACK	F_BOOL	Acknowledgment	0
Outputs:	OUT_AVG	F_REAL	Average of INx	0.0
	OUT_MAX	F_REAL	Maximum of INx	0.0
	OUT_MIN	F_REAL	Minimum of INx	0.0
	QBAD_1CH	F_BOOL	One INx input invalid	0
	QBAD_ALL	F_BOOL	All INx inputs invalid	0
	DIS	F_BOOL	Discrepancy error	0
	DIS_D	BOOL	DATA component of DIS	0
	ACK_REQ	BOOL	Acknowledgment required	0

⚠ WARNING

Fail-safe user times

When determining your response times when using an F-block with time monitoring, take into account the following timing uncertainties:

- The timing uncertainty familiar from the standard program that arises due to the cyclic processing
- The tolerance of the internal monitoring of the times in the F-CPU
  - For time values from 10 ms to 50 s: 5 ms
  - For time values from > n × 50 s to (n+1) × 50 s: ± (n+1) × 5 ms

FSW-105

Use together with F-channel driver F_CH_AI

If you interconnect the INx input of F_1oo2AI with the V output of F_CH_AI, you must observe the following:

- Interconnect the QBADx input of F_1oo2AI with the QBAD output of the F_CH_AI whose V output you want to interconnect with the INx input of F_1oo2AI.

Error handling

- If an INx input is an invalid floating-point number (NaN), it is handled as an invalid INx input with QBADx = 1.
- If the DELTA input is an invalid floating-point number (NaN), DIS and DIS_D are set to 1.
- If calculations result in invalid floating-point numbers (NaN) in the F-block, the substitute value SUBS_V is provided at the OUT_AVG, OUT_MAX, and OUT_MIN outputs, QBAD_1CH and QBAD_ALL = 1 is set, and the following diagnostics event is entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Invalid REAL number in DB" (Event ID 16#75D9).
- An F_STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.5 Blocks and F-Blocks for data conversion

A.2.5.1 Blocks and F-blocks for data conversion

Overview

F-blocks

Block name	Block number	Description
F_SWC_CB	FB 614	Processing of a parameter of data format F_BOOL for operator input via the OS (Change process values)
F_SWC_CR	FB 615	Processing of a parameter of data format F_REAL for operator input via the OS (Change process values)
F_SWC_P	FB 335	Centralized control of operator input via the OS (Change process values, Maintenance Override, Fail-safe acknowledgment)
F_SWC_BO	FB 336	Processing of a parameter of data type F_BOOL for operator input via the OS (Maintenance Override, Fail-safe acknowledgment)
F_SWC_R	FB 337	Processing of a parameter of data type F_REAL for operator input via the OS (Maintenance Override)
F_FR_FDI	FB 339	Conversion from F_REAL to F_DINT
F_FDI_FR	FB 340	Conversion from F_DINT to F_REAL
F_BO_FBO	FB 361	Conversion from BOOL to F_BOOL
F_R_FR	FB 362	Conversion from REAL to F_REAL
F_QUITES	FB 367	Fail-safe acknowledgment via the ES/OS
F_TI_FTI	FB 368	Conversion from TIME to F_TIME
F_I_FI	FB 369	Conversion from INT to F_INT
F_FI_FR	FB 460	Conversion from F_INT to F_REAL
F_FR_FI	FB 461	Conversion from F_REAL to F_INT
F_CHG_R	FB 478	Safety Data Write for F_REAL
F_CHG_BO	FB 479	Safety Data Write for F_BOOL

Blocks

Block name	Block number	Description
F_FBO_BO	FC 303	Conversion from F_BOOL to BOOL
F_FR_R	FC 304	Conversion from F_REAL to REAL
F_FI_I	FC 305	Conversion from F_INT to INT
F_FTI_TI	FC 306	Conversion from F_TIME to TIME
SWC_CHG	FB 482	Operator function for "Change process values"
SWC_MOS	FB 338	Operator function for "Maintenance Override"
SWC_QOS	FB 481	Operator function for "Fail-safe acknowledgment"

Validity check

⚠ WARNING

Validity check

The F-blocks F_BO_FBO, F_I_FI, F_TI_FTI and F_R_FR only convert data. For this reason, you must program additional measures for validity checks in the safety program.

FSW-120

The simplest type of validity check is a range specification with fixed high limit and low limit, e.g. with F_LIM_R.

Not all input parameters can be checked for validity in a sufficiently easy manner.

A.2.5.2 F_SWC_CB: Processing of a parameter of data format F-BOOL for operator input via the OS

Function

The F-block F_SWC_CB enables changes to be made to F-parameters of data type F_BOOL in the safety program of the F-CPU from an OS (Change process values).

The OUT output is interconnected in the safety program with the I/O whose value is to be changed.

If a change was made on the faceplate in the required operator sequence within the time assigned for MAX_TIME of the F_SWC_P, the value entered on the faceplate is made available at the OUT output.

⚠ WARNING

The "Secure Write Command++" functionality allows changes to the safety program to be made during RUN mode

As a result, the following additional safety measures are required:

- Ensure that changes that may compromise plant safety cannot be made. You can use the EN_SWC input of the F-block F_SWC_P for this purpose, for example, by controlling it with a keyswitch or on a process-dependent basis via the safety program.
- Ensure that only authorized persons can make changes.

Examples:

- Control the EN_SWC input of the F-block F_SWC_P with a keyswitch.
- Set up access protection for the operator stations where the "Secure Write Command++" function can be performed.

FSW-121

When input CS_MODE = 1, the value made available at the OUT output is applied to the CS_VAL input, and output CHANGED = 1 is set.

⚠ WARNING

The CHANGED output cannot be evaluated in the safety program

CHANGED = 1 merely indicates that a change at the OUT output has been transferred to the CS_VAL input.

If the value changed using the "Secure Write Command++" function is to be in effect after a cold restart, you must manually correct the value at the CS_VAL input in the offline program and load memory.

FSW-122

I/Os

	Name	Data type	Explanation	Default
Inputs:	CS_VAL	F_BOOL	Initial value for OUT at a cold restart	0
	CS_MODE	F_BOOL	Switch for CS_VAL 1 = Apply changed OUT to CS_VAL 0 = CS_VAL remains unchanged	0
	WS_MODE	F_BOOL	Switch for warm restart 1 = At a warm restart/RESTART for F_SHUTDN, the value at the OUT output is retained 0 = At a warm restart/RESTART for F_SHUTDN, OUT receives the value of CS_VAL	1
Outputs:	OUT	F_BOOL	Current value of the operator-controlled parameter	0
	AKT_VAL	BOOL	Current value of the operator-controlled parameter for the OS	0
	CHANGED	BOOL	Indication of whether CS_VAL was changed 1 = CS_VAL was changed via the HMI	0
	CS_USED	F_BOOL	Indicates the value that was made available for OUT after startup. 1 = CS_VAL 0 = Last valid value	0

Note

The interconnection of the AKT_VAL output establishes the connection to the OS.

⚠ WARNING

Interconnection input CS_VAL

Interconnection of the CS_VAL input is not permitted.

FSW-123

Startup behavior

After an F-startup, the F-block behaves as follows:

- After a CPU STOP followed by a cold restart of the F-CPU or during initial run:
  In the first cycle after a cold restart or during the initial run, the value assigned at the CS_VAL input is made available at the OUT output. The CS_USED output is set to 1. CS_USED is reset to 0 as soon as "Secure Write Command++" has been successfully completed for the first time.
- After a CPU STOP followed by a warm restart of the F-CPU or after an F-STOP followed by a positive edge at the RESTART input of the F-block F_SHUTDN:
  In the first cycle after a warm restart or after a positive edge at the RESTART input of the F-block F_SHUTDN, the last valid value of OUT is made available at the OUT output when input WS_MODE = 1. The CS_USED output retains its default value (0). When input WS_MODE = 0, the F-block behaves the same as after a cold restart.

Note

Prior to the initial processing of the F-block after an F-startup, the default value is at the OUT and CS_USED outputs.

⚠ WARNING

F-startup

After an F-startup, plant safety must not be compromised due to either the presence of the CS_VAL value at the OUT output or the presence of the last valid value at the OUT output.

If necessary, evaluate the CS_USED output to determine whether the CS_VAL value or the last valid value was made available at the OUT output after an F-startup. You are not permitted to change the default value "0" of CS_USED. If a warm restart is performed after a cold restart, CS_USED is reset to the default value "0", even if the CS_VAL value is currently present at the OUT output.

FSW-124

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

See also

SWC_CHG: Operator function for Change process values (Page 325)

A.2.5.3 F_SWC_CR: Processing of a parameter of data format F-REAL for operator input via the OS

Function

The F-block F_SWC_CR enables changes to be made to F-parameters of data type F_REAL in the safety program of the F-CPU from an OS (Change process values).

The OUT output is interconnected in the safety program with the I/O whose value is to be changed.

The limits for the change are specified using the MIN and MAX inputs.

The maximum increment of the change is specified at the MAXDELTA input.

If a change was made on the faceplate in the required operator sequence within the time assigned for MAX_TIME of the F_SWC_P, the value entered on the faceplate is made available at the OUT output, provided it meets the following conditions:

- The value is within the limits assigned for the MIN and MAX inputs.
- The maximum increment of the change assigned for the MAXDELTA input is not exceeded.

⚠ WARNING

The "Secure Write Command++" functionality allows changes to the safety program to be made during RUN mode.

As a result, the following additional safety measures are required:

- Ensure that changes that may compromise plant safety cannot be made. You can use the EN_SWC input of the F-block F_SWC_P for this purpose, for example, by controlling it with a keyswitch or on a process-dependent basis via the safety program.
- Ensure that only authorized persons can make changes.

Examples:

- Control the EN_SWC input of the F-block F_SWC_P with a keyswitch.
- Set up access protection for the operator stations where the "Secure Write Command++" function can be performed.

FSW-121

As an alternative to the measures above, select the MIN and MAX inputs in such a way that values that could compromise plant safety cannot be specified using the "Change process data" function.

When input CS_MODE = 1, the value made available at the OUT output is applied to the CS_VAL input, and output CHANGED = 1 is set.

⚠ WARNING

The CHANGED output cannot be evaluated in the safety program.

CHANGED = 1 merely indicates that a change at the OUT output has been transferred to the CS_VAL input.

If the value changed using the "Secure Write Command++" function is to be in effect after a cold restart, you must manually correct the value at the CS_VAL input in the offline program and load memory.

FSW-126

I/Os

	Name	Data type	Explanation	Default
Inputs:	MIN	F_REAL	Low limit for F-parameter change	0.0
	MAX	F_REAL	High limit for F-parameter change	100.0
	MAXDELTA	F_REAL	Maximum change between the current value (OUT) and the new value	10.0
	CS_VAL	F_REAL	Initial value for OUT at a cold restart	0
	CS_MODE	F_BOOL	Switch for CS_VAL 1 = Apply changed OUT to CS_VAL 0 = CS_VAL remains unchanged	0
	WS_MODE	F_BOOL	Switch for warm restart 1 = At a warm restart/RESTART for F_SHUTDN, the value at the OUT output is retained 0 = At a warm restart/RESTART for F_SHUTDN, OUT receives the value of CS_VAL	1
Outputs:	OUT	F_BOOL	Current value of the operator-controlled parameter	0
	AKT_VAL	F_BOOL	Current value of the operator-controlled parameter for the OS	0
	CHANGED	BOOL	Indication of whether CS_VAL was changed 1 = CS_VAL was changed via the HMI.	0
	CS_USED	F_BOOL	Indicates the value that was made available for OUT after startup. 1 = CS_VAL 0 = Last valid value	0
	CURR_R	REAL	Copy of OUT.DATA Here, the unit of measurement to be displayed in the faceplate can be assigned using the "Unit" I/O property.	0.0

Note

The interconnection of the AKT_VAL output establishes the connection to the OS.

⚠ **WARNING**

Interconnection inputs CS_VAL, MIN, MAX and MAXDELTA

The CS_VAL, MIN, MAX and MAXDELTA inputs must not be interconnected.

FSW-127

Startup behavior

After an F-startup, the F-block behaves as follows:

- After a CPU STOP followed by a cold restart of the F-CPU or during initial run:
  In the first cycle after a cold restart or during the initial run, the value assigned at the CS_VAL input is made available at the OUT output. The CS_USED output is set to 1. CS_USED is reset to 0 as soon as "Secure Write Command++" has been successfully completed for the first time.
- After a CPU STOP followed by a warm restart of the F-CPU or after an F-STOP followed by a positive edge at the RESTART input of the F-block F_SHUTDN:
  In the first cycle after a warm restart or after a positive edge at the RESTART input of the F-block F_SHUTDN, the last valid value of OUT is made available at the OUT output when input WS_MODE = 1. The CS_USED output retains its default value ("0"). When input WS_MODE = 0, the F-block behaves the same as after a cold restart.
- During startup, OUT and ACT_VAL are initialized with the cold restart value CS_VAL if this value is within the MIN and MAX limits. If CS_VAL < MIN, OUT and AKT_VAL are initialized with the MIN value. If CS_VAL > MAX, OUT and AKT_VAL are initialized with the MAX value.

Note

Prior to the initial processing of the F-block after an F-startup, the default value is at the OUT and CS_USED outputs.

⚠ **WARNING**

F-startup

After an F-startup, plant safety must not be compromised due to either the presence of the CS_VAL value at the OUT output or the presence of the last valid value at the OUT output.

If necessary, evaluate the CS_USED output to determine whether the CS_VAL value or the last valid value was made available at the OUT output after an F-startup. You are not permitted to change the default value "0" of CS_USED. If a warm restart is performed after a cold restart, CS_USED is reset to the default value "0", even if the CS_VAL value is currently present at the OUT output.

FSW-124

Principle

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

See also

SWC_CHG: Operator function for Change process values (Page 325)

A.2.5.4 F_SWC_P: Centralized control of operator input via the OS

Function

This F-block performs the protocol handling with the OS for controlling the F_BOOL and F_REAL parameters. For this purpose, it implements a special safety protocol and monitors the required operator sequence. It has no dependency on the function behind the operator input. At least one F_SWC_P must be placed for each F-shutdown group so that one or more operator functions (SWC_CHG, SWC_MOS, SWC_QOS) can be controlled.

For the "Change process values", "Maintenance Override", and "Fail-safe acknowledgment" functions, you must assign an identifier for the utilized F-CPU that is unique from all others in the system. There are two ways of doing this:

- Assign the IDENT input for the F-block F_SWC_P
- Assign the identifier to the HID of the F-CPU

The identifier at the IDENT input has precedence. If you assign the identifier to the HID of the F-CPU and you do not use the IDENT input, the IDENT input remains empty when the program is compiled.

Use of a keyswitch

To ensure that only authorized persons perform operator inputs via the OS, you can connect the EN_SWC input of the F-block F_SWC_P to a keyswitch.

Input EN_SWC = 'true' must be set during an operator input. If EN_SWC = 'false' is reset after an operator input, all existing bypasses will be deactivated. However, set fail-safe values are retained.

⚠ WARNING

The "Secure Write Command++" functionality allows changes to the safety program to be made during RUN mode

As a result, the following additional safety measures are required:

- Identification of the F-CPU must be unique system-wide. S7 F Systems uses the IDENT parameter of F_SWC_P or the HID of the F-CPU.
- Ensure that changes that may compromise plant safety cannot be made. You can use the EN_SWC input of the F-block F_SWC_P for this purpose, for example, by controlling it with a keyswitch or on a process-dependent basis via the safety program.
- Ensure that only authorized persons can make changes.
  Examples:
  - Control the EN_SWC input of the F-block F_SWC_P with a keyswitch.
  - Set up access protection for the operator stations where the "Secure Write Command++" function can be executed.

FSW-121

I/Os

	Name	Data type	Explanation	Default
Inputs:	EN_SWC	F_BOOL	Key-operated switch: 0=No operator input allowed 1=Operator input allowed	0
	IDENT	STRING [32]	CPU identifier	''
	MAX_TIME	F_TIME	Maximum duration of an operator input, Timeout time	1 m
Outputs:	ADR_OSPA	DWORD	Connection between protocol and operator control block	0

A.2.5.5 F_SWC_BO: Processing of a parameter of data type F_BOOL for operator input via the OS

Function

The F-block F_SWC_BO enables changes to be made to F-parameters of data type F_BOOL in the safety program of the F-CPU from an OS using "Maintenance Override" or "Fail-safe acknowledgment".

The OUT output is interconnected in the safety program with the I/O whose value is to be changed.

If a change was made on the faceplate in the required operator sequence within the time assigned for MAX_TIME of the F_SWC_P, the value entered on the faceplate is made available at the OUT output.

- Interconnection with SWC_MOS ("Maintenance Override"):
  The S and R inputs can be used to set or reset the OUT and AKT_VAL outputs independent of an operator input. OUT and AKT_VAL are set using the positive edge at S. Resetting has priority, so the resetting occurs as long as R = 1. The setting of OUT and AKT_VAL is also possible when the keyswitch is not active because this is relevant only for a bypass by the operator input (soft bypass).
  S and R can be used as a hard bypass for connection of a sensor. This always has precedence over the soft bypass controlled via the OS. For this reason, an active operator input is cancelled when the hard bypass is active.
- Interconnection with SWC_QOS ("Fail-safe acknowledgment"):
  Operator control of the S and R inputs is only possible via the OS. Setting and resetting by the running program is not supported.

⚠ WARNING

The "Secure Write Command++" functionality allows changes to the safety program to be made during RUN mode.

As a result, the following additional safety measures are required:

- Ensure that changes that may compromise plant safety cannot be made. You can use the EN_SWC input of the F-block F_SWC_P for this purpose, for example, by controlling it with a keyswitch or on a process-dependent basis via the safety program.
- Ensure that only authorized persons can make changes. Examples:
  - Control the EN_SWC input of the F-block F_SWC_P with a keyswitch.
  - Set up access protection for the operator stations where the "Secure Write Command++" function can be performed.

FSW-121

I/Os

	Name	Data type	Explanation	Default
Inputs:	S	F_BOOL	Set input	0
	R	F_BOOL	Reset input	0
	CS_VAL	F_BOOL	Cold restart	0
Outputs:	OUT	F_BOOL	Current value of the operator-controlled parameter	0
	AKT_VAL	BOOL	Current value of the operator-controlled parameter for the OS	0

Note

The interconnection of the AKT_VAL output establishes the connection to the OS.

⚠ **WARNING**

Interconnection input CS_VAL

Interconnection of the CS_VAL input is not permitted.

FSW-131

Startup behavior

During startup, OUT and ACT_VAL are initialized with the value of CS_VAL at a cold restart.

⚠ **WARNING**

F-startup

After an F-startup, plant safety must not be compromised due to the presence of the CS_VAL value at the OUT and AKT_VAL outputs.

FSW-132

Error handling

- An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

See also

SWC_MOS: Command function for Maintenance Override (Page 326)

A.2.5.6 F_SWC_R: Processing of a parameter of data type F_REAL for operator input via the OS

Function

The F-block F_SWC_CR enables changes to be made to F-parameters of data type F_REAL in the safety program of the F-CPU from an OS using "Maintenance Override".

The OUT output is interconnected in the safety program with the I/O whose value is to be changed.

The limits for the change are specified using the MIN and MAX inputs.

If a change was made on the faceplate in the required operator sequence within the time assigned for MAX_TIME of the F_SWC_P, the value entered on the faceplate is made available at the OUT output, provided it meets the following conditions:

- The value is within the limits assigned for the MIN and MAX inputs.

⚠ WARNING

The "Secure Write Command++" functionality allows changes to the safety program to be made during RUN mode.

As a result, the following additional safety measures are required:

- Ensure that changes that may compromise plant safety cannot be made. You can use the EN_SWC input of the F-block F_SWC_P for this purpose, for example, by controlling it with a keyswitch or on a process-dependent basis via the safety program.
- Ensure that only authorized persons can make changes.
  Examples:
  - Control the EN_SWC input of the F-block F_SWC_P with a keyswitch.
  - Set up access protection for the operator stations where the "Secure Write Command++" function can be performed.

FSW-121

As an alternative to the measures above, select the MIN and MAX inputs in such a way that values that could compromise plant safety cannot be specified using the "Maintenance Override" function.

I/Os

	Name	Data type	Explanation	Default
Inputs:	MIN	F_REAL	Minimum value for IN	0.0
	MAX	F_REAL	Maximum value for IN	100.0
	CS_VAL	F_REAL	Cold restart value	0.0
Outputs:	OUT	F_REAL	Current value of the operator-controlled parameter	0.0
	AKT_VAL	REAL	Current value of the operator-controlled parameter for the OS	0.0

⚠ WARNING

Interconnection inputs CS_VAL, MIN and MAX

The CS_VAL, MIN and MAX inputs must not be interconnected.

FSW-134

Note

The interconnection of the AKT_VAL output establishes the connection to the OS.

Startup behavior

During startup, OUT and ACT_VAL are initialized with the cold restart value CS_VAL if this value is within the MIN and MAX limits. If CS_VAL < MIN, OUT and AKT_VAL are initialized with the MIN value. If CS_VAL > MAX, OUT and AKT_VAL are initialized with the MAX value.

⚠ **WARNING**

F-startup

After an F-startup, plant safety must not be compromised due to the presence of the CS_VAL value at the OUT and AKT_VAL outputs.

FSW-135

Error handling

- An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

See also

SWC_MOS: Command function for Maintenance Override (Page 326)

A.2.5.7 F_FR_FDI: Conversion from F_REAL to F_DINT

Function

This F-Block converts the F_REAL F-Data type at the IN input to the F_DINT F-Data type at the OUT output.

Following the conversion of F_REAL to F_DINT, if the value at the IN input exceeds the upper limit that can be portrayed by the F_INT data type, 2,147,483,647 is output at the OUT output and output OUTU is set to 1. At F_DINT values greater than (>) 2,147,483,583, the range is already exceeded.

If the range is undershot (IN is less than (<) the F_DINT value that can be portrayed), the smallest F_DINT value of -2,147,483,648 is output at output OUT, and output OUTL is set to 1.

Inaccuracies/rounding

If the value at input IN is located outside the range -16777216,0 to 16777215,0, it is possible for the output value to be rounded in F_DINT format, as values in the F_REAL format require 8 bits of the 32-bit real value to represent the exponent.

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	F_REAL	Input	0.0
Outputs:	OUT	F_DINT	Output	0
	OUTU	F_BOOL	Upper number range violation	0
	OUTL	F_BOOL	Lower number range violation	0

Error handling

- If the IN input is an invalid floating point number (NaN), 0 is output at the OUT output and OUTU and OUTL are set to 1.
- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.5.8 F_FDI_FR: Conversion from F_DINT to F_REAL

Function

This F-Block converts the F_DINT F-Data type at the IN input to the F_REAL F-Data type at the OUT output.

Inaccuracies/rounding

If the value at input IN is greater than (>) 16,777,215 or less than (<) -16,777,216, this can result in an inaccuracy in the output value of 127, maximum, compared to the input value. That is, the value in F_DINT format is rounded up or rounded off for representation in F_REAL format, as 8 bits of the 32-bit real value are required to represent the exponent. If the value is rounded off, RND_OFF = 1 is set. If the value is rounded up, RND_UP = 1 is set.

If values at input IN are greater than or equal to (>=) 2,147,483,584, the output value of data type F_REAL is always rounded up. In this case, RND_UP =1 is always set.

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	F_DINT	Input	0
Outputs:	OUT	F_REAL	Output	0.0
	RND_UP	F_BOOL	Output value is a rounded-up value	0
	RND_OFF	F_BOOL	Output value is a rounded-off value	0

Error handling

An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA).

A.2.5.9 F_BO_FBO: Conversion from BOOL to F_BOOL

Function

This F-Block converts the BOOL data type at the IN input to the corresponding F_BOOL F-Data type at the OUT output.

This enables signals formed in the standard user program to be evaluated in the safety program following a validity check.

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	BOOL	Input	0
Output:	OUT	F_BOOL	Output	0

Error handling

None

A.2.5.10 F_R_FR: Conversion from REAL to F_REAL

Function

This F-Block converts the REAL data type at the IN input to the corresponding F_REAL F-Data type at the OUT output.

This enables signals formed in the standard user program to be evaluated in the safety program following a validity check (using F-Block F_LIM_R, for example).

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	REAL	Input	0.0
Output:	OUT	F_REAL	Output	0.0

Error handling

None

A.2.5.11 F_QUITES: Fail-safe acknowledgment via the ES/OS

Function

This F-block enables fail-safe acknowledgment from a non-fail-safe ES/OS. As a result, it is possible, for example, to control the reintegration of F-I/O using the ES/OS. An acknowledgment consists of two steps:

1. Change of input IN to the value 6
2. Change of input IN from value 6 to 9 within one minute

The F-block evaluates whether the value is changed to 9 **no sooner than one second** or **no later than one minute** after the IN input is changed to the value 6. The OUT output (output for acknowledgment) is then set to 1 for the duration of one cycle.

If an invalid value is entered, or the value is not changed to 9 within one minute or before one second has elapsed, the IN input is reset to 0 and the two steps above must be repeated.

During the time in which the change from 6 to 9 is to occur, the non-fail-safe output Q is set to 1. Otherwise Q has the value 0.

⚠ WARNING

Reintegration through user acknowledgment with F_QUITES

The two acknowledgment steps must not be triggered by a single operation, e.g. by entering the acknowledgment steps including time conditions automatically in a program and triggering by a single operation! The two separate acknowledgment steps will also prevent erroneous tripping of an acknowledgment by your non-fail-safe OS.

FSW-136

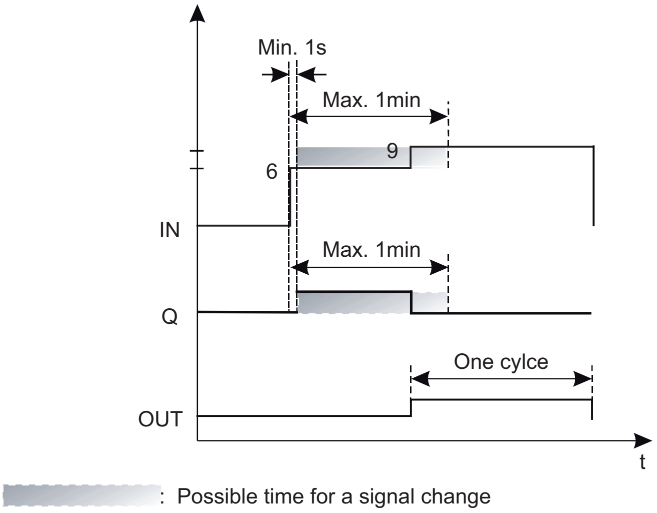
I/Os

	Name	Data type	Explanation	Default
Input:	IN	INT	Input	0
Outputs:	OUT	F_BOOL	Output for acknowledgment	0
	Q	BOOL	Status of time evaluation	0

Change of the collective signature of the offline safety program

If the two above-mentioned acknowledgment steps are entered directly via the ES in the CFC test mode instead of via the OS, the collective signature of the offline safety program changes as a result of the acknowledgment. To avoid this, be sure to enter 0 after entering 9 or an invalid value.

Time diagram



Operator control and monitoring

The IN and Q parameters have the system attribute S7_m_c. They can therefore be operated or monitored directly from an OS.

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA).

A.2.5.12 F_TI_FTI: Conversion from TIME to F_TIME

Function

This F-Block converts the TIME data type at the IN input to the corresponding F_TIME F-Data type at the OUT output.

This enables signals formed in the standard user program to be evaluated in the safety program following a validity check (using F-Block F_LIM_TI, for example).

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	TIME	Input	T# 0ms
Output:	OUT	F_TIME	Output	T# 0ms

Error handling

None

A.2.5.13 F_I_FI: Conversion from INT to F_INT

Function

This F-Block converts the INT data type at the IN input to the corresponding F_INT F-Data type at the OUT output.

This enables signals formed in the standard user program to be evaluated in the safety program following a validity check (using F-Block F_LIM_I, for example).

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	INT	Input	0
Output:	OUT	F_INT	Output	0

Error handling

None

A.2.5.14 F_FI_FR: Conversion from F_INT to F_REAL

Function

This F-Block converts the F_INT F-Data type at the IN input to the F_REAL F-Data type at the OUT output.

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	F_INT	Input	0
Output:	OUT	F_REAL	Output	0.0

Error handling

None

A.2.5.15 F_FR_FI: Conversion from F_REAL to F_INT

Function

This F-Block converts the F_REAL F-Data type at the IN input to the F_INT F-Data type at the OUT output.

If the value at the IN input exceeds the upper limit which can be portrayed by the INT data type (range: -32768 to +32767), +32767 is output at the OUT output and output OUTU is set to 1. If the value lower range is violated, -32768 is output and the OUTL output is set to 1.

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	F_REAL	Input	0.0
Output:	OUT	F_INT	Output	0
	OUTU	F_BOOL	Upper number range violation	0
	OUTL	F_BOOL	Lower number range violation	0

Error handling

- If the IN input is an invalid floating point number (NaN), 0 is output at the OUT output and OUTU and OUTL are set to 1.
- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.5.16 F_CHG_R: Safety Data Write for F_REAL

Function

The F-block F_CHG_R enables changes to be made to F-parameters in the safety program of the F-CPU from an operator station (Safety Data Write). For this purpose, the F-block implements a special safety protocol and monitors the required operator sequence.

The F-block can only be used in conjunction with the associated faceplate in the OS (see "Connection to the faceplate" below).

The OUT output is interconnected in the safety program with the I/O whose value is to be changed.

The limits for the change are specified using the MIN and MAX inputs.

The maximum increment of the change is specified at the MAXDELTA input.

The time during which the change must be completed is specified at the TIMEOUT input.

If a change was made on the faceplate in the required operator sequence within the F-monitoring time assigned for the TIMEOUT input, the value entered on the faceplate is made available at the OUT output, provided it meets the following conditions:

- The value is within the limits assigned for the MIN and MAX inputs.
- The maximum increment of the change assigned for the MAXDELTA input is not exceeded.

The "Safety Data Write" functionality must be enabled using input EN_CHG = 1.

Note

If EN_CHG changes to 0 during a transaction that has started already, the final value that is confirmed by the Confirmer is made available at the OUT output only when the EN_CHG input changes back to 1 (within the F-monitoring time).

⚠ WARNING

The "Safety Data Write" functionality allows changes to the safety program to be made during RUN mode.

As a result, the following additional safety measures are required:

- Ensure that changes that may compromise plant safety cannot be made. You can use the EN_CHG input for this purpose, for example, by controlling it with a key-operated switch or on a process-specific basis via the safety program.
- Ensure that only authorized persons can make changes. Examples:
  - Control the EN_CHG input with a keyswitch.
  - Set up access protection for operator stations where the "Safety Data Write" function can be performed.

As an alternative to the measures above, select the MIN, MAX and MAXDELTA inputs in such a way that values that could compromise plant safety cannot be specified using Safety Data Write.

FSW-137

When input CS_MODE = 1, the value made available at the OUT output is applied to the CS_VAL input, and output CHANGED = 1 is set.

⚠ WARNING

The CHANGED output cannot be evaluated in the safety program.

CHANGED = 1 merely indicates that a change at the OUT output has been transferred to the CS_VAL input.

If the value changed using the "Safety Data Write" function is to be in effect after a cold restart, you must manually correct the value at the CS_VAL input in the offline program and load memory.

FSW-138

I/Os

	Name	Data type	Explanation	Default
Inputs:	SAFE_ID1	F_DINT	Unique ID (Part 1) for interconnecting the block instance with the faceplate	0
	SAFE_ID2	F_DINT	Unique ID (Part 2) for interconnecting the block instance with the faceplate	0
	TIMEOUT	F_TIME	Permissible time between initiation of an F-parameter change and completion of the transaction.	T#60000 ms
	MIN	F_REAL	Low limit for F-parameter change.	0.0
	MAX	F_REAL	High limit for F-parameter change	100.0
	MAXDELTA	F_REAL	Maximum change between the current value (OUT) and the new value.	10.0
	CS_VAL	F_REAL	Initial value for OUT at a cold restart	0.0
	CS_MODE	F_BOOL	1 = Apply changed OUT to CS_VAL 0 = CS_VAL remains unchanged	0
	WS_MODE	F_BOOL	1 = At a warm restart/RESTART for F_SHUTDN, the value at the OUT output is retained 0 = At a warm restart/RESTART for F_SHUTDN, OUT receives the value of CS_VAL	1
	EN_CHG	F_BOOL	Allows Safety Data Write to be enabled and disabled. 1 = Enable 0 = Disable	0

	Name	Data type	Explanation	Default
Outputs:	OUT	F_REAL	Current fail-safe REAL value that is being used by the F-program	0.0
	CHANGED	BOOL	1 = CS_VAL was changed via the HMI.	0
	CS_USED	F_BOOL	Indicates the value that was made available for OUT after F-startup 1 = CS_VAL 0 = Last valid value	0
	DIAG	WORD	Diagnostic information Bit 0 = 1: Error in safety data format Bit 1 = 1: MIN error Bit 2 = 1: MAX error Bit 3 = 1: DELTA error Bit 4 = 1: TIMEOUT error Bit 5 = 1: ID1 error Bit 6 = 1: ID2 error Bit 7 = 1: ID1_C error Bit 8 = 1: ID2_C error Bit 9 = 1: Test_ID1 error Bit 10 = 1: Test_ID2 error Bit 11 = 1: Error in safety data format IN Bit 12 = 1: TIMEOUT error during OS test Bit 13 = 1: Error: Negative number at the TIMEOUT input Bits 14-15: Reserve	W#16#0
	USER	STRING [24]	Login of current operator on the OS.	''
	CURR_R	REAL	Copy of OUT.DATA Here, the unit of measurement to be displayed in the faceplate can be assigned using the "Unit" I/O property.	0.0

⚠ **WARNING**

Interconnection inputs MIN, MAX and MAXDELTA

The MIN, MAX and MAXDELTA inputs must not be interconnected.

FSW-139

Connection to the faceplate

Communication between a block instance and the assigned faceplate takes place in the background by means of a special safety protocol. To configure the communication relationship between a block instance and the assigned faceplate, select a pair of numbers (Part 1 and Part 2) that is unique from all others in the system. Assign the pair of numbers to the SAFE_ID1 and SAFE_ID2 parameters as follows:

- To the SAFE_ID1 and SAFE_ID2 inputs of F_CHG_R in your safety program in *CFC*
- SAFE_ID1 and SAFE_ID2 parameters of the associated block icon in the WinCC Graphics Designer

⚠ WARNING

Parameters SAFE_ID1 and SAFE_ID2

The pair of numbers SAFE_ID1 and SAFE_ID2 of an F-block instance must be unique from all others in the system.

An instance of the F-block and the block icon of the associated faceplate must be given the same pair of numbers for the SAFE_ID1 and SAFE_ID2 parameters.

The SAFE_ID1 parameter must be programmed not equal to 0 and unique from all others in the program.

FSW-140

Startup behavior

After an F-startup, the F-block behaves as follows:

- After a CPU STOP followed by a cold restart of the F-CPU or during initial run:
  In the first cycle after a cold restart or during the initial run, the value assigned at the CS_VAL input is made available at the OUT output. The CS_USED output is set to 1. CS_USED is reset to 0 as soon as "Secure Write Command++" has been successfully completed for the first time.

  Note

  The configured value at the CS_VAL input must be between the MIN and MAX values.

- After a CPU STOP followed by a warm restart of the F-CPU or after an F-STOP followed by a positive edge at the RESTART input of the F-block F_SHUTDN:
  In the first cycle after a warm restart or after a positive edge at the RESTART input of the F-block F_SHUTDN, the last valid value of OUT is made available at the OUT output when input WS_MODE = 1. The CS_USED output retains its default value (0). When input WS_MODE = 0, the F-block behaves the same as after a cold restart.

  Note

  Prior to initial processing of the F-block after an F-startup, the default value is at the OUT and CS_USED outputs.

  ⚠ **WARNING**

  F-startup

  After an F-startup, plant safety must not be compromised due to either the presence of the CS_VAL value at the OUT output or the presence of the last valid value at the OUT output.

  If necessary, evaluate the CS_USED output to determine whether the CS_VAL value or the last valid value was made available at the OUT output after an F-startup. You are not permitted to change the default value "0" of CS_USED.

  If a restart (warm restart) is performed after a cold restart, CS_USED is reset to the default value (0), even if the CS_VAL value is currently present at output OUT.

  FSW-141

Error handling

- An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)
- The DIAG output of the F-block signals if an error has been detected. This output must be checked if a transaction (Safety Data Write) fails. The individual errors remain active until the failed action has been repeated successfully. The individual bits have the following meanings:

All bits = 0	No problem; error-free operation
Bit 0 = 1	Error in the safety data format at an input of the F-block
Bit 1 = 1	MIN error: Transaction failed because the changed value is less than the MIN limit.
Bit 2 = 1	MAX error: Transaction failed because the changed value is greater than the MAX limit.
Bit 3 = 1	DELTA error: Transaction failed because the increment of the change exceeds the permissible MAXDELTA value; the changed value must be between OUT ± MAXDELTA.
Bit 4 = 1	TIMEOUT error: A transaction was initiated but not completed within the specified time.
Bit 5 = 1	ID1 error: Transaction failed because SAFE_ID1 does not match at the F-block instance and the faceplate in the OS.
Bit 6 = 1	ID2 error: Transaction failed because SAFE_ID2 does not match at the F-block instance and the faceplate in the OS.
Bit 7 = 1	ID1_C error: Transaction failed because SAFE_ID1 does not match at the F-block instance and the faceplate in the OS.
Bit 8 = 1	ID2_C error: Transaction failed because SAFE_ID2 does not match at the F-block instance and the faceplate in the OS.
Bit 9=1	Test_ID1 error: OS test failed because SAFE_ID1 does not match at the F-block instance and the faceplate in the OS.
Bit 10 = 1	Test_ID2 error: OS test failed because SAFE_ID2 does not match at the F-block instance and the faceplate in the OS.
Bit 11 = 1	Error in safety data format IN: Transaction failed because of an error in the safety data format of the new value of the faceplate
Bit 12 = 1	TIMEOUT error: During OS test
Bit 13 = 1	TIMEOUT error: Negative number at the TIMEOUT input of the F-block

See also

Configuring the Faceplate for Safety Data Write. (Page 179)

A.2.5.17 F_CHG_BO: Safety Data Write for F_BOOL

Function

The F-block F_CHG_BO enables changes to be made to F-parameters in the safety program of the F-CPU from an operator station (Safety Data Write). For this purpose, the F-block implements a special safety protocol and monitors the required operator sequence.

The F-block can only be used in conjunction with the associated faceplate in the OS (see "Connection to the faceplate" below).

The OUT output is interconnected in the safety program with the I/O whose value is to be changed.

The time during which the change must be completed is specified at the TIMEOUT input.

If a change was made on the faceplate in the required operator sequence within the F-monitoring time assigned for the TIMEOUT input, the value entered on the faceplate is made available at the OUT output.

The "Safety Data Write" functionality must be enabled using input EN_CHG = 1.

Note

If EN_CHG changes to 0 during a transaction that has started already, the final value that is confirmed by the Confirmer is made available at the OUT output only when the EN_CHG input changes back to 1 (within the F-monitoring time).

⚠ **WARNING**

The "Safety Data Write" functionality allows changes to the safety program to be made during RUN mode.

As a result, the following additional safety measures are required:

- Ensure that changes that may compromise plant safety cannot be made. You can use the EN_CHG input for this purpose, for example, by controlling it with a key-operated switch or on a process-specific basis via the safety program.
- Ensure that only authorized persons can make changes. Examples:
  - Control the EN_CHG input with a keyswitch.
  - Set up access protection for operator stations where the "Safety Data Write" function can be performed.

FSW-142

When input CS_MODE = 1, the value made available at the OUT output is applied to the CS_VAL input, and output CHANGED = 1 is set.

⚠ **WARNING**

The CHANGED output cannot be evaluated in the safety program.

CHANGED = 1 merely indicates that a change at the OUT output has been transferred to the CS_VAL input.

If the value changed using the "Safety Data Write" function is to be in effect after a cold restart, you must manually correct the value at the CS_VAL input in the offline program and load memory.

FSW-143

I/Os

	Name	Data type	Explanation	Default
Inputs:	SAFE_ID1	F_DINT	Unique ID (Part 1) for interconnecting the block instance with the faceplate	0
	SAFE_ID2	F_DINT	Unique ID (Part 2) for interconnecting the block instance with the faceplate	0
	TIMEOUT	F_TIME	Permissible time between initiation of an F-parameter change and completion of the transaction.	T#60000 ms
	CS_VAL	F_BOOL	Initial value for OUT at a cold restart	0
	CS_MODE	F_BOOL	1 = Apply changed OUT to CS_VAL 0 = CS_VAL remains unchanged	0
	WS_MODE	F_BOOL	1 = At a warm restart/RESTART for F_SHUTDN, the value at the OUT output is retained 0 = At a warm restart/RESTART for F_SHUTDN, OUT receives the value of CS_VAL	1
	EN_CHG	F_BOOL	Allows Safety Data Write to be enabled and disabled. 1 = Enable 0 = Disable	0

	Name	Data type	Explanation	Default
Outputs:	OUT	F_BOOL	Current fail-safe BOOL value that is being used by the safety program	0
	CHANGED	BOOL	1 = CS_VAL was changed via the HMI.	0
	CS_USED	F_BOOL	Indicates the value that was made available for OUT after startup. 1 = CS_VAL 0 = Last valid value	0
	DIAG	WORD	Diagnostic information Bit 0 = 1: Error in safety data format Bit 1 = 1: Reserve Bit 2 = 1: Reserve Bit 3 = 1: Reserve Bit 4 = 1: TIMEOUT error Bit 5 = 1: ID1 error Bit 6 = 1: ID2 error Bit 7 = 1: ID1_C error Bit 8 = 1: ID2_C error Bit 9 = 1: Test_ID1 error Bit 10 = 1: Test_ID2 error Bit 11 = 1: Error in safety data format IN Bit 12 = 1: TIMEOUT error during OS test Bit 13 = 1: Error: Negative number at the TIMEOUT input Bits 14-15: Reserve	W#16#0
	USER	STRING [24]	Login of current operator on the OS.	"

Connection to the faceplate

Communication between a block instance and the assigned faceplate takes place in the background by means of a special safety protocol. To configure the communication relationship between a block instance and the assigned faceplate, select a pair of numbers (Part 1 and Part 2) that is unique from all others in the system. Assign the pair of numbers to the SAFE_ID1 and SAFE_ID2 parameters as follows:

- SAFE_ID1 and SAFE_ID2 inputs of F_CHG_BO in your safety program in CFC
- SAFE_ID1 and SAFE_ID2 parameters of the associated block icon in the WinCC Graphics Designer

⚠ WARNING

Parameters SAFE_ID1 and SAFE_ID2

The pair of numbers SAFE_ID1 and SAFE_ID2 of an F-block instance must be unique from all others in the system.

An instance of the F-block and the block icon of the associated faceplate must be given the same pair of numbers for the SAFE_ID1 and SAFE_ID2 parameters.

The SAFE_ID1 parameter must be programmed not equal to 0 and unique from all others in the program.

FSW-144

Startup behavior

After an F-startup, the F-block behaves as follows:

- After a CPU STOP followed by a cold restart of the F-CPU or during initial run:
  In the first cycle after a cold restart or during the initial run, the value assigned at the CS_VAL input is made available at the OUT output. The CS_USED output is set to 1. CS_USED is reset to 0 as soon as "Secure Write Command++" has been successfully completed for the first time.
- After a CPU STOP followed by a warm restart of the F-CPU or after an F-STOP followed by a positive edge at the RESTART input of the F-block F_SHUTDN:
  In the first cycle after a warm restart or after a positive edge at the RESTART input of the F-block F_SHUTDN, the last valid value of OUT is made available at the OUT output when input WS_MODE = 1. The CS_USED output retains its default value (0). When input WS_MODE = 0, the F-block behaves the same as after a cold restart.

Note

Prior to the initial processing of the F-block after an F-startup, the default value is at the OUT and CS_USED outputs.

⚠ **WARNING**

F-startup

After an F-startup, plant safety must not be compromised due to either the presence of the CS_VAL value at the OUT output or the presence of the last valid value at the OUT output.

If necessary, evaluate the CS_USED output to determine whether the CS_VAL value or the last valid value was made available at the OUT output after an F-startup. You are not permitted to change the default value "0" of CS_USED.

If a restart (warm restart) is performed after a cold restart, CS_USED is reset to the default value (0), even if the CS_VAL value is currently present at output OUT.

FSW-145

Error handling

- An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)
- The DIAG output of the F-block signals if an error has been detected. This output must be checked if a transaction (Safety Data Write) fails. The individual errors remain active until the failed action has been repeated successfully. The individual bits have the following meanings:

All bits = 0	No problem; error-free operation
Bit 0 = 1	Error in the safety data format at an input of the F-block
Bit 1 = 1	Reserve
Bit 2 = 1	Reserve
Bit 3 = 1	Reserve

Bit 4 = 1	TIMEOUT error: A transaction was initiated but not completed within the specified time.
Bit 5 = 1	ID1 error: Transaction failed because SAFE_ID1 does not match at the F-block instance and the faceplate in the OS.
Bit 6 = 1	ID2 error: Transaction failed because SAFE_ID2 does not match at the F-block instance and the faceplate in the OS.
Bit 7 = 1	ID1_C error: Transaction failed because SAFE_ID1 does not match at the F-block instance and the faceplate in the OS.
Bit 8 = 1	ID2_C error: Transaction failed because SAFE_ID2 does not match at the F-block instance and the faceplate in the OS.
Bit 9 = 1	Test_ID1 error: OS test failed because SAFE_ID1 does not match at the F-block instance and the faceplate in the OS.
Bit 10 = 1	Test_ID2 error: OS test failed because SAFE_ID2 does not match at the F-block instance and the faceplate in the OS.
Bit 11 = 1	Error in safety data format IN: Transaction failed because of an error in the safety data format of the new value of the faceplate
Bit 12 = 1	TIMEOUT error: During OS test
Bit 13 = 1	TIMEOUT error: Negative number at the TIMEOUT input of the F-block

See also

Configuring the Faceplate for Safety Data Write. (Page 179)

A.2.5.18 F_FBO_BO: Conversion from F_BOOL to BOOL

Function

This block converts F-Data type F_BOOL at input IN to the elementary data type BOOL at output OUT.

This enables you to evaluate signals that were generated in the safety program in the standard user program, as well.

This block must be placed in the standard user program.

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	F_BOOL	Input	—
Output:	OUT	BOOL	Output	—

Error handling

None

A.2.5.19 F_FR_R: Conversion from F_REAL to REAL

Function

This block converts F-Data type F_REAL at input IN to the elementary data type REAL at output OUT.

This enables you to evaluate signals that were generated in the safety program in the standard user program, as well.

This block must be placed in the standard user program.

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	F_REAL	Input	—
Output:	OUT	REAL	Output	—

Error handling

None

A.2.5.20 F_FI_I: Conversion from F_INT to INT

Function

This block converts F-Data type F_INT at input IN to the elementary data type INT at output OUT.

This enables you to evaluate signals that were generated in the safety program in the standard user program, as well.

This block must be placed in the standard user program.

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	F_INT	Input	—
Output:	OUT	INT	Output	—

Error handling

None

A.2.5.21 F_FTI_TI: Conversion from F_TIME to TIME

Function

This block converts F-Data type F_TIME at input IN to the elementary data type TIME at output OUT.

This enables you to evaluate signals that were generated in the safety program in the standard user program, as well.

This block must be placed in the standard user program.

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	F_TIME	Input	—
Output:	OUT	TIME	Output	—

Error handling

None

A.2.5.22 SWC_CHG: Operator function for Change process values

Function

This block is a standard block that establishes the connection to the faceplate. In addition, it provides all values for the display or handling of the protocol to the block icon and faceplate on the OS and generates messages for PCS 7 using the ALARM_8P.

Depending on the operator function, a SWC_CHG must be placed and inserted in the plant hierarchy.

Note

When used with PCS 7, one PO license is used for each instance of the SWC_CHG block in the safety program.

The following ALARM_8P messages are generated by this block for the alarm system:

- End-of-operator-input status
- "Confirmation request is active"

Note

When assigning the block name, note that the following illegal characters will be automatically replaced by the "$" character during the transfer to the OS:

`Space ? * ' :`

Avoid these characters because an operator input is otherwise not possible.

Note

The creation of F-block types based on the "Secure Write Command++" function is not supported.

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_SWC	DWORD	Connection between protocol block and operator control block	0
	NOTE	STRING [32]	Faceplate title	—
	AKT_V_B	BOOL	Actual value for the changed BOOL value	0
	AKT_V_R	REAL	Actual value for the changed REAL value	0.0

A.2.5.23 SWC_MOS: Command function for Maintenance Override

SWC_MOS

This block is a standard block that establishes the connection to the faceplate. It also provides the block icon and faceplate on the OS with all values for displaying or processing the protocol, and generates messages for PCS 7 via ALARM_8P.

Depending on the operator function, a SWC_MOS must be placed and inserted in the plant hierarchy.

With the SWC_MOS block, only operator control of a fail-safe value is possible.

Note

When used with PCS 7, one PO license is used for each instance of the SWC_MOS block in the safety program.

The following ALARM_8P messages are generated by this block for the alarm system:

- Prewarning message for expiration of bypass time
- End-of-operator-input status
- Bypass active/not active
- "Confirmation request is active"

Note

When assigning the block name, note that the following illegal characters will be automatically replaced by the $ character during the transfer to the OS:

`Space ? * ' :`

Avoid these characters because an operator input is otherwise not possible.

Note

The creation of F-block types based on the "Secure Write Command++" function is not supported.

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_SWC	DWORD	Connection between protocol block and operator control block	0
	NOTE	STRING [32]	Faceplate title	—
	AKT_B1	BOOL	Actual value of the 1st parameter for OS	0
	VMOD_B1B	BOOL	Status of channel (BOOL)	0
	Q_B1B	BOOL	Process value	0
	VMOD_B1R	REAL	Status of channel (REAL)	0.0
	V_B1R	REAL	Process value	0.0
	AKT_B2	BOOL	Actual value of the 2nd parameter for OS	0
	VMOD_B2B	BOOL	Status of channel (BOOL)	0
	Q_B2B	BOOL	Process value	0
	VMOD_B2R	REAL	Status of channel (REAL)	0.0
	V_B2R	REAL	Process value	0.0
	AKT_B3	BOOL	Actual value of the 3rd parameter for OS	0
	VMOD_B3B	BOOL	Status of channel (BOOL)	0
	Q_B3B	BOOL	Status of channel (BOOL)	0
	VMOD_B3R	REAL	Status of channel (REAL)	0.0
	V_B3R	REAL	Process value	0.0
	AKT_TR	BOOL	Actual value of retrigger signal for OS	0
	T_WARN	TIME	Prewarning time for active bypass	0 s
	AKT_V_B	BOOL	Actual value of BOOL fail-safe value for OS	0
	AKT_V_R	REAL	Actual value of REAL fail-safe value for OS	0.0
	MODE	WORD	Mutual interlock	W#16#0

A.2.5.24 SWC_QOS: Operator function for fail-safe acknowledgment

Function

This block is a standard block that establishes the connection to the faceplate. In addition, it provides all values for the display or handling of the protocol to the block icon and faceplate on the OS and generates messages for PCS 7 using the ALARM_8P.

Depending on the operator function, a SWC_QOS must be placed and inserted in the plant hierarchy.

Note

When used with PCS 7, one PO license is used for each instance of the SWC_QOS block in the safety program.

The following ALARM_8P messages are generated by this block for the alarm system:

- End-of-operator-input status
- "Confirmation request is active"
- "Acknowledgment required"

Note

When assigning the block name, note that the following illegal characters will be automatically replaced by the "$" character during the transfer to the OS:

```
Space ? * ' :
```

Avoid these characters because an operator input is otherwise not possible.

Note

The creation of F-block types based on the "Secure Write Command++" function is not supported.

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_SWC	DWORD	Connection between protocol block and operator control block	0
	NOTE	STRING [32]	Faceplate title	—
	AKT_Q	BOOL	Actual value for the acknowledgment	0
	ACK_REQ	BOOL	Actual value of the interconnected ACK_REQ	0

A.2.6 F-Channel drivers for F-I/O

Overview

Block name	Block number	Description
F_CH_BI	FB 354	F-channel driver for inputs of data type BOOL of fail-safe DP standard slaves and fail-safe IO standard devices
F_CH_QBI	FB 620	F-channel driver for inputs of data type BOOL (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices
F_CH_BO	FB 355	F-channel driver for outputs of data type BOOL of fail-safe DP standard slaves and fail-safe IO standard devices
F_CH_QBO	FB 621	F-channel driver for outputs of data type BOOL (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices
F_PA_AI	FB 356	F-channel driver for fail-safe PA field device "Transmitter"
F_PA_DI	FB 357	F-channel driver for fail-safe PA field device "Discrete Input"
F_CH_DI	FB 377	F-channel driver for digital inputs of F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices)
F_CH_DO	FB 378	F-channel driver for digital outputs of F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices)
F_CH_AI	FB 379	F-channel driver for analog inputs of F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices)
F_CH_II	FB 454	F-channel driver for inputs of data type INT of fail-safe DP standard slaves and fail-safe IO standard devices
F_CH_QII	FB 622	F-channel driver for inputs of data type INT (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices
F_CH_IO	FB 455	F-channel driver for outputs of data type INT of fail-safe DP standard slaves and fail-safe IO standard devices
F_CH_QIO	FB 623	F-channel driver for outputs of data type INT (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices
F_CH_DII	FB 465	F-channel driver for inputs of data type DINT of fail-safe DP standard slaves and fail-safe IO standard devices
F_CH_DIO	FB 466	F-channel driver for outputs of data type DINT of fail-safe DP standard slaves and fail-safe IO standard devices
F_CH_RI	FB 616	F-channel driver for inputs of data type REAL of fail-safe DP standard slaves and fail-safe IO standard devices

A.2.6.1 F_CH_BI: F-Channel driver for inputs of data type BOOL of fail-safe DP standard slaves and fail-safe standard I/O devices

Function

The F-block is used for signal processing of an input value of data type BOOL of fail-safe DP standard slaves and fail-safe IO standard devices.

The F-block cyclically reads the input value addressed at the VALUE input of data type BOOL of a fail-safe DP standard slave/IO standard device from the associated F-module driver F_PS_12 that communicates with the fail-safe DP standard slave/IO standard device via a safety message frame according to the PROFIsafe bus profile. The F-module driver is automatically positioned and interconnected with the CFC function "Generate module drivers".

If the digital input value is valid, it is made available at the Q output.

A quality code (QUALITY output) that can have the following states is generated for the result value at the Q output:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	to be automatically supplied *
	VALUE	BOOL	Address of the digital input channel	0
	SIM_I	F_BOOL	Simulation value	0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1 = Enable assignment of I-parameters	0
Outputs:	PASS_OUT	F_BOOL	1 = Passivation due to error	0
	QBAD	F_BOOL	1 = Process value invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	Q	F_BOOL	Process value	0
	QN	F_BOOL	Process value inverted	1
	Q_DATA	BOOL	DATA component of the process value (for visualization)	0
	QUALITY	BYTE	Value status (quality code) of the process value	0
	Q_MOD	BOOL	Value from fail-safe DP standard slave/IO standard device	0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of

safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Note

Forcing the VALUE input

Forcing of the VALUE input is not possible because VALUE is not the value itself but rather a pointer for the address of the digital input channel.

Addressing

Link the symbol generated with HW Config in the symbol table for the input value of the BOOL data type with the VALUE input.

Note

An inversion of the VALUE input in the CFC editor is ineffective. Use the QN output instead.

Normal value

If the input value received from the fail-safe DP standard slave/IO standard device is valid, it is output at the Q output with quality code (QUALITY) 16#80.

Simulation

A simulation value can be output at the Q output instead of the normal value that is received from the fail-safe DP standard slave/IO standard device.

When input SIM_ON = 1, the value of the SIM_I input with quality code (QUALITY) 16#60 is output. Simulation has the highest priority. QBAD is always set to "0". QSIM = 1 is set if the block is in simulation state.

When simulation is switched on, the input value received from the fail-safe DP standard slave/IO standard device is output at the Q_MOD output. If no communication is possible with the fail-safe DP standard slave/IO standard device or if there is still no user acknowledgment after an error, 0 is output.

When simulation is switched off, Q_DATA is output.

Fail-safe value

The fail-safe value 0 is output at the Q output in the following cases:

- The digital input value is invalid due to a communication error (PROFIsafe).
- The digital input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.

- An F-startup is present.
- FV_ACTIVATED is signaled by the module.

The quality code (QUALITY) is set to 16#48 and QBAD = 1 is set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Parameter reassignment of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe DP standard slave/IO standard device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe standard DP slave/IO standard device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel driver belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Reintegration after error elimination

After elimination of an error, the input value received from the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the fail-safe DP standard slave/IO standard device starts up using the Slave State (20) "system start"

according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

⚠ WARNING

Parameter assignment input ACK_NEC

Parameter assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave / IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slaves/IO standard devices (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe DP standard slave/IO standard device that lasts longer than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device, the F-system detects a communication error.

FSW-147

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe DP standard slave/IO standard device. During this time, the substitute value 0 with quality code (QUALITY output) 16#48 is output and outputs QBAD = 1 and PASS_OUT = 1 are additionally set.

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.2 F_CH_QBI: F-channel driver for inputs of data type BOOL (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices

Function

The F-block is used for signal processing of an input value of data type BOOL (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices.

The F-block cyclically reads the input value of the data type BOOL of a fail-safe DP standard slave/IO standard device from the associated F-module driver F_PS_13, which communicates with the fail-safe DP standard slave/IO standard device via a safety message frame in accordance with the PROFIsafe bus profile. The F-module driver is automatically positioned and interconnected with the CFC function "Generate module drivers".

If the digital input value is valid, it is made available at the Q output.

A quality code (QUALITY output) that can have the following states is generated for the result value at the Q output:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	to be automatically supplied *
	VALUE	BOOL	Address of the digital input channel	0
	SIM_I	F_BOOL	Simulation value	0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	1
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1 = Enable assignment of I-parameters	0

	Name	Data type	Explanation	Default
Outputs:	PASS_OUT	F_BOOL	1 = Passivation due to error	0
	QBAD	F_BOOL	1 = Process value invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	Q	F_BOOL	Process value	0
	QN	F_BOOL	Process value inverted	1
	Q_DATA	BOOL	DATA component of the process value (for visualization)	0
	QUALITY	BYTE	Value status (quality code) of the process value	0
	Q_MOD	BOOL	Value from fail-safe DP standard slave/IO standard device	0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0
	QBIT	F_BOOL	Qualifier bit; value status from the input signal of the module 1 = Valid process value is output 0 = Substitute value is output	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Note

Forcing the VALUE input

Forcing of the VALUE input is not possible because VALUE is not the value itself but rather a pointer for the address of the digital input channel.

Addressing

Link the symbol generated with HW Config in the symbol table for the input value of the BOOL data type with the VALUE input.

Note

An inversion of the VALUE input in the CFC editor is ineffective. Use the QN output instead.

Normal value

If the input value received from the fail-safe DP standard slave/IO standard device is valid, it is output at the Q output with quality code (QUALITY) 16#80.

Simulation

A simulation value can be output at the Q output instead of the normal value that is received from the fail-safe DP standard slave/IO standard device.

When input SIM_ON = 1, the value of the SIM_I input with quality code (QUALITY) 16#60 is output. Simulation has the highest priority. QBAD is always set to "0". QSIM = 1 is set if the block is in simulation state.

When simulation is switched on, the input value received from the fail-safe DP standard slave/IO standard device is output at the Q_MOD output. If no communication is possible with the fail-safe DP standard slave/IO standard device or if there is still no user acknowledgment after an error, 0 is output.

When simulation is switched off, Q_DATA is output.

Fail-safe value

The fail-safe value 0 is output at the Q output in the following cases:

- The digital input value is invalid due to a communication error (PROFIsafe).
- The digital input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- An F-startup is present.
- FV_ACTIVATED is signaled by the module.

The quality code (QUALITY) is set to 16#48 and QBAD = 1 is set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Value status QBIT

One value status bit (Qualifier bit) exists for each input channel in the input address space.

Regardless of the diagnostics enables, each value status provides information about the validity of the corresponding process value (output Q).

- Value status (output QBIT) = 1: Valid process value is output
  The value status is set to "1" when the input signal at the module can be received without errors.
- Value status (output QBIT) = 0: Substitute value is output
  The value status is set to "0" in the following cases:
  - The input signal cannot be detected by the module due to an error.

Parameter reassignment of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe

Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe DP standard slave/IO standard device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe standard DP slave/IO standard device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel driver belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Reintegration after error elimination

After elimination of an error, the input value received from the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the fail-safe DP standard slave/IO standard device starts up using the Slave State (20) "system start" according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

⚠ WARNING

Parameter assignment input ACK_NEC

Parameter assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave / IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slaves/IO standard devices (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe DP standard slave/IO standard device that lasts longer than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device, the F-system detects a communication error.

FSW-147

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe DP standard slave/IO standard device. During this time, the substitute value 0 with quality code (QUALITY output) 16#48 is output and outputs QBAD = 1 and PASS_OUT = 1 are additionally set.

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.3 F_CH_BO: F-Channel driver for outputs of data type BOOL of fail-safe DP standard slaves and fail-safe standard I/O devices

Function

The F-block is used for signal processing of an output value of data type BOOL of fail-safe DP standard slaves and fail-safe IO standard devices.

The F-block cyclically writes the output value of data type BOOL for the output of a fail-safe DP standard slave/IO standard device addressed at the VALUE output to the associated F-module driver F_PS_12 that communicates with the fail-safe DP standard slave/IO standard device via a safety message frame according to the PROFIsafe bus profile. The F-module driver is automatically positioned and interconnected with the CFC function "Generate module drivers".

A quality code, which can take the following states, is generated for the output value that is written to the fail-safe DP standard slave/IO standard device:

State	Quality code
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	to be automatically supplied *
	I	F_BOOL	Process value	0
	SIM_I	F_BOOL	Simulation value	0
	SIM_MOD	F_BOOL	1 = Simulation has priority	0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1 = Enable assignment of I-parameters	0
Outputs:	PASS_OUT	F_BOOL	1 = Passivation due to error	0
	QBAD	F_BOOL	1 = Process value invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	VALUE	BOOL	Address of the digital output channel	0
	QUALITY	BYTE	Value status (quality code) of the process value	0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE output.

Addressing

Link the symbol generated with HW Config in the symbol table for the output value of the BOOL data type with the VALUE output.

Normal value

The process value active at the I input is written to the fail-safe DP standard slave/IO standard device. The quality code (QUALITY) is set to 16#80.

Simulation

A simulation value can also be written to the fail-safe DP standard slave/IO standard device instead of the process value active at the I input.

When input SIM_ON = 1 and input SIM_MOD = 0, the value of the SIM_I input is written to the fail-safe DP standard slave/IO standard device and output at the VALUE output, if no communication error (PROFIsafe), no module or channel fault (e.g. wire break) and no F-startup is present. The quality code (QUALITY) is set to 16#60.

When input SIM_ON = 1 and input SIM_MOD = 1, the value of the SIM_I input is output at the VALUE output even when a communication error (PROFIsafe), module or channel fault (e.g. wire break) or F-startup is present, in order to simulate an "error-free" operation without the presence of a real fail-safe DP standard slave/IO standard device.

In both cases, the quality code (QUALITY) is set to 16#60 and QSIM = 1.

Note

If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, a simulation value is not written if the PASS_ON input of another F-channel driver for outputs of the fail-safe DP standard slave/IO standard device is "1" and the SIM_ON input is 0.

Fail-safe value

The fail-safe value 0 is written to the fail-safe DP standard slave/IO standard device when any of the following occurs:

- A communication error (PROFIsafe)
- A module or channel fault (e.g. wire break)
- An F-startup
- Passivation with PASS_ON = 1

The quality code (QUALITY) is set to 16#48 and QBAD = 1 is set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Note

With fail-safe DP standard slaves/IO standard devices, channel-specific passivation via PASS_ON is not possible. If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, the fail-safe value 0 is written for all outputs of the fail-safe DP standard slave/IO standard device following a passivation with PASS_ON = 1 at one of the F-channel drivers. If you want to evaluate the QBAD and QUALITY outputs of the other F-channel drivers in case of PASS_ON = 1 at one of the F-channel drivers, you must address the PASS_ON inputs of all F-channel drivers at the same time.

Parameter reassignment of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe DP standard slave/IO standard device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe standard DP slave/IO standard device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel driver belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Reintegration after error elimination

After elimination of an error, the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment. With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the fail-safe DP standard slave/IO standard device starts up using the Slave State (20) "system start"

according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

Note

With fail-safe DP standard slaves/IO standard devices, channel-specific reintegration is not possible for outputs. When you place more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, you mut address the ACK_REI inputs of all F-channel drivers for outputs of the fail-safe DP standard slave/IO standard device at the same time.

⚠ WARNING

Parameter assignment input ACK_NEC

Parameter assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave / IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slaves/IO standard devices (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe DP standard slave/IO standard device that lasts longer than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device, the F-system detects a communication error.

FSW-147

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe DP standard slave/IO standard device. During this time, the fail-safe value 0 is written to the fail-safe DP standard slave/IO standard device. The quality code (QUALITY) is set to 16#48 and outputs QBAD = 1 and PASS_OUT = 1 are set.

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.4 F_CH_QBO: F-channel driver for outputs of data type BOOL (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices

Function

The F-block is used for signal processing of an output value of data type BOOL (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices.

The F-block cyclically writes the output value of the BOOL data type for the output of a fail-safe DP standard slave/IO standard device addressed at the VALUE output to the associated F-module driver F_PS_13, which uses a safety message frame in accordance with the PROFIsafe bus profile to communicate with the fail-safe DP standard slave/IO standard device. The F-module driver is automatically positioned and interconnected with the CFC function "Generate module drivers".

A quality code, which can take the following states, is generated for the output value that is written to the fail-safe DP standard slave/IO standard device:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	to be automatically supplied *
	I	F_BOOL	Process value	0
	SIM_I	F_BOOL	Simulation value	0
	SIM_MOD	F_BOOL	1 = Simulation has priority	0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	1
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1 = Enable assignment of I-parameters	0
Outputs:	PASS_OUT	F_BOOL	1 = Passivation due to error	0
	QBAD	F_BOOL	1 = Process value invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	VALUE	BOOL	Address of the digital output channel	0
	QUALITY	BYTE	Value status (quality code) of the process value	0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1 = New I-parameter values were assigned	0
	QBIT	F_BOOL	Qualifier bit; value status from the output signal of the module 1 = Valid process value is output 0 = Substitute value is output	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE output.

Addressing

Link the symbol generated with HW Config in the symbol table for the output value of the BOOL data type with the VALUE output.

Normal value

The process value active at the I input is written to the fail-safe DP standard slave/IO standard device. The quality code (QUALITY) is set to 16#80.

Simulation

A simulation value can also be written to the fail-safe DP standard slave/IO standard device instead of the process value active at the I input.

When input SIM_ON = 1 and input SIM_MOD = 0, the value of the SIM_I input is written to the fail-safe DP standard slave/IO standard device and output at the VALUE output, if no communication error (PROFIsafe), no module or channel fault (e.g. wire break) and no F-startup is present. The quality code (QUALITY) is set to 16#60.

When input SIM_ON = 1 and input SIM_MOD = 1, the value of the SIM_I input is output at the VALUE output even when a communication error (PROFIsafe), module or channel fault (e.g. wire break) or F-startup is present, in order to simulate an "error-free" operation without the presence of a real fail-safe DP standard slave/IO standard device.

In both cases, the quality code (QUALITY) is set to 16#60 and QSIM = 1.

Note

If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/ IO standard device, a simulation value is not written if the PASS_ON input of another F-channel driver for outputs of the fail-safe DP standard slave/IO standard device is "1" and the SIM_ON input is 0.

Fail-safe value

The fail-safe value 0 is written to the fail-safe DP standard slave/IO standard device when any of the following occurs:

- A communication error (PROFIsafe)
- F-startup
- Passivation with PASS_ON = 1

The quality code (QUALITY) is set to 16#48 and QBAD = 1 is set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Value status QBIT

One value status bit (Qualifier) exists for each output channel in the input address space.

Regardless of the diagnostics enables, each value status provides information about the validity of the corresponding process value at the output channel.

- Value status (output QBIT) = 1: Valid process value is output
  The value status is set to "1" when the process value (from the program logic) can be output without errors at the output channel.
- Value status (output QBIT) = 0: Substitute value is output
  The value status is set to "0" in the following cases:
  - The process value (from the program logic) cannot be output at the output channel due to an error.

Parameter reassignment of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe DP standard slave/IO standard device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe standard DP slave/IO standard device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel driver belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Reintegration after error elimination

After elimination of an error, the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment. With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the fail-safe DP standard slave/IO standard device starts up using the Slave State (20) "system start" according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

Note

With fail-safe DP standard slaves/IO standard devices, channel-specific reintegration is not possible for outputs. When you place more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, you mut address the ACK_REI inputs of all F-channel drivers for outputs of the fail-safe DP standard slave/IO standard device at the same time.

⚠ WARNING

Parameter assignment input ACK_NEC

Parameter assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave / IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slaves/IO standard devices (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe DP standard slave/IO standard device that lasts longer than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device, the F-system detects a communication error.

FSW-147

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe DP standard slave/IO standard device. During this time, the fail-safe value 0 is written to the fail-safe DP standard slave/IO standard device. The quality code (QUALITY) is set to 16#48 and outputs QBAD = 1 and PASS_OUT = 1 are set.

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.5 F_PA_AI: Fail-safe channel driver for fail-safe "Transmitter" PA field device

Function

The block is used for signal processing of an analog input value from a fail-safe slot (F-slot) of a "Transmitter" fail-safe PA field device.

The F-block cyclically reads the process value addressed at the VALUE input with status byte (quality code) of the fail-safe PA field device from the associated F-module driver that communicates with the F-slot of a fail-safe PA field device via a safety message frame according to the PROFIsafe bus profile. The F-module driver is automatically placed and interconnected with the *CFC* function "Generate module drivers".

If the process value exists as a physical quantity, it is made available at the V output. The status byte (quality code) is made available at the STATUS output and contains information about the status of the fail-safe PA field device.

A quality code (QUALITY output) that can have the following states is generated for the result value at the V output:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Last valid value	16#44
Uncertain, device-related	16#68
Uncertain, process-related	16#78
Uncertain, device-related, range violation	16#54
Maintenance demanded	16#A4
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	to be automatically supplied*
	VALUE	REAL	Address of the analog input channel	0
	SIM_V	F_REAL	Simulation value	0.0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	SUBS_V	F_REAL	Fail-safe value	0.0
	SUBS_ON	F_BOOL	1 = Enable fail-safe value injection	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1 = Enable assignment of I-parameters	0

	Name	Data type	Explanation	Default
Outputs:	PASS_OUT	F_BOOL	1 = Passivation due to error	0
	QBAD	F_BOOL	1 = Process value invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	QSUBS	F_BOOL	1 = Fail-safe value injection active	0
	V	F_REAL	Process value	0.0
	V_DATA	REAL	DATA component of the process value (for visualization)	0.0
	QUALITY	BYTE	Value status (quality code) of the process value	0
	STATUS	BYTE	Process value status	0
	V_MOD	REAL	Value of F-PA field device	0.0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Addressing

Link the symbol generated with HW Config in the symbol table for the analog input channel with the VALUE input.

Normal value

If the analog input value received from the fail-safe PA field device is valid, it is output at the V output. The quality code (QUALITY) is set to 16#80, 16#54, 16#60, 16#68, 16#78 or 16#A4 depending on the quality code received from the fail-safe PA field device.

Simulation

A simulation value can be output at the V output instead of the normal value that is received from the fail-safe PA field device.

When input SIM_ON = 1, the value of the SIM_V input with quality code (QUALITY) 16#60 is output. Simulation has the highest priority. QBAD and QSUBS are always set = 0. If the block is in simulation state due to SIM_ON = 1, then QSIM = 1 is set.

Note

Quality code (QUALITY) 16#60 is also output, if a simulation was started on the fail-safe PA field device and there is no event for the output of a fail-safe value or last valid value.

When simulation is switched on, the input value received from the fail-safe PA field device is output at the V_MOD output. If no communication is possible with the fail-safe PA field device or if there is still no user acknowledgment after an error, 0.0 is output.

When simulation is switched off, V_DATA is output.

Fail-safe value

When input SUBS_ON = 1, the fail-safe value SUBS_V is output at the V output in the following cases:

- The analog input value is invalid due to a communication error (PROFIsafe).
- The analog input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- An F-startup is present.
- FV_ACTIVATED is signaled by the module.

The quality code (QUALITY) is set to 16#48 and QSUBS = 1 and QBAD = 1 are set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Keep last value

When input SUBS_ON = 0, the last valid value of V is output at the V output in the following cases:

- The analog input value is invalid due to a communication error (PROFIsafe).
- The analog input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- FV_ACTIVATED is signaled by the module.

The quality code (QUALITY) is set to 16#44 and QSUBS = 0 and QBAD = 1 are set.

If the output of the last valid value is not caused by a passivation, then output PASS_OUT = 1 is additionally set in order to passivate other channels.

Parameter reassignment of a fail-safe PA field device

For parameter reassignment of a fail-safe PA field device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the IPar_EN_C variable and the IPAR_OK output corresponds to the IPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe PA field device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe PA field device.

If more than one F-channel driver is placed for an F-slot of a fail-safe PA field device, IPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel drivers belonging to the F-slot of the fail-safe PA field device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Reintegration after error elimination

After elimination of an error, the analog input value received from the fail-safe PA field device can be reintegrated automatically or only after user acknowledgment.
With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the fail-safe PA field device starts up using the Slave State (20) "system start" according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

⚠ WARNING

Parameter assignment input ACK_NEC

Parameter assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe PA field device

After power failure of the fail-safe PA field device, which is shorter than the F-monitoring time set in HW Config for the fail-safe PA field device (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe PA field device that lasts longer than the F-monitoring time set in HW Config for the fail-safe PA field device, the F-system detects a communication error.

FSW-148

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe PA field device. During this time, the fail-safe value SUBS_V with quality code (QUALITY output) 16#48 is output irrespective of the parameter assignment at the SUBS_ON input and outputs QSUBS = 1, QBAD = 1 and PASS_OUT = 1 are additionally set.

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY and STATUS outputs and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.6 F_PA_DI: Fail-safe channel driver for fail-safe "Discrete Input" PA field device

Function

The F-block is used for signal processing of a digital input value from a fail-safe slot (F-slot) of a "Discrete Input" fail-safe PA field device.

The F-block cyclically reads the process value addressed at the I_OUT_D input with status byte (quality code) of the fail-safe PA field device from the associated F-module drive that communicates with the F-slot of a fail-safe PA field device via a safety message frame according to the PROFIsafe bus profile. The F-module driver is automatically positioned and interconnected with the CFC function "Generate module drivers".

If the process value is valid, the bit (0 to 7) assigned at the BIT_NR input is made available by the process value (byte) at the Q output. The status byte (quality code) is made available at the STATUS output and contains information about the status of the fail-safe PA field device.

A quality code (QUALITY output) that can have the following states is generated for the result value at the Q output:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Uncertain, device-related	16#68
Uncertain, process-related	16#78
Uncertain, device-related, range violation	16#54
Maintenance demanded	16#A4
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for I_OUT_D interconnection	to be automatically supplied*
	BIT_NR	F_INT	REQUIRED BIT NUMBER 0 ... 7	0
	I_OUT_D	BYTE	Address of the process value	0
	SIM_I	F_BOOL	Simulation value	0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1 = Enable assignment of I-parameters	0
Outputs:	PASS_OUT	F_BOOL	1 = Passivation due to error	0
	QBAD	F_BOOL	1 = Process value invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	Q	F_BOOL	Process value	0
	QN	F_BOOL	Process value inverted	1
	Q_DATA	BOOL	DATA component of the process value (for visualization)	0
	QUALITY	BYTE	Value status (quality code) of the process value	0
	STATUS	BYTE	Status of the process value	0
	Q_MOD	BOOL	Value from the fail-safe PA field device	0
	Q0	BOOL	Process value bit 0	0
	...		...	
	Q7	BOOL	Process value bit 7	0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the I_OUT_D input.

Addressing

Link the symbol generated with HW Config in the symbol table for the process value with the I_OUT_D input.

Note

If the symbol for the process value that was generated using HW Config in the symbol table was not generated with the data type "BYTE", but rather with the data type "BOOL", you have to add a symbol with the data type BYTE yourself to the symbol table.

Normal value

If the digital input value received from the fail-safe PA field device is valid, it is output at the Q output. The quality code (QUALITY) is set to 16#80, 16#54, 16#60, 16#68, 16#78 or 16#A4 depending on the quality code received from the fail-safe PA field device.

Simulation

A simulation value can be output at the Q output instead of the normal value that is received from the fail-safe PA field device.

When input SIM_ON = 1, the value of the SIM_I input with quality code (QUALITY) 16#60 is output. Simulation has the highest priority. QBAD is always set to "0". If the F-block is in simulation state due to SIM_ON = 1, then QSIM = 1 is set.

Note

Quality code (QUALITY) 16#60 is also output, if a simulation was started on the fail-safe PA field device and there is no event for the output of a fail-safe value.

When simulation is switched on, the digital input value received from the fail-safe PA field device is output at the Q_MOD output. If no communication is possible with the fail-safe PA field device or if there is still no user acknowledgment after an error, 0 is output.

When simulation is switched off, Q_DATA is output.

Fail-safe value

The fail-safe value 0 is output at the Q output in the following cases:

- The digital input value is invalid due to a communication error (PROFIsafe).
- The digital input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- An F-startup is present.
- FV_ACTIVATED is signaled by the module.

The quality code (QUALITY) is set to 16#48 and QBAD = 1 is set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Parameter reassignment of a fail-safe PA field device

For parameter reassignment of a fail-safe PA field device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe PA field device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe PA field device.

If more than one F-channel driver is placed for an F-slot of a fail-safe PA field device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel drivers belonging to the F-slot of the fail-safe PA field device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Reintegration after error elimination

After elimination of an error, the digital input value received from the fail-safe PA field device can be reintegrated automatically or only after user acknowledgment.
With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the F-I/O starts up using the Slave State (20) "system start" according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

⚠ **WARNING**

Parameter assignment input ACK_NEC

Parameter assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe PA field device

After power failure of the fail-safe PA field device, which is shorter than the F-monitoring time set in HW Config for the fail-safe PA field device (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe PA field device that lasts longer than the F-monitoring time set in HW Config for the fail-safe PA field device, the F-system detects a communication error.

FSW-148

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe PA field device. During this time, the substitute value 0 with quality code (QUALITY output) 16#48 is output and outputs QBAD = 1 and PASS_OUT = 1 are additionally set.

Error handling

- If the BIT_NR input is assigned a value <> 0…7, the fail-safe value 0 is output at the Q output.
- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY and STATUS outputs and QBAD.DATA = 1 is set. All other variables are frozen.

See also

Configuring fail-safe PA field devices (Page 67)

A.2.6.7 F_CH_DI: F-channel driver for digital inputs of F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices)

Function

The F-block is used for signal processing of a digital input value of an F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices). It supports channel-specific passivation and redundantly configured F-I/O.

The F-block cyclically reads the digital input value of an I/O device addressed at the VALUE input from the associated F-module driver F_PS_12 or F_PS_13, which communicates with the F-I/O via a safety message frame in accordance with the PROFIsafe bus profile. The F-module driver F_PS_13 is used in PROFISafe V2.6.1 XP, for example, when using ET 200SP HA.

The F-module driver is automatically positioned and interconnected with the CFC function "Generate module drivers".

If the digital input value is valid, it is made available at the Q output.

For redundantly configured F-I/O, the digital input value of the corresponding channel of the redundantly configured F-I/O is additionally read.

A quality code (QUALITY output) that can have the following states is generated for the result value at the Q output:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	to be automatically supplied*
	VALUE	BOOL	Address of the digital input channel	0
	SIM_I	F_BOOL	Simulation value	0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0

	Name	Data type	Explanation	Default
Outputs:	PASS_OUT	F_BOOL	1 = Passivation due to error	0
	QBAD	F_BOOL	1 = Process value invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	Q	F_BOOL	Process value	0
	QN	F_BOOL	Process value inverted	1
	Q_DATA	BOOL	DATA component of the process value (for visualization)	0
	QUALITY	BYTE	Value status (quality code) of the process value	0
	Q_MOD	BOOL	Value of F-I/O	0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	DISCF	BOOL	Discrepancy error on F-I/O	0
	DISCF_R	BOOL	Discrepancy error on redundant F-I/O	0
	QMODF	BOOL	1 = F-I/O removed/faulty	0
	QMODF_R	BOOL	1 = Redundant F-I/O removed/faulty	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Note

Forcing the VALUE input

Forcing of the VALUE input is not possible because VALUE is not the value itself but rather a pointer for the address of the digital input channel.

Addressing

Link the symbol generated with HW Config in the symbol table for the input channel with the VALUE input.

Note

An inversion of the VALUE input in the CFC editor is ineffective. Use the QN output instead.

Normal value

If the digital input value received from the F-I/O is valid, it is output at the Q output with quality code (QUALITY) 16#80.

Normal value for redundantly configured F-I/O

If both digital input values received from the redundantly configured F-I/O are valid, they are ORed and the result is output at the Q output with quality code (QUALITY) 16#80. If only one of the two received digital input values is valid, it is output at the Q output with quality code (QUALITY) 16#80.

Display redundancy loss on OS

The non-fail-safe outputs QMODF and QMODF_R can be read out via an OS or evaluated in the standard user program for servicing.

Simulation

A simulation value can be output at the Q output instead of the normal value that is received from the F-I/O.

When input SIM_ON = 1, the value of the SIM_I input with quality code (QUALITY) 16#60 is output. Simulation has the highest priority. QBAD is always set to "0". If the F-block is in simulation state, QSIM = 1 is set.

When simulation is switched on, the digital input value received from the F-I/O is output at the Q_MOD output. If no communication is possible with the F-I/O or if there is still no user acknowledgment after an error, 0 is output. When simulation is switched off, Q_DATA is output.

Fail-safe value

The fail-safe value 0 is output at the Q output in the following cases:

- The digital input value is invalid due to a communication error (PROFIsafe).
- The digital input value is invalid due to a module or channel fault (e.g. wire break) or a fail-safe value is received from the module.
- For redundantly configured F-I/O: Both digital input values are invalid due to a communication error (PROFIsafe) or a module or channel fault (e.g. wire break).
- A passivation with PASS_ON = 1 is present.
- An F-startup is present.

The quality code (QUALITY) is set to 16#48 and QBAD = 1 is set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Reintegration after error elimination

After elimination of an error, the digital input value received from the F-I/O can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

For redundantly configured F-I/O, user acknowledgment is required even if the named errors occurred only on one F-I/O and therefore did not result in the output of a fail-safe value at the Q output.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for a reintegration after PASS_ON = 1 of an F-startup after CPU STOP.

⚠ WARNING

Parameter assignment input ACK_NEC

Parameter assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the F-I/O

After power failure of the fail-safe I/O, which is shorter than the F-monitoring time set in HW Config for the fail-safe I/O (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe I/O that lasts longer than the F-monitoring time set in HW Config for the fail-safe I/O, the F-system detects a communication error.

FSW-149

Discrepancy analysis for redundantly configured F-I/O

The F-block performs a discrepancy analysis for redundantly configured fail-safe I/O if a discrepancy time <> 0 was configured during redundancy configuration in HW Config.

If there is a discrepancy between the digital input channel addressed at the VALUE input and its redundant channel that lasts longer than the discrepancy time, a discrepancy error is detected. The F-block sets the DISCF output if the digital input channel addressed at the VALUE input supplies the 0 signal, or the DISCF_R output if the redundant channel supplies the 0 signal. DISCF/DISCF_R is reset as soon as a discrepancy is no longer present.

For example, the discrepancy analysis allows defective sensors to be detected because it is assumed that faulty fail-safe sensors supply the 0 signal. This can significantly increase the availability of the plant. Discrepancy errors have no effect on the Q, QBAD and PASS_OUT outputs. The non-fail-safe outputs DISCF/DISCF_R can be read out for service purposes via an OS or evaluated in the standard user program.

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the F-I/O. During this time, the substitute value 0 with quality code (QUALITY output) 16#48 is output and outputs QBAD = 1 and PASS_OUT = 1 are additionally set. For redundantly configured F-I/O, the fail-safe value 0 is output until communication with one of the redundant F-I/O is established.

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.8 F_CH_DO: F-channel driver for digital outputs of F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices)

Function

The F-block is used for signal processing of a digital output value of an F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices). It supports channel-specific passivation and redundantly configured F-I/O.

The F-block cyclically writes the digital output value of a, F-I/O addressed at the VALUE output to the associated F-module driver F_PS_12 or F_PS_13, which communicates with the F-I/O via a safety message frame in accordance with the PROFIsafe bus profile. The F-module driver F_PS_13 is used in PROFISafe V2.6.1 XP, for example, when using ET 200SP HA.

The F-module driver is automatically positioned and interconnected with the CFC function "Generate module drivers".

For redundantly configured F-I/O, the digital output value is additionally written to the F-module driver of the redundantly configured F-I/O.

A quality code that can have the following states is generated for the digital output value that is written to the F-I/O:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60

State	Quality code (QUALITY output)
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	to be automatically supplied*
	I	F_BOOL	Process value	0
	SIM_I	F_BOOL	Simulation value	0
	SIM_MOD	F_BOOL	1 = Simulation has priority	0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
Outputs:	PASS_OUT	F_BOOL	1 = Passivation due to error	0
	QBAD	F_BOOL	1 = Process value invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	VALUE	BOOL	Address of the digital output channel	0
	QUALITY	BYTE	Value status (quality code) of the process value	0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	QMODF	BOOL	1 = F-I/O removed/faulty	0
	QMODF_R	BOOL	1 = Redundant F-I/O removed/faulty	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE output.

Addressing

Link the symbol generated with HW Config in the symbol table for the digital output channel with the VALUE output.

Normal value

The process value active at the I input is written to the F-I/O. The quality code (QUALITY) is set to 16#80.

Normal value for redundantly configured F-I/O

For redundantly configured F-I/O, the process value active at the I input is written to both F-I/O, if both F-I/O have no communication error (PROFIsafe), no module or channel fault (e.g. wire break) and no F-startup. If one F-I/O has a communication error (PROFIsafe), module or channel fault (e.g. wire break) or an F-startup, the fail-safe value 0 is written to this F-I/O. The quality code (QUALITY) 16#80 is output.

Display redundancy loss on OS

The non-fail-safe outputs QMODF and QMODF_R can be read out via an OS or evaluated in the standard user program for servicing.

Simulation

A simulation value can also be written to the F-I/O instead of the process value active at the I input.

When input SIM_ON = 1 and input SIM_MOD = 0, the value of the SIM_I input is written to the F-I/O and output at the VALUE output, if no communication error (PROFIsafe), no module or channel fault (e.g. wire break) and no F-stop is present.

When input SIM_ON = 1 and input SIM_MOD = 1, the value of the SIM_I input is output at the VALUE output even when a communication error (PROFIsafe), module or channel fault (e.g. wire break) or F-startup is present, in order to simulate an "error-free" operation without the presence of a real F-I/O.

In both cases, the quality code (QUALITY) is set to 16#60 and QSIM = 1 is set.

Fail-safe value

The fail-safe value 0 is written to the F-I/O when any of the following occurs:

- A communication error (PROFIsafe)
- A module or channel fault (e.g. wire break)
- An F-startup
- For redundantly configured F-I/O: a communication error (PROFIsafe), a module or channel fault (e.g. wire break) or an F-startup on both F-I/O
- Passivation with PASS_ON = 1

The quality code (QUALITY) is set to 16#48 and QBAD = 1 is set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Reintegration after error elimination

After elimination of an error, the F-I/O can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

For redundantly configured F-I/O, a user acknowledgment is also required under the following conditions:

- If the named errors occurred only on one F-I/O and therefore did not result in the output of a fail-safe value to the process.
- If communication errors (PROFIsafe) occurred on only one F-I/O and therefore did not result in the output of a fail-safe value to the process.
  The acknowledgment of this error of the output module is made at the F_CH_DO F-channel driver for the whole module. After acknowledgment at an F-channel driver, all channels of the affected module are activated. To fully activate redundancy again for all channels, however, the error must also be acknowledged at the remaining "F_CH_DO" F-channel drivers.
  The PROFISAFE output signals a pending communication error (PROFIsafe) at the module driver, F_PS_12/F_PS_13. This output can be used to enable automatic acknowledgment of all channels for this error. This requires that a corresponding acknowledgment is allowed for the process.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for a reintegration after PASS_ON = 1 or an F-startup following a CPU STOP.

WARNING

Parameter assignment input ACK_NEC

Parameter assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the F-I/O

After power failure of the fail-safe I/O, which is shorter than the F-monitoring time set in HW Config for the fail-safe I/O (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe I/O that lasts longer than the F-monitoring time set in HW Config for the fail-safe I/O, the F-system detects a communication error.

FSW-149

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the F-I/O. During this time, the fail-safe value 0 is written to the F-I/O. The quality code (QUALITY) is set to 16#48 and outputs QBAD = 1 and PASS_OUT = 1 are set. For redundantly configured F-I/O, the quality code (QUALITY) is set to 16#80 and outputs QBAD = 0 and PASS_OUT = 0 are set as soon as the communication with an F-I/O is established.

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.9 F_CH_AI: F-channel driver for analog inputs of F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices)

Function

The F-block is used for signal processing of an analog input value of an F-I/O (except fail-safe DP standard slaves and fail-safe IO standard devices). It supports channel-specific passivation and redundantly configured I/O.

The F-block cyclically reads the analog input value (raw value) addressed at the VALUE input of an F-I/O from the associated F-module driver F_PS_12 that communicates with the F-I/O via a safety message frame according to the PROFIsafe bus profile. The F-module driver is automatically positioned and interconnected with the CFC function "Generate module drivers".

If the analog input value is valid, it is adjusted to its physical quantity and made available at the V output.

For redundantly configured F-I/O, the analog input value of the corresponding channel of the redundantly configured F-I/O is additionally read.

A quality code (QUALITY output) that can have the following states is generated for the result value at the V output:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Last valid value	16#44
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	To be automatically supplied*
	MODE	F_WORD	Measuring range coding	To be automatically supplied*
	VALUE	WORD	Address of the analog input channel	0
	VHRANGE	F_REAL	High limit of the process value	0.0
	VLRANGE	F_REAL	Low limit of the process value	0.0
	CH_F_ON	F_BOOL	1 = Activate limit monitoring	0
	CH_F_HL	F_REAL	Overrange limit of the input value (mA)	0.0
	CH_F_LL	F_REAL	Underrange limit of the input value (mA)	0.0
	SIM_V	F_REAL	Simulation value	0.0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	SUBS_V	F_REAL	Fail-safe value	0.0
	SUBS_ON	F_BOOL	1 = Enable fail-safe value injection	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN **	F_BOOL	1 = Enable assignment of I-parameters	0
	IPAR_EN **	F_BOOL	1 = Enable assignment of I-parameters (redundant module)	0
	DISC_ON	BOOL	1= Discrepancy analysis is performed	0
	DISC_TIME	DINT	Time in ms after which the discrepancy is displayed	0
	DELTA	REAL	Max. tolerable difference between the process values of the two modules, e.g. mA value acc. to the measuring range coding of the input signal.	0.0

	Name	Data type	Explanation	Default
Outputs:	PASS_OUT	F_BOOL	1 = Passivation due to error	0
	QCHF_HL	F_BOOL	1 = Input value in overrange	0
	QCHF_LL	F_BOOL	1 = Input value in underrange	0
	QBAD	F_BOOL	1 = Process value invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	QSUBS	F_BOOL	1 = Fail-safe value injection active	0
	OVHRANGE	F_REAL	High limit of the process value (copy)	0.0
	OVLRANGE	F_REAL	Low limit of the process value (copy)	0.0
	V	F_REAL	Process value	0.0
	V_DATA	REAL	DATA component of the process value (for visualization)	0.0
	QUALITY	BYTE	Value status (quality code) of the process value	0
	V_MOD	REAL	Value of F-I/O	0.0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK **	F_BOOL	1= New I-parameter values were assigned	
	IPAR_OKR **	F_BOOL	1= New I-parameter values were assigned (redundant module)	
	QMODF	BOOL	1 = F-I/O removed/faulty	0
	QMODF_R	BOOL	1 = Redundant F-I/O removed/faulty	0
	AL_STATE	STRUCT	Alarm status	
	RAW_VALUE	WORD	Raw value	0
	OVHRANGE	REAL	Copy of OVHRANGE	0.0
	OVLRANGE	REAL	Copy of OVLRANGE	0.0
	PASS_ON	BOOL	Copy of PASS_ON	0
	PASS_OUT	BOOL	Copy of PASS_OUT	0
	QCHF_HL	BOOL	Copy of QCHF_HL	0
	QCHF_LL	BOOL	Copy of QCHF_LL	0
	QBAD	BOOL	Copy of QBAD	0
	QSIM	BOOL	Copy of QSIM	0
	QSUBS	BOOL	Copy of QSUBS	0
	ACK_REQ	BOOL	Copy of ACK_REQ	0
	V_DATA	REAL	Copy of V_DATA	0.0
	QUALITY	BYTE	Copy of QUALITY	0
	V_MOD	REAL	Copy of V_MOD	0.0
	DISCF	BOOL	Discrepancy error on F-I/O	0

*) The inputs ADR_CODE and MODE are automatically supplied when the S7 program is compiled, and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE input. The MODE input is displayed as changed if changes in the configuration of the F-I/O have occurred.

**) These inputs/outputs are not visible. If you use this F-channel driver with an F-module with HART function, you may make these inputs/outputs visible and use them.

Note

Forcing the VALUE input

Forcing of the VALUE input is not possible because VALUE is not the value itself but rather a pointer for the address of the digital input channel.

Addressing

Link the symbol generated with HW Config in the symbol table for the analog input channel with the VALUE input.

Raw value check

Depending on the measuring mode and range, there is a nominal range of the F-I/O with analog inputs in which the analog signal is converted into a digitized raw value. There is also an overrange and underrange in which the analog signal can still be converted. Outside these limits, an overflow or underflow occurs. The F-channel driver indicates whether the raw value is within the nominal range of the F-I/O with analog inputs.

- When the nominal range is fallen below, output parameter QCHF_LL = 1 is set.
- When the nominal range is exceeded, output parameter QCHF_HL = 1 is set.

At an overflow or underflow, output QBAD = 1 is additionally set and – depending on the parameter assignment for the SUBS_ON input – the fail-safe value SUBS_V or the last valid value is output.

In the event of channel faults (e.g. wire break), 16#7FFF (overflow) or 16#8000 (underflow) is output by the F-I/O with analog inputs. Accordingly, the F-channel driver detects an overflow or underflow and sets outputs QCHF_HL or QCHF_LL = 1 and QBAD = 1.

(NAMUR) limit check for measuring range 4 mA to 20 mA

In the NAMUR guidelines for analog signal processing, limits are defined for Life Zero (4 to 20 mA) analog signals for which a channel fault is present:

3.6 mA < analog signal < 21 mA.

The above NAMUR limits are set as fixed limits for the limit check by default. If other channel fault limits are to be set, input CH_F_ON = 1 must be set and the CH_F_HL and CH_F_LL inputs must be set with corresponding new limits in mA:

CH_F_LL < Analog signal < CH_F_HL

When the active channel fault limits are exceeded or fallen below, output QBAD = 1 is additionally set and – depending on the parameter assignment for the SUBS_ON input – the fail-safe value SUBS_V or the last valid value is output.

Note

The selectable limits must lie below the high limit of the overrange and above the low limit of the underrange of the F-I/O with analog inputs. Values outside the NAMUR range are thus also possible, if the F-I/O with analog inputs does not automatically limit the measured values to these.

Normal value

If the raw value received from the F-I/O is valid, it is adjusted to its physical quantity based on the VLRANGE and VHRANGE inputs and the measuring range coding and output at the V output with quality code (QUALITY) = 16#80.

In order for the settings of VLRANGE and VHRANGE to be interconnected with other block parameters, these settings are written to the OVLRANGE and OVHRANGE outputs.

The calculation algorithm assumes that the input signal is linear.

When VLRANGE = 0.0 and VHRANGE = 100.0, a percentage is output.

If VHRANGE = VLRANGE is set, the input signal of the F-I/O with analog inputs (e.g. mA value) is output according to the measuring range coding.

A parameter assignment of VHRANGE < VLRANGE is not permitted and results in invalid outputs.

Measuring range coding of the F-I/O with analog inputs

The measuring range is coded in HW Config by configuring the parameters "measuring range" and, if necessary, "measurement type". The measuring range coding is automatically transferred to the MODE parameter of the F-channel driver. The F-channel driver supports the following measuring range codes:

Measuring method	Measuring range	MODE (decimal/hex.)
4-wire transducer or Measuring mode irrelevant	0 to 20 mA 4 to 20 mA	514 / 16#0202 515 / 16#0203
2-wire transducer	4 to 20 mA	771 / 16#0303

Note

Note on warning "The MODE parameter at F_CH_AI could not be automatically adjusted" in the compilation log

This message can occur during compilation of the F-program.

Set the "MODE" input of the associated F_CH_AI to 16#303 for measuring range of 4...20 mA and to 16#202 for a measuring range of 0...20 mA. The MODE input is invisible by default. If you have not supplied the "MODE" input, the F-Tool sets it to the default measuring range of 4...20 mA (16#303).

Normal value for redundantly configured F-I/O

For redundantly configured F-I/O, the raw value of the F-I/O that first supplies a valid value after an F-startup or initial run is output with quality code (QUALITY) = 16#80 at the V output after adjustment to its physical quantity. A changeover to the analog input value of the redundantly configured F-I/O then occurs if the currently output analog input value is invalid.

Display redundancy loss on OS

The non-fail-safe outputs QMODF and QMODF_R can be read out via an OS or evaluated in the standard user program for servicing.

Simulation

A simulation value can be output at the V output instead of the normal value that is received from the F-I/O.

When input SIM_ON = 1, the value of the SIM_V input with quality code (QUALITY) 16#60 is output. Simulation has the highest priority. QSIM = 1 is set if the block is in simulation state.

Note

Ensure for the simulation that no invalid floating-point number (NaN) is present when there is an interconnected SIM_V input. This can be achieved, for example, by using the F-block F_LIM_R.

When VLRANGE = 0.0 and VHRANGE = 100.0, the value at the SIM_V input must be a percentage value.

So that the states of the QCHF_LL and QCHF_HL outputs can also be simulated, the simulation value is converted to a raw value based on the VHRANGE und VLRANGE inputs and the measuring range coding and checked like a raw value received from the F-I/O.

In the case of overflow/underflow or overshoot/undershoot of the active channel error limits (with measuring range 4-20 mA), the simulation value SIM_V will not be displayed. Instead, depending on the parameterization at the SUBS_ON input, the substitute value SUBS_V or the last valid value is output at the V output with quality code (QUALITY) 16#60. QBAD = 1 is set.

When simulation is switched on, the analog input value received from the F-I/O is output as the process value at the V_MOD output. If no communication is possible with the F-I/O or if there is still no user acknowledgment after an error, 0.0 is output.

When simulation is switched off, V_DATA is output.

Fail-safe value

When input SUBS_ON = 1, the fail-safe value SUBS_V is output at the V output in the following cases:

- The analog input value is invalid due to a communication error (PROFIsafe).
- The analog input value is invalid due to a module or channel fault (e.g. wire break) or a fail-safe value is received from the module.
- The analog input value is invalid due to overflow or underflow.
- The analog input value is invalid due to exceeding or falling below the active channel error limits (with measuring range 4-20 mA).
- For redundantly configured F-I/O: Both analog input values are invalid due to a communication error (PROFIsafe) caused by a module or channel error (e.g. wire break), over/underflow, or exceeding/undershooting of active channel limits (for measuring range 4-20 mA).
- A passivation with PASS_ON = 1 is present.
- An F-startup is present.

The quality code (QUALITY) is set to 16#48 and QSUBS = 1 and QBAD = 1 are set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Keep last value

When input SUBS_ON = 0, the last valid value of V is output at the V output in the following cases:

- The analog input value is invalid due to a communication error (PROFIsafe).
- The analog input value is invalid due to a module or channel fault (e.g. wire break) or a fail-safe value is received from the module.
- The analog input value is invalid due to overflow or underflow.
- The analog input value is invalid due to exceeding or falling below the active channel error limits (with measuring range 4-20 mA).
- For redundantly configured F-I/O: Both analog input values are invalid due to a communication error (PROFIsafe) caused by a module or channel error (e.g. wire break), over/underflow, or exceeding/undershooting of active channel limits (for measuring range 4-20 mA).
- A passivation with PASS_ON = 1 is present.

The quality code (QUALITY) is set to 16#44, QSUBS = 0, and QBAD = 1.

If the output of the last valid value is not caused by a passivation, then output PASS_OUT = 1 is additionally set in order to passivate other channels.

Reintegration after error elimination

After elimination of an error, the analog input value received from the F-I/O can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

For redundantly configured F-I/O, user acknowledgment is required even if the named errors occurred only on one F-I/O and therefore did not result in the output of a fail-safe value at the V output.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for a reintegration after PASS_ON = 1 or an F-startup following a CPU STOP.

⚠ WARNING

Parameter assignment input ACK_NEC

Parameter assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the F-I/O

After power failure of the fail-safe I/O, which is shorter than the F-monitoring time set in HW Config for the fail-safe I/O (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe I/O that lasts longer than the F-monitoring time set in HW Config for the fail-safe I/O, the F-system detects a communication error.

FSW-149

Configurable alarm limits

The raw value and inputs/outputs of the F-channel driver are additionally bundled in a structure and made available as non-fail-safe information at the AL_STATE output. This allows you to evaluate configurable alarm limits in the standard user program. The mapping to a structure allows the information to be exchanged between an F-channel driver and a standard block via a single interconnection.

Parameter reassignment of an F-I/O

For parameter reassignment of an F-I/O, the IPAR_EN input and the IPAR_OK output are available. The IPAR_EN input and the IPAR_OK output are not visible. When an F-module with HART function is used, make the input and output visible.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of an F-I/O and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the F-I/O.

If more than one F-channel driver is placed for an F-I/O, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel drivers belonging to the F-I/O.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

For the redundantly configured F-I/O, the IPAR_ENR/IPAR_OKR signals are used.

The IPAR_EN and IPAR_ENR inputs and the IPAR_OK and IPAR_OKR outputs are not visible. When an F-module with HART function is used, make the input and output visible.

For an F-module with HART function, the IPAR_EN/IPAR_OK inputs/outputs are used for deactivation of the HART protocol. For a detailed description of how the signals are processed in the safety program, refer to the manual of the F-module, e.g. SM 336; F-AI 6 x 0/4 ... 20 mA HART, on the Internet (http://support.automation.siemens.com/WW/view/en/19026151).

Discrepancy analysis for redundantly configured F-I/O

The F-block performs a discrepancy analysis for redundantly configured F-I/O. To do this, the following settings must be configured in the CFC:

- DISC_ON must be set in order to activate the discrepancy analysis
- A value must be entered for DISC_TIME. The value specifies how long the discrepancy must last before it is indicated.
- For DELTA, a value must be set that specifies the maximum absolute deviation between the process values of the modules, e.g. mA value corresponding to the measuring range coding of the input signal.
  If the deviation is > DELTA, the discrepancy error is detected.

If there is a discrepancy between the analog input channel addressed at the VALUE input and its redundant channel that lasts longer than the discrepancy time DISC_TIME, a discrepancy error is detected. The F-block sets the DISCF output if the analog input channel addressed at the VALUE input deviates from the redundant channel by a value > DELTA. DISCF is reset as soon as a discrepancy is no longer present.

Discrepancy errors have no effect on the V, QBAD and PASS_OUT outputs. The non-fail-safe output DISCF can be read out via an OS or evaluated in the standard user program for servicing.

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the F-I/O. During this time, the fail-safe value SUBS_V with quality code (QUALITY output) 16#48 is output irrespective of the parameter assignment at the SUBS_ON input and outputs QSUBS = 1, QBAD = 1 and PASS_OUT = 1 are additionally set. For redundantly configured F-I/O, the fail-safe value SUBS_V is output until communication with one of the redundant F-I/O is established.

Error handling

- If measuring range coding at the MODE input is not supported, an invalid raw value is assumed.
- If one of the VHRANGE, VLRANGE, CH_F_HL, CH_F_LL, and SUBS_V inputs is an invalid floating-point number (NaN) or if invalid floating-point numbers (NaN) result from the calculation in the F-block, the fail-safe value SUBS_V or the last valid value is output at the V output, depending on the parameter assignment for the SUBS_ON input. The QBAD, QCHF_LL and QCHF_HL outputs are set to 1. Quality code (QUALITY) and QSUBS are formed appropriately for this.
  For the SIM_V input, note the information under "Simulation".
  For the case that invalid floating-point numbers (NaN) result from the calculation in the F-block, the following diagnostics event is entered in the diagnostics buffer of the CPU:
  - "Safety program: Invalid REAL number in DB" (Event ID 16#75D9).
- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.10 F_CH_II: F-Channel driver for inputs of data type INT of fail-safe DP standard slaves and fail-safe standard I/O devices

Function

The F-block is used for signal processing of an input value of data type INT of fail-safe DP standard slaves/fail-safe IO standard devices.

The F-block cyclically reads the input value addressed at the VALUE input of data type INT of a fail-safe DP standard slave/IO standard device from the associated F-module driver F_PS_12 that communicates with the fail-safe DP standard slave/IO standard device via a safety message frame according to the PROFIsafe bus profile. The F-module driver is automatically placed and interconnected with the CFC function "Generate module drivers".

If the input value is valid, it is made available at the V output as F_Real and at the V_INT output as Integer.

A quality code (QUALITY output) that can have the following states is generated for the result value at the V output:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Last valid value	16#44
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	To be automatically supplied*
	VALUE	INT	Address of the input channel	0
	SIM_V	F_INT	Simulation value	0
	SIM_ON	F_BOOL	1=Activate simulation value	0
	SUBS_V	F_INT	Fail-safe value	0
	SUBS_ON	F_BOOL	1=Enable fail-safe value injection	0
	PASS_ON	F_BOOL	1=Enable passivation	0
	ACK_NEC	F_BOOL	1=User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1=Enable assignment of I-parameters	0

	Name	Data type	Explanation	Default
Outputs:	PASS_OUT	F_BOOL	1=Passivation due to error	0
	QBAD	F_BOOL	1=Process value invalid	0
	QSIM	F_BOOL	1=Simulation active	0
	QSUBS	F_BOOL	1=Fail-safe value injection active	0
	V	F_REAL	Process value	0.0
	V_DATA	REAL	DATA component of the process value (for visualization)	0.0
	QUALITY	BYTE	Value status (quality code) of the process value	B#16#0
	V_INT	F_INT	INT process value	0
	V_MOD	REAL	Value of F-I/O	0.0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Note

Forcing the VALUE input

Forcing of the VALUE input is not possible because VALUE is not the value itself but rather a pointer for the address of the digital input channel.

Addressing

Link the symbol generated with HW Config in the symbol table for the input value of the INT data type with the VALUE input.

Normal value

If the input value received from the fail-safe DP standard slave/IO standard device is valid, it is output at the V and V_INT output with quality code (QUALITY) 16#80.

Simulation

A simulation value can be output at the V and V_INT output instead of the normal value that is received from the fail-safe DP standard slave/IO standard device.

When input SIM_ON = 1, the value of the SIM_V input with quality code (QUALITY) 16#60 is output. Simulation has the highest priority. QBAD is always set to "0". QSIM = 1 is set if the block is in simulation state.

When simulation is switched on, the input value received from the fail-safe DP standard slave/IO standard device is output at the V_MOD output. If no communication is possible with the fail-safe DP standard slave/IO standard device or if there is still no user acknowledgment after an error, 0 is output.

When simulation is switched off, V_DATA is output.

Fail-safe value

When input SUBS_ON = 1, the fail-safe value SUBS_V is output at the V and V_INT output in the following cases:

- The input value is invalid due to a communication error (PROFIsafe).
- The input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- An F-startup is present.
- FV_ACTIVATED is reported by the module.

The quality code (QUALITY) is set to 16#48 and QSUBS = 1 and QBAD = 1 are set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Keep last value

When input SUBS_ON = 0, the last valid value of V is output at the V and V_INT output:

- The input value is invalid due to a communication error (PROFIsafe) or a fail-safe value is received from the module.
- The input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- FV_ACTIVATED is reported by the module.

The quality code (QUALITY) is set to 16#44 and QSUBS = 0 and QBAD = 1 are set.

If the output of the last valid value is not caused by a passivation, then output PASS_OUT = 1 is additionally set in order to passivate other channels.

Reintegration

After elimination of an error, the input value received from the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the F-I/O starts up using the Slave State (20) "system start" according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

⚠ WARNING

Parameterization of input ACK_NEC

Assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave/IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe I/O that lasts longer than the F-monitoring time set in HW Config for the fail-safe I/O, the F-system detects a communication error.

FSW-147

Parameter reassignment of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe DP standard slave/IO standard device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe standard DP slave/IO standard device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel drivers belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe DP standard slave/IO standard device. During this time, the fail-safe value SUBS_V with quality code (QUALITY output) 16#48 is output irrespective of the parameter assignment at the SUBS_ON input and outputs QSUBS = 1, QBAD = 1 and PASS_OUT = 1 are additionally set.

Error handling

- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.11 F_CH_QII: F-channel driver for inputs of data type INT (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices

Function

The F-block is used for signal processing of an input value of the data type INT (with value status) of fail-safe DP standard slaves/ fail-safe IO standard devices.

The F-block cyclically reads the input value of the data type INT of a fail-safe DP standard slave/ IO standard device from the associated F-module driver F_PS_13, which communicates with the fail-safe DP standard slave/IO standard device via a safety message frame in accordance with the PROFIsafe bus profile. The F-module driver is automatically placed and interconnected with the CFC function "Generate module drivers".

If the input value is valid, it is made available at the V output as F_Real and at the V_INT output as Integer.

A quality code (QUALITY output) that can have the following states is generated for the result value at the V output:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Last valid value	16#44
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	To be automatically supplied*
	VALUE	INT	Address of the input channel	0
	SIM_V	F_INT	Simulation value	0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	SUBS_V	F_INT	Fail-safe value	0
	SUBS_ON	F_BOOL	1 = Enable substitute value connection	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	1
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1 = Enable assignment of I-parameters	0
Outputs:	PASS_OUT	F_BOOL	1 = Passivation because of error	0
	QBAD	F_BOOL	1 = Process value is invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	QSUBS	F_BOOL	1 = Active substitute value connection	0
	V	F_REAL	Process value	0.0
	V_DATA	REAL	DATA component of the process value (for visualization)	0.0
	QUALITY	BYTE	Value status (quality code) of the process value	B#16#0
	V_INT	F_INT	INT process value	0
	V_MOD	REAL	Value of F-I/O	0.0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1 = New I-parameter values were assigned	0
	QBIT	F_BOOL	Qualifier bit; value status from the input signal of the module 1 = Valid process value is output 0 = Substitute value is output	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of

safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Note

Forcing the VALUE input

Forcing of the VALUE input is not possible because VALUE is not the value itself but rather a pointer for the address of the digital input channel.

Addressing

Link the symbol generated with HW Config in the symbol table for the input value of the INT data type with the VALUE input.

Normal value

If the input value received from the fail-safe DP standard slave/IO standard device is valid, it is output at the V and V_INT output with quality code (QUALITY) 16#80.

Simulation

A simulation value can be output at the V and V_INT output instead of the normal value that is received from the fail-safe DP standard slave/IO standard device.

When input SIM_ON = 1, the value of the SIM_V input with quality code (QUALITY) 16#60 is output. Simulation has the highest priority. QBAD is always set to "0". QSIM = 1 is set if the block is in simulation state.

When simulation is switched on, the input value received from the fail-safe DP standard slave/IO standard device is output at the V_MOD output. If no communication is possible with the fail-safe DP standard slave/IO standard device or if there is still no user acknowledgment after an error, 0 is output.

When simulation is switched off, V_DATA is output.

Fail-safe value

When input SUBS_ON = 1, the fail-safe value SUBS_V is output at the V and V_INT output in the following cases:

- The input value is invalid due to a communication error (PROFIsafe).
- The input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- An F-startup is present.
- FV_ACTIVATED is reported by the module.

The quality code (QUALITY) is set to 16#48 and QSUBS = 1 and QBAD = 1 are set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Keep last value

When input SUBS_ON = 0, the last valid value of V is output at the V and V_INT output:

- The input value is invalid due to a communication error (PROFIsafe) or a fail-safe value is received from the module.
- The input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- FV_ACTIVATED is reported by the module.

The quality code (QUALITY) is set to 16#44 and QSUBS = 0 and QBAD = 1 are set.

If the output of the last valid value is not caused by a passivation, then output PASS_OUT = 1 is additionally set in order to passivate other channels.

Value status QBIT

One value status bit (Qualifier bit) exists for each input channel in the input address space.

Regardless of the diagnostics enables, each value status provides information about the validity of the corresponding process value (output Q).

- Value status (output QBIT) = 1: Valid process value is output
  The value status is set to "1" when the input signal at the module can be received without errors.
- Value status (output QBIT) = 0: Substitute value is output
  The value status is set to "0" in the following cases:
  - The input signal cannot be detected by the module due to an error.

Reintegration

After elimination of an error, the input value received from the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the F-I/O starts up using the Slave State (20) "system start" according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

⚠ WARNING

Parameterization of input ACK_NEC

Assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave/IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe I/O that lasts longer than the F-monitoring time set in HW Config for the fail-safe I/O, the F-system detects a communication error.

FSW-147

Parameter reassignment of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe DP standard slave/IO standard device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe standard DP slave/IO standard device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel drivers belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe DP standard slave/IO standard device. During this time, the fail-safe value SUBS_V with quality code (QUALITY output) 16#48 is output irrespective of the parameter assignment at the SUBS_ON input and outputs QSUBS = 1, QBAD = 1 and PASS_OUT = 1 are additionally set.

Error handling

- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.12 F_CH_IO: F-Channel driver for outputs of data type INT of fail-safe DP standard slaves and fail-safe standard I/O devices

Function

The F-block is used for signal processing of an output value of data type INT of fail-safe DP standard slaves/fail-safe IO standard devices.

The block cyclically writes the output value of the INT data type for the output of a fail-safe DP standard slave/IO standard device addressed at the VALUE output to the associated F-module driver F_PS_12, which uses a safety message frame to communicate with the fail-safe DP standard slave/IO standard device in accordance with the PROFIsafe bus profile. The F-module driver is automatically placed and interconnected with the CFC function "Generate module drivers".

A quality code that can have the following states is generated for the output value that is written to the fail-safe DP standard slave/IO standard device:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	To be automatically supplied*
	I	F_INT	Process value	0
	SIM_I	F_INT	Simulation value	0
	SIM_MOD	F_BOOL	1=Simulation value takes precedence	0
	SIM_ON	F_BOOL	1=Activate simulation value	0
	PASS_ON	F_BOOL	1=Enable passivation	0
	ACK_NEC	F_BOOL	1=User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1=Enable assignment of I-parameters	0
Outputs:	PASS_OUT	F_BOOL	1=Passivation due to error	0
	QBAD	F_BOOL	1=Process value invalid	0
	QSIM	F_BOOL	1=Simulation active	0
	VALUE	INT	Address of the output channel	0
	QUALITY	BYTE	Value status (quality code) of the process value	B#16#0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Addressing

Link the symbol generated with HW Config in the symbol table for the input value of the INT data type with the VALUE input.

Normal value

The process value active at the I input is written to the fail-safe DP standard slave/IO standard device. The quality code (QUALITY) is set to 16#80.

Fail-safe value

The fail-safe value 0 is written to the fail-safe DP standard slave/IO standard device when any of the following occurs:

- A communication error (PROFIsafe)
- A module fault or a channel fault (such as wire break)
- F-startup
- Passivation with PASS_ON = 1

The quality code (QUALITY) is set to 16#48 and QBAD = 1 is set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Note

For fail-safe DP standard slaves/IO standard devices, channel-specific passivation is not possible for outputs using PASS_ON. If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, the fail-safe value 0 is written for all outputs of the fail-safe DP standard slave/IO standard device following a passivation with PASS_ON = 1 at one of the F-channel drivers. If you want to evaluate the QBAD and QUALITY outputs of the other F-channel drivers when PASS_ON = 1 at one of the F-channel drivers, you must control the PASS_ON inputs of all F-channel drivers synchronously.

Simulation

A simulation value can also be written to the fail-safe DP standard slave/IO standard device instead of the process value active at the I input.

If the input SIM_ON = 1 and SIM_MOD = 0, the value of the input SIM_I is written to the fail-safe DP standard slave/IO standard device and output at the VALUE output, if there is no communication error (PROFIsafe), no module or channel error (such as wire break), and no F-startup.

If the input SIM_ON = 1 and SIM_MOD = 1, the value of the input SIM_I is output at the VALUE output even in the event of a communication error (PROFIsafe), a module or channel error (e.g. wire break), or an F-startup, so that an "error-free" operation can be simulated even without fail-safe DP standard slave/IO standard device being present.

In both cases, the quality code (QUALITY) is set to 16#60 and QSIM = 1 is set.

Note

If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, a simulation value is not written if the PASS_ON input of another F-channel driver for outputs of the fail-safe DP standard slave/IO standard device is 1 and the SIM_ON input is 0.

Reintegration

After elimination of an error, the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the fail-safe DP standard slave/IO standard device starts up using the Slave State (20) "system start" according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

Note

For fail-safe DP standard slaves/IO standard devices, channel-specific reintegration is not possible for outputs using PASS_ON. If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, you must synchronously control the ACK_REI inputs of all F-channel drivers for outputs of the fail-safe DP standard slave/IO standard device.

⚠ **WARNING**

Parameter assignment input ACK_NEC

Assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave/IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe I/O that lasts longer than the F-monitoring time set in HW Config for the fail-safe I/O, the F-system detects a communication error.

FSW-147

Re-configuration of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe DP standard slave/IO standard device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe standard DP slave/IO standard device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel drivers belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe DP standard slave/IO standard device. During this time, the fail-safe value 0 is written to the fail-safe DP standard slave/IO standard device. The quality code (QUALITY) is set to 16#48 and outputs QBAD = 1 and PASS_OUT = 1 are set.

Error handling

- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.13 F_CH_QIO: F-channel driver for outputs of data type INT (with value status) of fail-safe DP standard slaves and fail-safe standard I/O devices

Function

The F-block is used for signal processing of an output value of the data type INT (with value status) of fail-safe DP standard slaves/ fail-safe IO standard devices.

The block cyclically writes the output value of the INT data type for the output of a fail-safe DP standard slave/IO standard device addressed at the VALUE output to the associated F-module driver F_PS_13, which uses a safety message frame to communicate with the fail-safe DP standard slave/IO standard device in accordance with the PROFIsafe bus profile. The F-module driver is automatically placed and interconnected with the CFC function "Generate module drivers".

A quality code that can have the following states is generated for the output value that is written to the fail-safe DP standard slave/IO standard device:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	To be automatically supplied*
	I	F_INT	Process value	0
	SIM_I	F_INT	Simulation value	0
	SIM_MOD	F_BOOL	1=Simulation value takes precedence	0
	SIM_ON	F_BOOL	1=Activate simulation value	0
	PASS_ON	F_BOOL	1=Enable passivation	0
	ACK_NEC	F_BOOL	1=User acknowledgment for reintegration after error required	1
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1=Enable assignment of I-parameters	0

	Name	Data type	Explanation	Default
Outputs:	PASS_OUT	F_BOOL	1=Passivation due to error	0
	QBAD	F_BOOL	1=Process value invalid	0
	QSIM	F_BOOL	1=Simulation active	0
	VALUE	INT	Address of the output channel	0
	QUALITY	BYTE	Value status (quality code) of the process value	B#16#0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0
	QBIT	F_BOOL	Qualifier bit; value status from the output signal of the module 1 = Valid process value is output 0 = Substitute value is output	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Addressing

Link the symbol generated with HW Config in the symbol table for the input value of the INT data type with the VALUE input.

Normal value

The process value active at the I input is written to the fail-safe DP standard slave/IO standard device. The quality code (QUALITY) is set to 16#80.

Fail-safe value

The fail-safe value 0 is written to the fail-safe DP standard slave/IO standard device when any of the following occurs:

- A communication error (PROFIsafe)
- F-startup
- Passivation with PASS_ON = 1

The quality code (QUALITY) is set to 16#48 and QBAD = 1 is set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Simulation

A simulation value can also be written to the fail-safe DP standard slave/IO standard device instead of the process value active at the I input.

If the input SIM_ON = 1 and SIM_MOD = 0, the value of the input SIM_I is written to the fail-safe DP standard slave/IO standard device and output at the VALUE output, if there is no communication error (PROFIsafe), no module or channel error (such as wire break), and no F-startup.

If the input SIM_ON = 1 and SIM_MOD = 1, the value of the input SIM_I is output at the VALUE output even in the event of a communication error (PROFIsafe), a module or channel error (e.g. wire break), or an F-startup, so that an "error-free" operation can be simulated even without fail-safe DP standard slave/IO standard device being present.

In both cases, the quality code (QUALITY) is set to 16#60 and QSIM = 1 is set.

Note

If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, a simulation value is not written if the PASS_ON input of another F-channel driver for outputs of the fail-safe DP standard slave/IO standard device is 1 and the SIM_ON input is 0.

Value status QBIT

One value status bit (Qualifier) exists for each output channel in the input address space.

Regardless of the diagnostics enables, each value status provides information about the validity of the corresponding process value at the output channel.

- Value status (output QBIT) = 1: Valid process value is output
  The value status is set to "1" when the process value (from the program logic) can be output without errors at the output channel.
- Value status (output QBIT) = 0: Substitute value is output
  The value status is set to "0" in the following cases:
  - The process value (from the program logic) cannot be output at the output channel due to an error.

Reintegration

After elimination of an error, the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the fail-safe DP standard slave/IO standard device starts up using the Slave State (20) "system start"

according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

Note

For fail-safe DP standard slaves/IO standard devices, channel-specific reintegration is not possible for outputs using PASS_ON. If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, you must synchronously control the ACK_REI inputs of all F-channel drivers for outputs of the fail-safe DP standard slave/IO standard device.

⚠ **WARNING**

Parameter assignment input ACK_NEC

Assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ **WARNING**

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave/IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe I/O that lasts longer than the F-monitoring time set in HW Config for the fail-safe I/O, the F-system detects a communication error.

FSW-147

Re-configuration of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe DP standard slave/IO standard device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe standard DP slave/IO standard device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel drivers belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe DP standard slave/IO standard device. During this time, the fail-safe value 0 is written to the fail-safe DP standard slave/IO standard device. The quality code (QUALITY) is set to 16#48 and outputs QBAD = 1 and PASS_OUT = 1 are set.

Error handling

- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.14 F_CH_DII: F-Channel driver for inputs of data type DINT of fail-safe DP standard slaves and fail-safe standard I/O devices

Function

The F-block is used for signal processing of an input value of data type DINT of fail-safe DP standard slaves/fail-safe IO standard devices.

The F-block cyclically reads the input value addressed at the VALUE input of data type DINT of a fail-safe DP standard slave/IO standard device from the associated F-module driver F_PS_12 that communicates with the fail-safe DP standard slave/IO standard device via a safety message frame according to the PROFIsafe bus profile. The F-module driver is automatically placed and interconnected with the CFC function "Generate module drivers".

If the input value is valid, it is made available at the V output as F_Real and at the V_DINT output of data type F_DINT.

Note

When converting values from F_DINT to F_REAL, an inaccuracy of up to 127 results for values > +16.777.215 or <-16.777.216. That is, the value in F_DINT format is rounded up or down to be displayed in F_REAL format, since 8 bits of the 32-bit real value are needed to display the exponent.

A quality code (QUALITY output) that can have the following states is generated for the result value at the V output:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Last valid value	16#44
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	To be automatically supplied*
	VALUE	DINT	Address of the input channel	0
	SIM_V	F_DINT	Simulation value	0
	SIM_ON	F_BOOL	1=Activate simulation value	0
	SUBS_V	F_DINT	Fail-safe value	0
	SUBS_ON	F_BOOL	1=Enable fail-safe value injection	0
	PASS_ON	F_BOOL	1=Enable passivation	0
	ACK_NEC	F_BOOL	1=User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1=Enable assignment of I-parameters	0
Outputs:	PASS_OUT	F_BOOL	1=Passivation due to error	0
	QBAD	F_BOOL	1=Process value invalid	0
	QSIM	F_BOOL	1=Simulation active	0
	QSUBS	F_BOOL	1=Fail-safe value injection active	0
	V	F_REAL	Process value	0.0
	V_DATA	REAL	DATA component of the process value (for visualization)	0.0
	QUALITY	BYTE	Value status (quality code) of the process value	B#16#0
	V_DINT	F_DINT	DINT process value	0
	V_MOD	REAL	Value of F-I/O	0.0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Note

Forcing the VALUE input

Forcing of the VALUE input is not possible because VALUE is not the value itself but rather a pointer for the address of the digital input channel.

Addressing

Link the symbol generated with HW Config in the symbol table for the input value of the DINT data type with the VALUE input.

Normal value

If the input value received from the fail-safe DP standard slave/IO standard device is valid, it is output at the V and V_INT output with quality code (QUALITY) 16#80.

Simulation

A simulation value can be output at the V and V_DINT output instead of the normal value that is received from the fail-safe DP standard slave/IO standard device.

When input SIM_ON = 1, the value of the SIM_V input with quality code (QUALITY) 16#60 is output. Simulation has the highest priority. QBAD is always set to "0". QSIM = 1 is set if the block is in simulation state.

When simulation is switched on, the input value received from the fail-safe DP standard slave/ IO standard device is output at the V_MOD output. If no communication is possible with the fail-safe DP standard slave/IO standard device or if there is still no user acknowledgment after an error, 0 is output.

When simulation is switched off, V_DATA is output.

Fail-safe value

When input SUBS_ON = 1, the fail-safe value SUBS_V is output at the V and V_DINT output in the following cases:

- The input value is invalid due to a communication error (PROFIsafe).
- The input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- An F-startup is present.
- FV_ACTIVATED is reported by the module.

The quality code (QUALITY) is set to 16#48 and QSUBS = 1 and QBAD = 1 are set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Keep last value

When input SUBS_ON = 0, the last valid value of V is output at the V and V_DINT output in the following cases:

- The input value is invalid due to a communication error (PROFIsafe).
- The input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- FV_ACTIVATED is reported by the module.

The quality code (QUALITY) is set to 16#44 and QSUBS = 0 and QBAD = 1 are set.

If the output of the last valid value is not caused by a passivation, then output PASS_OUT = 1 is additionally set in order to passivate other channels.

Reintegration

After elimination of an error, the input value received from the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the F-I/O starts up using the Slave State (20) "system start" according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

⚠ **WARNING**

Parameter assignment input ACK_NEC

Assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave/IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe I/O that lasts longer than the F-monitoring time set in HW Config for the fail-safe I/O, the F-system detects a communication error.

FSW-147

Parameter reassignment of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input when parameters of a fail-safe standard DP slave/IO device are reassigned, or how to evaluate the IPAR_OK output, refer to the PROFIsafe specification V1.30 or higher or the documentation for the fail-safe DP standard slave/standard I/O device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel drivers belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe DP standard slave/IO standard device. During this time, the fail-safe value SUBS_V with quality code (QUALITY output) 16#48 is output irrespective of the parameter assignment at the SUBS_ON input and outputs QSUBS = 1, QBAD = 1 and PASS_OUT = 1 are additionally set.

Error handling

- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.15 F_CH_DIO: F-Channel driver for outputs of data type DINT of fail-safe DP standard slaves and fail-safe standard I/O devices

Function

The F-block is used for signal processing of an output value of data type DINT of fail-safe DP standard slaves/fail-safe IO standard devices.

The block cyclically writes the output value of data type DINT for the output of a fail-safe DP standard slave/IO standard device addressed at the VALUE output to the associated F-module driver F_PS_12 that communicates with the fail-safe DP standard slave/IO standard device via a safety message frame according to the PROFIsafe bus profile. The F-module driver is automatically placed and interconnected with the CFC function "Generate module drivers".

A quality code that can have the following states is generated for the output value that is written to the fail-safe DP standard slave/IO standard device:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	To be automatically supplied*
	I	F_DINT	Process value	0
	SIM_I	F_DINT	Simulation value	0
	SIM_MOD	F_BOOL	1=Simulation value takes precedence	0
	SIM_ON	F_BOOL	1=Activate simulation value	0
	PASS_ON	F_BOOL	1=Enable passivation	0
	ACK_NEC	F_BOOL	1=User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1=Enable assignment of I-parameters	0

	Name	Data type	Explanation	Default
Outputs:	PASS_OUT	F_BOOL	1=Passivation due to error	0
	QBAD	F_BOOL	1=Process value invalid	0
	QSIM	F_BOOL	1=Simulation active	0
	VALUE	DINT	Address of the output channel	0
	QUALITY	BYTE	Value status (quality code) of the process value	B#16#0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Addressing

Link the symbol generated with HW Config in the symbol table for the output value of the DINT data type with the VALUE output.

Normal value

The process value active at the I input is written to the fail-safe DP standard slave/IO standard device. The quality code (QUALITY) is set to 16#80.

Simulation

A simulation value can also be written to the fail-safe DP standard slave/IO standard device instead of the process value active at the I input.

If the input SIM_ON = 1 and SIM_MOD = 0, the value of the input SIM_I is written to the fail-safe DP standard slave/IO standard device and output at the VALUE output, if there is no communication error (PROFIsafe), no module or channel error (such as wire break), and no F-startup.

If the input SIM_ON = 1 and SIM_MOD = 1, the value of the input SIM_I is output at the VALUE output even in the event of a communication error (PROFIsafe), a module or channel error (e.g. wire break), or an F-startup, so that an "error-free" operation can be simulated even without fail-safe DP standard slave/IO standard device being present.

In both cases, the quality code (QUALITY) is set to 16#60 and QSIM = 1 is set.

Note

If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/ IO standard device, a simulation value is not written if the PASS_ON input of another F-channel driver for outputs of the fail-safe DP standard slave/IO standard device is 1 and the SIM_ON input is 0.

Fail-safe value

The fail-safe value 0 is written to the fail-safe DP standard slave/IO standard device when any of the following occurs:

- A communication error (PROFIsafe)
- A module fault or a channel fault (such as wire break)
- F-startup
- Passivation with PASS_ON = 1

The quality code (QUALITY) is set to 16#48 and QBAD = 1 is set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Note

For fail-safe DP standard slaves/IO standard devices, channel-specific passivation is not possible for outputs using PASS_ON. If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, the fail-safe value 0 is written for all outputs of the fail-safe DP standard slave/IO standard device following a passivation with PASS_ON = 1 at one of the F-channel drivers. If you want to evaluate the QBAD and QUALITY outputs of the other F-channel drivers when PASS_ON = 1 at one of the F-channel drivers, you must control the PASS_ON inputs of all F-channel drivers synchronously.

Reintegration

After elimination of an error, the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment.

With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the fail-safe DP standard slave/IO standard device starts up using the Slave State (20) "system start" according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

Note

For fail-safe DP standard slaves/IO standard devices, channel-specific reintegration is not possible for outputs using PASS_ON. If you have placed more than one F-channel driver for outputs for a fail-safe DP standard slave/IO standard device, you must synchronously control the ACK_REI inputs of all F-channel drivers for outputs of the fail-safe DP standard slave/IO standard device.

⚠ WARNING

Parameter assignment input ACK_NEC

Assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave/IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe I/O that lasts longer than the F-monitoring time set in HW Config for the fail-safe I/O, the F-system detects a communication error.

FSW-147

Parameter reassignment of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe DP standard slave/IO standard device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe standard DP slave/IO standard device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel drivers belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Startup behavior

After an F-startup, communication must first be established between the F-module driver and the fail-safe DP standard slave/IO standard device. During this time, the fail-safe value 0 is written to the fail-safe DP standard slave/IO standard device. The quality code (QUALITY) is set to 16#48 and outputs QBAD = 1 and PASS_OUT = 1 are set.

Error handling

- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY output and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.6.16 F_CH_RI: F-channel driver for inputs of data type "REAL" of fail-safe DP standard slaves and fail-safe IO standard devices

Function

The F-block is used for signal processing of an input value of data type REAL of fail-safe DP standard slaves and fail-safe IO standard devices.

The F-block cyclically reads the input value addressed at the VALUE input of data type REAL of a fail-safe DP standard slave/IO standard device from the associated F-module driver F_PS_12 that communicates with the fail-safe DP standard slave/IO standard device via a safety message frame according to the PROFIsafe bus profile. The F-module driver is automatically placed and interconnected with the CFC function "Generate module drivers".

If the input value is valid, it is provided at output V as REAL.

A quality code (QUALITY output) that can have the following states is generated for the result value at the V output:

State	Quality code (QUALITY output)
Valid value	16#80
Simulation	16#60
Fail-safe value	16#48
Last valid value	16#44
Invalid value (F-STOP)	16#00

I/Os

	Name	Data type	Explanation	Default
Inputs:	ADR_CODE	DWORD	Coding for VALUE interconnection	To be automatically supplied*
	VALUE	REAL	Address of the analog input channel	0.0
	SIM_V	F_REAL	Simulation value	0.0
	SIM_ON	F_BOOL	1 = Activate simulation value	0
	SUBS_V	F_REAL	Fail-safe value	0.0
	SUBS_ON	F_BOOL	1 = Enable fail-safe value injection	0
	PASS_ON	F_BOOL	1 = Activate passivation	0
	ACK_NEC	F_BOOL	1 = User acknowledgment for reintegration after error required	0
	ACK_REI	F_BOOL	Acknowledgment for reintegration	0
	IPAR_EN	F_BOOL	1 = Enable assignment of I-parameters	0
Outputs:	PASS_OUT	F_BOOL	1 = Passivation due to error	0
	QBAD	F_BOOL	1 = Process value invalid	0
	QSIM	F_BOOL	1 = Simulation active	0
	QSUBS	F_BOOL	1 = Fail-safe value injection active	0
	V	F_REAL	Process value	0.0
	V_DATA	REAL	DATA component of the process value (for visualization)	0.0
	QUALITY	BYTE	Value status (quality code) of the process value	0
	V_MOD	REAL	Value from fail-safe DP standard slave/IO standard device	0.0
	ACK_REQ	BOOL	Acknowledgment for reintegration required	0
	IPAR_OK	F_BOOL	1= New I-parameter values were assigned	0

*) The ADR_CODE input is automatically supplied when the S7 program is compiled and must not be changed. The ADR_CODE input is displayed as changed during the comparison of safety programs if changes were made to the address or the symbol of the signal at the VALUE input.

Note

Forcing the VALUE input

Forcing of the VALUE input is not possible because VALUE is not the value itself but rather a pointer for the address of the digital input channel.

Addressing

Link the symbol generated with HW Config in the symbol table for the input value of the REAL data type with the VALUE input.

Normal value

If the input value received from the fail-safe DP standard slave/IO standard device is valid, it is output at the Q output with quality code (QUALITY) 16#80.

Simulation

A simulation value is output at the V output instead of the normal value that is received from the fail-safe DP standard slave/IO standard device.

When input SIM_ON = 1, the value of the SIM_V input with quality code (QUALITY) 16#60 is output. Simulation has the highest priority. QBAD is always set to "0". QSIM = 1 is set if the block is in simulation state.

When simulation is switched on, the input value received from the fail-safe DP standard slave/IO standard device is output at the V_MOD output. If no communication is possible with the fail-safe DP standard slave/IO standard device or if there is still no user acknowledgment after an error, 0 is output.

When simulation is switched off, V_DATA is output.

Fail-safe value

When input SUBS_ON = 1, the fail-safe value SUBS_V is output at the V output in the following cases:

- The analog input value is invalid due to a communication error (PROFIsafe).
- The analog input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- An F-startup is present.
- FV_ACTIVATED is signaled by the module.

The quality code (QUALITY) is set to 16#48 and QSUBS = 1 and QBAD = 1 are set.

If the output of the fail-safe value is not caused by a passivation, PASS_OUT = 1 is additionally set for passivation of other channels.

Keep last value

When input SUBS_ON = 0, the last valid value of V is output at the V output in the following cases:

- The analog input value is invalid due to a communication error (PROFIsafe).
- The analog input value is invalid due to a module fault or a fail-safe value is received from the module.
- A passivation with PASS_ON = 1 is present.
- FV_ACTIVATED is signaled by the module.

The quality code (QUALITY) is set to 16#44 and QSUBS = 0 and QBAD = 1 are set.

If the output of the last valid value is not caused by a passivation, then output PASS_OUT = 1 is additionally set in order to passivate other channels.

Parameter reassignment of a fail-safe DP standard slave/IO standard device

For parameter reassignment of a fail-safe DP standard slave/IO standard device, the IPAR_EN input and the IPAR_OK output are available.

The IPAR_EN input corresponds to the iPar_EN_C variable and the IPAR_OK output corresponds to the iPar_OK_S variable in the PROFIsafe bus profile as of PROFIsafe Specification V1.30. To find out when you must set/reset the IPAR_EN input following parameter reassignment of a fail-safe DP standard slave/IO standard device and how you can evaluate the IPAR_OK output, refer to the PROFIsafe Specification V1.30 or higher and the documentation for the fail-safe standard DP slave/IO standard device.

If more than one F-channel driver is placed for a fail-safe DP standard slave/IO standard device, iPar_EN_C is formed from an OR logic operation of all IPAR_EN of the F-channel driver belonging to the fail-safe DP standard slave/IO standard device.

If passivation is to be carried out when IPAR_EN = 1, you must additionally set variable PASS_ON = 1.

Reintegration after error elimination

After elimination of an error, the input value received from the fail-safe DP standard slave/IO standard device can be reintegrated automatically or only after user acknowledgment.
With parameter assignment ACK_NEC = 1, a user acknowledgment is required at the ACK_REI input after error elimination. With parameter assignment ACK_NEC = 0, reintegration occurs automatically.

Output ACK_REQ = 1 is used to signal that the error is eliminated and a user acknowledgment at the ACK_REI input is required for reintegration.

No user acknowledgment is required for reintegration after PASS_ON = 1. For reintegration after an F-startup following a CPU STOP, no user acknowledgment is required if the fail-safe DP standard slave/IO standard device starts up using the Slave State (20) "system start" according to the PROFIsafe Specification V1.30 and higher. Otherwise, a communication error (PROFIsafe) is detected.

⚠ WARNING

Parameter assignment input ACK_NEC

Parameter assignment of input ACK_NEC = 0 is only allowed if an automatic reintegration is permissible under safety aspects for the process.

Communication errors (PROFIsafe) must always be acknowledged at the ACK_REI input independent of ACK_NEC. For this purpose, you must interconnect the ACK_REI input with a signal generated by an operator input. An interconnection with an automatically generated signal is not permissible.

FSW-146

⚠ WARNING

Startup protection for short-term power failure of the fail-safe DP standard slave/IO standard device

After power failure of the fail-safe DP standard slave/IO standard device, which is shorter than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device (see chapter "Run times, F-Monitoring times, and response times (Page 482)"), automatic reintegration may occur independent of your parameterization of the ACK_NEC input, as described in the parameterization of ACK_NEC = 0.

If automatic reintegration is not permitted for the process involved, you must program a startup protection for this situation by evaluating the QBAD or PASS_OUT outputs.

In the event of a power failure of the fail-safe DP standard slave/IO standard device that lasts longer than the F-monitoring time set in HW Config for the fail-safe DP standard slave/IO standard device, the F-system detects a communication error.

FSW-147

Startup behavior

After an F-startup, the communication between the F-module driver and the fail-safe DP standard slave/IO standard device must first be established. During this time, the fail-safe value SUBS_V with quality code (QUALITY output) 16#48 is output irrespective of the parameter assignment at the SUBS_ON input and outputs QSUBS = 1, QBAD = 1 and PASS_OUT = 1 are additionally set.

Error handling

An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

Response to F-STOP

Following an F-STOP, 16#00 is output at the QUALITY and STATUS outputs and QBAD.DATA = 1 is set. All other variables are frozen.

A.2.7 F-System blocks

Overview

Block name	Block number	Description
F_S_BO	FB 390	Sending of 10 data elements of data type F_BOOL in a fail-safe manner to another F-Shutdown group
F_R_BO	FB 391	Receiving of 10 data elements of data type F_BOOL in a fail-safe manner from another F-Shutdown group
F_S_R	FB 392	Sending of 5 data elements of data type F_REAL in a fail-safe manner to another F-Shutdown group
F_R_R	FB 393	Receiving of 5 data elements of data type F_REAL in a fail-safe manner from another F-Shutdown group
F_START	FB 394	F-Start detection
F_PSG_M	FB 471	Marker block for F-Shutdown groups

Integration in F Block types

With the exception of F_START, the F-System blocks must not be integrated in F-Block types.

A.2.7.1 F_S_BO: Sending of 10 data elements of data type F_BOOL in a fail-safe manner to another F-Shutdown group.

Function

The F-block sends the data of the data type F_BOOL, that is present at the SD_BO_xx inputs, with to another F-shutdown group in a fail-safe operation. The data must be received there with the F-block F_R_BO.

You must interconnect output S_DB with the input of the corresponding F_R_BO that has the same name.

Note

Initialization

You must not initialize the S_DB output with values <> 0.

I/Os

	Name	Data type	Explanation	Default
Inputs:	SD_BO_00	F_BOOL	Send data 00	0
	…		…	
	SD_BO_09	F_BOOL	Send data 09	0

	Name	Data type	Explanation	Default
Output:	S_DB	F_WORD	Connection to F_R_BO	0

Error handling

None

A.2.7.2 F_R_BO: Receiving of 10 data elements of data type F_BOOL in a fail-safe manner from another F-Shutdown group

Function

In a fail-safe operation, the F-block receives 10 data elements of the F_BOOL data type from another F-switch-off group, and provides them to RD_BO_xx outputs. The data must be sent from the other F-shutdown group with the F-block F_S_BO. Interconnect the data received at the RD_BO_xx outputs with other F-blocks for further processing.

You must interconnect the S_DB input with the output of the corresponding F_R_BO that has the same name.

You must assign the desired F-monitoring time at the TIMEOUT input. For information regarding the calculation of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

I/Os

	Name	Data type	Explanation	Default
Inputs:	TIMEOUT	F_TIME	F-monitoring time in ms for lifebeat monitoring	T# 0ms
	S_DB	F_WORD	Connection to F_S_BO	0
	SUBBO_00	F_BOOL	Substitute value for receive data 00	0
	…		…	
	SUBBO_09	F_BOOL	Substitute value for receive data 09	0
Outputs:	SUBS_ON	F_BOOL	1 = Substitute values are output	0
	RD_BO_00	F_BOOL	Receive data 00	0
	…		…	
	RD_BO_09	F_BOOL	Receive data 09	0

Substitute values

In the following cases, the substitute values configured at the SUBBO_xx inputs are output at the RD_BO_xx outputs:

- The associated F_S_BO does not receive updated data within the F-monitoring time configured at the TIMEOUT input, for example, because there is a partial shutdown for the F-shutdown group with the associated F_S_BO.
- An F-startup is present.

The SUBS_ON output is set to 1.

Startup behavior

After an F-startup, the data exchange with the associated F_S_BO must first be established. During this time, the substitute values configured at the SUBBO_xx inputs are output at the RD_BO_xx outputs, and the SUBS_ON output is set to 1.

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostic buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.7.3 F_S_R: Sending of 5 data elements of data type F_REAL in a fail-safe manner to another F-Shutdown group

Function

In a fail-safe operation, this F-block sends the data of the data type F_REAL, which is present at the SD_R_xx inputs, to another F-shutdown group. The data must be received there with the F-block F_R_R.

You must interconnect the S_DB output with the input of the corresponding F_R_R that has the same name.

Note

Initialization

You must not initialize the S_DB output with values <> 0.

I/Os

	Name	Data type	Explanation	Default
Inputs:	SD_R_00	F_REAL	Send data 00	0.0
	…		…	
	SD_R_04	F_REAL	Send data 04	0.0

	Name	Data type	Explanation	Default
Output:	S_DB	F_WORD	Connection to F_R_R	0

Error handling

None

A.2.7.4 F_R_R: Receiving of 5 data elements of data type F_REAL in a fail-safe manner from another F-Shutdown group.

Function

In a fail-safe operation, this F-block receives 5 data elements of data type F_REAL from another F-switch-off group, and provides them to RD_BO_xx outputs. The data must be sent by the other F-shutdown group with the F-block F_S_R.

You must interconnect the S_DB input with the output of the corresponding F_S_R that has the same name.

You must assign the desired F-monitoring time at the TIMEOUT input. For information regarding the calculation of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

I/Os

	Name	Data type	Explanation	Default
Inputs:	TIMEOUT	F_TIME	F-monitoring time in ms for live monitoring	T# 0ms
	S_DB	F_WORD	Connection to F_S_R	0
	SUBR_00	F_REAL	Substitute value for receive data 00	0.0
	…		…	
	SUBR_04	F_REAL	Substitute value for receive data 04	0.0
Outputs:	SUBS_ON	F_BOOL	1 = Substitute values are output	0
	RD_R_00	F_REAL	Receive data 00	0.0
	…		…	
	RD_R_04	F_REAL	Receive data 04	0.0

Substitute values

In the following cases, the substitute values configured at the SUBR_xx inputs are output at the RD_R_xx outputs:

- The associated F_S_R does not receive updated data within the F-monitoring time configured at the TIMEOUT input, for example, because there is a partial shutdown for the F-shutdown group with the associated F_S_R.
- An F-startup is present.

The SUBS_ON output is set to 1.

Startup behavior

After an F-startup, the data exchange with the associated F_S_R must first be established. During this time, the substitute values configured at the SUBR_xx inputs are output at the RD_R_xx outputs, and the SUBS_ON output is set to 1.

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostic buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.7.5 F_START: F-Startup identifier

Function

In the first cycle after an F-Startup or a initial run, the F-Block signals with 1 at output COLDSTRT that an F-Startup was executed. COLDSTRT remains present until the next call of F_START.

The F_START must be called before the evaluating F-Blocks.

Inputs/outputs

	Name	Data type	Description	Default
Output:	COLDSTRT	F_BOOL	F-Startup identifier	1

Error handling

None

A.2.7.6 F_PSG_M: Marker block for F-Shutdown groups

Function

With the F_PSG_M block you have the possibility to split an F-Shutdown group into two F-Shutdown groups.

In the sequence editor of the CFC editor, place the block F_PSG_M in the last F-Runtime group, which should belong to the first F-Shutdown group. Any following F-Runtime groups then form the second F-Shutdown group. The F_PSG_M block is not an F-Block. However, you are still permitted to place it in F-Runtime groups.

Inputs/outputs:

None

Error handling:

None

See also

F-Shutdown groups (Page 90)

A.2.8 Flip-flop blocks

Overview

Block name	Block number	Description
F_RS_FF	FB 307	RS Flip-Flop, resetting dominant
F_SR_FF	FB 308	SR Flip-Flop, setting dominant

A.2.8.1 F_RS_FF: RS Flip-Flop, resetting dominant

Function

This F-Block executes the function of an RS Flip-Flops (resetting dominant). The output Q is set when input R = 0 and input S = 1. The output Q is reset when input R = 1 and input S = 0. Output Q is reset if 1 is at both inputs. The QN output corresponds to the negated Q output.

Truth table

R	S	Qn	QNn
0	0	Qn-1	QNn-1
0	1	1	0
1	0	0	1
1	1	0	1

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	R	F_BOOL	Reset	0
	S	F_BOOL	Set	0
Outputs:	Q	F_BOOL	Output	0
	QN	F_BOOL	Negated output	1

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.8.2 F_SR_FF: SR Flip-Flop, setting dominant

Function

The F-Block executes the function of an *SR Flip-Flop* (setting dominant). The output Q is set when input R = 0 and input S = 1. The output Q is reset when input R = 1 and input S = 0. Output Q is set if 1 is at both inputs. The QN output corresponds to the negated Q output.

Truth table

R	S	Qn	QNn
0	0	Qn-1	QNn-1
0	1	1	0
1	0	0	1
1	1	1	0

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	R	F_BOOL	Reset	0
	S	F_BOOL	Set	0
Outputs:	Q	F_BOOL	Output	0
	QN	F_BOOL	Negated output	1

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID16#75DA).

A.2.9 IEC pulse and counter blocks

Overview

Block name	Block number	Description
F_CTUD	FB 341	Up and down counter
F_TP	FB 342	Timer pulse
F_TON	FB 343	Timer switch-on delay
F_TOF	FB 344	Timer switch-off delay

A.2.9.1 F_CTUD: Up and down counter

Function

This F-Block is an edge-controlled up/down counter.

The CV count value responds to rising edges of the CU and CD inputs as well as to the level of the LOAD and R inputs:

- Rising edge at CU: CV is increased by 1.
  When the counter value reaches the upper limit (32.767), it no longer counts up.
- Rising edge at CD: CV is decreased by 1.
  When the counter value reaches the lower limit (-32.768), it no longer counts down.
- LOAD = 1: CV is preset with the value of the PV input.
  The values at inputs CU and CD are ignored.
- R = 1: CV is reset to 0.
  The values at inputs CU, CD, and LOAD are ignored.

If a rising edge is available at both the CU input and the CD input during a cycle, the counter keeps its current value.

The QU output is set if the count value is greater than or equal to the preset value PV. The QD output is set if the count value is less than or equal to zero.

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	CU	F_BOOL	COUNT UP	0
	CD	F_BOOL	COUNT DOWN	0
	R	F_BOOL	RESET	0
	LOAD	F_BOOL	LOAD PV	0
	PV	F_INT	PRESET VALUE	0
Outputs:	QU	F_BOOL	COUNTER UP QU has the value • 1: If CV ≥ PV • 0: If CV < PV	0
	QD	F_BOOL	COUNTER DOWN QD has the value • 1: If CV ≤ 0 • 0: If CV > 0	0
	CV	F_INT	COUNTER VALUE	0

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.9.2 F_TP: Timer pulse

Function

The F-block generates a pulse with the duration PT at the Q output.

A positive edge at the IN input starts the pulse. Output Q remains set for the time PT, regardless of the subsequent course of the input signal (in other words even if input IN changes again from 0 to 1 before the time PT has elapsed).

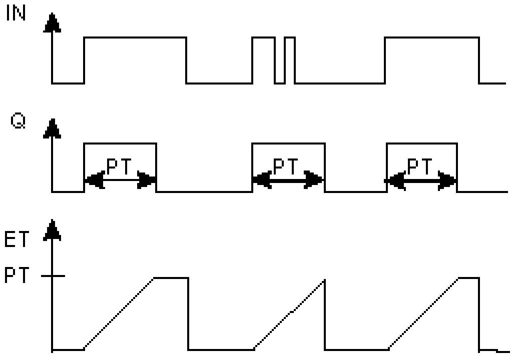
The output ET indicates for how long the output Q has already been set. The maximum value of the ET output is the value of the PT input. ET output is reset when input IN changes to 0, however, not before the time PT has expired.

If PT < 0, the outputs Q and ET are reset.

I/Os

	Name	Data type	Explanation	Default
Inputs:	IN	F_BOOL	Start input	0
	PT	F_TIME	Duration of the pulse	T# 0ms
Outputs:	Q	F_BOOL	Output	0
	ET	F_TIME	Elapsed time	T# 0ms

Time diagram



User times

WARNING

Fail-safe user times

When determining your response times when using an F-block with time monitoring, take into account the following timing uncertainties:

- The timing uncertainty familiar from the standard program that arises due to the cyclic processing
- The tolerance of the internal monitoring of the times in the F-CPU
  - For time values from 10 ms to 50 s: 5 ms
  - For time values from > n × 50 s to (n+1) × 50 s: ± (n+1) × 5 ms

FSW-170

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostic buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.9.3 F_TON: Timer switch-on delay

Function

The F-block delays a positive edge by the time PT.

A positive edge at the IN input causes a positive edge at output Q after the time PT has expired. Q then remains set until the IN input changes to 0 again.

If the IN input changes again to 0 before time PT has elapsed, output Q remains set to 0.

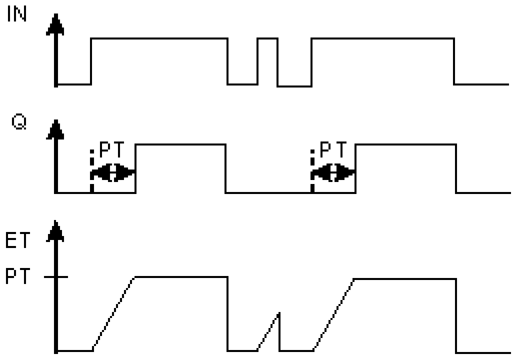
The ET output supplies the time that has elapsed since the last positive edge at the IN input. Its maximum value is the value of the PT input. ET is reset when the IN input changes to 0.

If PT < 0, the outputs Q and ET are reset.

I/Os

	Name	Data type	Explanation	Default
Inputs:	IN	F_BOOL	Start input	0
	PT	F_TIME	Duration of the delay	T# 0ms
Outputs:	Q	F_BOOL	Output	0
	ET	F_TIME	Elapsed time	T# 0ms

Time diagram



User times

⚠ WARNING

Fail-safe user times

When determining your response times when using an F-block with time monitoring, take into account the following timing uncertainties:

- The timing uncertainty familiar from the standard program that arises due to the cyclic processing
- The tolerance of the internal monitoring of the times in the F-CPU
  - For time values from 10 ms to 50 s: 5 ms
  - For time values from > n × 50 s to (n+1) × 50 s: ± (n+1) × 5 ms

FSW-170

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostic buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.9.4 F_TOF: Timer switch-off delay

Function

The F-block delays a negative edge by the time PT.

A positive edge on input IN causes a positive edge on output Q. A negative edge on input IN causes a negative edge on output Q after the time PT has elapsed.

If the IN input changes again to 1 before time PT has expired, output Q remains set to 1.

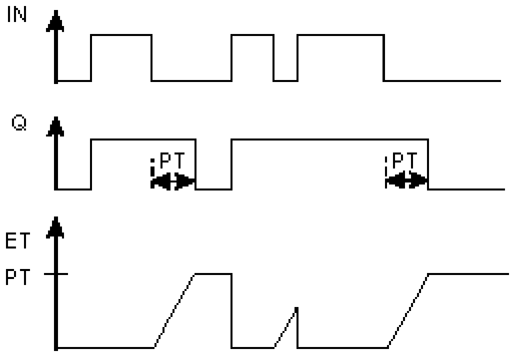
The output ET supplies the time that has elapsed since the last negative edge on input IN, however its maximum value is the value of the PT input. ET is reset when the IN input changes to 1.

If PT < 0, the ET output is reset and the Q output corresponds to the IN input.

I/Os

	Name	Data type	Explanation	Default
Inputs:	IN	F_BOOL	Start input	0
	PT	F_TIME	Duration of the delay	T# 0ms
Outputs:	Q	F_BOOL	Output	0
	ET	F_TIME	Elapsed time	T# 0ms

Time diagram



User times

WARNING

Fail-safe user times

When determining your response times when using an F-block with time monitoring, take into account the following timing uncertainties:

- The timing uncertainty familiar from the standard program that arises due to the cyclic processing
- The tolerance of the internal monitoring of the times in the F-CPU
  - For time values from 10 ms to 50 s: 5 ms
  - For time values from > n × 50 s to (n+1) × 50 s: ± (n+1) × 5 ms

FSW-170

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.10 Pulse blocks

Overview

Block name	Block number	Description
F_REPCYC	FB 309	Clock
F_ROT	FB 310	Timer with on delay and hold function
F_LIM_TI	FB 345	Asymmetrical limiter of a TIME value

Block name	Block number	Description
F_R_TRIG	FB 346	Detection of a rising edge
F_F_TRIG	FB 347	Detection of a falling edge

A.2.10.1 F_REPCYC: Clock

Function

The F-block implements a clock generator with adjustable cycle duration, pulse duration, and interpulse period.

A positive edge at the IN input starts the clock generator. Depending on the setting at the START input, the clock generator at output Q starts with 0 or 1:

- At input START = 0, the clock generator at output Q initially outputs 0 for the interpulse period, then for the interpulse period 1.
- At input START = 1, the clock generator at output Q initially outputs 1 for the interpulse period, then for the interpulse period 0.

The cycle is repeated until IN changes to 0. Then Q = 0 is set.

The output ET always returns the time that has elapsed since the start of a new cycle. The output RT returns the time remaining until the end of the cycle. ET is reset at the end of a cycle or with IN = 0. RT is reset to the cycle duration at the end of a cycle or with IN = 0.

Cycle duration, pulse duration, and interpulse period depend on the settings on the OFFTIME, ONTIME, and PCTON inputs (with 0 ≤ PCTON ≤ 100). OFFTIME, ONTIME, and PCTON must be specified such that the cycle duration does not exceed the maximum value of the TIME data type.

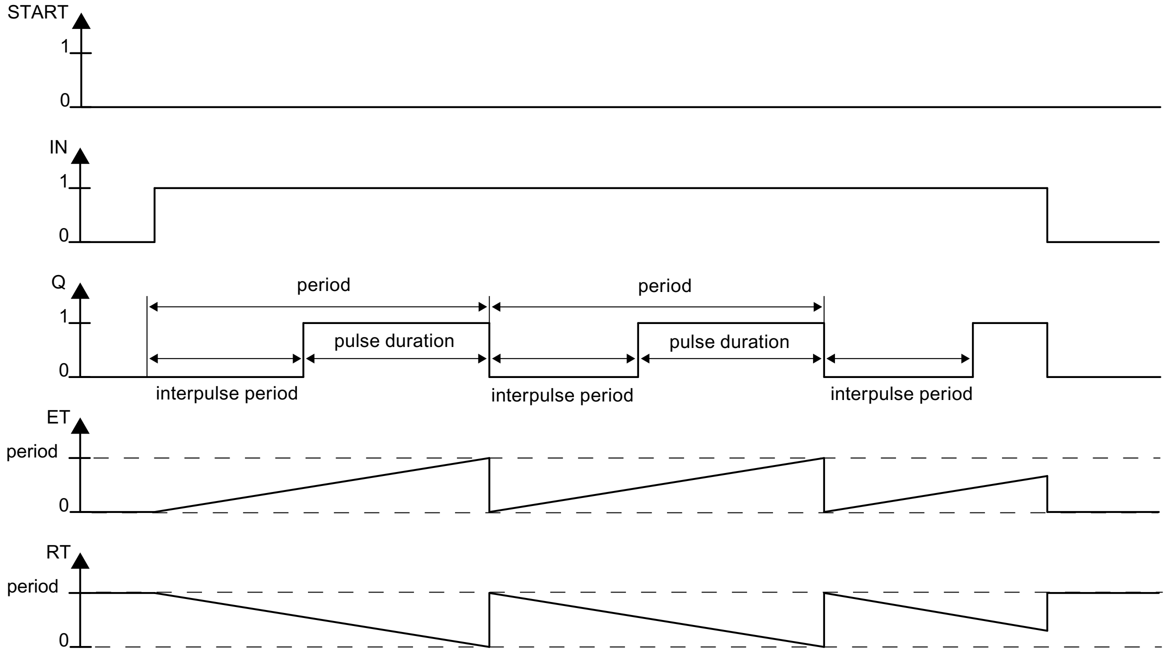
- For OFFTIME > 0 ms the following applies:
  Interpulse period = OFFTIME
  Pulse duration = PCTON × ONTIME
  Cycle duration = OFFTIME + (PCTON × ONTIME)
- For OFFTIME = 0 ms, the following applies:
  Interpulse period = ONTIME - (PCTON × ONTIME)
  Pulse duration = PCTON × ONTIME
  Cycle duration = ONTIME

While the input IN = 1, the time values at the inputs ONTIME and OFFTIME must not be changed.

I/Os

	Name	Data type	Explanation	Default
Inputs:	IN	F_BOOL	Start input	0
	PCTON	F_REAL	Percent value for pulse duration	0
	START	F_BOOL	0 = Cycle start with Q = 0 1 = Cycle start with Q = 1	1
	OFFTIME	F_TIME	Parameters for interpulse interval	0 ms
	ONTIME	F_TIME	Parameters for pulse duration	0 ms
Outputs:	Q	F_BOOL	Output	0
	ET	F_TIME	Elapsed time	0 ms
	RT	F_TIME	Remaining time	0 ms

Time diagram



User times

WARNING

Fail-safe user times

When determining your response times when using an F-block with time monitoring, take into account the following timing uncertainties:

- The timing uncertainty familiar from the standard program that arises due to the cyclic processing
- The tolerance of the internal monitoring of the times in the F-CPU
  - For time values from 10 ms to 50 s: 5 ms
  - For time values from > n × 50 s to (n+1) × 50 s: ± (n+1) × 5 ms

FSW-170

Error handling

- If the PCTON input is an invalid floating-point number (NaN) or if there is a negative time at the ONTIME or OFFTIME inputs, the clock generator switches off (it behaves as with IN = 0). If there is no invalid floating-point number (NaN) or no negative time left and IN = 1, the clock generator restarts (it behaves as with positive edge at input IN).
- With PCTON < 0.0, ET and RT are formed as with PCTON = 0, and Q is set to 0. With PCTON > 100.0, ET and RT are formed as with PCTON = 100, and Q is set to 1.
- If the cycle duration exceeds the maximum value of the TIME data type, the behavior of the F-block is not specified.
- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.10.2 F_ROT: Timer with on delay and hold function

Function

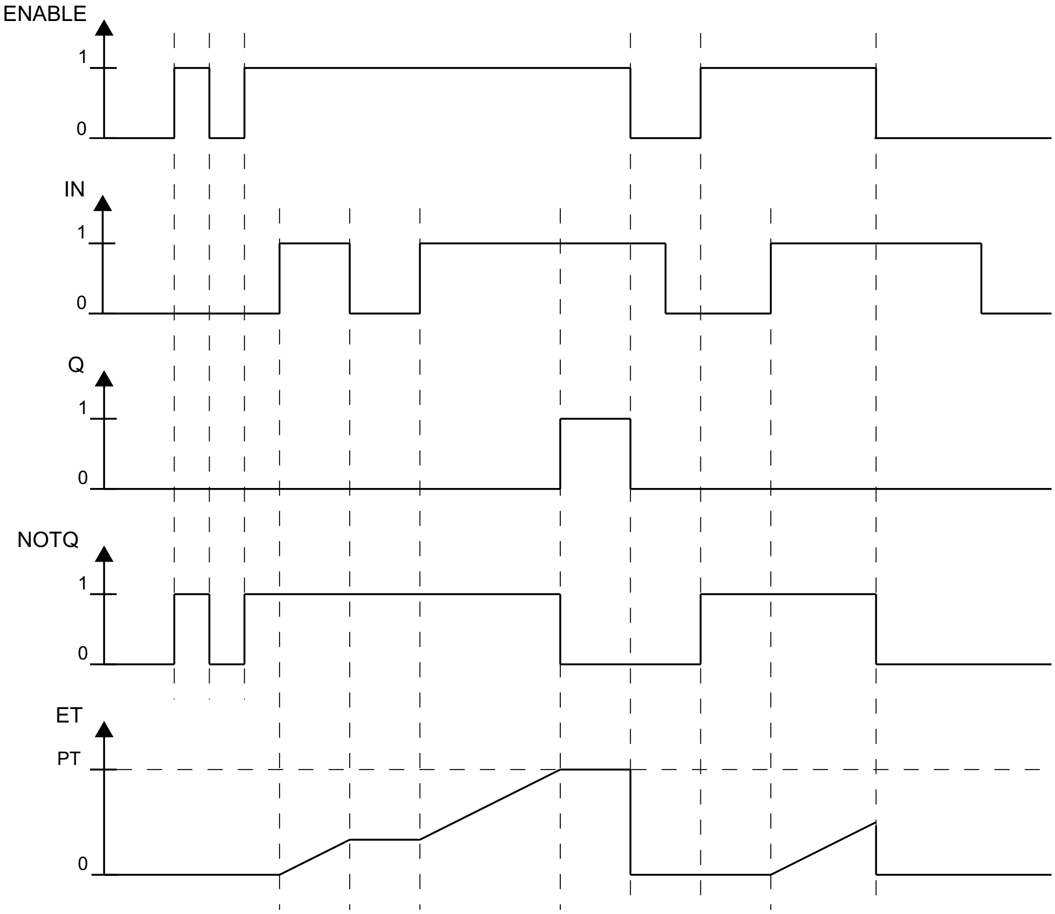
The F-block implements a timer with switch-on delay and hold function.

- The timer is enabled with ENABLE = 1 input. If the input IN = 1, the time at the output ET is incremented, at most up to the value of the input PT. If IN changes to 0, the time is stopped. Q is set to 1 as soon as ET = PT. NOTQ corresponds to the negated Q.
- The timer is reset with ENABLE = 0 input. The ET output is set to 0 ms, and Q and NOTQ are set to 0.

I/Os

	Name	Data type	Explanation	Default
Inputs:	ENABLE	F_BOOL	1=Timer released	0
	IN	F_BOOL	Start input	0
	PT	F_TIME	Duration	0 ms
Outputs:	Q	F_BOOL	Output	0
	NOTQ	F_BOOL	Output inverted (if ENABLE = 1)	0
	ET	F_TIME	Elapsed time	0 ms

Time diagram



User times

⚠ **WARNING**

Fail-safe user times

When determining your response times when using an F-block with time monitoring, take into account the following timing uncertainties:

- The timing uncertainty familiar from the standard program that arises due to the cyclic processing
- The tolerance of the internal monitoring of the times in the F-CPU
  - For time values from 10 ms to 50 s: 5 ms
  - For time values from > n × 50 s to (n+1) × 50 s: ± (n+1) × 5 ms

FSW-170

Error handling

- If there is a negative time at input PT, the timer is stopped (behavior as with IN = 0). If there is no negative time left and IN = 1, the timer continues to run.
- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.10.3 F_LIM_TI: Asymmetrical limiter of a TIME value

Function

This F-Block checks whether input IN is within or outside the interval between MIN and MAX. If input IN lies within the interval, it is passed through to output OUT. If it lies outside of the interval it is limited to MIN or MAX.

- Is IN > MAX, then an upper limit violation exists. MAX is output to output OUT. OUTU is set to 1 and OUTL to 0.
- If IN < MIN, then a lower limit violation exists. MIN is output to output OUT. OUT is set to 0 and OUTL to 1.
- If input IN lies between MIN and MAX, IN is passed through to output OUT. OUTU and OUTL are always set to 0.

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	IN	F_TIME	INPUT	T# 0ms
	MIN	F_TIME	MINIMUM	T# 0ms
	MAX	F_TIME	MAXIMUM	T# 24d 20h 31m 23s 647ms

	Name	Data type	Description	Default
Outputs:	OUT	F_TIME	Output	T# 0ms
	OUTU	F_BOOL	UPPER LIMIT	0
	OUTL	F_BOOL	LOWER LIMIT	0

Error handling

- Is MIN ≥ MAX, MAX is output at output OUT. OUTU and OUTL are always set to 1.
- An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.10.4 F_R_TRIG: Detection of a rising edge

Function

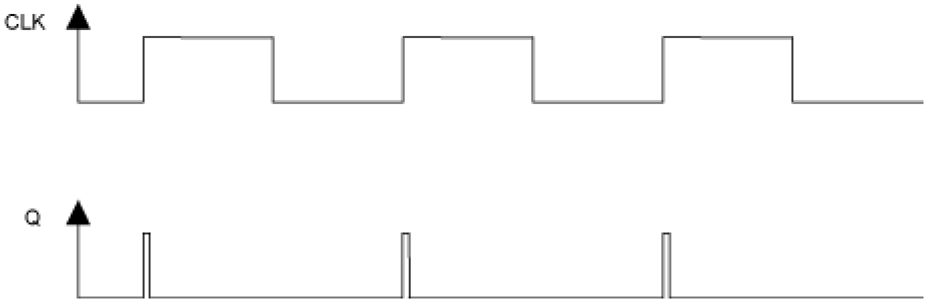
The F-Block checks input CLK for the occurrence of a rising edge.

At a rising edge of input CLK, output Q is set to 1 until the next call of the block.

Inputs/outputs

	Name	Data type	Description	Default
Input:	CLK	F_BOOL	Input	0
Output:	Q	F_BOOL	Output	0

Timing diagram



Startup characteristics

If input CLK has a value of 1 during the first cycle after a F-Startup or an initial run 1, no edge is detected and output Q is set to 0 until the next rising edge on output CLK.

Error handling

None

A.2.10.5 F_F_TRIG: Detection of a falling edge

Function

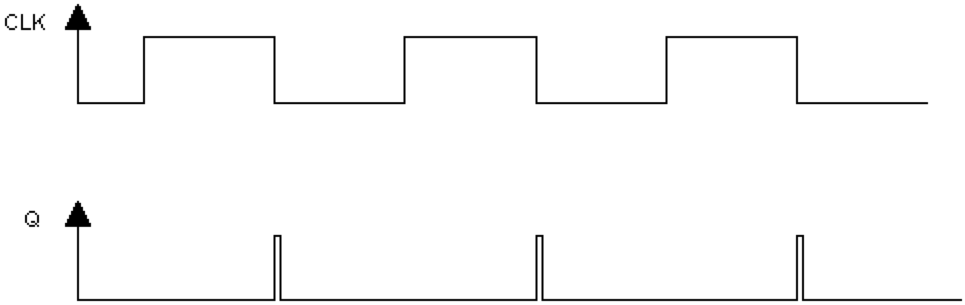
This F-Block checks input CLK for the occurrence of a falling edge.

At a falling edge of input CLK, output Q is set to 1 until the next call of the block.

Inputs/outputs

	Name	Data type	Description	Default
Input:	CLK	F_BOOL	Input	0
Output:	Q	F_BOOL	Output	0

Timing diagram



Startup characteristics

During the first cycle after a F-Start or initial run, no edge is detected.

Error handling

None

A.2.11 Arithmetic blocks with the REAL data type

Overview

Block name	Block number	Description
F_ADD_R	FB 321	Addition of two REAL values
F_SUB_R	FB 322	Subtraction of two REAL values
F_MUL_R	FB 323	Multiplication of two REAL values
F_DIV_R	FB 324	Division of two REAL values
F_ABS_R	FB 325	Absolute value of a REAL value
F_MAX3_R	FB 326	Maximum of three REAL values
F_MID3_R	FB 327	Mean value of three REAL values
F_MIN3_R	FB 328	Minimum of three REAL values
F_LIM_R	FB 329	Asymmetrical limiter of a REAL value
F_SQRT	FB 330	Square root of a REAL value
F_AVEX_R	FB 331	Mean value of a maximum of nine REAL values
F_SMP_AV	FB 333	Sliding mean value of maximum 33 REAL values
F_2oo3_R	FB 456	Median value of three REAL values with 2oo3 evaluation
F_1oo2_R	FB 457	1oo2 evaluation of inputs of data type REAL

A.2.11.1 F_ADD_R: Addition of two REAL values

Function

This F-Block adds the inputs IN1 and IN2 and outputs the sum at output OUT.

OUT = IN1 + IN2

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_REAL	Input 1	0.0
	IN2	F_REAL	Input 2	0.0
Output:	OUT	F_REAL	Output	0.0

Error handling

If an invalid floating-point number (NaN) has been created due to the calculation at output OUT, the following diagnostic event is entered in the diagnostic buffer of the F-CPU:

- "Safety program: invalid REAL number in DB" (Event ID 16#75D9)

A.2.11.2 F_SUB_R: Subtraction of two REAL values

Function

This F-Block subtracts the IN2 input from the IN1 input and outputs the difference at the output OUT.

OUT = IN1 - IN2

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_REAL	Input 1	0.0
	IN2	F_REAL	Input 2	0.0
Output:	OUT	F_REAL	Output	0.0

Error handling

If an invalid floating-point number (NaN) has been created due to the calculation at output OUT, the following diagnostic event is entered in the diagnostic buffer of the F-CPU:

- "Safety program: invalid REAL number in DB" (Event ID 16#75D9)

A.2.11.3 F_MUL_R: Multiplication of two REAL values

Function

This F-Block multiplies the inputs IN1 and IN2 and outputs the product at output OUT.

OUT = IN1 × IN2

Inputs/Outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_REAL	Input 1	0.0
	IN2	F_REAL	Input 2	0.0
Output:	OUT	F_REAL	Output	0.0

Error handling

If an invalid floating-point number (NaN) has been created due to the calculation at output OUT, the following diagnostic event is entered in the diagnostic buffer of the F-CPU:

- "Safety program: invalid REAL number in DB" (Event ID 16#75D9)

A.2.11.4 F_DIV_R: Division of two REAL values

Function

This F-Block divides the IN1 input by the IN2 input and outputs the quotient at output OUT.

OUT = IN1 / IN2

Inputs/Outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_REAL	Input 1	0.0
	IN2	F_REAL	Input 2	1.0
Output:	OUT	F_REAL	Output	0.0

Error handling

If an invalid floating-point number (NaN) has been created due to the calculation at output OUT, the following diagnostic event is entered in the diagnostic buffer of the F-CPU:

- "Safety program: invalid REAL number in DB" (Event ID 16#75D9)

See also

Behavior of F-Blocks with floating-point operations in the event of a number range overflow (Page 246)

A.2.11.5 F_ABS_R: Absolute value of a REAL value

Function

This F-Block outputs the absolute value (amount) of input IN at the output OUT.

OUT = | IN |

Inputs/Outputs

	Name	Data type	Description	Default
Input:	IN	F_REAL	Input	0.0
Output:	OUT	F_REAL	Output	0.0

Error handling

None

A.2.11.6 F_MAX3_R: Maximum of three REAL values

Function

This F-Block compares the inputs IN1, IN2 and IN3 and outputs its maximum at output OUT. All the inputs are preset with a value of -3,402823e+38 (largest negative REAL number), so that even a maximum value can be formed from only two inputs.

OUT = MAX {IN1, IN2 , IN3}

Inputs/Outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_REAL	Input 1	-3.402823e+38
	IN2	F_REAL	Input 2	-3.402823e+38
	IN3	F_REAL	Input 3	-3.402823e+38
Output:	OUT	F_REAL	Output	-3.402823e+38

Error handling

- If one of the inputs IN1, IN2 and IN3 is an invalid floating-point number (NaN), an invalid floating-point number (NaN) is output at output OUT.
- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.11.7 F_MID3_R: Mean value of three REAL values

Function

This F-block compares inputs IN1, IN2 and IN3 and outputs the median at the OUT output.

- OUT = Median {IN1, IN2, IN3}

I/Os

	Name	Data type	Explanation	Default
Inputs:	IN1	F_REAL	Input 1	0.0
	IN2	F_REAL	Input 2	0.0
	IN3	F_REAL	Input 3	0.0
Output:	OUT	F_REAL	Output	0.0

Error handling

- If one of the inputs IN1, IN2 and IN3 is an invalid floating-point number (NaN), an invalid floating-point number (NaN) is output at the OUT output.
- An F_STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.11.8 F_MIN3_R: Minimum of three REAL values

Function

This F-Block compares the inputs IN1, IN2 and IN3 and outputs its minimum at output OUT. All the inputs are preset with a value of 3,402823e+38 (largest positive REAL number), so that even a minimum value can be formed from only two inputs.

OUT = MIN {IN1, IN2, IN3}

Inputs/Outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_REAL	Input 1	3.402823e+38
	IN2	F_REAL	Input 2	3.402823e+38
	IN3	F_REAL	Input 3	3.402823e+38
Output:	OUT	F_REAL	Output	3.402823e+38

Error handling

- If one of the inputs IN1, IN2 and IN3 is an invalid floating-point number (NaN), an invalid floating-point number (NaN) is output at output OUT.
- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.11.9 F_LIM_R: Asymmetrical limiter of a REAL value

Function

This F-Block checks whether input IN is within or outside the interval between MIN and MAX. If input IN lies within the interval, it is passed through to output OUT. If it lies outside of the interval it is limited to MIN or MAX.

With the F-Block you can also check the result of a floating-point operation for overflow (± infinity) and invalid floating-point number (NaN).

- Is IN > MAX or "+ infinity", then an upper limit violation exists. MAX is output at output OUT. OUTU is set to 1 and OUTL to 0.
- Is IN < MIN or "- infinity", then a lower limit violation exists. MIN is output to output OUT. OUT is set to 0 and OUTL on 1.
- If IN lies between MIN and MAX, input IN is passed through to output OUT. OUTU and OUTL are always set to 0.
- If IN is an invalid floating-point number (NaN), the fail-safe value SUBS_INis is output at output OUT. OUTU and OUTL are always set to 1.

Inputs/Outputs

	Name	Data type	Description	Default
Inputs:	IN	F_REAL	INPUT	0.0
	MIN	F_REAL	LOWER LIMIT	-100.0
	MAX	F_REAL	UPPER LIMIT	100.0
	SUBS_IN	F_REAL	SUBSTITUTE VALUE	0.0
Outputs:	OUT	F_REAL	OUTPUT	0.0
	OUTU	F_BOOL	UPPER LIMIT VIOLATION	0
	OUTL	F_BOOL	LOWER LIMIT VIOLATION	0

Error handling

- Is MIN ≥ MAX, MAX is output at output OUT. OUTU and OUTL are always set to 1.
- If one of the inputs IN, MIN, MAX or SUBS_IN is an invalid floating-point number (NaN) the fail-safe value SUBS_IN is output at output OUT. OUTU and OUTL are always set to 1.
- An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  – "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.11.10 F_SQRT: Square root of a REAL value

Function

This F-Block calculates the square root of the input IN and then outputs it at the output OUT.

OUT = √(IN)

The IN input must be positive.

Inputs/outputs

	Name	Data type	Description	Default
Input:	IN	F_REAL	Input	0.0
Output:	OUT	F_REAL	Output	0.0

Error handling

- If the calculation at output OUT yields an invalid floating-point number (NaN) or a negative value is pending at IN, NaN is output to OUT and the following diagnostic event is entered in the diagnostic buffer of the F-CPU:
  - "Safety program: invalid REAL number in DB" (Event ID 16#75D9)
- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.11.11 F_AVEX_R: Mean value of a maximum of nine REAL values

Function

This F-Block calculates the mean value from the inputs INx and outputs the result at output OUT.

OUT = (IN1 + IN2 + ... + IN8 + IN9) / 9

Inputs without a set validity bit VALIDINx are not included in the mean value calculation. If at least MIN inputs are valid, output VALIDOUT = 1 is set. If less than MIN inputs are valid, output VALIDOUT = 0 is set.

Inputs/Outputs

	Name	Data type	Description	Default
Inputs:	IN1	F_REAL	INPUT 1	0.0
	...		...	
	IN9	F_REAL	INPUT 9	0.0
	VALIDIN1	F_BOOL	INPUT 1 VALID	1
	...		...	
	VALIDIN9	F_BOOL	INPUT 9 VALID	1
	MIN	F_INT	MINIMUM NUMBER OF VALID INPUTS	9
Outputs:	OUT	F_REAL	OUTPUT	0.0
	VALIDOUT	F_BOOL	OUTPUT VALID	1

Error handling

- If an invalid floating-point number (NaN) has been created due to the calculation at output OUT, the following diagnostic event is entered in the diagnostic buffer of the F-CPU:
  - "Safety program: invalid REAL number in DB" (Event ID 16#75D9)
- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.11.12 F_SMP_AV: Sliding mean value of maximum 33 REAL values

Function

This F-Block outputs the mean value of the last N input values IN at output OUT.

$OUT = (IN_k + IN_{k-1} + \ldots + IN_{k-N+1}) / N$

IN_k is the current input value.

The number N of input values must fulfill the condition 0 < N < 33.

Inputs/Outputs

	Name	Data type	Description	Default
Inputs:	IN	F_REAL	Input	0.0
	N	F_INT	NUMBER OF INPUTS MONITORED	1
Output:	OUT	F_REAL	OUTPUT	0.0

Startup characteristics

As long as N input values have not been read in after an F-Start or after an initial run, only the available input values (< N) are taken into account for averaging. Input values saved before the start are not taken into account.

Error handling

- If the condition 0 < N < 33 is not fulfilled, the current existing value at input IN is output at output OUT.
- If an invalid floating-point number (NaN) has been created due to the calculation at output OUT, the following diagnostic event is entered in the diagnostic buffer of the CPU:
  - "Safety program: invalid REAL number in DB" (Event ID 16#75D9)
- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.11.13 F_2oo3_R: Middle value of three REAL values with 2oo3 evaluation

Function

This F-block compares the three inputs IN1, IN2 and IN3 independent of the QBADx inputs and then outputs the median at the OUT output:

- OUT = Median {IN1, IN2, IN3}

If two or more INx inputs are invalid (two or more QBADx = 1), the OUT output is also invalid and the QBAD output is set to 1.

If the value of one INx input differs from the median of the three inputs IN1, IN2 and IN3 by more than the assigned tolerance DELTA, a discrepancy is detected and the DISx output is set.

So that, in the case of only one invalid INx input, its value is not output as the median at the OUT output and thus a discrepancy is detected for the invalid INx input, the fail-safe value for an invalid INx input must differ from the values typically occurring at the INx input during operation by more than the tolerance window DELTA.

I/Os

	Name	Data type	Explanation	Default
Inputs:	IN1	F_REAL	Input 1	0.0
	IN2	F_REAL	Input 2	0.0
	IN3	F_REAL	Input 3	0.0
	QBAD1	F_BOOL	1 = IN1 input invalid	0
	QBAD2	F_BOOL	1 = IN2 input invalid	0
	QBAD3	F_BOOL	1 = IN3 input invalid	0
	DELTA	F_REAL	Tolerance between INx	0.0

	Name	Data type	Explanation	Default
Outputs:	OUT	F_REAL	OUTPUT output	0.0
	QBAD	BOOL	1 = OUT output is invalid	0
	DIS1	BOOL	Discrepancy IN1 input	0
	DIS2	BOOL	Discrepancy IN2 input	0
	DIS3	BOOL	Discrepancy IN3 input	0

Use together with F-channel driver F_CH_AI

If you interconnect the INx input of F_2oo3_R with the V output of F_CH_AI, you must observe the following:

1. Interconnect the QBADx input of F_2oo3_R with the QBAD output of the F_CH_AI whose V output you interconnect with the INx input of F_2oo3_R.
2. Assign the SUBS_V input of F_CH_AI with a value that differs from the values typically occurring at the INx inputs during operation by more than the tolerance window DELTA.
3. Assign the SUBS_ON input of F_CH_AI with 1.

Error handling

- If one of the inputs IN1, IN2 and IN3 is an invalid floating-point number (NaN), an invalid floating-point number (NaN) is output at the OUT output. DIS1, DIS2 and DIS3 are set to 1.
- If the DELTA input is an invalid floating-point number (NaN) or if calculations in the F-block result in invalid floating-point numbers (NaN), DIS1, DIS2 and DIS3 are set to 1.
  For the case that invalid floating-point numbers (NaN) result from the calculations in the F-block, the following diagnostics event is entered in the diagnostics buffer of the F-CPU:
  – "Safety program: Invalid REAL number in DB" (Event ID 16#75D9).
- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostic buffer of the F-CPU:
  – "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.11.14 F_1oo2_R: 1oo2 evaluation of inputs of data type REAL

Function

This F-block puts out one of the inputs IN1 or IN2 at the OUT output depending on the QBAD1 input:

- QBAD1 = 0: OUT = IN1
- QBAD1 = 1: OUT = IN2

If both inputs, IN1 and IN2, are invalid (QBAD1 and QBAD2 = 1), the output OUT is also invalid and the output QBAD is set to 1.

If input IN1 and input IN2 differ by more than the configured tolerance DELTA, a discrepancy is detected and the output

- DIS1 = 1 is set when IN2 is output at the output OUT
- DIS2 = 1 is set when IN1 is output at the output OUT

I/Os

	Name	Data type	Explanation	Default
Inputs:	IN1	F_REAL	Input 1	0.0
	IN2	F_REAL	Input 2	0.0
	QBAD1	F_BOOL	1 = IN1 input invalid	0
	QBAD2	F_BOOL	1 = IN2 input invalid	0
	DELTA	F_REAL	Tolerance between INx	0.0
Outputs:	OUT	F_REAL	Output	0.0
	QBAD	F_BOOL	1 = OUT output invalid	0
	DIS1	F_BOOL	Discrepancy input IN1	0
	DIS2	F_BOOL	Discrepancy input IN2	0

Use together with F-channel driver F_CH_AI

If you interconnect the INx input of F_1oo2_R with the V output of F_CH_AI, you must observe the following:

- Interconnect the QBADx input of F_1oo2_R with the QBAD output of the F_CH_AI whose V output you want to interconnect with the INx input of F_1oo2_R.
- Configure the SUBS_V input of the F_CH_AI with a value that differs by more than the tolerance window DELTA from the values usually occurring during operation at the INx inputs.
- Configure the SUBS_ON input of the F_CH_AI with 1.

Error handling

- DIS1 and DIS2 are set to 1 if one of the inputs IN1, IN2 or DELTA is an invalid floating-point number (NaN) or if invalid floating-point numbers (NaN) resulted from calculations in the F-block.
  In case invalid floating-point numbers (NaN) resulted from the calculations in the F-block, the following diagnostics event is entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Invalid REAL number in DB" (Event ID 16#75D9).
- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.12 Arithmetic blocks with the INT data type

Overview

Block name	Block number	Description
F_LIM_I	FB 350	Asymmetrical limiter of an INT value

A.2.12.1 F_LIM_I: Asymmetrical limiter of an INT value

Function

This block checks whether input IN is within or outside the interval between MIN and MAX. If input IN lies within the interval, it is passed through to output OUT. If it lies outside of the interval it is limited to MIN or MAX.

- Is IN > MAX, then an upper limit violation exists. MAX is output at output OUT. OUTU is set to 1 and OUTL to 0.
- If IN < MIN, then a lower limit violation exists. MIN is output to output OUT. OUT is set to 0 and OUTL on 1.
- If IN lies between MIN and MAX, input IN is passed through to output OUT. OUTU and OUTL are always set to 0.

Inputs/Outputs

	Name	Data type	Description	Default
Inputs:	IN	F_INT	Input	0
	MIN	F_INT	MINIMUM	-32768
	MAX	F_INT	MAXIMUM	32767
Outputs:	OUT	F_INT	OUTPUT	0
	OUTU	F_BOOL	UPPER LIMIT	0
	OUTL	F_BOOL	LOWER LIMIT	0

Error handling

- Is MIN ≥ MAX, MAX is output at output OUT. OUTU and OUTL are always set to 1.
- An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.13 Multiplex blocks

A.2.13.1 Multiplex blocks

Overview

Block name	Block number	Description
F_MOV_R	FB 311	Copy 15 values of data type REAL
F_MUX2_R	FB 332	Multiplexer for 2 REAL values with BOOL selection
F_MUX16R	FB 334	Multiplexer for 16 REAL values with INT selection

A.2.13.2 F_MOV_R: Copy 15 values of data type REAL

Function

The F-block copies the inputs INx to the outputs OUTx at input ENABLE = 1. If ENABLE = 0, the last valid values are retained at the outputs OUTx.

The OENABLE output corresponds to the ENABLE input.

I/Os

	Name	Data type	Explanation	Default
Inputs:	ENABLE	F_BOOL	1 = Enable copying	0
	IN1	F_REAL	Input 1	0.0
	...		...	
	IN15	F_REAL	Input 15	0.0
Outputs:	OENABLE	F_BOOL	1 = Copying is enabled	0
	OUT1	F_REAL	Output 1	0.0
	...		...	
	OUT15	F_REAL	Output 15	0.0
	CS_USED	F_BOOL	1 = Default values are used	0

Startup behavior

Following an F-startup, the F-block behaves as follows:

- After a CPU STOP followed by a cold restart of the F-CPU or at an initial run:
  If ENABLE = 0, the (configured) default values are provided at the outputs OUTx. The CS_USED output is set to 1. CS_USED is reset to 0 as soon as ENABLE changes to 1.
  If ENABLE = 1, the INx inputs are copied to the OUTx outputs. The CS_USED output is set to 0.
- After a CPU STOP followed by a restart (warm restart) of the F-CPU or after an F-STOP followed by a positive edge at the RESTART input of the F_SHUTDN block:
  If ENABLE = 0, the last valid values are provided at the OUTx outputs. The CS_USED output retains its default value (0).
  If ENABLE = 1, the INx inputs are copied to the OUTx outputs. The CS_USED output is set to 0.

Note

Before initial processing of the F-block after an F-startup, the default values are applied to the outputs OUTx and CS_USED.

⚠ **WARNING**

F-startup

After an F-startup, the safety of the system must not be impaired by applying the (configured) default values to the outputs OUTx, or by applying the last valid values to the outputs OUTx.

If necessary, evaluate the CS_USED output to determine whether the (configured) default values or the last valid values have been provided at the outputs OUTx following an F-startup. In addition, the default value "0" of CS_USED must not be changed.

If a restart (warm restart) is performed after a cold restart, CS_USED is reset to the default value (0), even if the default values are currently present at outputs OUTx.

FSW-175

Error handling

An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.13.3 F_MUX2_R: Multiplexer for 2 REAL values with BOOL selection

Function

This F-Block outputs one of the IN0 or IN1 inputs, depending on selection input K, at output OUT:

- K = 0: OUT = IN0
- K = 1: OUT = IN1

Inputs/Outputs

	Name	Data type	Description	Default
Inputs:	K	F_BOOL	Selection input	0
	IN0	F_REAL	Input 0	0.0
	IN1	F_REAL	Input 1	0.0
Output:	OUT	F_REAL	Output	0.0

Error handling

An F_STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:

- "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.13.4 F_MUX16R: Multiplexer for 16 REAL values with INT selection

Function

This block outputs one of the inputs INx, depending on selection input K, at output OUT:

- 0 ≤ K ≤ 15 OUT = IN[K]

Inputs/Outputs

	Name	Data type	Description	Default
Inputs:	K	F_INT	Selection input	0
	IN0	F_REAL	Input 0	0.0
	...		...	
	IN15	F_REAL	Input 15	0.0
Output:	OUT	F_REAL	Output	0.0

Error handling

- If K < 0 or K > 15 0.0 is output at output OUT.
- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.14 F-Control blocks

Overview

Block name	Block number	Description
F_POLYG	FB 467	Polyline or non-linear characteristic with 24 data points, maximum
F_INT_P	FB 468	Integration function with integration and track mode
F_PT1_P	FB 469	First order delay

A.2.14.1 F_POLYG: F-Control block with non-linear characteristic

Function/mode of operation

The polygon function is used to approach any analog function by means of a specific number of intervals. These are defined by their X/Y coordinates. Within the limits of the approach, up to 24 X/Y coordinate pairs can be defined. The number of X/Y coordinate pairs must be assigned via input N.

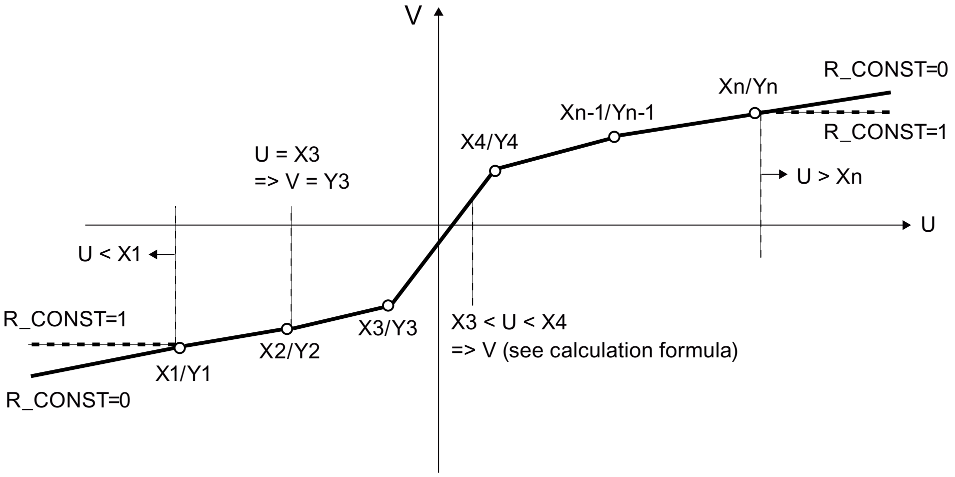
The F-Block converts input U to output V following the non-linear characteristic defined by means of the X/Y coordinate pairs, where X is the value of the analog input and Y the value of the analog output. Linear interpolation is carried out between the Xn/Yn data points.

When R_CONST = "0", extrapolation occurs outside of the end data points based on the first two and last two data points.

If R_CONST = "1" and U is less than (<) X_1, Y_1 is written to output V; similarly, if U is greater than (>) X_N, Y_N is written to output V.

In the event of an invalid parameter assignment of N (2 > N > 24). V = U is output; the same applies for an invalid sequence of X/Y coordinate pairs (Xn ≥ Xn+1 for n = 1, 2, ... N-1).

The figure below provides a graphical illustration of the functionality of this F-Block.



If input value U lies between two X/Y points (Xn < U < Xn+1), V is calculated based on the following formula:

$$V = Y_n + (U - X_n) * \left(\frac{Y_{n+1} - Y_n}{X_{n+1} - X_n} \right)$$

V	Output value
U	Input value
Yn/Xn	Data point n
Yn+1/Xn+1	Data point n+1

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	U	F_REAL	Input value	0.0
	IERR	F_BOOL	1=input value invalid	0
	N	F_INT	Number of data points	0
	R_CONST	F_BOOL	0=extrapolation 1=lowest/highest Y value	0
	X1	F_REAL	X coordinate 1	0.0
	Y1	F_REAL	Y coordinate 1	0.0
	:			
	X24	F_REAL	X coordinate 24	0.0
	Y24	F_REAL	Y coordinate 24	0.0
Outputs:	V	F_REAL	Output value	0.0
	QERR	F_BOOL	Output value invalid	0

Error handling

The validity of input signal U is read in via input IERR. This input parameter can be connected to QBAD of the corresponding input channel driver or of a voter block.

Output QERR is set when one of the following conditions is met:

- U = NaN or one Xn/Yn = NaN
  NaN is assigned to output V.
- The calculation yields NaN.
  NaN is assigned to output V.
- Parameter assignment error Xn >= Xn+1
  U is assigned to output V.
- Input IERR = 1

Diagnostic buffer entry

- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA).
- If an invalid REAL number is determined for V during the calculation, an entry is made in the diagnostic buffer (event ID 16#75D9).

A.2.14.2 F_INT_P: Integration function with integration and track mode

The F-block F_INT_P operates in two different modes:

- Integration mode
- TRACK mode

These two modes are described separately below.

Integration mode

Function / principle of operation

In the integration mode, the output signal V rises with the positive input signal and decreases with a negative input signal U.

The F-block works in the integration mode by summation according to the trapezoidal rule per scanning interval (Ts). The resulting V_{intern} is in the range of V_HL+hyst to V_LL-hyst, as shown in the figure. The value is then written to the output V after an additional limitation to the range V_LL to V_HL.

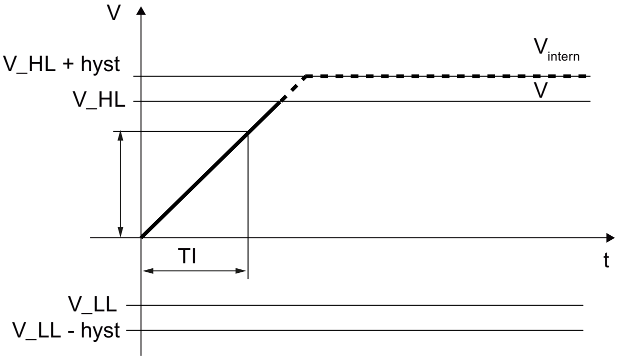


Figure A-1 Step response of the F_INT_P

The V output value is calculated using the following formula:

$$V_X = V_{X-1} + U_X * \frac{Ts}{TI}$$

V_X Current internal output value

V_{X-1} Last internal output value ($V_{internal}$)

Ts Scanning time (elapsed time between 2 processing steps of the F-block) in seconds

TI Integration time in seconds

U_X Current input value

The following further parameterizations influence the output value V and its calculation:

- HOLD: If HOLD = 1, the last output value is maintained for V.
- RESET: If there is a positive edge at the RESET, the output value V is reset (V = 0.0).
- EN_INC and EN_DEC: The processing of the integration function also depends on the input parameters EN_INC and EN_DEC.
  - EN_INC and EN_DEC = 1
    The step response at output V decreases or increases depending on U.
  - EN_INC = 0 and EN_DEC = 1:
    The output value V does not increase. This means that, with a positive input value at U, the last output value is maintained for V.
  - EN_INC = 1 and EN_DEC = 0:
    The output value V does not decrease. This means that, with negative input value at U, the last output value is maintained for V.
  - EN_INC and EN_DEC = 0:
    Regardless of the input value U, the last output value is always maintained for V.

In addition to this functionality, threshold value monitoring is also used:

- V_HL limits V upward.
  If $V_{internal}$ exceeds V_HL, V is limited to V_HL and, in addition, QVHL = 1.
- V_LL limits V downward.
  If $V_{internal}$ falls below V_LL, V is limited to V_LL and, in addition, QVLL = 1.

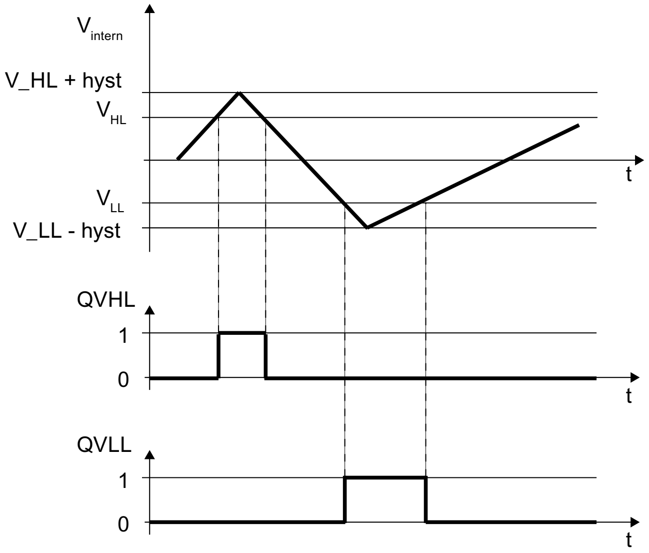


Figure A-2 Limit monitoring of the F_INT_P

Special cases:

- Hysteresis HYS < 0:
  HYS is set internally to 1%. HYS = 0.0 is allowed. In this case, V_{intern} = V if V_HL is exceeded or V_LL is undershot.
- V_LL > V_HL:
  V_HL is set internally to V_LL. In this case, V always corresponds to V_LL.
- TI <= 0:
  TI is set internally to Ts. Thus, the ratio of times in the equation is 1.

The validity of the input signal U is read in via the input IERR. This input parameter can be connected to QBAD of the corresponding input channel driver or a voter.

If U, V_HL, or V_LL = NaN, the value at output V is maintained. If HYS = NaN, this has no effect on the formation of V, but only on $V_{internal}$. In this case, V_{intern} = V. The output QERR is set to 1 with NaN at one of the input parameters.

Note

Denormalized values at U are processed and no error message is output to V.

TRACK mode

In TRACK mode, the input signal VTRACK is applied to output V. This allows using the TRACK mode to preset the integration function.

The mode is activated with the digital input TRACK = 1.

If the input signal VTRACK = NaN, NaN is output at the output V. The output QERR is then set to 1.

There is threshold value monitoring also in the TRACK mode:

- V_HL limits V upward.
  If VTRACK exceeds V_HL, V is limited to V_HL and, in addition, QVHL = 1.
- V_LL limits V downward.
  If VTRACK falls below V_LL, V is limited to V_LL and, in addition, QVLL = 1.

Special cases:

- Hysteresis HYS < 0:
  HYS is set internally to 1%. HYS = 0.0 is allowed. In this case, V_{intern} = V if V_HL is exceeded or V_LL is undershot. HYS has no influence on the formation of V in the track mode.
- V_LL > V_HL:
  V_HL is set internally to V_LL. In this case, V always corresponds to V_LL.

I/Os

	Name	Data type	Explanation	Default
Inputs:	TI	F_TIME	Integration time	1 s
	V_HL	F_REAL	High limit	100.0
	V_LL	F_REAL	Low limit	0.0
	U	F_REAL	Input value	0.0
	HYS	F_REAL	Hysteresis in %	1.0
	VTRACK	F_REAL	Input value for track mode	0.0
	TRACK	F_BOOL	Mode: 1=Track mode	0
	HOLD	F_BOOL	1 = maintain the integration value	0
	RESET	F_BOOL	1 = reset V	0
	EN_INC	F_BOOL	1 = increasing output value is allowed	1
	EN_DEC	F_BOOL	1 = Decreasing output value is allowed	1
	IERR	F_BOOL	1 = input value invalid	0
Outputs:	V	F_REAL	Output value	0.0
	QERR	F_BOOL	1 = output value invalid	0
	QVHL	F_BOOL	1 = exceeding the upper limit value active	0
	QVLL	F_BOOL	1 = undershooting the lower limit value active	0

Error handling

The validity of the input signal U is read in via the input IERR. This input parameter can be connected to QBAD of the corresponding input channel driver or a voter.

The QERR output is set in the integration mode when one of the following conditions is met:

- The input signal U = NaN
- Input IERR = 1

The output QERR is set in the TRACK mode when the following condition is met:

- VTRACK = NaN

And, regardless of the mode, if:

- The calculation returned NaN: The output V retains the last value.
- NaN is present at one of the input parameters V_LL, V_HL, HYS

Diagnostic buffer entry

- If an invalid REAL number is returned by a calculation, a diagnostic buffer entry is made (Event ID 16#75D9)
- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

A.2.14.3 F_PT1_P: First order delay

Function/mode of operation

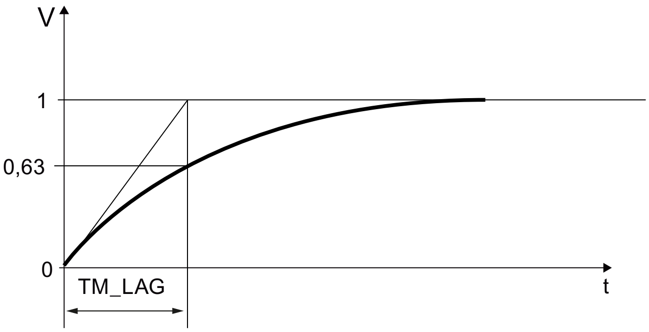
Output value V is calculated according to the following formula:

$$V_X = V_{X-1} + (U_X - V_{X-1}) * \left(\frac{Ts}{\frac{Ts}{2} + TM\_LAG} \right)$$

V_X	Current output value V
V_{X-1}	Last output value V
Ts	Sampling time (time elapsed between two block processing cycles (Diff)) in seconds
TM_LAG	Delay time in seconds
U_X	Current input value U

Input value U is output to output V with a delay corresponding to time constant TM_LAG.

The step response of an amplitude with the value U = 1.0 is reproduced in the figure below:



STOP_RES: When STOP_RES = 1, the arithmetic procedure is stopped. The last output value for V is held. During the changeover from STOP_RES 1 to 0, output V is reset to input value U.

D_OFF: When D_OFF = 1, the delay time is switched off. This means that input value U is applied at output V.

The following boundary conditions are applicable:

- TM_LAG < Ts/2:
  TM_LAG is set to Ts/2. Thus the times ratio assumes a value of 1 in the equation. This means that output value V corresponds to input value U in this case.

The validity of input signal U is read in via input IERR. This input parameter can be connected to QBAD of the corresponding input channel driver or of a voter block.

Note

Denormalized values at U are processed and do not generate an error message.

If an approach to 0 occurs (U = 0.0), V = 0.0 is output when a denormalized value is reached at V (-1.18E-38 or +1.18E-38).

If U is equal to (=) NaN, the value at output V is retained. Output QERR is set to 1.

Inputs/outputs

	Name	Data type	Description	Default
Inputs:	TM_LAG	F_TIME	Delay time	0 s
	U	F_REAL	Input value	0.0
	STOP_RES	F_BOOL	Stop/reset	0
	D_OFF	F_BOOL	1=delay switched off	0
	IERR	F_BOOL	1=input value invalid	0
Outputs:	V	F_REAL	Output value	0.0
	QERR	F_BOOL	1=output value invalid	0

Startup characteristics

During startup input value U is applied at output V. V does not behave in accordance with PT1 behavior until a change to input value U has been made subsequently.

Error handling

Output QERR is set when one of the following conditions is met:

- Input signal U is NaN.
- The calculation yields NaN: Output V retains the last value.
- Input IERR = 1

Diagnostic buffer entry

- If an invalid REAL number is determined during the calculation, an entry is made in the diagnostic buffer (event ID 16#75D9).
- An F-STOP is triggered when an error occurs in the safety data format in the corresponding instance DB. The following diagnostic event is then entered in the diagnostic buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA).

A.2.15 Additional F-Blocks

Overview

Block name	Block number	Description
F_DEADTM	FB 320	Monitoring of changes in F_REAL values at the same measuring point

A.2.15.1 F_DEADTM: Monitoring of changes in F_REAL values at the same measuring point

Function and principle of operation

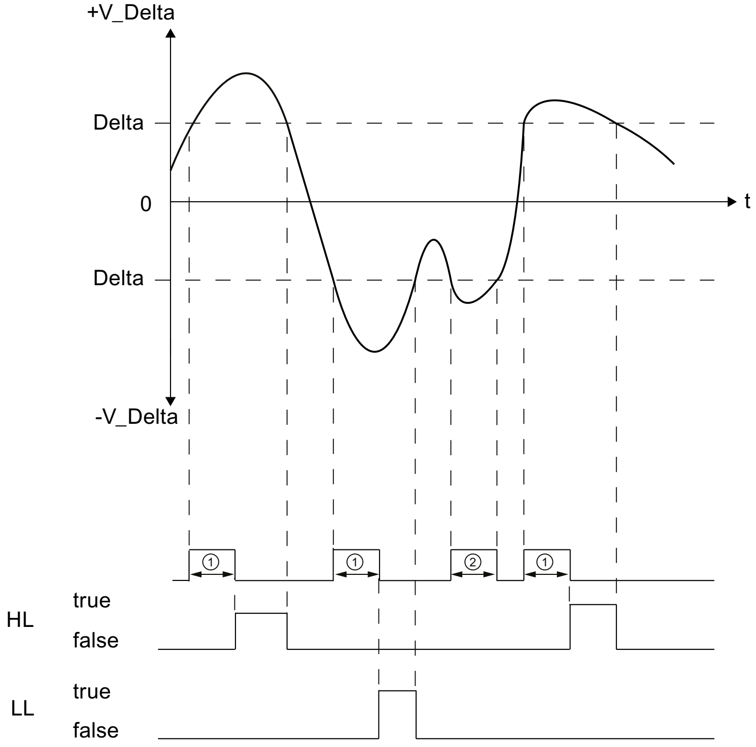
This block outputs the IN value delayed by the deadtime at the output OUT. The deadtime can be configured at the DEADTM input. In addition, the delta from the current IN value and the delayed IN value output at OUT is calculated. It is output at the V_DELTA output.

If the calculated delta (V_DELTA) exceeds the delta configured in the DELTA input parameter beyond a time configured under DELAYTM, the output parameter HL (IN > OUT) or LL (IN <OUT) is activated depending on the values of IN and OUT.

If the time DELAYTM is configured with 0, then, when the difference DELTA is exceeded, there is no additional delay in the activation of the output HL or LL. However, there is a delay due to a configured time DEADTM, because this time value DEADTM delays output of the IN value at the output OUT, and thus the calculation of the V_DELTA value. It thus indirectly causes a delay for the outputs HL and LL.

The following constraint applies:

- If DELTA has a negative value:
  DELTA considers the amount.
- If DEADTM has a negative value:
  DEADTM is internally set to 0.0
- If DEADTM > 2E+8 (corresponds to approx. 6 years):
  DEADTM is internally limited to 2E+8



① Time configured in DELAYTM expires

② Time configured in DELAYTM does not expire

Figure A-3 Delta processing

I/Os

	Name	Data type	Explanation	Default
Inputs:	IN	F_REAL	Input value	0.0
	DELTA	F_REAL	Delta between IN and OUT	0.0
	DEADTM	F_REAL	Deadtime (in seconds)	0.0
	DELAYTM	F_TIME	Delay time for HL and LL	0 s
	RESTART	F_BOOL	1 = reset all values (restart)	0

	Name	Data type	Explanation	Default
Outputs:	OUT	F_REAL	Output value	0.0
	V_DELTA	F_REAL	Current delta between IN and OUT	0.0
	HL	F_BOOL	1=Delta overshot (IN > OUT)	0
	LL	F_BOOL	1=Delta undershot (IN < OUT)	0

Startup behavior, reset

During startup or when there is a positive edge at the input parameter RESTART, all stored values of IN are reset to the current value of IN. As long as the deadtime has not yet elapsed for the first time, this IN value is output at the output parameter OUT. Thus, in the first cycle, following the above events, V_DELTA is always 0, and in the following cycles until the first complete deadtime has expired, the V_DELTA is calculated for the elapsed time.

Change of DEADTM

If the deadtime is changed, the correspondingly delayed IN values will be output only after this time expires for the first time. During the transitional period until the new deadtime expires, the output values relate to the previous *and* the new time.

Tolerances for the deadtime

When determining the value to be output at the OUT, a maximum of 100 different IN values can be stored within the deadtime.

The values created under IN are stored and the OUT and the delta are processed in accordance with the OB cyclic interrupt time.

This results in the following tolerances for the deadtime:

Deadtime	Max. tolerance for deadtime
DEADTM > = 100 × OB cyclic interrupt time	DEADTM + OB cyclic interrupt time
DEADTM < 100 × OB cyclic interrupt time	DEADTM + (DEADTM / 100)
DEADTM < MAX_CYC (at F_CYC_CO)	MAX_CYC (at F_CYC_CO)
DEADTM < OB cyclic interrupt time	

Error handling

The following error handling takes place in case of errors at the input parameters DEADTM, DELTA, and IN:

- DEADTM:
  If the input value is DEADTM = NaN, the output values of OUT and V_DELTA also become NaN and LL, and HL = 1.
- DELTA/V_DELTA:
  If the input value is DELTA = NaN, OUT and V_DELTA is still output and LL and HL is set to 1, since a comparison with DELTA cannot be made.
  If an invalid REAL number (NaN) is determined when calculating V_DELTA, the response is the same as for a NaN on DELTA.
  If a denormalized or infinite value is found for V_DELTA, this value is considered valid. There is no error handling in this case.
- IN:
  A NaN at the input parameter IN is initially considered a normal IN value. When the deadtime has elapsed and the stored NaN IN value is output to the OUT output, the output values of OUT and V_DELTA become NaN, LL, and HL = 1.

Diagnostic buffer entry

- If the calculation returns an invalid REAL number, a diagnostic buffer entry is made (Event ID 16#75D9)
- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)

See also

F_CYC_CO: F-Control block "F-Cycle time monitoring" (Page 458)

A.3 F-Control blocks S7 F Systems Library V1.3 SP3

Overview

When the S7 program is compiled, F-control blocks are automatically inserted into automatically generated (F-)system charts and automatically generated (F-)runtime groups with the ID "@F_" or "@SDW_" and interconnected to generate an executable safety program from the safety program programmed by the user.

⚠ WARNING

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

Block name	Block number	Description
F_MOVRWS	FB 312	F-control block
F_DIAG	FB 360	F-control block
F_CYC_CO	FB 395	F-control block "F-cycle time monitoring"
F_PLK	FB 396	F-control block
F_PLK_O	FB 397	F-control block
F_TEST	FB 398	F-control block
F_TESTC	FB 399	F-control block
F_TESTM	FB 400	F-control block "Deactivating safety mode"
F_SHUTDN	FB 458	F-control block "Shutdown and F-startup of F-shutdown groups"
RTGLOGIC	FB 459	F-control block
F_PS_12	FB 464	F-control block "F-module driver"
F_PS_13	FB 617	F-control block "F-module driver"
F_CHG_WS	FB 477	F-control block
DB_INIT	FC 180	F-control block
DB_RES	FC 301	F-control block
F_PS_MIX	FC 302	F-control block
F_VFSTP1	FC 307	F-control block
F_VFSTP2	FC 308	F-control block
FORCEOFF	FC 310	F-control block "Deactivating F-Force"
F_MNR_H	FC 312	F-control block

A.3.1 F_MOVRWS: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated system chart and an automatically generated runtime group with the ID "@SDW_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

> ⚠ WARNING
>
> **Safety instruction - Do not change automatically inserted F-control blocks**
>
> Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).
>
> Failure to do so may result in errors in the next compilation.
>
> FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

A.3.2 F_DIAG: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated F-system chart and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

> ⚠ WARNING
>
> **Safety instruction - Do not change automatically inserted F-control blocks**
>
> Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).
>
> Failure to do so may result in errors in the next compilation.
>
> FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

A.3.3 F_CYC_CO: F-Control block "F-Cycle time monitoring"

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated F-system chart "@F_CycCo-OB3x" and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

The F-CPU monitors the F-cycle time for each cyclic interrupt OB 3x which contains F-runtime groups. When you first compile the S7 program, you will be prompted via a dialog to enter a value for the maximum cycle time "MAX_CYC" that may pass between two calls to this OB.

If you have to modify the maximum F-cycle time after the initial compilation of the S7 program, you need to perform the F-cycle time at the MAX_CYC input of the F_CYC_CO-OB3x block in the @F_CycCo-OB3x F-system chart.

For information regarding the setting of the F-monitoring time, see section "Run times, F-Monitoring times, and response times (Page 482)".

⚠ WARNING

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

	Name	Data type	Explanation	Default
Input:	MAX_CYC	F_TIME	Maximum F-cycle time	It is automatically supplied with 3000 ms if no change is made in the dialog during the first compilation

⚠ WARNING

Default setting of the maximum MAX_CYC

The default setting for the maximum F-cycle time is 3000 milliseconds. Check whether this setting is suitable for your process. Change the defaults, if required.

FSW-177

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

Error handling

- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)
- If a safety-related error is detected, an F-STOP is triggered. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error detected in the F_CYC_CO" (Event ID 16#75E1)

A.3.4 F_PLK: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated F-system chart and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ WARNING

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

Error handling

- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)
- If a safety-related error is detected, an F-STOP is triggered. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error detected in the F_PLK" (Event ID 16#75E1)

A.3.5 F_PLK_O: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated F-system chart and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ **WARNING**

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

Error handling

- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)
- If a safety-related error is detected, an F-STOP is triggered. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error detected in the F_PLK_O" (Event ID 16#75E1)

A.3.6 F_TEST: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated F-system chart and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

> ⚠ **WARNING**
>
> **Safety instruction - Do not change automatically inserted F-control blocks**
>
> Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).
>
> Failure to do so may result in errors in the next compilation.
>
> FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

Error handling

- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)
- If a safety-related error is detected, an F-STOP is triggered. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error detected in the F_TEST" (Event ID 16#75E1)

A.3.7 F_TESTC: F-Control block

Function

The F-control block is automatically inserted and interconnected in an automatically generated F-system chart and in an automatically generated F-runtime group with identifier "@F_" when the S7 program is compiled. This is done in order to generate an executable safety program from the safety program created the user.

⚠ **WARNING**

Safety note: Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the "@F_" or "@SDW_" identifier are visible after compiling. You must not delete these or make any changes to them (unless expressly described).

Failure to observe this may result in errors at the next compile operation.

FSW-176

Note

As of S7 F Systems V6.2 with S7 F Systems Library V1.3 SP2, a change of the "Test cycle time" parameter (see "CPU > Object properties > H-Parameters") in HW Config and subsequent compiling of the HW configuration and the safety program causes the collective signature of your safety program to change.

I/Os

Undocumented I/Os are automatically supplied or interconnected when the S7 program is compiled and must not be changed. Online changes to undocumented I/Os can trigger an F-STOP. Remove any manipulations to these I/O by compiling the S7 program again.

Error handling

- An F-STOP is triggered when there is an error in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)
- If a safety-related error is detected, an F-STOP is triggered. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error detected in the F_TESTC (Event ID 16#75E1)

A.3.8 F_TESTM: F-Control block "Deactivate Safety Mode"

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated F-system chart "@F_TestMode" and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

You can evaluate whether the safety mode is deactivated at the TEST output. The TEST output has the system attribute S7_m_c. It can, therefore, be monitored directly from an OS. System displays will thus show if the safety mode is deactivated.

> ⚠ **WARNING**
>
> **Safety instruction - Do not change automatically inserted F-control blocks**
>
> Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).
>
> Failure to do so may result in errors in the next compilation.
>
> FSW-176

I/Os

	Name	Data type	Explanation	Default
Output:	TEST	BOOL	1 = Sfety mode deactivated	0

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

Error handling

- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)
- If a safety-related error is detected, an F-STOP is triggered. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error detected "(Event ID 16#75E1)

A.3.9 F_SHUTDN: F-Control block "Control of shutdown and F-Startup of the safety program"

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated system chart "@F_ShutDn" and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

With the F-control block, you can configure the shutdown behavior and control the shutdown and the F-startup of the safety program:

If you have set the "Shutdown behavior" dialog for the behavior in an F-STOP "according to the parameterization on the F_SHUTDN" in the "Safety program" dialog, you can configure how the safety program should behave in an F-STOP at the SHUTDOWN input:

- SHUTDOWN = full: Complete shutdown
- SHUTDOWN = partial: Partial shutdown

Note

The parameterization at the SHUTDOWN input may only be changed if no shutdown is active.

With input RQ_FULL = 1, you can trigger a complete shutdown of the safety program.

With a positive edge at the RESTART input, you can perform an F-startup after a shutdown of the safety program (F-STOP) and elimination of the reasons for the shutdown, if you do not want to restart (warm restart) or cold restart the F-CPU.

After an F-startup, the safety program starts up automatically with the initial values. After a partial shutdown of the safety program, only the F-shutdown groups that were in F-STOP perform an F-startup. The F-startup may take several seconds to complete initialization with the initial values. The output EN_INIT = 1 during initialization.

Note

After carrying out an F-startup with a positive edge at the RESTART input, a user acknowledgment at the ACK_REI input of the F-channel driver is required to reintegrate the fail-safe I/Os affected by the shutdown.

Output FULL_SD indicates whether there is a complete shutdown of the safety program. The output SD_TYP can be used for reading out the shutdown behavior set in the "Safety program" dialog > "Shutdown behavior" dialog.

The SAFE_M output indicates whether the safety program is in safety mode (SAFE_M = 1) or whether safety mode is deactivated (SAFE_M = 0).

⚠ WARNING

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

	Name	Data type	Explanation	Default
Inputs:	RESTART	BOOL	1 = F-startup after shutdown	0
	SHUTDOWN	BOOL	Shutdown behavior	Full
	RQ_FULL	BOOL	1 = Tigger complete shutdown	0
	ALARM_EN	BOOL	1 = activate messages	1
Outputs:	FULL_SD	BOOL	1 = complete shutdown of the safety program	0
	SD_TYP	BOOL	Shutdown behavior from dialog: 1 = Complete shutdown	0
	EN_INIT	BOOL	1 = Initialization of safety program is running	0
	SAFE_M	BOOL	1 = safety program in the safety mode	0
	F_SIG_OUT	DWORD	Collective signature of the safety program	0
	MSG_DONE	BOOL	= Output DONE of SFB34 "ALARM_8"	0
	MSG_ERR	BOOL	= Output ERROR of SFB34 "ALARM_8"	0
	MSG_STAT	WORD	= Output STATUS of SFB34 "ALARM_8"	0
	MSG_ACK	WORD	= Output ACK_STATE of SFB34 "ALARM_8"	0
	NFY_DONE	BOOL	= Output DONE of SFB31 "NOTIFY_8P"	0
	NFY_ERR	BOOL	= Output ERROR of SFB31 "NOTIFY_8P"	0
	NFY_STAT	WORD	= Output STATUS of SFB31 "NOTIFY_8P"	0
Input-output:	MSG_TIME	TIME	Time for message repetition	8 h

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

Message behavior

- When the safety program is shut down (an F-STOP was triggered), the F-control block F_SHUTDN sets the following messages to the OS using SFB 34 "ALARM_8" as "AS process control message - error, with single acknowledgment":
  - "Safety program: partial shutdown", in case of a partial shutdown of one or more F-shutdown groups
  - "Safety program: complete shutdown", in case of a complete shutdown of the safety program
- In case of an F-startup following a positive edge at the RESTART input, the following message is sent to the OS using SFB 31 "NOTIFY_8P" as "Operating message - without acknowledgment":
  - "F-startup safety program on F_SHUTDN"
- When deactivating the safety mode, the following message is sent to the OS using SFB 31 "NOTIFY_8P", both as "Operating message - without acknowledgment" and as "AS process control message - error, with single acknowledgment". The "AS process control message" is repeated after expiry of the time MSG_TIME if the safety mode is still deactivated. There is no repetition with MSG_TIME = 0.
  - "Safety mode deactivated"

You can switch off the messages by setting the ALARM_EN input to 0 if no suitable signaling system is available.

Outputs MSG_xxx and NFY_xxx

At the outputs MSG_xxx and NFY_xxx, non-fail-safe information about errors in the messaging behavior is provided for service purposes. You can read out this information on your ES/OS or evaluate it in your standard user program if necessary. The outputs correspond to the outputs of SFB 34 "ALARM_8" and SFB 31 "NOTIFY_8P". See description in the online help for the SFB 34/SFB 31 or in the "System Software for S7 300/400 System and Standard Functions (http://support.automation.siemens.com/WW/view/en/1214574)" manual.

Troubleshooting/diagnostic buffer entry

- If a safety-relevant error is detected and an overall shutdown is performed (an F-STOP has been triggered), the F-control block F_SHUTDN enters the following event into the diagnostic buffer of the F-CPU:
  - "Complete shutdown of the F-program activated" or "Complete shutdown of the F-program deactivated" (Event ID 16#7xDE)
- In case of an F-startup following a positive edge at the RESTART input, the following event is entered to the F-CPU diagnostic buffer:
  - "Initialization of safety program started" or "Initialization of safety program ended" (Event ID 16#7xDF)
- When the safety mode is activated/deactivated, the following event is entered to the F-CPU diagnostic buffer:
  - "Safety program: safety mode deactivated" or "Safety program: Safety mode activated" (Event ID 16#7xDB)

See also

F-STOP (Page 99)

F-Startup and reprogramming restart/startup protection (Page 97)

A.3.10 RTGLOGIC: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated system chart and an automatically generated runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ **WARNING**

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

Error handling

If you have configured "partial shutdown" for the shutdown behavior and a safety-related error is detected in an F-shutdown group, the affected F-shutdown group is switched off (an F-STOP is triggered). The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:

- "Safety program: Shut down of a fail-safe runtime group" (Event ID 16#7xDD)

A.3.11 F_PS_12: F-Control block "F_Module_Driver"

Function

The F-control block F_PS_12 is used for PROFIsafe devices with the profile before V2.6.1 or V2.6.1 LP (Loop-back Extension Protocol).

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated F-system chart "@F_(x)" and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ **WARNING**

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

	Name	Data type	Explanation	Default
Outputs:	DIAG	DWORD	Error information	DW#16#0
	PROFISAFE	F_BOOL	1 = PROFIsafe communication error	0

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

DIAG output

At the DIAG output, non-fail-safe information about errors in the safety-related communication (communication error) between the F-CPU and the fail-safe I/Os is provided by the PROFIsafe safety protocol for servicing purposes. You can read out this information on your ES/OS or evaluate it in your standard user program if necessary.

Structure of DIAG

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 0	Timeout of fail-safe I/O detected	The PROFIBUS connection between the F-CPU and F-CPU devices is faulty. The F-monitoring time for the F-I/O devices has been set too low in HW Config. The F-I/O device is receiving invalid parameter settings or	Test the PROFIBUS connection to ensure that there are no sources of external interference. Check the parameter settings for the fail-safe I/O devices in HW Config. If necessary, set a higher F-monitoring time value. Compile the hardware configuration again and then download it to the F-CPU. Compile the S7 program again. Check the diagnostic buffer of the fail-safe I/O. Turn the power to the F-I/O devices off and then back on again.
		Internal error in the F-I/O or	Replace the F-I/O
		internal error in the F-CPU	Replace the F-CPU
Bit 1	F-I/O device error detected in I/O devices	See fail-safe I/O manuals	See fail-safe I/O manuals
Bit 2	CRC/sequence number error in F-I/O detected	See description for bit 0	See description for bit 0
Bit 3	Reserve	—	—
Bit 4	Timeout in F-system detected	See description for bit 0	See description for bit 0
Bit 5	Sequence number error in F-system detected	See description for bit 0	See description for bit 0
Bit 6	CRC error detected in F-system	See description for bit 0	See description for bit 0
Bit 7	Reserve	—	—
Bits 8 - 31	Reserve	—	—

Error handling

- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)
- The safety function requires that when passivating the entire F-I/O or individual channels of an F-I/O, substitute values are used instead of the process values in the following cases:
  - For an F-startup
  - When there are errors in safety-related communication (communication errors) between F-CPU and F-I/Os via the safety protocol according to PROFIsafe
  - When F-I/O or channel faults are detected, for example, wire break, short-circuit, or discrepancy error
  - As long as you activate passivation of fail-safe I/Os on the F-channel driver at PASS_ON input

  The following diagnostic events are then entered in the F-CPU diagnostic buffer (except for F-startup):
  - "Fail-safe I/O input channel passivated / fail-safe I/O input channel depassivated" (Event ID 16#7xE3)
  - "Fail-safe I/O output channel passivated / fail-safe I/O output channel depassivated" (Event ID 16#7xE4)
  - "Fail-safe I/O passivated / fail-safe I/O depassivated" (Event ID 16#7xE5)

A.3.12 F_PS_13: F-control block "F_module driver" PROFIsafe profile V2.6.1 XP

Function

The F-control block F_PS_13 is used for PROFIsafe devices with the profile V2.6.1 XP (Expanded Protocol).

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated F-system chart "@F_(x)" and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ **WARNING**

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

	Name	Data type	Explanation	Default
Outputs:	DIAG	DWORD	Error information	DW#16#0
	PROFISAFE	F_BOOL	1 = PROFIsafe communication error	0

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

DIAG output

At the DIAG output, non-fail-safe information about errors in the safety-related communication (communication error) between the F-CPU and the fail-safe I/Os is provided by the PROFIsafe safety protocol for servicing purposes. You can read out this information on your ES/OS or evaluate it in your standard user program if necessary.

Structure of DIAG

Bit no.	Assignment	Possible error causes	Corrective measures
Bit 0	Timeout of fail-safe I/O detected	The PROFIBUS connection between the F-CPU and F-CPU devices is faulty. The F-monitoring time for the F-I/O devices has been set too low in HW Config. The F-I/O device is receiving invalid parameter settings or	Test the PROFIBUS connection to ensure that there are no sources of external interference. Check the parameter settings for the fail-safe I/O devices in HW Config. If necessary, set a higher F-monitoring time value. Compile the hardware configuration again and then download it to the F-CPU. Compile the S7 program again. Check the diagnostic buffer of the fail-safe I/O. Turn the power to the F-I/O devices off and then back on again.
		Internal error in the F-I/O or	Replace the F-I/O
		internal error in the F-CPU	Replace the F-CPU
Bit 1	F-I/O device error detected in I/O devices	See fail-safe I/O manuals	See fail-safe I/O manuals
Bit 2	CRC/sequence number error in F-I/O detected	See description for bit 0	See description for bit 0
Bit 3	Reserve	—	—
Bit 4	Timeout in F-system detected	See description for bit 0	See description for bit 0
Bit 5	Sequence number error in F-system detected	See description for bit 0	See description for bit 0
Bit 6	CRC error detected in F-system	See description for bit 0	See description for bit 0
Bit 7	Reserve	—	—
Bits 8 - 31	Reserve	—	—

Error handling

- An F-STOP is triggered when an error occurs in the safety data format in the associated instance DB. The following diagnostics event is then entered in the diagnostics buffer of the F-CPU:
  - "Safety program: Error in safety data format in DB" (Event ID 16#75DA)
- The safety function requires that when passivating the entire F-I/O or individual channels of an F-I/O, substitute values are used instead of the process values in the following cases:
  - For an F-startup
  - When there are errors in safety-related communication (communication errors) between F-CPU and F-I/Os via the safety protocol according to PROFIsafe
  - When F-I/O or channel faults are detected, for example, wire break, short-circuit, or discrepancy error
  - As long as you activate passivation of fail-safe I/Os on the F-channel driver at PASS_ON input

  The following diagnostic events are then entered in the F-CPU diagnostic buffer (except for F-startup):
  - "Fail-safe I/O input channel passivated / fail-safe I/O input channel depassivated" (Event ID 16#7xE3)
  - "Fail-safe I/O output channel passivated / fail-safe I/O output channel depassivated" (Event ID 16#7xE4)
  - "Fail-safe I/O passivated / fail-safe I/O depassivated" (Event ID 16#7xE5)

A.3.13 F_CHG_WS: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated system chart and an automatically generated runtime group with the ID "@SDW_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ **WARNING**

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

A.3.14 DB_INIT: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated system chart and an automatically generated runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ WARNING

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

A.3.15 DB_RES: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated system chart and an automatically generated runtime group at the start of the run sequence in the OB 100 with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ WARNING

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

A.3.16 F_PS_MIX: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated F-system chart and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ WARNING

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

A.3.17 F_VFSTP1: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into the S7 program in order to generate an executable safety program from the user-programmed safety program.

⚠ WARNING

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

A.3.18 F_VFSTP2: F-Control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into the S7 program in order to generate an executable safety program from the user-programmed safety program.

⚠ WARNING

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

A.3.19 FORCEOFF: Deactivation of F-Force

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated system chart and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ WARNING

Safety note: Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

A.3.20 F_MNR_H: F-control block

Function

When the S7 program is compiled, the F-control block is automatically inserted into an automatically generated F-system chart and an automatically generated F-runtime group with the ID "@F_", and is interconnected in order to generate an executable safety program from the user-programmed safety program.

⚠ WARNING

Safety instruction - Do not change automatically inserted F-control blocks

Automatically inserted F-control blocks and automatically inserted (F-)system charts and (F-)runtime groups with the ID "@F_" or "@SDW_" are visible after compiling. You must not delete them or change them (except for expressly described changes).

Failure to do so may result in errors in the next compilation.

FSW-176

I/Os

Undocumented connections are not automatically supplied or interconnected during compilation of the S7 program and you must not change them. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

A.4 Differences between the S7 F Systems Lib F-libraries

A.4.1 Differences between the F-libraries S7 F Systems Library V1.3 and V1.3 SP1

The following section describes the differences between the F-library S7 F Systems Library V1.3 and V1.3 SP1. Only the user-relevant changes of the F-blocks that affect the function, including start-up behavior and error handling, and the I/Os of the F-block are described.

For information on the runtimes of the F-blocks, refer to section "Run times, F-Monitoring times, and response times (Page 482)", You can obtain changes in the memory requirement, if needed, from SIMATIC Manager.

Note the changes of the F-blocks following a migration to a new version of the F-library and check whether the described changes have any effects on the behavior of your safety program. Note also section "Acceptance test of safety program changes (Page 237)".

Signatures/initial value signatures for the F-blocks

You can find the signatures/initial value signatures for the F-blocks of the S7 F systems V1.3 SP1 in Annex 1 of the Certificate Report.

Even if "None" is indicated for the change, the signatures/initial value signatures of an F-block may have changed compared to a previous version of the F-library, e.g. due to code optimizations, changes in diagnostics buffer entries or changes in the internal interaction of the F-blocks.

F-blocks	Delta download-capable	Change of S7 F Systems Library V1.3 to V1.3 SP1
F_FR_FDI	-	New F-block in S7 F Systems Library V1.3 SP1
F_FDI_FR	-	New F-block in S7 F Systems Library V1.3 SP1
F_QUITES	Yes	None
F_CHG_BO	Yes	None
F_CHG_R	Yes	None
F_CH_BI	Yes	IPAR_EN and IPAR_OK are visible
F_CH_BO	Yes	IPAR_EN and IPAR_OK are visible
F_PA_AI	Yes	IPAR_EN and IPAR_OK are visible and update to V_MOD
F_PA_DI	Yes	IPAR_EN and IPAR_OK are visible
F_CH_DO	With this change, the F-channel driver F_CH_DO can no longer be compiled in versions of S7 F Systems earlier than V6.1.	The output of ACK_REQ has been delayed.
F_CH_AI	Yes	IPAR_EN and IPAR_OK are visible and update to V_MOD and AL_STATE
F_CH_II	-	New F-block in S7 F Systems Library V1.3 SP1
F_CH_IO	-	New F-block in S7 F Systems Library V1.3 SP1
F_CH_DII	-	New F-block in S7 F Systems Library V1.3 SP1
F_CH_DIO	-	New F-block in S7 F Systems Library V1.3 SP1
F_SQRT	Yes	None
F_POLYG	-	New F-block in S7 F Systems Library V1.3 SP1
F_INT_P	-	New F-block in S7 F Systems Library V1.3 SP1

F-blocks	Delta download-capable	Change of S7 F Systems Library V1.3 to V1.3 SP1
F_PT1_P	-	New F-block in S7 F Systems Library V1.3 SP1
F_SWC_P	-	New F-block in S7 F Systems Library V1.3 SP1
F_SWC_BO	-	New F-block in S7 F Systems Library V1.3 SP1
F_SWC_R	-	New F-block in S7 F Systems Library V1.3 SP1
SWC_MOS	-	New block in S7 F Systems Library V1.3 SP1
F_DEADTM	-	New block in S7 F Systems Library V1.3 SP1
FORCEOFF	-	New F-block in S7 F Systems Library V1.3 SP1

A.4.2 Differences between the F-libraries S7 F Systems Library V1.3 SP1 and SP2

Overview

The following description points out the differences between the F-library S7 F Systems Library V1.3 SP1 and V1.3 SP2.

Only the user-relevant changes of the F-blocks that affect the function, including start-up behavior and error handling, and the I/Os of the F-block are described.

For information on the runtimes of the F-blocks, refer to section "Run times, F-Monitoring times, and response times (Page 482)",

You can obtain changes in the memory requirement, if needed, from SIMATIC Manager.

Note the changes of the F-blocks following a migration to a new version of the F-library and check whether the described changes have any effects on the behavior of your safety program. Note also section "Acceptance test of safety program changes (Page 237)".

Note

As of S7 F/FH Systems V6.2 with Lib V1.3 SP2, a change of the "Test cycle time" parameter (CPU > Object properties > H-Parameters) in HW Config and subsequent compiling of the HW configuration and safety program causes the collective signature of your safety program to change.

Signatures/initial value signatures for the F-blocks

You can find the signatures/initial value signatures for the F-blocks of the S7 F systems V1.3 SP2 in Annex 1 of the Certificate Report.

Even if "None" is indicated for the change, the signatures/initial value signatures of an F-block may have changed compared to a previous version of the F-library, e.g. due to code optimizations, changes in diagnostics buffer entries or changes in the internal interaction of the F-blocks.

F-blocks	Delta download-capable	Change of S7 F Systems Library V1.3 SP1 to SP2
F_2oo3AI	-	MODE input added Changed MED_MAX/MED_MIN Changed OUT_AVG behavior
F_CH_AI	-	Discrepancy analysis added
F_CH_RI	-	New F-block in S7 F Systems Library V1.3 SP2
F_PLK	-	None
F_RCVBO	-	New COMMVER_USED input
F_RDS_BO	-	New COMMVER_USED input
F_SDS_BO	Yes	None
F_SENDR	Yes	None
F_SWC_BO	Yes	Behavior when interconnected with SWC_MOS and SWC_QOS
F_SWC_CB	-	New F-block in S7 F Systems Library V1.3 SP2
F_SWC_CR	-	New F-block in S7 F Systems Library V1.3 SP2
F_SWC_P	Yes	ADR_OPSA output made visible
F_TESTC	-	None
F_XoutY	-	OUT_AE output added
F_RCVR	-	New COMMVER_USED input
F_SENDBO	Yes	None
SWC_CHG	-	New F-block in S7 F Systems Library V1.3 SP2
SWC_MOS	-	ADR_SWC input made visible
SWC_QOS	-	New F-block in S7 F Systems Library V1.3 SP2

A.4.3 Differences between the F-libraries S7 F Systems Library V1.3 SP2 and SP3

Overview

The following description points out the differences between the F-library S7 F Systems Library V1.3 SP2 and V1.3 SP3.

Only the user-relevant changes of the F-blocks that affect the function, including start-up behavior and error handling, and the I/Os of the F-block are described.

For information on the runtimes of the F-blocks, refer to section "Run times, F-Monitoring times, and response times (Page 482)",

You can obtain changes in the memory requirement, if needed, from SIMATIC Manager.

Note the changes of the F-blocks following a migration to a new version of the F-library and check whether the described changes have any effects on the behavior of your safety program. Note also section "Acceptance test of safety program changes (Page 237)".

Note

As of S7 F/FH Systems V6.2 with Lib V1.3 SP2, a change of the "Test cycle time" parameter (CPU > Object properties > H-Parameters) in HW Config and subsequent compiling of the HW configuration and safety program causes the collective signature of your safety program to change.

Signatures/initial value signatures for the F-blocks

You can find the signatures/initial value signatures for the F-blocks of the S7 F systems V1.3 SP3 in Annex 1 of the Certificate Report.

Even if "None" is indicated for the change, the signatures/initial value signatures of an F-block may have changed compared to a previous version of the F-library, e.g. due to code optimizations, changes in diagnostics buffer entries or changes in the internal interaction of the F-blocks.

F-blocks	Delta download-capable	Change of S7 F Systems Library V1.3 SP2 to SP3
F_PS_13	-	New F-block in S7 F Systems V1.3 SP3
F_MNR_H	-	New block in S7 F Systems Library V1.3 SP3
F_CH_QBI	-	New F-block in S7 F Systems V1.3 SP3
F_CH_QBO	-	New F-block in S7 F Systems V1.3 SP3
F_CH_QII	-	New F-block in S7 F Systems V1.3 SP3
F_CH_QIO	-	New F-block in S7 F Systems V1.3 SP3
F_PS_12	No	Extensions for PROFIsafe profile 2.6.1 LP
F_PS_MIX	Yes	Extensions for PROFIsafe profile 2.6.1 XP
F_RCVBO	Yes	Behavior with short-time network faults has been improved
F_RCVR	Yes	Behavior with short-time network faults has been improved
F_RDS_BO	Yes	Behavior with short-time network faults has been improved
F_SWC_BO	No	Behavior with short-term use of hard bypass and soft bypass has been improved
F_SDS_BO	Yes	Behavior with short-time network faults has been improved
F_SENDBO	Yes	Behavior with short-time network faults and high communication loads has been improved
F_SENDR	Yes	Behavior with short-time network faults and high communication loads has been improved
F_CH_DO	No	Extensions for ET 200SP HA F-DQ module
F_CH_AI	No	NaN evaluation extended Behavior with configuration change from redundant to non-redundant has been improved
SWC_MOS	Yes	Display of Confirm request in the faceplate
SWC_QOS	Yes	Display of Confirm request in the faceplate
SWC_CHG	Yes	Display of Confirm request in the faceplate

A.5 Run times, F-Monitoring times, and response times

Excel table S7FTIMEB.XLS contains information regarding:

- Execution times of F-Blocks in the various F-CPUs and aids for their calculation
- Maximum runtime of an F-Shutdown group
- Minimum F-Monitoring times
- Maximum response time of your F-System

This file is available for download on the Web (http://support.automation.siemens.com/WW/view/en/22557362).

See also

Safety engineering in SIMATIC S7 System Manual (http://support.automation.siemens.com/WW/view/en/12490443)

Checklist B

Introduction

The table below contains a checklist summarizing all activities in the life cycle of a fail-safe S7 F/FH System, including requirements and rules that must be observed in the various phases.

Checklist

Key:

- Stand-alone section references refer to this documentation.
- "*SM*" refers to the "Safety Engineering in SIMATIC S7 (http://support.automation.siemens.com/WW/view/en/12490443)" system manual.
- "*F-SMs manual*" refers to the "Automation System S7-300 Fail-Safe Signal Modules (http://support.automation.siemens.com/WW/view/en/19026151)" manual.
- "*ET 200S manual*" refers to the "Distributed I/O System ET 200S, Fail-Safe Modules (http://support.automation.siemens.com/WW/view/en/12490437)" manual.
- "*ET 200SP manual*" refers to the "SIMATIC ET 200SP Manual Collection (https://support.industry.siemens.com/cs/ww/en/view/84133942)" manual collection.
- "*HB ET 200SP HA*" refers to the "ET 200SP HA Distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/109761547)" manual.
- "*ET 200pro manual*" refers to the "ET 200pro Distributed I/O Device - Fail-Safe Modules (http://support.automation.siemens.com/WW/view/en/22098524)" manual.
- "*ET 200eco manual*" refers to the "ET 200eco Distributed I/O Station Fail-safe I/O Module (http://support.automation.siemens.com/WW/view/en/19033850)" manual.
- "*ET 200iSP manual*" refers to the "ET 200iSP Distributed I/O Device - Fail-safe Modules (http://support.automation.siemens.com/WW/view/en/47357221)" manual.

Phase	Requirement/Rule	Reference	Check
Planning			
Requirement: A specification with the safety requirements must be available for the planned application.	Process-dependent	—	
Specification of the system architecture	Process-dependent	—	
Assignment of functions and subfunctions to the system components	Process-dependent	Section 3 *SM*, section 1.5 *SM*, section 2.4	

Phase	Requirement/Rule	Reference	Check
Selection of sensors and actuators	Requirements for actuators	*SM*, section 4.8 *F-SMs manual*, section 6.5 *ET 200S manual*, section 4.5 *ET 200SP manual*, Basic information *HB ET 200SP HA* *ET 200pro manual*, section 4.4 *ET 200eco manual*, section 5.5 *ET 200iSP manual*, section 4.5	
Definition of required safety properties of the components	IEC 61508:2010	*SM*, sections 4.7, 4.8	
Configuring			
Installation of optional package	Requirements for installation	Section 4.1	
Selection of S7 components	Rules for configuration	Section 3.2 *SM*, section 2.4 *F-SMs manual*, section 3 *ET 200S manual*, section 3 *ET 200SP manual*, Basic information *HB ET 200SP HA* *ET 200pro manual*, section 2 *ET 200eco manual*, section 3 *ET 200iSP manual,* sec. 2.1	
Configuration of hardware	Rules for S7 F/FH Systems Verification of utilized hardware components based on Annex 1 of Certification Report	Section 5 Annex 1 of Certification Report	
Configuring the F-CPU	Protection level, "CPU contains safety program" Password	Sections 5.3, 6 Manual for Standard S7-400(H)	
Configuring the F-I/O	Settings for safety mode Configuring the monitoring times Module redundancy (optional) Defining the type of sensor interconnection/ evaluation	Sections 5.2, 5.4 - 5.8 *SM*, Appendix A *F-SMs manual*, sections 3, 9, 10 *ET 200S manual*, sections 2.4, 7 *ET 200SP manual*, Device-specific information *HB ET 200SP HA* *ET 200pro manual*, sections 2.4, 8 *ET 200eco manual*, sections 3, 8 *ET 200iSP manual,* section 2.4	
Programming			
Defining program design and structure	Warnings and notes on programming Verifying the utilized software components based on Annex 1 of Certification Report	Sections 7.1, 7.2, 7.6 Annex 1 of Certification Report	

Phase	Requirement/Rule	Reference	Check
Inserting the CFC charts	Rules for the CFC charts of the safety program	Sections 7.2.4 ff, 7.3, 7.7	
Inserting F-Runtime groups	Rules for F-Runtime groups of the safety program	Sections 7.2.7, 7.3	
Defining F-Shutdown groups	Rules for F-Shutdown groups of the safety program	Section 7.2.8	
Inserting and interconnecting the F blocks	Rules for F blocks	Section 7, Appendix A	
	Rules for F-Channel drivers and module drivers	Section 8	
	Rules for interconnecting the F-block F_CYC_CO	Section 7.2.3 *SM*, Appendix A	
	Rules for safety-related communication between F-CPUs	Section 9	
	Configuring the F-Monitoring times	Section 7.2.3, Appendix A.6 *SM*, Appendix A	
	Startup characteristics	Section 7.5	
	Creating F block types	Section 7.7	
	Passivation and reintegration	Sections 8.3, 8.4	
	Data exchange between F-Shutdown groups	Section 7.8	
	Data exchange with standard user program	Section 7.9	
	Changing F-parameters from one OS	Section 10	
	User acknowledgment	Section 7.10	
Compiling the safety program	Rules for compiling	Section 12.1	
Installation			
Hardware configuration	Rules for mounting Rules for wiring	Section 14.2 *F-SMs manual*, sections 5, 6 *ET 200S manual*, sections 3, 4 *ET 200SP manual*, Basic information *HB ET 200SP HA* *ET 200pro manual*, sections 2, 3 *ET 200eco manual*, sections 3, 4 *ET 200iSP manual,* section 4	
Commissioning, Testing			
Powering up	Rules for commissioning (in standard case)	Manual for Standard S7-400(H)	
Downloading the safety program	Rules for downloading	Sections 12.6, 12.8	
Testing the safety program	Rules for deactivating safety mode Rules for testing the safety program	Sections 12.5.1, 12.7	
Changing the safety program	Rules for deactivating safety mode	Section 12.5.1	
	Rules for changing the safety program	Sections 12.3, 12.8	

Phase	**Requirement/Rule**	**Reference**	**Check**
Check of safety-related parameters	Rules for configuration	Sections 12.4, 11 *F-SMs manual*, sections 4, 9, 10 *ET 200S manual*, sections 2.4, 7 *ET 200SP manual*, Basic information *HB ET 200SP HA* *ET 200pro manual*, sections 2.4, 8 *ET 200eco manual*, sections 3, 8 *ET 200iSP manual,* section 2.4	
Acceptance test	Rules and notes on the acceptance test Generating printouts	Section 13	
Operation, Maintenance			
General operation	Notes on operation	Section 14	
Access protection		Section 6	
Diagnostics	Responses to faults and events	Appendix A	
Replacement of software and hardware components	Rules for module replacement Rules for updating the operating system of the F-CPU - same as for standard system Rules for updating software components Notes on IM operating system update Notes on preventive maintenance	Section 14.2, Manual for Standard S7-400(H)	
Removing, disassembly	Notes for removing software components Notes for disassembling modules	Sections 4.2, 14.2	

Requirements for virtual environments and remote access C

C.1 Summary

SIMATIC S7 F/FH Systems with S7 F Systems V6.0 and higher and Safety Matrix V6.1 SP1 and higher enable use in virtual environments for ES and OS under the following conditions.

All restrictions and notes in the corresponding releases of S7 F Systems and Safety Matrix, as well as of STEP 7 and PCS 7 continue to be valid for virtual environments and remote access.

Virtual environments

In information technology, a virtual machine refers to the emulation of a real computer system (hardware) on an abstraction layer which can execute multiple virtual machines at the same time. The abstraction layer is known as a hypervisor. Well-known manufacturers are Microsoft (Microsoft Hyper-V), VMware (VMware vSphere Hypervisor (ESXi)) and Citrix (XenServer).

A virtual environment enables, for example, very convenient test environments, simplifies the transfer of systems and saves space.

Remote Access and Control

In information technology, "remote access" designates the takeover of a graphical user interface and can be employed for different types of access. In this document, "remote access" refers to the unique access to the graphical user interface and the transfer of keyboard actions and mouse movements of an Engineering Station or Operator Station. Well-known software products include Microsoft Remote Desktop Protocol (RDP) and the RealVNC Open Source Software VNC (RFC 6143).

Recommended software requirements

SIMATIC STEP 7 and PCS 7 are released for virtual environments and remote access and can be integrated in your plant under the environment descriptions linked here.

Products	Product news
PCS 7 V9.0 SP1 and higher: • VMware vSphere V6.5	Industry Online Support, entry ID 109755764 (https://support.industry.siemens.com/cs/ww/en/view/109755764)
Service Pack 4 for STEP 7 V5.5 and higher*1): • VMware vSphere Hypervisor ESX(i) 5.5 • VMware Workstation 10.0 • VMware Player 5.02 • Microsoft Windows Server 2012 Hyper-V	Industry Online Support, entry ID 93842005 (https://support.industry.siemens.com/cs/ww/en/view/93842005)

[*1] Only configuration, programming and operation in STEP 7 Engineering.

Note

Siemens provides preconfigured virtualization solutions with its "SIMATIC Virtualization as a Service".

For more information, see the following entry: Industry Online Support, entry ID 3095 (https://support.industry.siemens.com/sc/ww/en/sc/3095)

C.2 Configuration and operation

C.2.1 Virtual environments

⚠ WARNING

Using virtual environments on ES/OS

Note that a HYPERVISOR or the client software of a HYPERVISOR is not permitted to perform functions that reproduce recorded frame sequences with correct time behavior on a network with connected plants.

Ensure that this is the case when using the following functions, for example:

- Reset of captured states (snapshots) of the virtual machine (VM)
- Suspending and resuming the VM (suspend & resume)
- Replay of recorded sequences in the VMs (replay)
- Moving of VMs between hosts in productive operation (e.g. Fault Tolerance (FT))
- Digital twins of VMs in the virtual environment

If in doubt, disable these functions in the settings (HYPERVISOR administrator console).

FSW-301

Note

How do you use VMware vSphere Client to assign operator permissions for a virtual machine?

Industry Online Support, entry ID 90142228 (https://support.industry.siemens.com/cs/ww/en/view/90142228)

Note

How do you use a controller to load from a VM (VMware Player/Workstation) via a PROFIBUS/MPI CP connected via PCI or PCIe?

Industry Online Support, entry ID 100450795 (https://support.industry.siemens.com/cs/ww/en/view/100450795)

Note

Configure Hyper-V for Role-based Access Control

https://technet.microsoft.com/en-us/library/dd283076(v=ws.10).aspx (https://technet.microsoft.com/en-us/library/dd283076(v=ws.10).aspx)

C.2.2 Remote Access and Control

⚠ WARNING

Remote access from higher-level control room and Engineering Center

Make sure that the plants are clearly distinguished from other accessible plants connected on the network before you start making changes or start operation.

Examples:

- Specify optical distinguishing marks (plant designation) at your operator stations.
- The pair of numbers for SAFE_ID1 and SAFE_ID2 with SDW must be unique for all the plants accessible in the network.
- Specify unique descriptions for title and project in the properties of the Safety Matrix for all the plants connected on the network and check this before starting operation.
- Specify Active Directory access limitations in the corporate directory service and use SIMATIC Logon for accessing projects and for logging on to operator stations.

FSW-302

⚠ WARNING

The "S7 F Systems HMI" and "Safety Matrix Viewer" functionality makes changes in the safety program during RUN mode.

As a result, the following additional safety measures are required:

- Make sure that operations that could compromise plant safety cannot be carried out. You can use the EN_SWC and EN_CHG input for this purpose, for example, by controlling it with a key-operated switch or on a process-specific basis via the safety program.
- Make sure that only authorized persons can carry out operations.
  Examples:
  - Control the EN_SWC or EN_CHG input with a key-operated switch.
  - Control the EN_SWC or EN_CHG input with separate key-operated switches.
  - Set up access protection at operator stations where process operation can be performed.

FSW-303

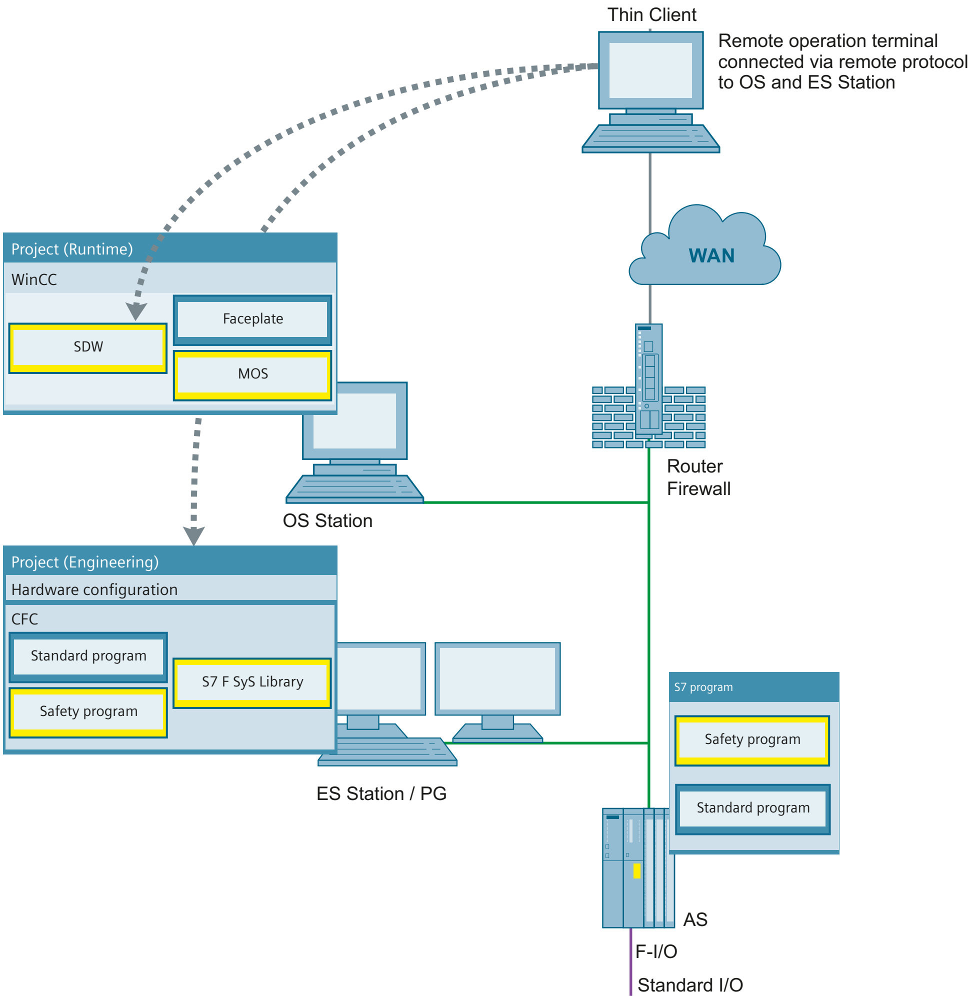
Carefully choose the persons who may have remote access to the plant and authorize them accordingly:

- Locally on the target computer "Remote Desktop User" (Workgroups)
  OR
- In the Active Directory, and inherit permissions to the target computer "Remote Desktop User" (Domain).

As required, make a distinction in the WinCC authorizations between:

- Process control
- Higher process control
- Safety application control (SIF)

Figure C-1: Diagram of Engineering Station and Operator Station in projects with safety applications



ES station

Table 1: Explanation of Figure C-1

Physical location	Installed software
At the same location as the AS station and connected to the plant/terminal bus.	SIMATIC PCS 7 (package: PCS 7 Engineering) or STEP 7

OS station

Table 2: Explanation of Figure C-1

Physical location	Installed software
At the same location as the AS station and connected to the plant/terminal bus.	SIMATIC PCS 7 (package: OS Client or OS Single Station)

Thin Client

Table 3: Explanation of Figure C-1

Physical location	Installed software
Not at the same location as the AS station and not connected to the plant bus.	No SIMATIC software installed.

Note

SIMATIC Process Control System PCS 7 - PC Configuration (V9.0 SP1) - Section 5.8.2

Industry Online Support; entry ID 109754983 (https://support.industry.siemens.com/cs/ww/en/view/109754983)

Note

Whitepaper; Security concept PCS 7 and WinCC - Basic document

Industry Online Support; entry ID 60119725 (https://support.industry.siemens.com/cs/ww/en/view/60119725)

Note

How do you access WinCC and PCS 7 plants with "RealVNC"?

Industry Online Support, entry ID 55422236 (https://support.industry.siemens.com/cs/ww/en/view/55422236)

Note

IP-based Remote Networks

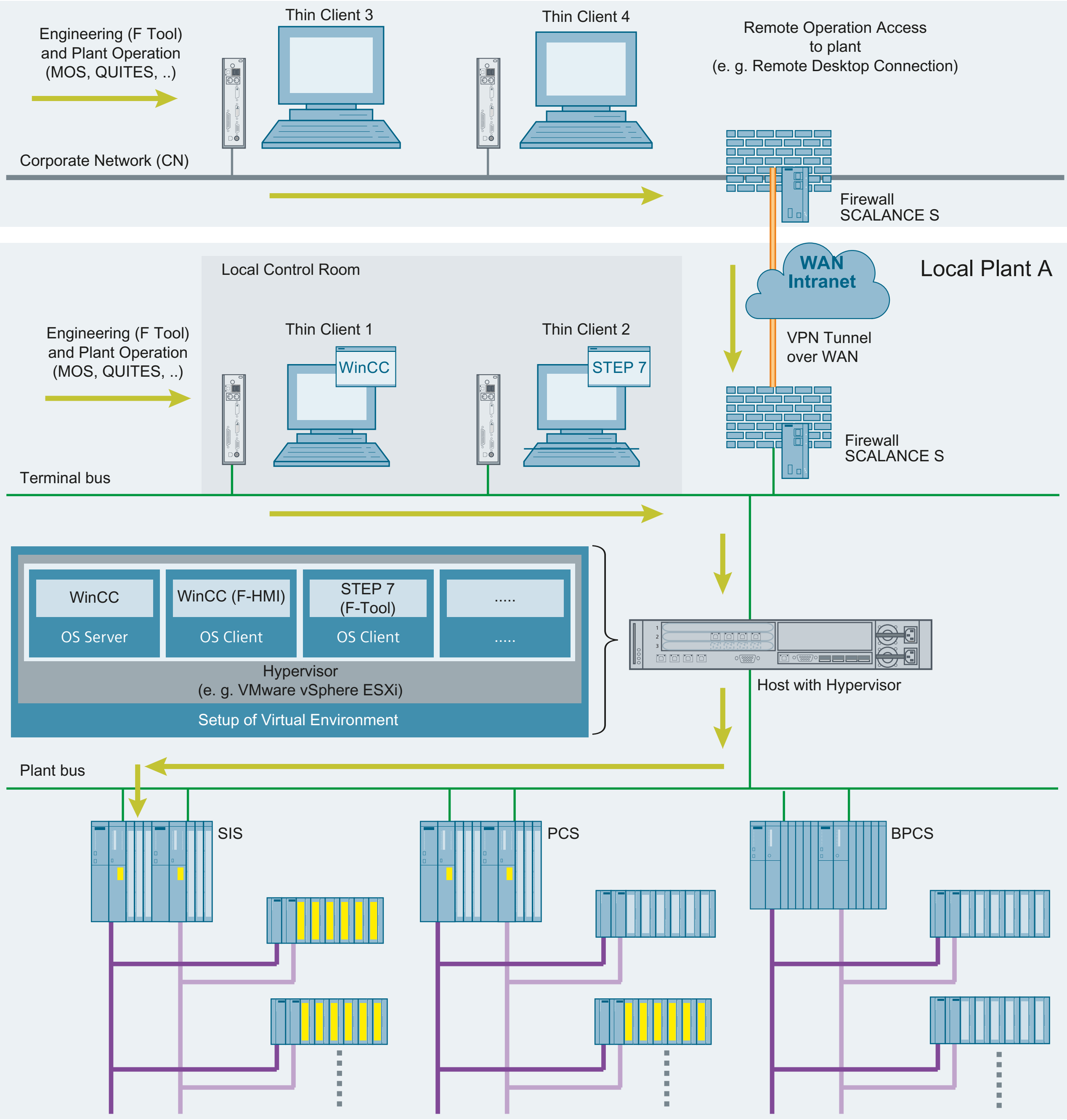
Industry Online Support, entry ID 26662448 (https://support.industry.siemens.com/cs/ww/en/view/26662448)

C.3 Examples of valid configurations in PCS 7

C.3.1 Example 1

The following figure shows a virtual environment for engineering and plant operation of safety applications including remote control.

Figure C-2:



C.3.2 Example 2

The following figure shows a configuration for remote access for configuration and maintenance operations as well as plant operation from higher-level control room in real and virtual environments.

Figure C-3a:

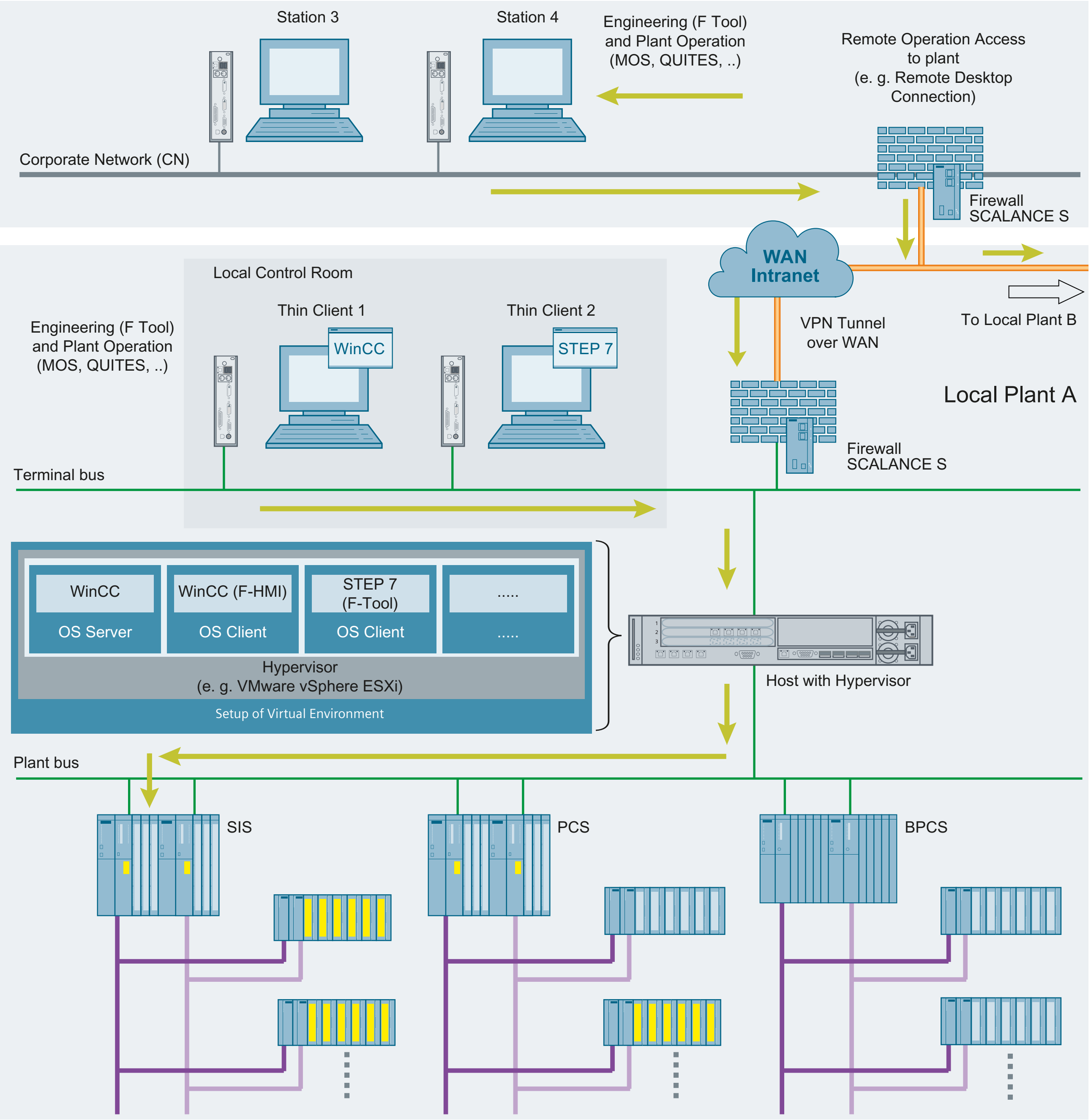
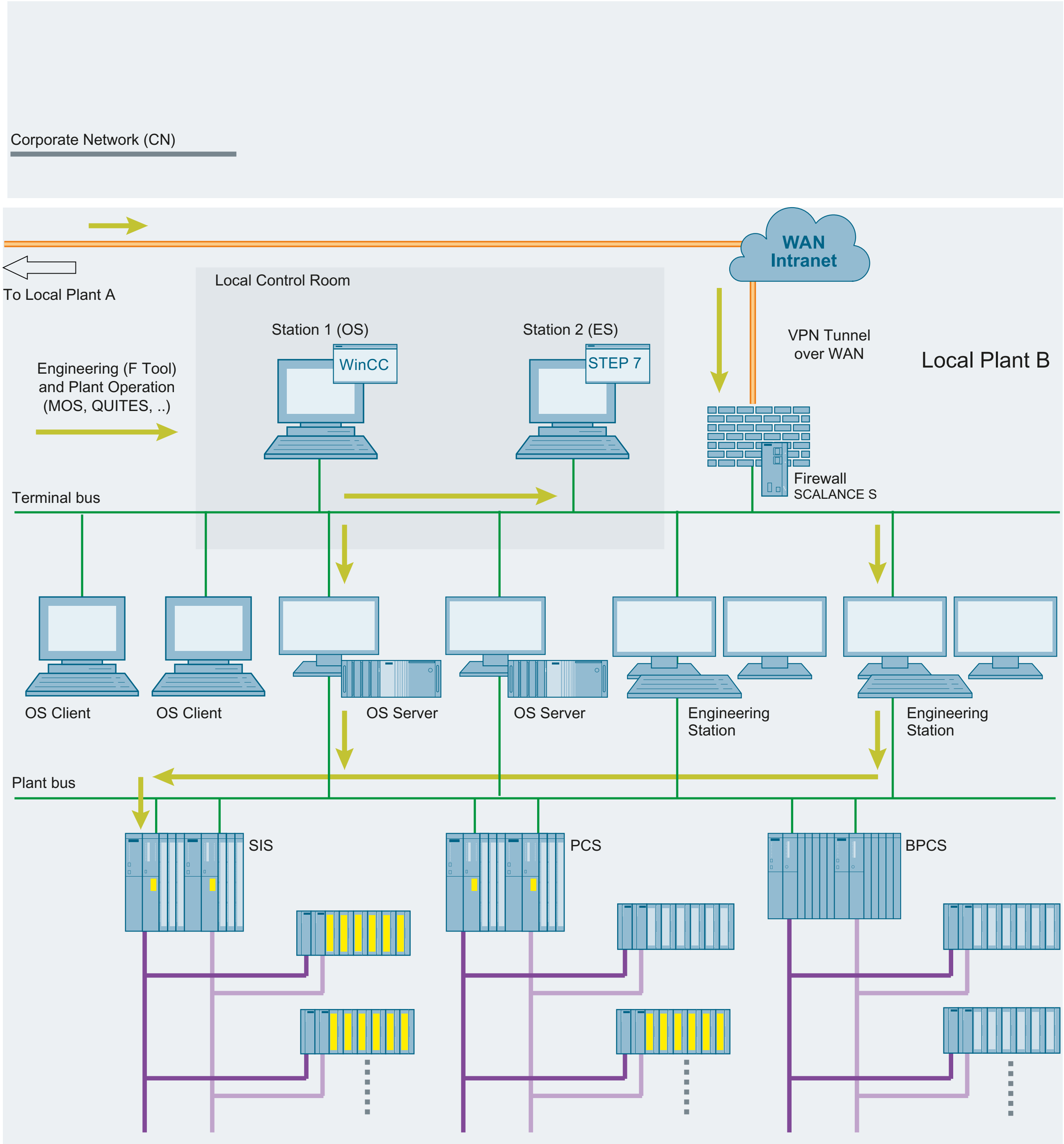


Figure C-3b:


Corporate Network (CN)
WAN
Intranet
To Local Plant A
Local Control Room
Station 1 (OS)
Station 2 (ES)
WinCC
STEP 7
VPN Tunnel
over WAN
Local Plant B
Engineering (F Tool)
and Plant Operation
(MOS, QUITES, ..)
Firewall
SCALANCE S
Terminal bus
OS Client
OS Client
OS Server
OS Server
Engineering
Station
Engineering
Station
Plant bus
SIS
PCS
BPCS

C.4 Abbreviations and explanations of terms

Abbreviation	Explanation of term
AD	Active Directory
BPCS	Basic Process Control System
CN	Corporate Network (company network/intranet)
ES	Engineering Station
LCR	Local Control Room
LER	Local Engineering Room
MOS	Maintenance Override Switch
OS	Operator Station
PCS	Process Control System
QUITES	Acknowledgment via ES/OS
ROC	Remote Operation Center (higher-level control than LCR)
SDW	Safety Data Write
SIF	Safety Instrumented Function
SIS	Safety Instrumented System
SWC++	Secure Write Command++
VM	Virtual Machine (guest operating system)
WAN	Wide Area Network

C.5 References

	Subject area	Link
\1\	SIMATIC Industrial Software Safety Engineering in SIMATIC S7	Industry Online Support, entry ID 12490443 (https://support.industry.siemens.com/cs/ww/en/view/12490443)
\2\	SIMATIC Industrial Software S7 F/FH Systems - Configuring and Programming	Industry Online Support, entry ID 109742100 (https://support.industry.siemens.com/cs/ww/en/view/109742100)
\3\	SIMATIC Industral Software Safety Matrix	Industry Online Support, entry ID 109766685 (https://support.industry.siemens.com/cs/ww/en/view/109766685)
\4\	SIMATIC PCS 7 technical documentation	Overview page of the "SIMATIC PCS 7 Technical Documentation" (http://w3.siemens.com/mcms/industrial-automation-systems-simatic/en/manual-overview/tech-doc-pcs7/Pages/Default.aspx)
\5\	SIMATIC PCS 7 OS Software Client V7.1 + SP2 and higher released for use in virtual operating environments	Industry Online Support, entry ID 51401737 (https://support.industry.siemens.com/cs/ww/en/view/51401737)
\6\	SIMATIC Virtualization as a Service	Industry Online Support, entry ID 109768788 (https://support.industry.siemens.com/cs/ww/en/view/109768788)
\7\	VMware vSphere Documentation V5.5	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html (https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html)
\8\	Microsoft Hyper-V	https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview (https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview)
\9\	XenServer Documentation	https://docs.citrix.com/en-en/citrix-hypervisor (https://docs.citrix.com/de-de/citrix-hypervisor)

Glossary

1oo1 evaluation

Type of sensor evaluation: For 1oo1 evaluation, a non-redundant sensor is connected via one channel to the F-I/O.

1oo2 evaluation

Type of sensor evaluation: In the case of 1oo2 evaluation, two input channels are occupied either by one two-channel sensor or by two single-channel sensors. The input signals are compared internally for equivalence or non-equivalence.

Access protection

Fail-safe systems must be protected against dangerous, unauthorized access. Access protection for F-systems is implemented by assigning two passwords (for the F-CPU and for the safety program).

Bypass

Bypass function that is normally used for maintenance purposes (e.g., for checking effect logic, replacing a sensor).

Category

Category according to ISO 13849-1:2015 or EN ISO 13849-1:2015

S7 F systems can be used in safety mode up to Category 4.

Channel fault

Channel-specific fault, such as a wire break or a short-circuit

Collective signatures

Collective signatures uniquely identify a specific state of the safety program. They are important for the preliminary acceptance test of the safety program, e.g., by experts.

CRC

Cyclic Redundancy Check, see CRC signature

CRC signature

The validity of the process values in the safety message frame, the accuracy of the assigned address references, and the safety-related parameters are validated by means of the CRC signature in the safety message frame.

Deactivated safety mode

Deactivated safety mode is the temporary deactivation of the safety mode for test purposes, commissioning, etc.

Whenever safety mode is deactivated, the safety of the plant must be ensured by other organizational measures, such as monitored operation and manual safety shutdown.

Depassivation

See reintegration

Discrepancy time

Assignable time for the discrepancy analysis. If the discrepancy time is set too high, the fault detection time and fault reaction time are extended unnecessarily. If the discrepancy time is set too low, availability is decreased unnecessarily because a discrepancy error is detected when, in reality, no error exists.

ES

Engineering Station (ES): Configuration system that enables convenient, visual adaptation of the process control system to the task at hand.

Fail-safe DP standard slaves

Fail-safe DP standard slaves are standard slaves that are operated on PROFIBUS with the DP protocol. They must comply with the IEC 61784-1:2019 CP 3/1 standard and the PROFIsafe bus profile. A GSD file is used for your configuration.

Fail-safe I/O modules

I/O modules that can be used for safety-related operation (see safety mode). These modules are equipped with integrated safety functions. They behave according to IEC 61784-1:2019 CP 3/1 and the PROFIsafe bus profile.

Fail-safe IO standard devices

Fail-safe IO standard devices are standard devices that are operated on PROFINET IO.

A GSDML file is used to configure them.

Fail-safe modules

ET 200S modules that can be used for safety-related operation (see also safety mode) in the ET 200S or ET 200pro distributed I/O system. These modules are equipped with integrated safety functions. They behave according to IEC 61784-1:2019 CP 3/1 and CP 3/3 standard and the PROFIsafe bus profile.

Fail-safe PA field devices

Fail-safe PA field devices are field devices that are operated on PROFIBUS with the PA protocol. They must comply with the IEC 61784-1:2019 CP 3/2 standard and the PROFIsafe bus profile. A GSD file is used for their configuration.

Fail-safe systems

Fail-safe systems (F-systems) are characterized by remaining in a safe state or immediately assuming another safe state when specific failures occur.

Fault reaction function

See user safety function

F-block type

F-block types are ready-made program sections that can be used in a CFC chart (e.g., fail-safe multiplexer F_MUX2_R, etc.). Block instances are generated on insertion. Any number of block instances can be created by one F-block type.

The F-block type specifies the characteristics (algorithm) for all applications of this type. The name of the F-block type is specified in the symbol table.

F-blocks

The following blocks are designated as F-blocks:

- Blocks selected by the user from an F-library.
- Blocks that are automatically added in the safety program.

F-CPU

An F-CPU is a central processing unit with fail-safe capability that is permitted for use in S7 F Systems. For S7 F-systems, the F-runtime license allows the user to operate the central module as an F-CPU. That is, a safety program can be run on it. A standard user program can also be run in the F-CPU.

F-Cycle time

Cyclic interrupt time for OBs with F-runtime groups

F-Data type

The standard user program and safety program use different data formats. Safety-related F-Data types are used in the safety program.

F-I/O

Group designation for fail-safe inputs and outputs available in SIMATIC S7 for integration in S7 F Systems, among others.

You can find additional information on the fail-safe I/Os available for S7 F Systems in the section "Overview of configuration".

F-Runtime group

When the safety program is created, the F-blocks cannot be inserted directly into tasks/OBs; rather, they must be inserted into F-runtime groups. The -> safety program consists of multiple F-Runtime groups.

F-shutdown groups

F-shutdown groups contain one or more F-runtime groups. F-runtime group communication blocks between the F-blocks in various F-runtime groups, all of which are assigned to one F-shutdown group, are not required. If an error is detected in an F-shutdown group, this F-shutdown group is shut down. Additional F-shutdown groups are shut down according to the configuration of F_SHUTDN.

F-SMs

S7-300 fail-safe signal modules that can be used for safety-related operation (see safety mode) as centralized modules in an S7-300 or as distributed modules in the ET 200M distributed I/O system. F-SMs are equipped with integrated safety functions.

F-Startup

An F-Startup is a restart following an F-STOP or an F-CPU STOP. S7 F Systems do not distinguish between a cold restart and warm restart of the F-CPU.

F-Systems

Fail-safe systems

Full shutdown

All F-blocks of the entire F-CPU are shut down. Initially, the F-Shutdown group in which the error was detected is shut down. All other F-Shutdown groups are then shut down within a period of time equal to twice the F-Monitoring time you assigned for the slowest OB.

Master-reserve switchover

In S7 FH Systems, a master/reserve switchover is triggered when the master goes to F-STOP mode. That is, the system switches from the master CPU to the reserve CPU.

Module redundancy

The module and a second identical module are operated in redundant mode in order to enhance availability.

OS

Operator Station (OS): A configurable operator station used to operate and monitor machines and systems.

Partial shutdown

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

Passivation

Passivation of digital output channels means that the outputs are de-energized.

Digital input channels are passivated when the inputs transmit a value of "0" to the F-CPU (by means of the fail-safe drivers), irrespective of the current process signal.

Analog input channels are passivated when the inputs transmit a fail-safe value or the last valid value to the F-CPU (by means of the fail-safe drivers), irrespective of the current process signal.

Process safety time

The process safety time of a process is the time interval during which the process can be left on its own without risk to life and limb of the operating personnel or damage to the environment.

Within the process safety time, any type of F-system process control is tolerated. That is, during this time, the F-system can control its process incorrectly or it can even exercise no control at all. The process safety time depends on the process type and must be determined on a case-by-case basis.

PROFIsafe

Safety-related bus profile of PROFIBUS DP/PA and PROFINET IO for communication between the safety program and the F-I/O in an F-system.

Proof-test interval

Period after which a component must be forced to fail-safe state, that is, it is either replaced with an unused component, or is proven faultless.

Redundancy, availability-enhancing

Multiple instances of components with the goal of maintaining component function even in the event of hardware faults.

Redundancy, safety-enhancing

Multiple availability of components with the focus set on exposing hardware faults based on comparison; for example, 1oo2 evaluation in fail-safe signal modules.

Reintegration

Switchover from fail-safe values (0) to process data (reintegration of an F-I/O module) occurs automatically or, alternatively, only after user acknowledgment at the F-Channel driver.

The reintegration method depends on the following:

- Cause of passivation of the F-I/O/the F-I/O channels
- Parameter assignment of the F-channel driver

For an F-I/O with inputs, the process values pending at the fail-safe inputs are provided again at the output of the F-Channel driver after reintegration. For an F-I/O with outputs, the F-System again transfers the output values pending at the input of the F-Channel driver to the fail-safe outputs.

S7 F Systems RT License (Copy License)

Formal authorization for use of the CPU as an F-CPU for S7 F/FH Systems.

S7 PLCSIM

S7-PLCSIM allows you to execute and test your S7 program on a simulated automation system on your ES/OS. Because the simulation takes place entirely in STEP 7, you do not require any hardware (CPU, F-CPU, I/O).

Safe state

The basic principle of the safety concept in a fail-safe system is the existence of a safe state for all process variables. For the digital F-I/O, the safe state is always "0".

Safety class

Safety level (Safety Integrity Level) SIL according to IEC 61508. The higher the Safety Integrity Level, the stricter the measures for prevention of systematic faults and for management of systematic faults and random hardware failures.

S7 F Systems can be used in safety mode up to safety class SIL3.

Safety function

Safety function is a mechanism integrated in F-CPU and F-I/O, which enables them to be used in fail-safe systems.

According to IEC 61508, the function is implemented by a safety device in order to maintain the system in a safe state or to place it into a safe state in the event of a particular fault (see also user safety function).

Safety message frame

In the safety mode, data is transferred in a safety message frame between the F-CPU and the F-I/O or, in safety-related CPU-to-CPU communication, between the F-CPUs.

Safety mode

1. An operating mode for F-I/Os in which safety-oriented communication using safety message frames is possible.
2. Operating mode of the safety program. In safety mode of the safety program, all safety mechanisms for fault detection and fault reaction are activated. In safety mode, the safety program cannot be modified during operation. Safety mode can be deactivated by the user (see deactivated safety mode).

Safety program

Safety-related user program

Safety protocol

See safety message frame

Safety-related communication

Communication used to exchange fail-safe data.

Sensor evaluation

There are two types of sensor evaluation:

- 1oo1 evaluation – sensor signal is read in once
- 1oo2 evaluation – the sensor signal is read twice by the same F-I/O and compared internally

Signature

See collective signatures

SIMIT

SIMIT enables comprehensive tests of automation projects and virtual commissioning of systems, machines and processes on one platform. In addition, the simulation platform can be used for realistic training environments to train the operating personnel.

Standard communication

Communication used to exchange non-safety-related data.

Standard mode

Operating mode of the F-I/O in which only standard communication, but no safety-oriented communication via safety message frames is possible.

Standard user program

Non-safety-related user program

User safety function

The safety function for the process can be provided through a user safety function or a fault reaction function. The user only has to program the user safety function. If the F-system is unable to perform the actual user safety function in the event of a fault, it performs instead the fault response function, e.g. the associated outputs are switched off and the F-CPU enters the STOP state.

Value status (Qualifier bit)

A value status bit (Qualifier bit) exists for each input/output channel of a module in the associated input address space.

Regardless of the diagnostics enables, each value status provides information about the validity of the corresponding process value at the input/output channel.

Index