SIEMENS

SIMATIC

Industrie Software
Safety Engineering in SIMATIC S7

System Manual

12/2008
A5E00109529-06

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
with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION
without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE
indicates that an unintended result or situation can occur if the corresponding information is not taken into account.

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 device/system may only be set up and used in conjunction with this documentation. Commissioning and operation of a device/system may only be performed by **qualified personnel**. Within the context of the safety notes in this documentation qualified persons are defined as persons who are authorized to commission, ground and label devices, systems and circuits in accordance with established safety practices and standards.

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 adhered to. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of the 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
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E00109529-06
℗ 01/2009

Preface

Purpose of the System Manual

This system manual provides an overview of the S7 Distributed Safety and S7 F/FH Systems fail-safe automation systems. It identifies the similarities and differences between S7 Distributed Safety and S7 F/FH Systems and presents detailed technical information applicable to both S7 Distributed Safety and S7 F/FH Systems.

The system manual helps you to decide which fail-safe system is best suited for your automation task. It is intended as starting information for decision makers and as a source of technical information on S7 Distributed Safety and S7 F/FH Systems fail-safe automation systems for service and commissioning personnel (e.g., detailed information on monitoring and response times of S7 Distributed Safety and S7 F/FH Systems is provided in the appendix).

Scope of the System Manual

This system manual is valid for the fail-safe S7 Distributed Safety and S7 F/FH systems.

In addition, this system description addresses integration of the following fail-safe I/O devices in S7 Distributed Safety and S7 F/FH Systems:

- S7-300 fail-safe signal modules
- ET 200S fail-safe modules
- ET 200pro fail-safe modules
- ET 200eco fail-safe I/O module
- Fail-safe DP standard slaves / I/O standard devices / PA field devices

The system manual describes current product versions dated 03/2008. If there is any uncertainty, the product information provided in more recent documents shall override the information provided in this system manual.

What's new?

The following table summarizes the most important technical changes in the add-on packages *S7 Distributed Safety V 5.4 SP4* and *S7 F Systems V6.0*. These changes have been taken into account in this system manual.

Technical Change	Change affects	
	S7 Distributed Safety	S7 F/FH Systems
Support of new F-CPUs	x	x
Support of new F I/O for S7-300, ET 200M, ET 200S and ET 200pro	x	x
Support of fail-safe PA field devices	-	x
Communication between F-Shutdown groups	-	x
Safety-related communication between I/O controllers	x	-
Safety-related communication between S7 Distributed Safety and S7 F/FH systems	x	x
F I/O access and safety-related communication communication via WLAN to IEEE 802.11	x	x
New F-Library blocks	x	x

Position in the Information Landscape

Depending on your application, you will need the documentation listed below when working with S7 Distributed Safety or S7 F/FH Systems:

References to this documentation are included in the system manual where appropriate.

Documentation	Brief Description of Relevant Contents
For the fail-safe system S7 F/FH Systems	• The Programming and Operating Manual "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) describes: • Configuration of the fail-safe CPU and of the fail-safe I/O • Programming of the F-CPU in CFC
	• The "S7-400 Automation System, Installation (http://support.automation.siemens.com/WW/view/en/1117849) installation manual describes the installation and wiring of S7-400 systems. • The "S7-400H Automation System, Fault-tolerant Systems" (http://support.automation.siemens.com/WW/view/en/1186523/) manual describes the CPU 41x-H central processing unit and the tasks involved in setting up and commissioning a fault-tolerant S7-400H system. • The "CFC for S7, Continuous Function Chart" (http://support.automation.siemens.com/WW/view/en/21401430) manual/online help provides a description of programming with CFC. • The "Safety Matrix" (http://support.automation.siemens.com/WW/view/en/19056619) configuration manual / online help describes the creation of safety programs for fail-safe S7 F/FH systems by means of cause-effect matrix.

Documentation	Brief Description of Relevant Contents
For the fail-safe system S7 Distributed Safety	The "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) Programming Manual / Online Help describes: • Configuration of the F-CPU and the F-I/O • Programming of the F-CPU in F-FBD or F-LAD
	Depending on which F-CPU you are using, you will need the following documentation: • The "S7-300, CPU 31xC and CPU 31x: Installation" (http://support.automation.siemens.com/WW/view/en/13008499) Operating Instructions describe the installation and wiring of S7-300 systems. • The "CPU 31xC and CPU 31x, Technical Data" (http://support.automation.siemens.com/WW/view/en/12996906) product manual describes the CPUs 315-2 DP and PN/DP and the CPUs 317-2 DP and PN/DP. • The "S7-400 Automation System, Installation (http://support.automation.siemens.com/WW/view/en/1117849) installation manual describes the installation and wiring of S7-400 systems. • The "S7-400 Automation System, CPU Data" (http://support.automation.siemens.com/WW/view/en/23904550) Reference Manual describes the CPU 416-2 and CPU 416F-3 PN/DP. • The "ET 200S Interface Module IM 151-7 CPU" (http://support.automation.siemens.com/WW/view/en/12714722) manual describes the IM 151-7 CPU. • The "ET 200S, Interface Module IM 151-8 PN/DP CPU" (http://support.automation.siemens.com/WW/view/en/29738847) manual describes the IM 151-8 PN/DP CPU. • Each F-CPU that can be used has its own product information. The product information only describes the deviations from the respective standard CPUs.
Hardware installation and operating manual "S7-300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151)	Describes the hardware of the S7-300 fail-safe signal modules (including installation, wiring, and technical specifications)
Operating instructions "ET 200S Distributed I/O System - Fail-Safe Modules" (http://support.automation.siemens.com/WW/view/en/12490437)	Describes the hardware of the ET 200S fail-safe modules (including installation, wiring, and technical specifications)
Operating instructions "ET 200pro Distributed I/O System, Fail-safe Modules" (http://support.automation.siemens.com/WW/view/en/22098524)	Describes the hardware of the ET 200pro fail-safe modules (including installation, wiring, and technical specifications)

Documentation	Brief Description of Relevant Contents
Manual "ET 200eco Distributed I/O Device, Fail-safe I/O Module" (http://support.automation.siemens.com/WW/view/en/19033850)	Describes the hardware of the ET 200eco fail-safe signal module (including installation, wiring, and technical specifications)
STEP 7 manuals	• The "Configuring hardware and connections in STEP 7 V5.x" (http://support.automation.siemens.com/WW/view/en/18652631) manual describes how to use the corresponding standard tools of *STEP 7*. • The "LAD for S7-300/400" (http://support.automation.siemens.com/WW/view/en/18654395) manual describes how to use the corresponding standard tools of *STEP 7*. • The "FBD for S7-300/400" (http://support.automation.siemens.com/WW/view/en/18652644) manual describes how to use the corresponding standard tools of *STEP 7*. • The "System Software for S7-300/400 System and Standard Functions" (http://support.automation.siemens.com/WW/view/en/1214574) Reference manual describes access / diagnostics functions of the distributed I/O / CPU. • The "Programming with STEP 7 V5.x" (http://support.automation.siemens.com/WW/view/en/18652056) describes programming procedures in *STEP 7*.
STEP 7 online help	• Describes the operation of *STEP 7* standard tools • Contains information about how to configure and assign parameters for modules and intelligent slaves with *HW Config* • Contains a description of the FBD and LAD programming languages
System Manual "PROFINET System Description" (http://support.automation.siemens.com/WW/view/en/19292127)	• Describes the basics for PROFINET IO
PCS 7 manuals	• Describe operation of the *PCS 7* process control system (necessary when the F-System is integrated in a higher-level control system)

The complete collection of SIMATIC S7 documentation is available on CD-ROM.

Guide

The system manual covers the following topics:

- Overview of fail-safe automation systems in general, and in SIMATIC S7, in particular
- Comparison of System Performance of S7 Distributed Safety and S7 F/FH Systems
- Description of the configuration variants for S7 Distributed Safety and S7 F/FH Systems
- Information to help you decide which F-System represents the best solution for your requirements
- Comparison of the similarities and differences between the communication options for S7 Distributed Safety and S7 F/FH Systems
- Overview of the safety mechanisms in S7 Distributed Safety and S7 F/FH Systems that are apparent to the user
- Standards upon which the S7 Distributed Safety and S7 F/FH Systems F-Systems are based
- Overview of configuring S7 Distributed Safety and S7 F/FH Systems
- Overview of programming S7 Distributed Safety and S7 F/FH Systems

  Configuring and programming are described in more detail in the respective programming and configuration manuals for S7 Distributed Safety and S7 F/FH Systems.
- Configuration of F-related monitoring times for F-Systems
- Calculating the maximum response time of the safety functions in S7 Distributed Safety and S7 F/FH systems

Conventions

The terms "safety engineering" and "fail-safe engineering" are used synonymously in this system manual. The same applies to the terms "fail-safe" and "F-".

"Safety program" refers to the fail-safe portion of the user program and is used instead of "fail-safe user program," "F-program," etc.

"*S7 Distributed Safety*" and "*S7 F Systems*" in italics refer to the optional packages for the two F-Systems "S7 Distributed Safety" and "S7 F/FH Systems".

Additional Support

Please contact your local Siemens representative if you have any queries about the products described in this manual.

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 (http://www.siemens.de/simatic-tech-doku-portal).

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

Training center

Siemens offers corresponding courses to help get you started with the S7 automation system. Contact your regional Training Center, or the central Training Center in D-90327 Nuremberg, Germany.

You will find more information on the Web (http://www.sitrain.com).

H/F Competence Center

The H/F Competence Center in Nuremberg offers special workshops on SIMATIC S7 fail-safe and fault-tolerant automation systems. The H/F Competence Center can also provide assistance with onsite configuration, commissioning, and troubleshooting.

For questions about workshops, etc., contact: hf-cc.aud@siemens.com

Technical Support

To contact Technical Support for all A&D products, use the Support Request Web form (http://www.siemens.com/automation/support-request).

You can find additional information about our Technical Support on the Web (http://www.siemens.com/automation/service).

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:

- Newsletters providing the latest information on your products
- Relevant documentation for your application via the search function in Service & Support
- A forum where users and experts from all over the world exchange ideas
- Our contacts database where you can find your local Automation & Drives representative
- Information about local service, repair, replacement parts, and much more.

Important Information for Preserving the Operational Safety of your System

Note

The operators of systems with safety-related characteristics must adhere to operational safety requirements. The supplier is also obliged to comply with certain actions when monitoring the product. To keep you informed, a special newsletter is therefore available containing information on product developments and properties that are important (or potentially important) for operating systems where safety is an issue. By subscribing to the relevant newsletter, you will always have the latest information and be able to make changes to your system, when necessary. Just visit us on the Web (http://www.siemens.de/automation/csi_en_WW/news).

There, you can register for the following newsletters:

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

Select the "Updates" check box for each newsletter.

Table of contents

1 Overview of Fail-safe Systems

1.1 Introduction

Objective of Safety Engineering

The objective of safety engineering is to minimize danger to humans and the environment as much as possible through use of safety-oriented technical installations without restricting industrial production and the use of machines and chemical products any more than necessary.

What are Fail-safe Automation Systems?

Fail-safe automation systems (F-systems) are used to control processes that can achieve a safe state immediately as a result of a shutdown. That is, F-systems control processes in which an immediate shutdown does not endanger humans or the environment.

Fail-safe systems go beyond conventional safety engineering to enable far-reaching intelligent systems that extend all the way to the electrical drives and measuring systems.

F-systems are used in systems with advanced safety requirements. Improved fault detection and localization in F-systems through detailed diagnostic information enables production to be resumed quickly following a safety-related interruption.

Overview

This chapter provides an introduction to safety engineering in SIMATIC S7.
S7 Distributed Safety and S7 F/FH Systems are introduced along with their areas of application. The important similarities and differences between the two fail-safe systems are also presented.
In the last part of the chapter, we introduce the user to the basic procedure to be followed when working with the fail-safe systems S7 Distributed Safety and S7 F/FH Systems.

1.2 Safety Integrated - the Integrated Safety Concept by Siemens

Safety Integrated

Safety Integrated is the integrated safety concept for automation and drives by Siemens.

Proven technologies and systems from automation engineering are used for safety engineering. Safety Integrated covers the entire chain of safety from sensors and actuators down to the controller, including safety-related communication over standard field buses.

In addition to their functional tasks, drives and controllers also take on safety tasks. A particular feature of Safety Integrated is that is ensures not only reliable safety, but also a high level of flexibility and productivity.

Safety-Related Input and Output Signals

Safety-related input and output signals form the interface to the process. This enables, for example, direct connection of single-channel and two-channel I/O signals from devices such as emergency STOP buttons or light barriers. Safety-related signals are redundantly combined internally. Safety-related input signals are read redundantly (e.g., 2 times) and compared. The unified read result is passed on to the central processing unit in a fail-safe manner for further processing. Safety-related actuators are driven based on redundant ANDing without any additional action on the part of the user. Interconnection of the inputs and outputs is also greatly simplified.
This eliminates the need for some of the individually mounted hardware switching devices, resulting in a simplified control cabinet design.

Fail-safe Distributed I/O Systems

Implementation of fail-safe distributed I/O systems allows you to replace standard safety technology with PROFIBUS DP and PROFINET IO components. This includes replacement of switching devices for emergency STOP, protective door monitors, two-hand operation, etc.

Advantages of Integrating Safety Engineering into Standard Automation Systems

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

- An automation system with integrated fail-safe engineering is more flexible than electromechanical solutions.
- Integration entails less complicated wiring solutions.
- Integration requires less engineering effort, as standard engineering tools are used for configuring and programming.
- Only one CPU is required, as safety-related sections of the program can be executed alongside standard sections in the CPU.
- Simple communication between safety-related and standard program components.

1.3 Fail-safe Systems in SIMATIC S7

What fail-safe systems are available in SIMATIC S7?

Two fail-safe systems are available for integrating safety engineering into SIMATIC S7 automation systems:

1. The **S7 Distributed Safety** system is available to implement safety concepts for machine and operator protection (e.g., for emergency STOP devices for operation of machine tools and processing machinery) and the process industry (e.g., for protection functions for instrumentation and control protective devices and burners).
2. The fail-safe and, in particular, the optional **S7 F/FH Systems** fault-tolerant automation system is well-suited for process engineering and oil industry applications.

Fail-safe and Fault-Tolerant S7 FH Systems

You can optionally set up fault-tolerant fail-safe S7 F-Systems (S7 FH systems) to increase the availability of the automation system and thereby avoid process failures caused by faults in the F-System, or at sensors and actuators. Increased availability is achieved through component redundancy (power supply, central processing unit, communication, and I/O).

Achievable Safety Requirements

S7 Distributed Safety and S7 F/FH Systems F-Systems can satisfy the following safety requirements:

- Safety class (Safety Integrity Level) SIL1 to SIL3 in accordance with IEC 61508
- Category 2 to Category 4 in accordance with EN 954-1

Principle of Safety Functions in S7 Distributed Safety and S7 F/FH Systems

Functional safety is implemented principally through safety functions in the software. Safety functions are executed by S7 Distributed Safety or S7 F/FH Systems to restore or maintain a safe state in a system when a dangerous event occurs. 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 (emergency STOP buttons, light barriers, motor control). They have all of the required hardware and software components for safe processing, in accordance with the required safety class. The user only programs 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 example, the associated outputs are deactivated, and the F-CPU switches to STOP mode, if necessary.

Example of User Safety Functions and Fault Reaction Functions

In the event of overpressure, the F-System opens a valve (user safety function). If a dangerous fault occurs in the F-CPU, all outputs are deactivated (fault reaction function), whereby the valve is opened and the other actuators also attain a safe state. If the F-System is intact, only the valve would be opened.

PROFIBUS DP or PROFINET IO with PROFIsafe bus profile

Safe communication between the safety program in the F-CPU and the fail-safe inputs and outputs takes place via the "standard" PROFIBUS DP or "standard" PROFINET IO with superimposed PROFIsafe safety profile.
The user data of the safety function plus the safety measures are transmitted within a standard data frame.

Advantages:

- Because both standard and safety-related communication takes place on the standard PROFIBUS DP or standard PROFINET IO, no additional hardware components are required.
- Safety-related communication tasks can be solved without resorting to previous conventional solutions (such as permanent wiring of emergency stop devices) or special buses. This enables safety-related distributed applications, for example in automobile chassis construction with presses and robots, burner management, passenger transportation on cable railway, and process automation.
- Fail-safe DP standard slaves can be integrated in S7 Distributed Safety and S7 F/FH Systems (sensors/actuators with bus capability and safety equipment of PROFIBUS partner companies that are DP standard slaves with characteristics based on the PROFIsafe bus profile).
- Fail-safe I/O standard devices can be integrated in S7 Distributed Safety F-Systems (sensors/actuators with bus capability and safety devices of PROFIBUS partner companies that are I/O standard devices with characteristics based on the PROFIsafe bus profile).
- Fail-safe PA field devices can be integrated in fail-safe S7 F/FH systems (field devices with characteristics based on the PROFIsafe bus profile, operated on PROFIBUS by means of PA protocol).

1.3.1 Areas of Application of S7 Distributed Safety and S7 F/FH Systems

Use of S7 Distributed Safety

Fail-safe S7 Distributed Safety systems are primarily used for machine and operator protection (e.g., for EMERGENCY-OFF equipment for operation of tooling and processing machinery) and in process control industry (e.g., for implementing protective functions for protective instrumentation and control equipment and for burners), where the safe state can be reached by shutting down the fails-safe outputs.

Integration options for S7 Distributed Safety fail-safe systems at the plant automation level are shown below.

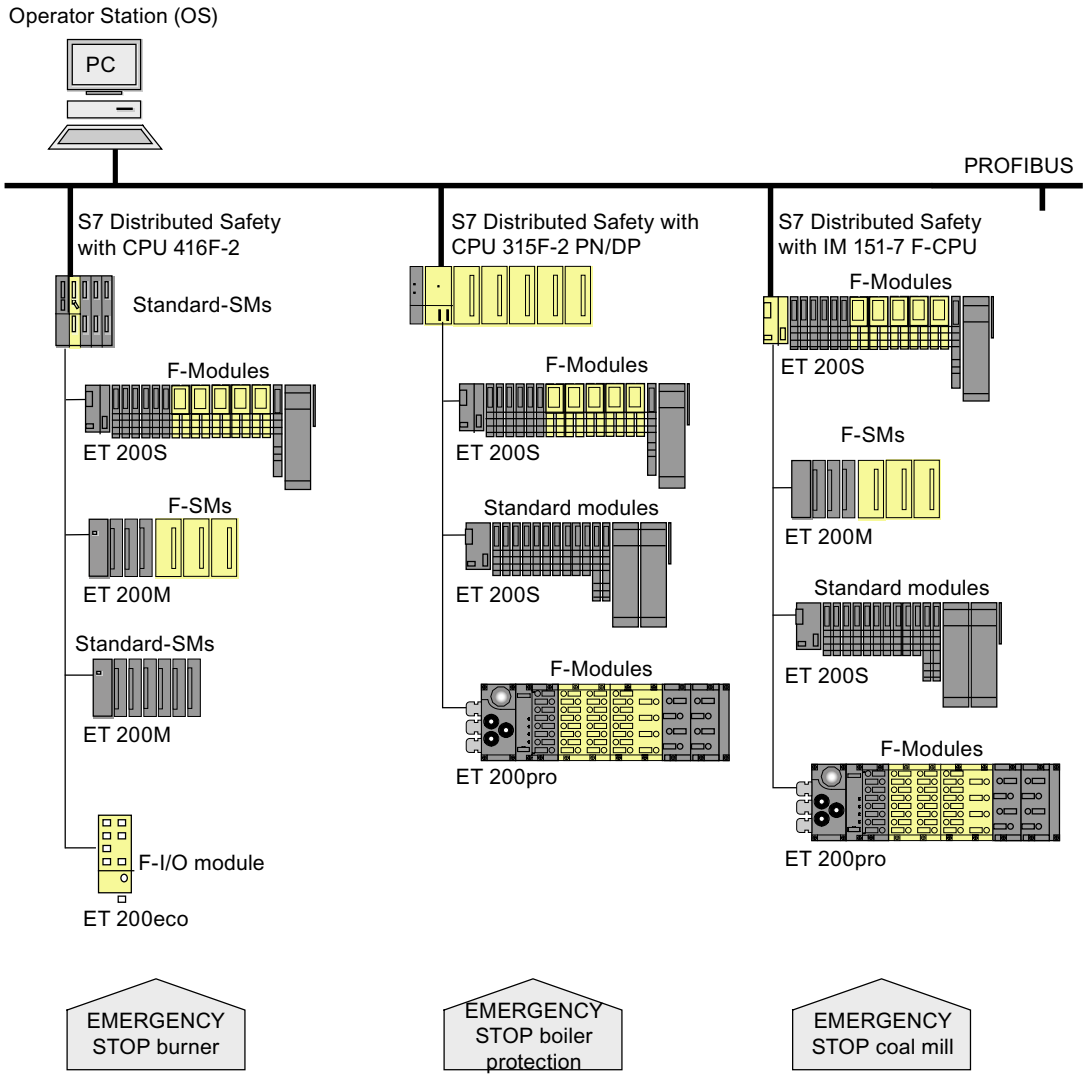


Figure 1-1 Use of S7 Distributed Safety

Use of S7 F/FH Systems

S7 F/FH Systems fail-safe systems are used primarily in process engineering and instrumentation and control applications in which a safe state can be attained by shutting down the fail-safe outputs.

Integration options for S7 F Systems and
S7 FH Systems in process automation systems using PCS 7 are shown below.

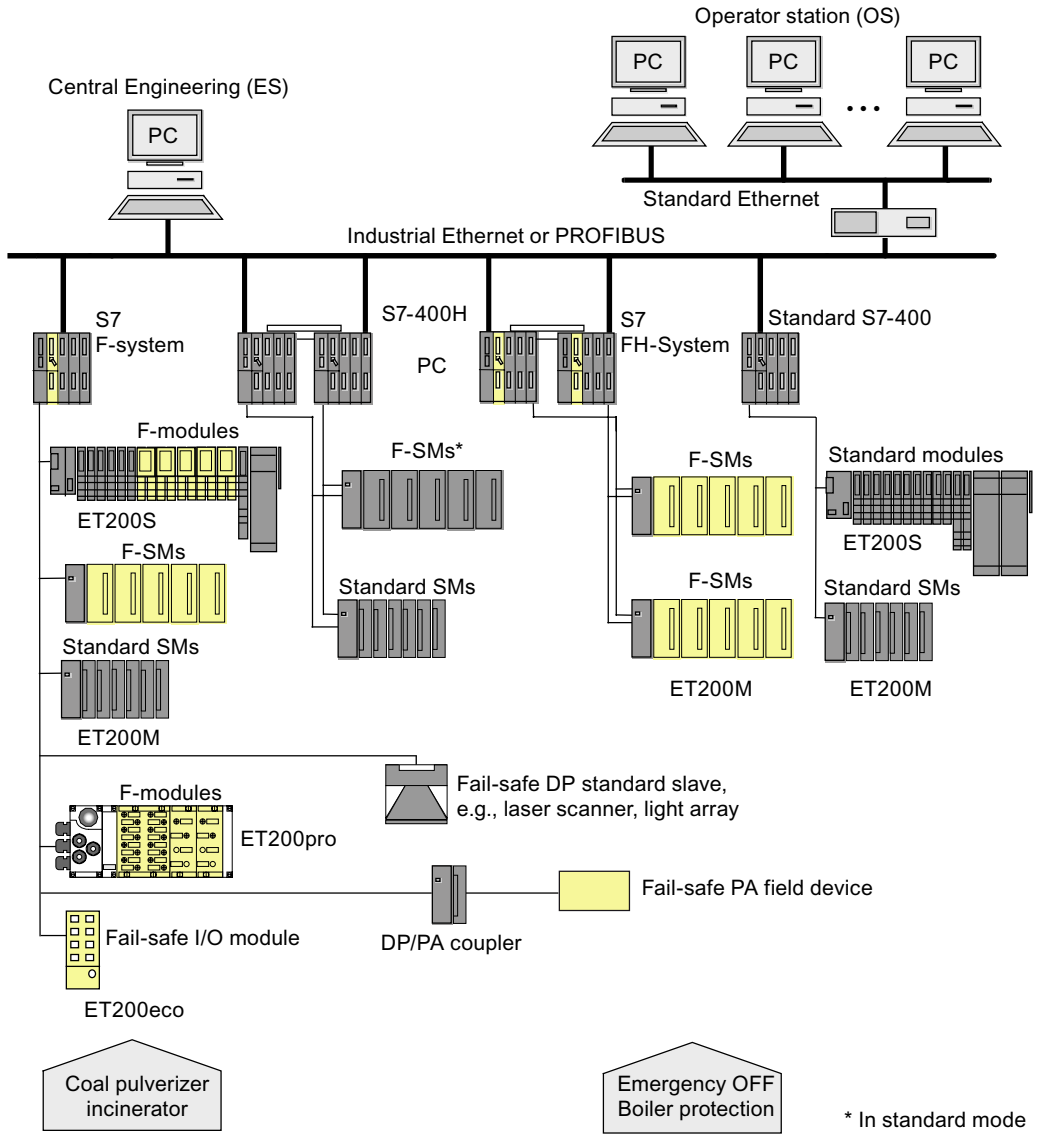


Figure 1-2 Use of S7 F/FH Systems

1.3.2 Performance Characteristics of S7 Distributed Safety and S7 F/FH Systems

Common Characteristics of S7 Distributed Safety and S7 F/FH Systems

S7 Distributed Safety and S7 F/FH Systems have the following important characteristics in common:

- Integration in S7-300 or S7-400 automation systems; the automation task determines the system design, and fail-safe engineering is integrated into the system
- Execution of standard control and protective functions on the same system (standard system with fail-safe capability, which eliminates the need for dedicated fail-safe solutions)
- Connection of distributed I/O via PROFIBUS DP with PROFIsafe
- Use of standard PROFIBUS components (copper and fiber-optic cable technology)
- Configuration integrated in *STEP 7*, same as for standard automation systems
- Creation of safety program using standard programming languages of *STEP 7*
- Flexible adaptation to the task requirements by providing a wide range of fail-safe I/O

Comparison of system performance of S7 Distributed Safety and S7 F/FH Systems

The following table identifies the differences between the fail-safe systems with regard to important performance characteristics.

Table 1- 1 Performance Characteristics of F-Systems

Performance Characteristic	S7 Distributed Safety	S7 F/FH Systems
Achievable safety classes	SIL3/Cat.4/PLe	SIL3/Cat.4/PLe
Fault tolerance feature available	No	Yes
Development stage	Fail-safe system	Fail-safe system Fail-safe and fault-tolerant system
Connection of fail-safe I/O	• Central • Distributed via PROFIBUS DP • Distributed via PROFINET IO (ET 200S and ET 200pro F-modules)	• Distributed via PROFIBUS DP
Minimum response time of F-System (dependent on configuration)	50 ms	100 ms
Typical response time of F-System	100 ms to 200 ms	200 ms to 500 ms
Communication	Safety-related master-master communication Safety-related master-I-slave communication Safety-related I-slave-I-slave communication Safety-related I-slave-slave communication Safety-related communication between I/O controllers Safety-related communication via S7 connections (Industrial Ethernet only) Safety-related communication via WLAN	Safety-related communication via S7 connections (via PROFIBUS, MPI, Industrial Ethernet, etc.) Safety-related communication via WLAN
Creation of safety program	In standard LAD or FBD languages in *STEP 7*	In CFC (optional software for *STEP 7*) via Safety Matrix
Modification of safety program in the F-CPU in RUN mode	Currently possible in deactivated safety mode, however, transition to safety mode possible only by switching the F-CPU to STOP mode	Partially possible in deactivated safety mode or via Safety Data Write; change of operating mode of F-CPU not required for transition to safety mode

Performance Characteristic	S7 Distributed Safety	S7 F/FH Systems
Fault reactions in the safety program	Passivation of channels or F-I/O F-CPU in STOP mode	Passivation of channels or F-I/O No STOP of the F-CPU and "F-STOP" instead, i.e., optional shutdown of all F-Shutdown groups of the F-CPU, or only of the F-Shutdown groups in which a fault was detected
Main areas of application	Operator and machine protection Burner control	Instrumentation and control and process industries (can be integrated in the PCS 7 process control system)

Table 1- 2 Memory Configuration of F-CPUs

F-System	Applicable F-CPU	Memory configuration (RAM)
S7 Distributed Safety	IM 151-7 F-CPU (6ES7151-7FA20-0AB0)	128 KB
	IM 151-8F PN/DP CPU (6ES7151-8FB00-0AB0)	192 Kbytes
	CPU 315F-2 DP (6ES7315-6FF01-0AB0)	192 Kbytes
	CPU 315F-2 PN/DP (6ES7315-2FH13-0AB0)	256 KB
	CPU 317F-2 DP (6ES7317-6FF03-0AB0)	1024 KB
	CPU 317F-2 PN/DP (6ES7317-2FK13-0AB0)	1024 KB
	CPU 319F-3 PN/DP (6ES7318-3FL00-0AB0)	1400 KB
	CPU 416F-2 (6ES7416-2FN05-0AB0)	2.8 MB for program + 2.8 MB for data
	CPU 416F-3 PN/DP (6ES7416-3FR05-0AB0)	5.6 MB for program + 5.6 MB for data
S7 F/FH Systems	CPU 412-3H (6ES7412-3HJ14-0AB0)	512 KB for program + 256 KB for data
	CPU 414-4H (6ES7414-4HM14-0AB0)	1.4 Mbytes for program + 1.4 Mbytes for data
	CPU 417-4H (6ES7417-4HT14-0AB0)	15 MB for program + 15 MB for data

Support of PROFINET IO (only *S7 Distributed Safety*):

The following F-CPUs and F-I/O support PROFINET IO:

- IM 151-8F PN/DP CPU (only via PN interface of the CPU)
- CPU 315F-2 PN/DP (only via PN interface of the CPU)
- CPU 317F-2 PN/DP (only via PN interface of the CPU)
- CPU 319F-3 PN/DP (only via PN interface of the CPU)
- CPU 416F-2 with PROFINET IO compatible CP
- CPU 416F-3 PN/DP
- S7-300 fail-safe signal modules
- ET 200S fail-safe modules
- ET 200pro fail-safe modules
- Fail-safe I/O standard devices

1.4 Components of S7 Distributed Safety and S7 F/FH Systems

Hardware and Software Components of F-Systems

An overview of the hardware and software components required for configuring and operating S7 Distributed Safety and S7 F/FH Systems F-Systems is shown below.

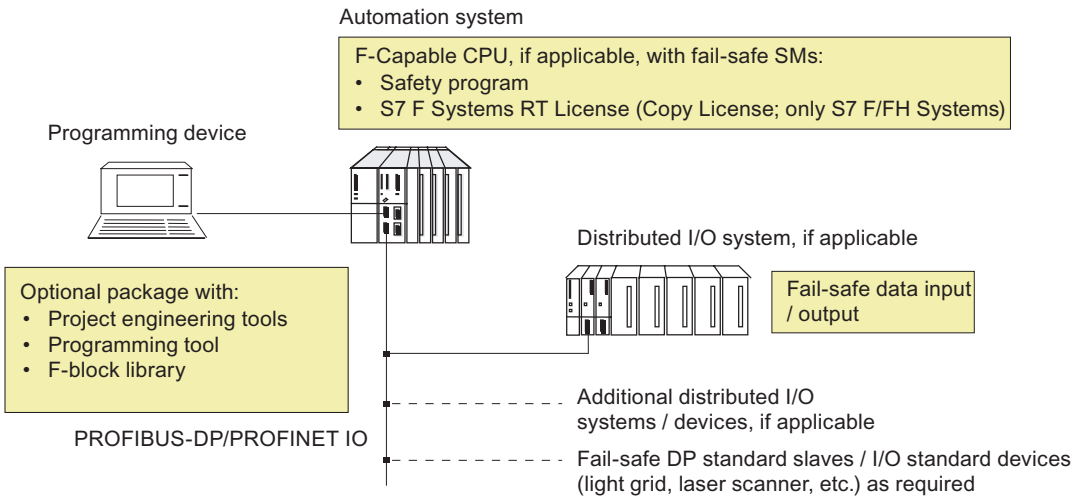


Figure 1-3 Overview of Hardware and Software Components of an F-System

Interaction of Components

To configure a fail-safe system, certain software and hardware components have to be combined.

Wiring Fail-safe I/O
The user wires the F-I/O to the sensors and actuators so as to be able to achieve the required safety class.

Configuring Hardware
The user configures the F-Capable CPU and the F-I/O in *STEP 7 HW Config*. This configuration must match the hardware configuration; that is, the circuit diagram of the F-I/O must reflect the parameter settings.

Creating safety programs
User created safety programs using a programming language in STEP 7.

For S7 Distributed Safety, the user creates fail-safe blocks in F-FBD or F-LAD. The associated F-block library provides fail-safe blocks that the user can use in his safety program. F-I/O systems are integrated similar to standard I/O by means of the process image (PII, PIO).

For S7 F/FH Systems, the user assigns parameters for the fail-safe blocks of the associated F-block library and interconnects them in CFC. Special F-Driver blocks are available to link the F-I/O. These driver blocks must also be parameterized and interconnected.

For both F-Systems, safety checks are performed and additional F-blocks for fault detection are incorporated automatically when the executable safety program is compiled.

1.4.1 Hardware components

Components

An F-System consists in part of hardware components that fulfill particular safety requirements:

Table 1- 3 Hardware components

F-System	F-Capable CPU	Fail-safe I/O
S7 Distributed Safety	• IM 151-7 F-CPU • IM 151-8F PN/DP CPU • CPU 315F-2 DP • CPU 315F-2 PN/DP • CPU 317F-2 DP • CPU 317F-2 PN/DP • CPU 319F-3 PN/DP • CPU 416-2 • CPU 416F-3 PN/DP	• Fail-safe signal modules in ET 200M (decentralized configuration) • Fail-safe signal modules in S7-300 station (local configuration with a CPU 3xxF) • Fail-safe electronic modules in ET 200S (DP master, DP slave, I slave, I/O controller, or I/O device) • ET 200pro fail-safe modules (DP slave or I/O device) • ET 200eco fail-safe I/O module • Fail-safe DP standard slaves • Fail-safe I/O standard devices
S7 F/FH Systems	• CPU 412-3H • CPU 414-4H • CPU 417-4H (each with S7 F Systems RT License (Copy License))	• Fail-safe signal modules in ET 200M (decentralized configuration) • Fail-safe electronic modules in ET 200S (DP slave) • ET 200pro fail-safe modules (DP slave) • ET 200eco fail-safe I/O module • Fail-safe DP standard slaves • Fail-safe PA field devices

In addition, the F-System can be expanded using standard components of the S7-300 and S7-400.

F-Capable CPU

A F-Capable CPU with fail-safe capability is a central processing unit that is approved for use in S7 Distributed Safety and S7 F/FH Systems.

For S7 F/FH systems, the S7 F Systems RT License (Copy License) allows users to operate the central processing unit as an F-CPU, that is, to run a safety program on this CPU.

S7 Distributed Safety does not require an S7 F Systems RT License (Copy License).

A standard user program can also be run in the F-CPU.
It is possible for a standard program and a safety program to coexist because unintentional interference of the safety program by the standard user program can be prevented.

Safety-related portions of the user program must be password-protected against unauthorized access in the F-CPU and the programming device or ES. In addition, the F-CPU applies highly effective measures to detect and eliminate faults.

Note
You can use the following F-CPUs in **S7 Distributed Safety**: IM 151-7 F-CPU, IM 151-8F PN/DP CPU, CPU 315F-2 DP, CPU 315F-2 PN/DP, CPU 317F-2 DP, CPU 317F-2 PN/DP, CPU 319F-3 PN/DP, CPU 416F-2, and CPU 416F-3 PN/DP. Note that these F-CPUs can **not** be used in S7 F/FH systems.
You can use the following F-CPUs in **S7 F/FH Systems**: CPU 412-3H, CPU 414-4H, and CPU 417-4H. Note that these F-CPUs can **not** be used in S7 Distributed Safety.

Restrictions of using F-I/O on PROFIBUS DP

Note that F-I/O cannot be operated in safety mode as DP master on PROFIBUS DP in combination with the following modules:

- CP 342-5
- CP 443-5DX00
- CP 443-5DX01
- IM 467-5GJ00
- IM 467-5GJ01
- IF 964-DP

S7-300 Fail-safe Signal Modules

The following fail-safe signal modules (F-SMs) are available:

- Fail-safe digital input modules:
  - SM 326; DI 8 × NAMUR
  - SM 326; DI 24 × DC 24V
- Fail-safe digital output modules:
  - SM 326; DO 10 × DC 24V/2A
  - SM 326; DO 8 × DC 24V/2A
- Fail-safe analog input modules:
  - SM 336; AI 6 × 13 Bit
  - SM 336; F-AI 6 × 0/4 ... 20 mA HART

F-SMs can also be used as standard SMs with standard CPUs in standard applications. From a user standpoint, the F-SMs can be distinguished from most standard SMs in that they have diagnostic interrupt capability.

In S7 Distributed Safety, the F-SMs can be operated as decentralized modules in ET 200M and as centralized modules in an S7-300 station.

In S7 F/FH Systems, the F-SMs can generally be operated only in the ET 200M distributed I/O system.

SM 326; DO 8 × DC 24V/2A can only be operated in safety mode. You can, however, installed it centrally with all F-CPUs of the S7-300 spectrum with:

- CPU 315F-2 DP (6ES7315-6FF01-0AB0) with firmware V 2.0.9 or higher
- CPU 317F-2 DP (6ES7317-6FF00-0AB0) with firmware V 2.1.4 or higher.

The module can be operated in a distributed configuration in in S7 Distributed Safety.

SM 336; F-AI 6 × 0/4 ... 20 mA HART can only be operated in safety mode. Operation with HART function requires distributed implementation in ET 200M.

Interface modules for ET 200M with fail-safe signal modules

One interface module is required per ET 200M. The interface modules which can be operated in combination with fail-safe signal modules are listed in the "S7300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151) Manual.

Restrictions on the Use of S7-300 Standard SMs

The restrictions for fault-tolerant systems apply to the operation of S7-300 standard SMs in S7 F/FH systems (see the "S7-400H Automation System, Fault-tolerant Systems" (http://support.automation.siemens.com/WW/view/en/1186523/) Manual).

For information on the restrictions for S7-300 standard SMs in safety mode of F-SMs, refer to the "S7300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151) Manual.

ET 200S Fail-safe Electronic Modules

The following fail-safe electronic modules (F-Modules) are available in ET 200S:

- PM-E F pm DC24V PROFIsafe power module with 2 additional fail-safe digital outputs
- PM-E F pp DC24V PROFIsafe power module
- PM-D F DC24V PROFIsafe power module
- 4/8 F-DO DC24V PROFIsafe digital electronic module
- 4 F-DI/3F-DO DC24V PROFIsafe digital electronic module
- 4 F-DO DC24V/2 A PROFIsafe digital electronic module
- 1 F-RO DC24V/AC 24 ... 230V/5A digital electronic module

F-Modules can **not** be operated on standard CPUs for standard applications (exception: 1 F-RO DC24V/AC 24 ... 230V/5A).

Interface Modules for ET 200S with Fail-safe Modules

One interface module is required for each ET 200S. The interface modules which can be used are listed in the "ET 200S Distributed I/O System - Fail-Safe Modules" (http://support.automation.siemens.com/WW/view/en/12490437) Manual.

ET 200pro Fail-safe Modules

The following fail-safe electronic modules (F-Modules for short) are available for an ET 200pro:

- 8/16 F-DI DC24V PROFIsafe Digital Electronic Module
- 4/8 F-DI/4 F-DO DC24V/2A PROFIsafe Digital Electronic Module
- F-Switch PROFIsafe digital electronic module

Interface modules for ET 200S with fail-safe modules

One interface module is required per ET 200pro. The interface modules which can be used are listed in the "ET 200pro Distributed I/O System, Fail-safe Modules" (http://support.automation.siemens.com/WW/view/en/22098524) Manual.

ET 200eco fail-safe I/O Module

The following fail-safe I/O modules (F-Modules) are available in ET 200eco:

- 4/8 F-DI DC24V PROFIsafe

Fail-safe DP Standard Slaves

Fail-safe DP standard slaves are standard slaves that are operated on PROFIBUS with the DP protocol and the PROFIsafe bus profile. Their behavior must comply with IEC 61784-1:2002 Ed1 CP 3/1 and the PROFIsafe bus profile.

Fail-safe DP standard slaves that are used in a mixed configurations on PROFIBUS DP and PROFINET IO after IE/PB links, must support the PROFIsafe bus profile in the V2 mode.

A GSD file is used to configure your devices.

Fail-safe I/O Standard Devices

Fail-safe I/O standard slaves are standard devices that are operated on PROFINET with the I/O protocol and the PROFIsafe (V2 mode) bus profile. They must behave in accordance with IEC 61784-1:2002 Ed1 CP 3/3 and the PROFIsafe bus profile (V2 MODE). A GSD file is used to configure your devices.

Fail-safe PA field devices

Fail-safe PA field devices are operated on PROFIBUS with PA protocol. Their behavior must comply with IEC 61784-1:2002 Ed1 CP 3/2 and the PROFIsafe bus profile. A GSD file is used to configure your devices.

1.4.2 Software Components

Introduction

The software components of an F-System include the following:

- Optional package on the programming device or ES for configuring and programming the F-System
- Safety program in the F-CPU

You also need the *STEP 7* basic software on the programming device or ES for configuring and programming the standard automation system.

For **S7 F/FH systems** you also need the *STEP 7* add-on software *CFC* and, where applicable, *PCS 7* (e.g. for applications with S7 F Systems HMI).

Optional Packages for Configuring and Programming F-Systems

The two optional packages are available for configuring and programming F-Systems as shown in the following table.

Table 1- 4 Optional Packages for Configuration and Programming

Optional package	Order Number	For F-System	Scope
S7 Distributed Safety	6ES7833-1FC02-0YA5	**S7 Distributed Safety**	Configuration and programming software with F-block library for: • IM 151-7 F-CPU, IM 151-8F PN/DP CPU, CPU 315F-2 DP, CPU 315F-2 PN/DP, CPU 317F-2 DP, CPU 317F-2 PN/DP, CPU 319F-3 PN/DP, CPU 416F-2, CPU 416 F-3 PN/DP • ET 200S F-Modules • ET 200pro F-Modules • ET 200eco F-Modules • S7-300 F-SMs • Fail-safe DP standard slaves • Fail-safe I/O standard devices
S7 F Systems	6ES7833-1CC01-0YA5	**S7 F/FH Systems**	Configuration and programming software with F-block library for: • CPU 412-3H • CPU 414-4H, CPU 417-4H • ET 200S F-Modules • ET 200pro F-Modules • ET 200eco fail-safe module • S7-300 F-SMs • Fail-safe DP standard slaves • Fail-safe PA field devices

The user receives the following with these optional packages:

- Support for configuring the F-CPU (only S7 Distributed Safety) and F-I/O in *STEP 7* using *HW Config*.
- F-library with fail-safe blocks for creating safety programs
- Support for creating the safety program and integrating fault detection functions in the safety program

Programming Language

Different programming languages are used to create safety programs:

Table 1- 5 Programming Languages

F-System	Programming Language	Description
S7 Distributed Safety	F-LAD, F-FBD	• The primary difference between the F-LAD and F-FBD programming languages and the standard LAD and FBD languages in *STEP 7* lies in the limitations in the instruction set and data types. • F-application blocks from the *Distributed Safety* F-library or custom F-libraries can be used.
S7 F/FH Systems	CFC	• Use of optional CFC software in *STEP 7* • Special F-blocks from the *S7 F Systems* F-library must be used.

Creating a Safety Program for S7 Distributed Safety

The user creates safety programs with F-FBD or F-LAD in fail-safe FBs and FCs. The F-library provided contains F-application blocks that the user can incorporate into his safety program.

The user also has the option of creating his own F-libraries for S7 Distributed Safety (custom F-libraries).

Creating a Safety Program for S7 F/FH Systems

The user creates safety programs with CFC by interconnecting fail-safe blocks in the F-library provided with the *S7 F Systems* optional package.

Optional packages *Safety Matrix* for configuring fail-safe S7 F/FH systems

SIMATIC Safety Matrix is a comprehensive tool for Safety Lifecycle Engineering and Management of fail-safe automation systems S7 F/FH Systems and provides support in all phases of the Safety Lifecycle:

- *Safety Matrix* is a tool for configuring processes requiring safety reactions to defined states.
- The *Safety Matrix* can be used to create a CFC safety program for S7 F/FH systems in accordance with the rules of a cause/effect matrix.
- The *Safety Matrix* is an integrated tool which can be used in runtime for all operations, for maintenance, for error handling, and for changes management.

The *Safety Matrix* consists of three products which can be ordered in three optional packages.

Table 1- 6 *Safety Matrix* optional packages

Optional package	Order number	Environment	Scope
Safety Matrix Editor	6ES7833-1SM41-0YA5	Standalone	Creating and configuring a *Safety Matrix* on a PC without *PCS 7* or *STEP 7*
Safety Matrix Engineering Tool	6ES7833-1SM01-0YA5	Engineering System (ES) *PCS 7* or *STEP 7* and *CFC*	Creation and configuration of a Safety Matrix, automatic generation of CFC charts and their and transfer to a PCS 7 project, operating and monitoring by means of STEP 7 *SIMATIC Manager* on a PCS 7 Engineering System (ES)
Safety Matrix Viewer	6ES7833-1SM61-0YA5	PCS 7 Operator Station (OS)	Operating and monitoring on a PCS 7 Operator Station (OS) by means of faceplates

Additional Information

For detailed information on configuring S7 Distributed Safety and S7 F/FH Systems, refer to chapter "Configuring F-Systems (Page 117)". Chapter "Programming F-Systems (Page 123)" describes how to program fail-safe systems.

A description of the *Safety Matrix* is provided in the "Safety Matrix" (http://support.automation.siemens.com/WW/view/en/19056619) Manual.

1.5 Guide to Working with F-Systems

Introduction

This section describes the basic procedure for working with fail-safe systems. Only the relevant steps for F-Systems that differ from the standard procedure are presented.

Planning tasks that depend on the process, such as creating a flowchart or process tag list, defining a structure, etc., are not described here.

Example Projects

You will find introductory example projects for configuration and programming of:

- S7 Distributed Safety in the "Getting Started S7 Distributed Safety" (http://support.automation.siemens.com/WW/view/en/19810812)
- S7 F/FH Systems on the product CD

Planning a System

Within the system planning phase, the planner specifies the applicable safety class (SIL/Cat./PL) for each required safety function based on a risk assessment. This is then used to determine the component requirements for implementing the safety functions (programmable logic controllers, sensors, actuators). These decisions influence additional activities such as hardware design, configuration, and programming.

Note

A functional division of standard and safety functions is important for planning.

Sequence of Steps Ranging from Selection of Components to Maintenance of F-Systems

The following table provides references to manuals for obtaining information. The relevant product information sheets provide additional information on the F-CPUs.

Table 1- 7 Sequence of Steps Ranging from Selection of Hardware to Maintenance of F-Systems

Step	Procedure	Reference
1.	**Plan system:** • Specification of safety functions with appropriate safety classes (SIL/Cat./PL) • Specify S7 Distributed Safety, S7 F Systems, or S7 FH Systems; select hardware and software components.	System Manual *Safety Engineering,* chapter "Overview of Fail-safe Systems" (Page 15) Product catalog
2.	**Configure hardware in *STEP 7*:** • Configure F-CPU and assign parameters for safety program. • Configure and assign parameters for fail-safe I/O (F-SMs, F-Modules) according to safety class and wiring diagram. • Integration and parameterization of fail-safe DP standard slaves / I/O standard devices / PA field devices.	*Safety Engineering* System Manual, chapter "Configuring F-Systems" (Page 117) S7 Distributed Safety: "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) S7 F/FH Systems: "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) ET 200S: "ET 200S Distributed I/O System - Fail-Safe Modules" (http://support.automation.siemens.com/WW/view/en/12490437) ET 200pro: "ET 200pro Distributed I/O System, Fail-safe Modules" (http://support.automation.siemens.com/WW/view/en/22098524) ET 200eco: "ET 200eco Distributed I/O Device, Fail-safe I/O Module" (http://support.automation.siemens.com/WW/view/en/19033850) F-SMs: "S7300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151)

Step	Procedure	Reference
3.	**Set up hardware:** • Set PROFIsafe addresses for F-I/O • Install modules. • Wire modules according to required wiring diagram.	ET 200S: "ET 200S Distributed I/O System - Fail-Safe Modules" (http://support.automation.siemens.com/WW/view/en/12490437) ET 200pro: "ET 200pro Distributed I/O System, Fail-safe Modules" (http://support.automation.siemens.com/WW/view/en/22098524) ET 200eco: "ET 200eco Distributed I/O Device, Fail-safe I/O Module" (http://support.automation.siemens.com/WW/view/en/19033850) F-SMs: "S7300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151)
4.	**Create safety program in STEP 7:** • Create F-blocks or select them from F-library; position, interconnect, and assign parameters for F-blocks. • Compile safety program and download it to the F-CPU. • Test safety program. • If necessary, modify safety program. • Document configuration and safety program.	*Safety Engineering* System Manual, chapter "Programming F-Systems" (Page 123) S7 Distributed Safety: "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) S7 F/FH Systems: "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) Safety Matrix: "Safety Matrix" (http://support.automation.siemens.com/WW/view/en/19056619)
5.	**Commission system:** • If necessary, arrange for acceptance testing of safety-related parts by the relevant authorities before starting safety mode. • Commission system. • Test of all safety functions	S7 Distributed Safety: "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) S7 F/FH Systems: "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072)
6.	**Perform system maintenance:** • Replace hardware and software components. • Update operating system. • Uninstall F-System.	S7 Distributed Safety: "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) S7 F/FH Systems: "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) Hardware manuals: See above: item 3.

Configurations and Help with Selection 2

2.1 Introduction

Overview

This chapter includes a description of the basic configuration of S7 Distributed Safety and S7 F/FH Systems fail-safe systems.

It also provides information about the configuration variants depending on the availability requirements of the F-System.

In the last part of the chapter, we present the main criteria used by customers to determine which fail-safe system - S7 Distributed Safety, S7 F Systems, or S7 FH Systems - is right for their automation task.

Additional information

For detailed information on the F-I/O, refer to:

- Manual "S7300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151)
- Manual "ET 200S Distributed I/O System - Fail-Safe Modules" (http://support.automation.siemens.com/WW/view/en/12490437)
- Manual "ET 200pro Distributed I/O System, Fail-safe Modules" (http://support.automation.siemens.com/WW/view/en/22098524)
- Manual "ET 200eco Distributed I/O Device, Fail-safe I/O Module" (http://support.automation.siemens.com/WW/view/en/19033850)

2.2 Configuration of F-Systems

Basic Configurations

This chapter describes the three basic configurations for F-systems:

- S7 Distributed Safety Fail-safe System
- S7 F Systems Fail-safe System
- S7 FH Systems Fail-safe and Fault-Tolerant System

2.2.1 S7 Distributed Safety Fail-safe System

Components of S7 Distributed Safety System

S7 Distributed Safety refers to a fail-safe automation system consisting of at least the following components:

- A central processing unit with fail-safe capability, such as CPU 315F-2 DP, on which a safety program is executed
- Fail-safe I/O, for example:
  - Fail-safe signal modules (F-SMs) in a centralized configuration with CPU 315F-2 DP
  - Fail-safe signal modules (F-SMs) in an ET 200M distributed I/O system
  - Fail-safe modules in an ET 200S distributed I/O system
  - Fail-safe modules in an ET 200pro distributed I/O device
  - ET 200eco fail-safe I/O module
  - Fail-safe DP standard slaves/standard I/O devices

Note

You can use the following F-CPUs in **S7 Distributed Safety**: IM 151-7 F-CPU, IM 151-8F PN/DP CPU, CPU 315F-2 DP, CPU 315F-2 PN/DP, CPU 317F-2 DP, CPU 317F-2 PN/DP, CPU 319F-3PN/DP, CPU 416F-2, and CPU 416F-3 PN/DP. Note that these F-CPUs **cannot** be used in S7 F/FH Systems.

You can use the following F-CPUs in **S7 F/FH Systems**: CPU 412-3H, CPU 414-4H, and CPU 417-4H. Note that these F-CPUs can **not** be used in S7 Distributed Safety.

Configuration Examples for S7 Distributed Safety F-Systems

The following figures illustrate three examples of S7 Distributed Safety F-systems.

Example 1 for PROFIBUS DP: The S7-300 station with CPU 315F-2 DP is the DP master. The F-CPU exchanges safety-related data with the fail-safe I/O in the centralized configuration and in the DP slaves.

The F-system can be expanded with additional fail-safe I/O and any number of standard modules.

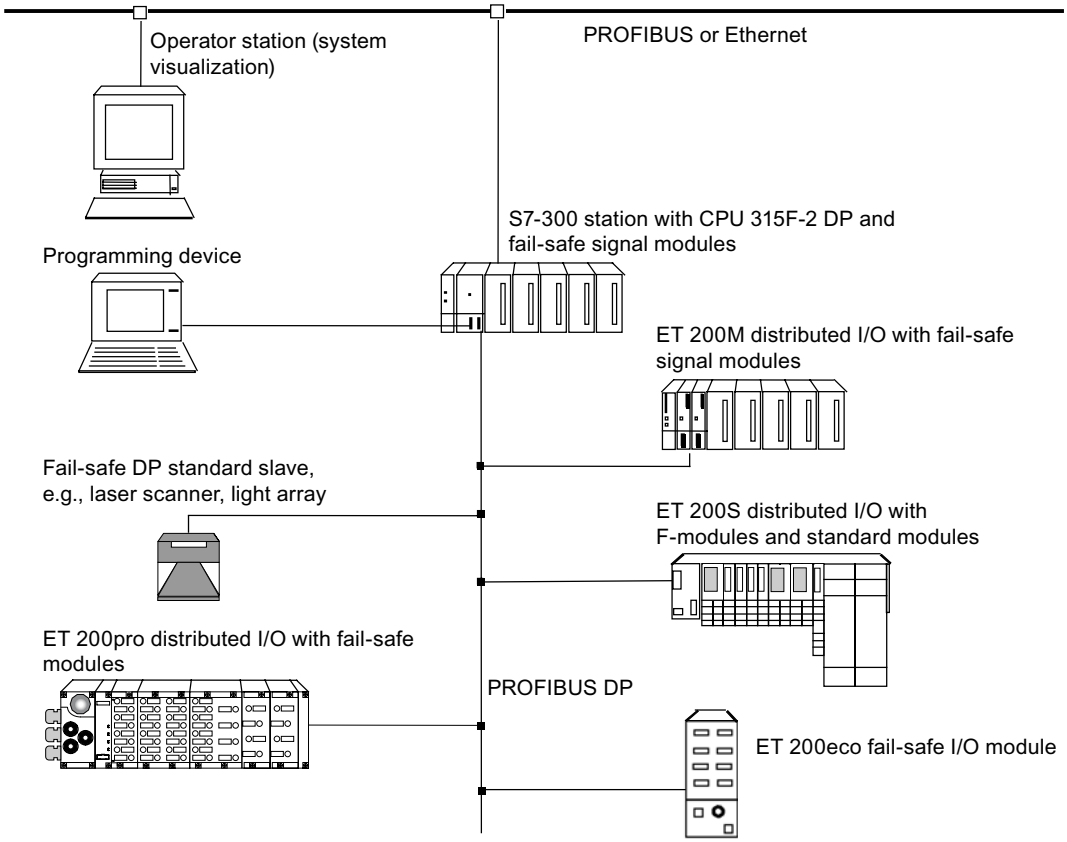


Figure 2-1 Example 1: F-System S7 Distributed Safety with PROFIBUS DP

Example 2 for PROFIBUS DP: The S7-400 station with CPU 416F-2 is the DP master. The F-CPU exchanges safety-related data with the IM 151-7 F-CPU in ET 200S. The IM 151-7 F-CPU acts as an intelligent preprocessing device (I-slave).

The F-system can be expanded with additional fail-safe I/O and any number of standard modules.

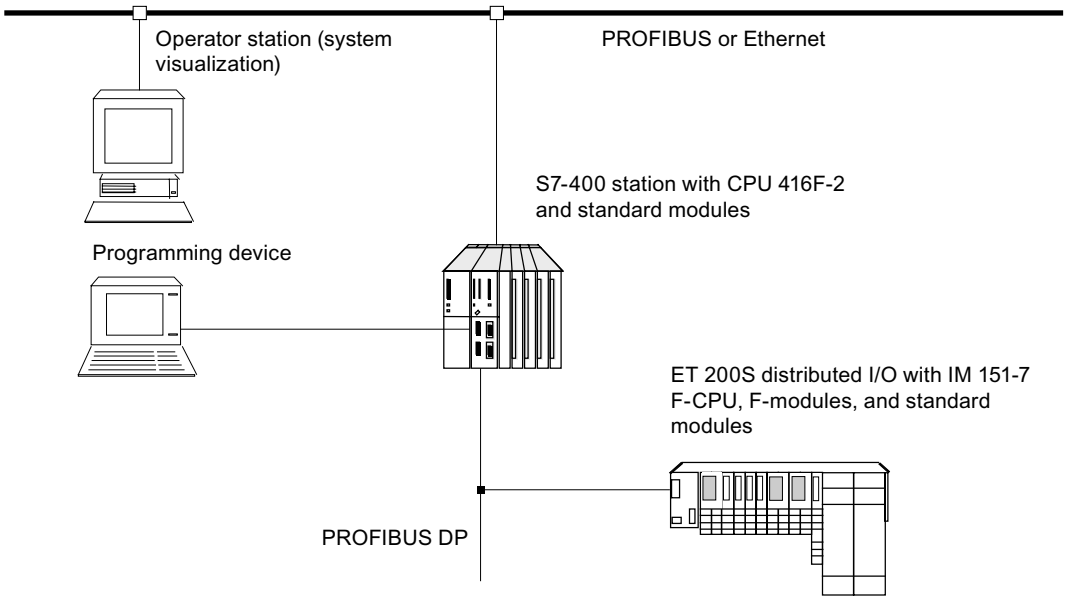


Figure 2-2 Example 2: F-System S7 Distributed Safety with PROFIBUS DP

Example 3 for PROFINET IO: The S7-300 station with CPU 315F-2 PN/DP is the I/O controller The F-CPU exchanges safety-relevant data with the fail-safe modules of ET 200pro, ET 200S and fail-safe I/O standard devices.

The fail-safe system can be expanded by any number of I/O devices.

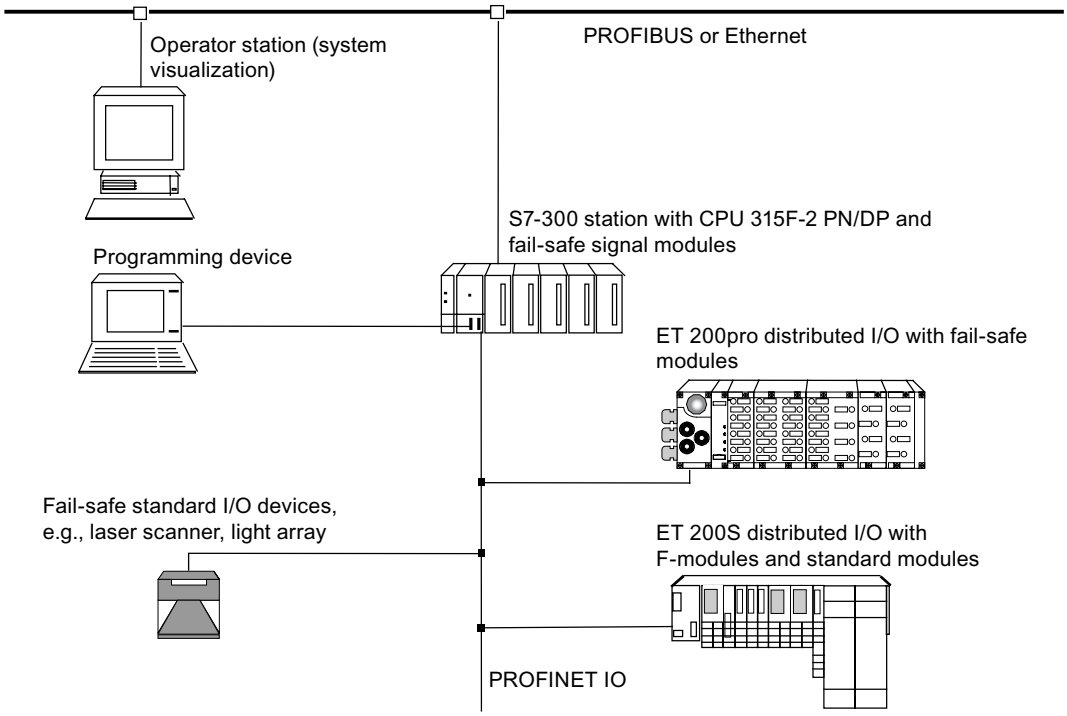


Figure 2-3 Example 3: F-System S7 Distributed Safety with PROFINET IO

2.2.2 S7 F Systems Fail-safe System

Components of S7 F Systems

S7 F Systems refers to a fail-safe automation system consisting of at least the following components:

- A central processing unit with fail-safe capability, such as CPU 417-4 H with an S7 F Systems RT license (copy license), on which a safety program is executed
- Fail-safe I/O, for example:
  - Fail-safe signal modules (F-SMs) in an ET 200M distributed I/O system (with optional redundancy)
  - Fail-safe modules in an ET 200S distributed I/O system
  - ET 200pro fail-safe modules
  - ET 200eco fail-safe I/O module
  - Fail-safe DP standard slaves
  - Fail-safe PA field devices

Configuration Example for an S7 F Systems F-System

The following figure illustrates an example of an S7 F Systems F-system.

The S7-400 station with CPU 417-4H is the DP master. The F-CPU exchanges safety-related data with the fail-safe I/O in the DP slaves. The F-system can be expanded with additional fail-safe I/O and any number of standard modules.

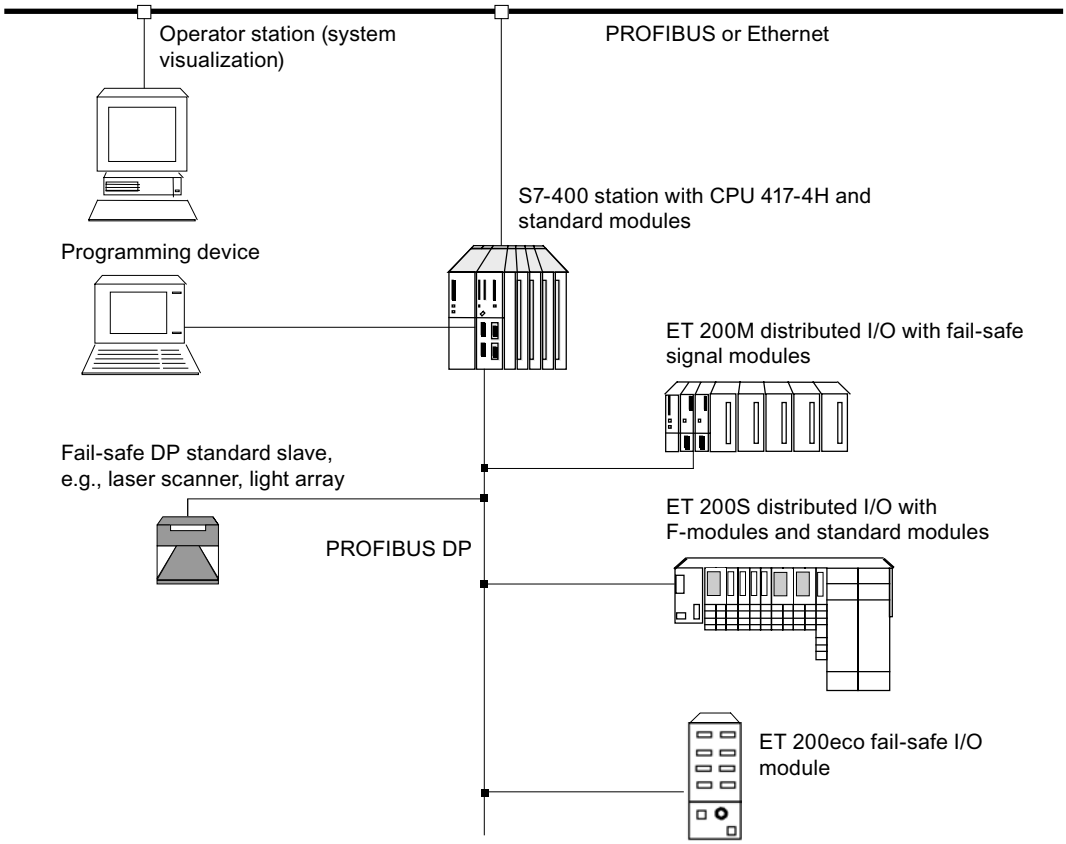


Figure 2-4 S7 F Systems Fail-safe System

2.2.3 S7 FH Systems Fail-safe and Fault-Tolerant System

Components of S7 FH Systems

S7 FH Systems refers to a fail-safe and fault-tolerant automation system consisting of at least the following components:

- S7-400H fault-tolerant system (master and standby) on which a safety program is executed
- Fail-safe signal modules (F-SMs) in an ET 200M distributed I/O system as switched I/O (with optional redundancy)

Configuration Example for an S7 FH Systems F-System

The following figure illustrates an example of an S7 FH Systems system with redundant F-CPU and shared, switched distributed I/O, as well as connection to a redundant system bus.

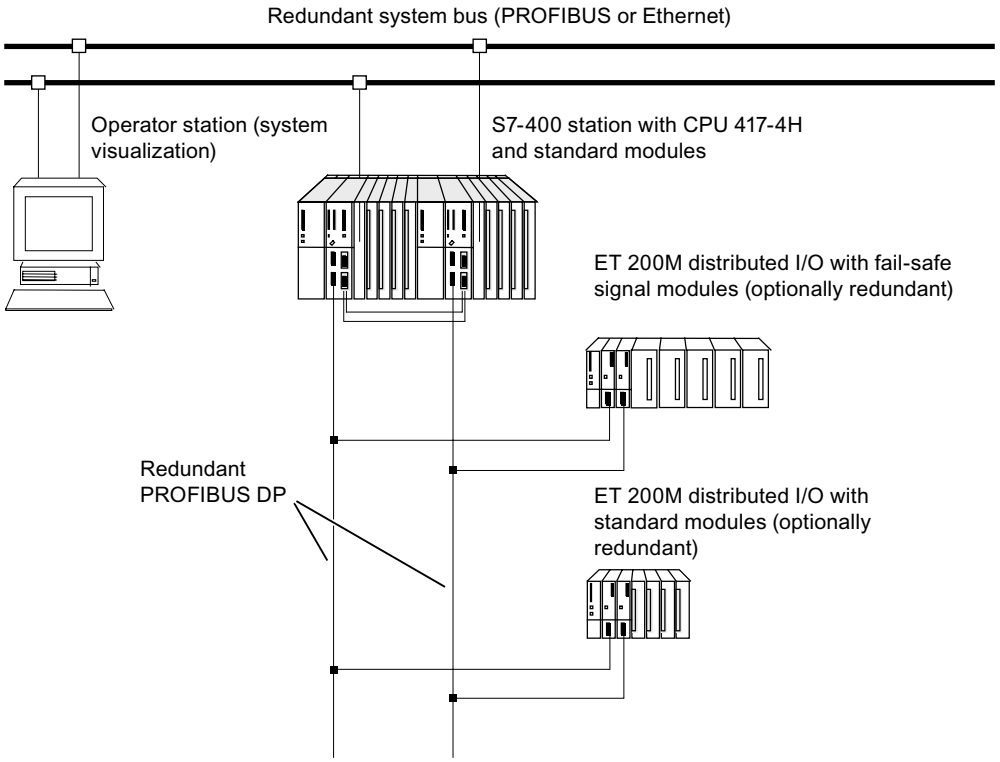


Figure 2-5 S7 FH Systems F-System

2.2.4 Coexistence of Standard and Fail-safe Components

Coexistence Is Possible

Standard, fault-tolerant (H-), and fail-safe (F-) components and systems can be used in combination as follows:

- Standard systems, H-systems, F-systems, and FH systems can coexist in a **system**.
- In an **F-system**:
  - Distributed I/O devices and systems can be operated with standard and fail-safe I/O, such as ET 200S, ET 200pro and ET 200eco.
  - S7-300 standard and fail-safe signal modules can be operated in safety mode both as centralized modules (in S7 Distributed Safety only) and as decentralized modules in ET 200M.
- In an F-system or FH-system, a standard user program can be executed along with the safety program.

Advantages

Coexistence of F-components, H-components, and standard components has the following advantages:

- It is possible to configure a totally integrated automation system that takes advantage of standard CPU innovation. At the same time, fail-safe components are implemented independently of standard components such as FMs or CPs. The entire system is configured and programmed with standard tools such as *HW Config*, FBD, LAD, or CFC.
- The coexistence of standard and fail-safe program parts in one F-CPU reduces the cost of acceptance tests because program parts not required to be fail-safe can be swapped out to the standard user program. This reduces the size of the safety program, that is, the part of the program that must pass an acceptance test.

  Maintenance costs can also be reduced if as many functions as possible are moved to the standard user program, since the standard user program can be modified during operation.

Boundary Conditions for Coexistence

⚠WARNING

For applications with safety class **SIL2/Category 3/PLd** and lower, physical contact protection measures for standard components are sufficient (see the *manuals for the F-CPU and F-I/O you are using*).

Applications with safety class **SIL3/Category 4/PLe** require certain measures beyond physical contact protection to prevent hazardous overvoltages via the power supply and backplane bus, even in the event of a fault on the F-circuits. Therefore, the following are provided for protection from backplane bus influence:

- Safety protector for centralized and decentralized configuration of S7-300 F-SMs
- For S7 F/FH Systems, PROFIBUS DP with fiber-optic cable design

ET 200S fail-safe modules and ET 200eco fail-safe I/O module exhibit a 250 VAC isolation internally.

To protect against influence by the power supply, configuration rules for power supplies, standard I/O, and fail-safe I/O are available (see *Fail-safe I/O manuals*).

Rules for Using the Safety Protector

The safety protector protects the F-SMs from possible overvoltages in the event of a fault.

⚠WARNING

The safety protector must be used for **SIL3/Category 4/PLe** applications:

- Generally, when the F-SMs are used as centralized modules in an S7-300
- Generally, when PROFIBUS DP is configured with copper cable
- When PROFIBUS DP is configured with fiber-optic cable and combined operation of standard and fail-safe SMs in one ET 200M is required

For a detailed description of the safety protector, refer to the "Automation System S7300, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151) manual.

2.3 Configuration Variants for Fail-safe Systems According to Availability Requirements

Options for Increasing Availability

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

For S7 F Systems, availability can be increased without fault-tolerant configuration. Fail-safe signal modules (F-SMs) can be used redundantly in one ET 200M or in several ET 200Ms.

The following section includes a description of how to achieve increased availability through redundancy of the F-CPU and F-I/O in S7 FH Systems.

Note

Availability of the fail-safe CPUs in S7 Distributed Safety and S7 F Systems cannot be increased by using the "SW Redundancy" software package.

Configuration Options in Safety Mode

Fail-safe systems can be configured three different ways, as follows:

Table 2- 1 Configuration Options for Fail-safe Systems According to Availability

System	Configuration Option	Description	Availability
S7 Distributed Safety S7 F Systems	• Single-channel I/O	Single-channel and fail-safe (F-CPU and F-I/O are not redundant)	Standard availability
S7 FH Systems	• Single-channel switched I/O	Single-channel switched and fail-safe (F-CPU is redundant, F-I/O is not redundant; in the event of a fault, the system switches over to the other F-CPU)	Increased availability
	• Redundant switched I/O	Multichannel and fail-safe (F-CPU, PROFIBUS DP, and F-I/O are redundant)	Highest availability

Typical configuration examples are presented below. A different level of availability of process data is achieved for each configuration variant.

Additional Information about Increased Availability

Communication between F-CPUs in S7 FH Systems is described in the "Safety-Related CPU-CPU Communication (Page 75)" section of this manual. For information about S7-400H fault-tolerant systems, refer to the "Automation System S7-400H Fault-Tolerant Systems" (http://support.automation.siemens.com/WW/view/en/1186523/) manual.

2.3.1 Single-channel I/O (S7 Distributed Safety)

What is single-channel I/O?

In a single-channel configuration, fail-safe I/O are not redundant. The fail-safe I/O is addressed by **one** F-CPU.

Required Hardware Components for S7 Distributed Safety

The hardware component requirements depend on whether the F-System is configured as a centralized system or as a decentralized system and whether the PROFIBUS DP is configured with a copper cable or a fiber-optic cable. The F-I/O is not redundant.

Centralized Configuration of S7 Distributed Safety

Centralized configuration of S7 Distributed Safety requires the following elements:

- One CPU 31xF-2 DP or CPU 31xF-2 PN/DP
- F-SMs and, if necessary, standard SMs
- Safety protector (required for SIL3/Category 4/PLe applications only)

Configuration Example of S7 Distributed Safety: Single-channel I/O (Centralized Configuration)

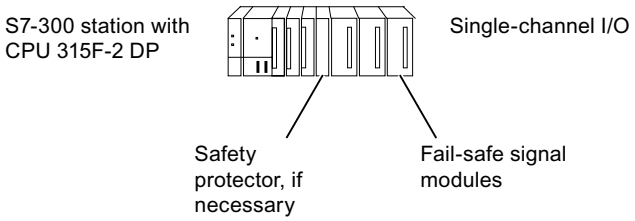


Figure 2-6 S7 Distributed Safety with Single-channel I/O (Centralized Configuration)

S7 Distributed Safety with Stand-Alone IM 151-7 F-CPU

Note

Unlike IM 151-1 HIGH FEATURE, for example, the IM 151-7 F-CPU is an intelligent preprocessing device (I-slave) and can also be used as a DP master. It can therefore exercise full and, if necessary, independent control over a technological functional unit and can be used as a stand-alone CPU or F-CPU. The IM151-7 F-CPU represents an addition to the line of F-CPUs for S7 Distributed Safety.

Configuration Example of S7 Distributed Safety: Single-channel I/O (Stand-alone IM 151-7 F-CPU)

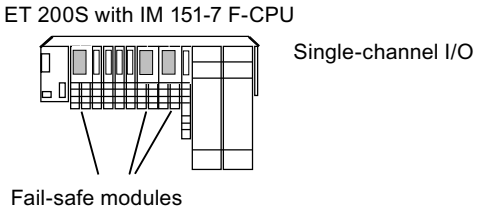


Figure 2-7 S7 Distributed Safety with Single-channel I/O (Stand-Alone IM 151-7 F-CPU)

Distributed Configuration of S7 Distributed Safety and PROFIBUS DP with Copper Cable

The following are required for distributed configuration with copper cable:

- One CPU 416F-2, CPU 416F-3 PN/DP, CPU 31xF-2 DP, CPU 31xF-x PN/DP, IM 151-7 F-CPU, or IM 151-8F PN/DP CPU
- One PROFIBUS DP line
- Fail-safe I/O, for example:
  - One ET 200M with:
    IM153-2, F-SMs, and, if necessary, standard SMs,
    safety protector (required for SIL3/Category 4/PLe applications only)
  - One ET 200S with:
    IM 151-1 HIGH FEATURE or IM 151-7 F-CPU,
    fail-safe modules, and, if necessary, ET 200S standard modules
  - One ET 200pro with:
    IM 154-2 DP HIGH FEATURE,
    fail-safe modules, and, if necessary, ET 200pro standard modules
  - ET 200eco fail-safe I/O module
  - Fail-safe DP standard slaves
- Bus connector for connecting the F-CPU and fail-safe I/O to the PROFIBUS DP

Configuration Example of S7 Distributed Safety: Single-channel I/O (Distributed Configuration with Copper Cable)

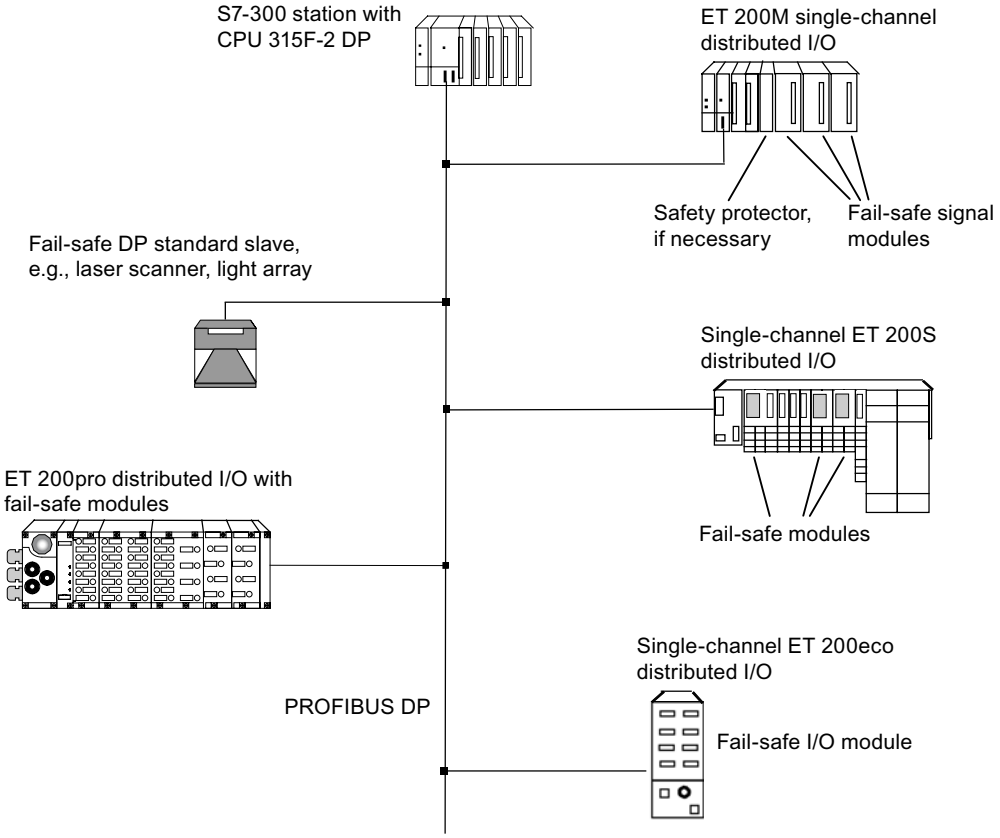


Figure 2-8 S7 Distributed Safety with Single-channel I/O (PROFIBUS DP, Copper Cable)

Distributed Configuration of S7 Distributed Safety and PROFIBUS DP with Fiber-optic Cable

The following are required to configure PROFIBUS DP with fiber-optic cables:

- One CPU 416F-2, CPU 416F-3 PN/DP, CPU 31xF-2 DP, CPU 31xF-x PN/DP, IM 151-7 F-CPU, or IM 151-8F PN/DP CPU
- One PROFIBUS DP line
- Fail-safe I/O, for example:
  - One ET 200M with:
    IM153-2 FO, F-SMs, and, if necessary, standard SMs,
    safety protector (required for SIL3/Category 4/PLe applications only if F-SMs and standard SMs are used together in an ET 200M)
  - One ET 200S with:
    IM 151-1 HIGH FEATURE or IM 151-7 F-CPU,
    fail-safe modules, and, if necessary, ET 200S standard modules
  - One ET 200pro with:
    IM 154-2 DP HIGH FEATURE,
    fail-safe modules, and, if necessary, ET 200pro standard modules
- Components for connecting the F-CPU and fail-safe I/O to the fiber-optic cable, for example, OBT

Configuration Example of S7 Distributed Safety: Single-channel I/O (Distributed Configuration with Fiber-optic Cable)

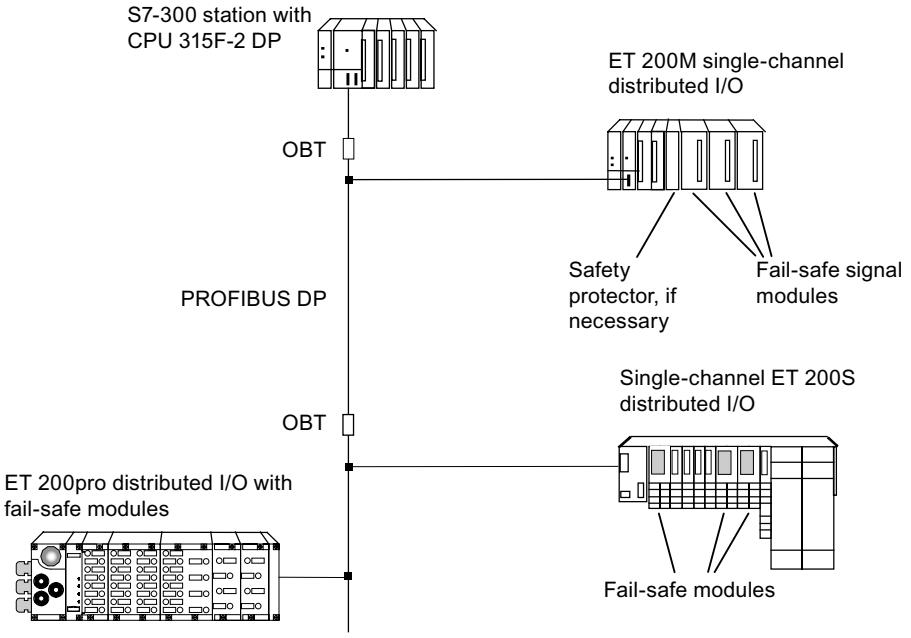


Figure 2-9 S7 Distributed Safety with Single-channel I/O (PROFIBUS DP, Fiber-optic Cable)

Distributed Configuration of S7 Distributed Safety and PROFINET IO

The following are required to set up PROFINET IO:

- One CPU 31xF-x PN/DP, CPU 416F-3 PN/DP, CPU 416F-2 (firmware version V 4.1 or later) with a PROFINET I/O-capable CP or IM 151-8F PN/DP CPU
- One PROFINET IO line
- Fail-safe I/O for PROFINET IO, for example:
  - One ET 200pro with:

    IM 154-4 PN HIGH FEATURE

    Fail-safe modules and ET 200pro standard modules, if necessary
  - One ET 200S with:

    IM 151-3 PN HIGH FEATURE

    Fail-safe modules and ET 200S standard modules, if necessary
  - Fail-safe standard I/O devices
- Components for configuring PROFINET
  - Passive network components (cables, plugs)
  - Active network components (switches, routers, etc.) if necessary

Configuration Example of S7 Distributed Safety and PROFINET IO

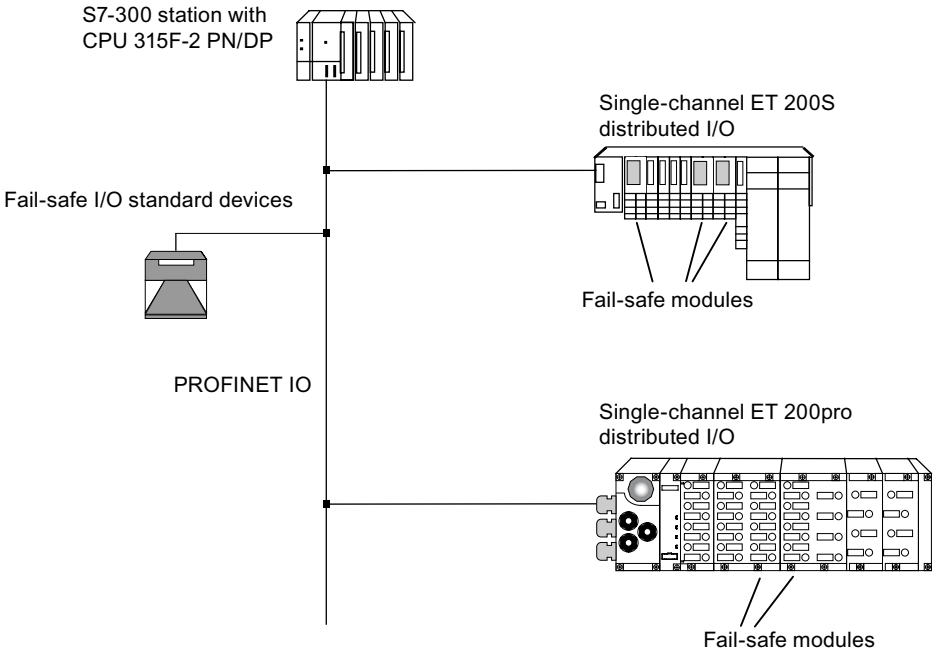


Figure 2-10 S7 Distributed Safety with Single-channel I/O (PROFINET IO)

Limits of Availability with Single-channel I/O

In the event of a fault, the I/O are no longer available. The F-I/O is passivated.

Possible fault causes:

- Failure of F-I/O
- Failure of interface module in an ET 200M, ET 200S or ET 200pro
- Failure of the PROFIBUS DP or PROFINET IO line
- Failure of the F-CPU

2.3.2 Single-channel I/O (S7 F Systems)

What is single-channel I/O?

In a single-channel configuration, fail-safe I/O are not redundant. The fail-safe I/O is addressed by **one** F-CPU.

Required Hardware Components for S7 F-Systems

Which hardware components are required depends on whether PROFIBUS DP is configured with copper cable or fiber-optic cable. The F-I/O is not redundant.

S7 F Systems and PROFIBUS DP with Copper Cable

The following are required to configure PROFIBUS DP with copper cable:

- One CPU 412-3H, CPU 414-4H, or CPU 417-4H
- One PROFIBUS DP line
- Fail-safe I/O, for example:
  - One ET 200M with:
    IM153-2,
    F-SMs, and, if necessary, standard SMs,
    safety protector (required for SIL3/Category 4/PLe applications only)
  - One ET 200S with:
    IM 151-1 HIGH FEATURE,
    fail-safe modules, and, if necessary, ET 200S standard modules
  - One ET 200pro with:

    IM 154-2 DP HIGH FEATURE,fail-safe modules, and, if necessary, ET 200pro standard modules
  - ET 200eco fail-safe I/O module
  - Fail-safe DP standard slave
- Bus connector for connecting the F-CPU and fail-safe I/O to the PROFIBUS DP

Configuration Example of S7 F Systems: Single-channel I/O with Copper Cable

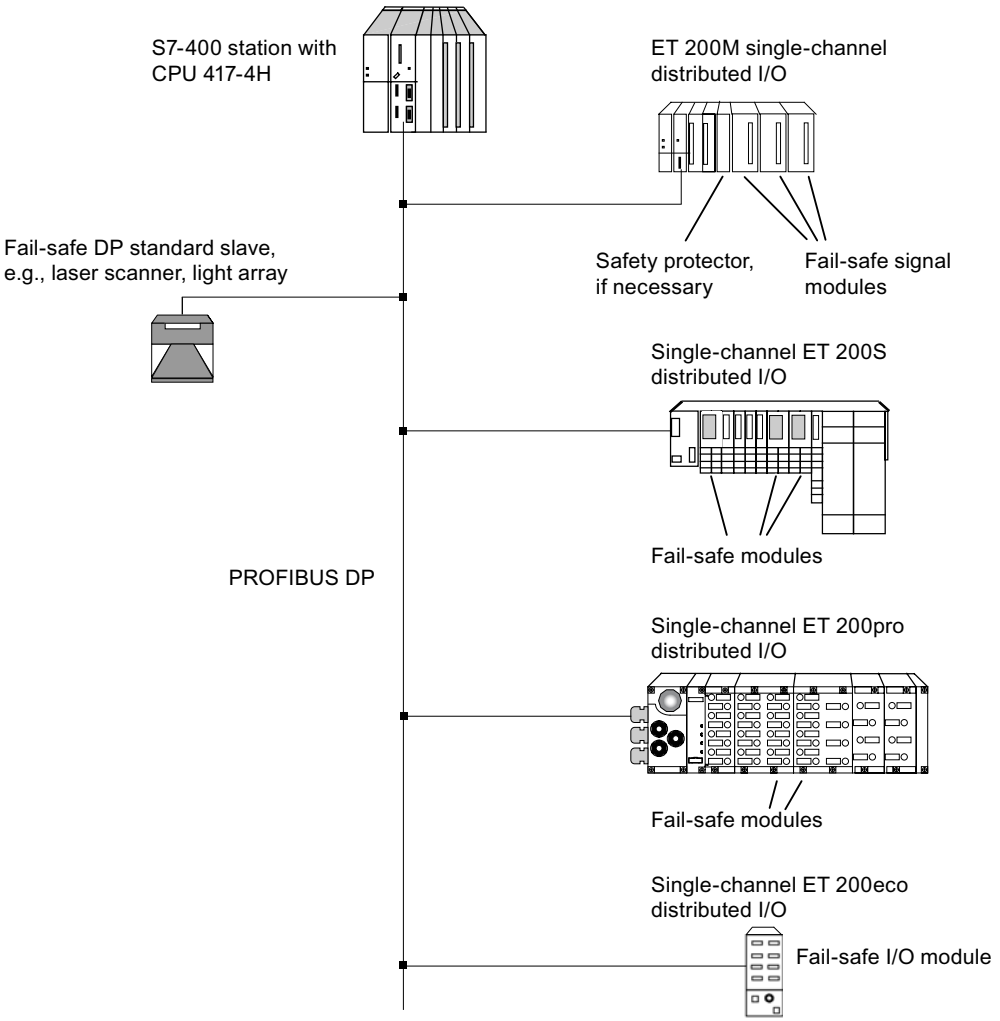


Figure 2-11 S7 F Systems with Single-channel I/O (Copper Cable)

S7 F Systems and PROFIBUS DP with Fiber-optic Cable

The following are required to configure PROFIBUS DP with fiber-optic cables:

- One CPU 412-3H, CPU 414-4H, or CPU 417-4H
- One PROFIBUS DP line
- Fail-safe I/O, for example:
  - One ET 200M with:
    IM153-2 FO, F-SMs, and, if necessary, standard SMs,
    safety protector (required for SIL3/Category 4/PLe applications only if F-SMs and standard SMs are used together in an ET 200M)
  - One ET 200S with:
    IM 151-1 HIGH FEATURE,
    fail-safe modules, and, if necessary, ET 200S standard modules
- Components for connecting the F-CPU and fail-safe I/O to the fiber-optic cable, for example, OBT

Configuration Example of S7 F Systems: Single-channel I/O with Fiber-optic Cable

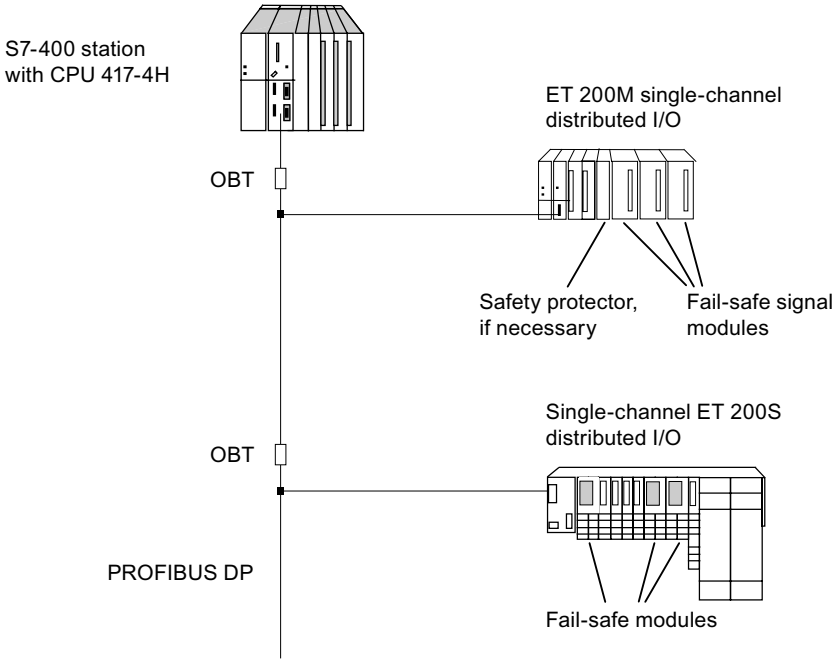


Figure 2-12 S7 F Systems with Single-channel I/O (Fiber-optic Cable)

Limits of Availability with Single-channel I/O

In the event of a fault, the I/O are no longer available. The F-I/O is passivated.

Possible fault causes:

- Failure of F-I/O
- Failure of interface module in an ET 200M, ET 200S, or ET 200pro
- Failure of the PROFIBUS DP line
- Failure of the F-CPU

2.3.3 Single-channel Switched I/O (S7 FH Systems only)

Characteristics of Single-channel Switched I/O

In a single-channel switched configuration, the F-I/O is not redundant. The F-I/O is addressed by **two F-CPUs**.

Only S7 FH Systems can have this configuration. F-I/O can only be used in ET 200M distributed I/O systems.

The ET 200M has a DP slave interface for each redundant PROFIBUS DP line, thus having a physical connection to both F-CPUs.

Required Hardware Components

Which hardware components are required depends on whether PROFIBUS DP is configured with copper cable or fiber-optic cable.

The F-I/O is not redundant.

S7 FH Systems and PROFIBUS DP with Copper Cable

The following are required to configure PROFIBUS DP with copper cable:

- Two CPU 412-3H, CPU 414-4H, or CPU 417-4H
- Two PROFIBUS DP lines
- One ET 200M with two (redundant) IM153-2 modules, each with a PROFIBUS DP interface
- Four bus connectors for connecting the two F-CPUs and the two IM153-2 modules to PROFIBUS DP
- Non-redundant fail-safe signal modules and, if necessary, standard signal modules
- Safety protector (required for SIL3/Category 4/PLe applications only)

S7 FH Systems and PROFIBUS DP with Fiber-optic Cable

The following are required to configure PROFIBUS DP with fiber-optic cables:

- Two CPU 412-3H, CPU 414-4H, or CPU 417-4H
- Two PROFIBUS DP lines
- One ET 200M with two (redundant) IM153-2 FO modules, each with a PROFIBUS DP interface
- Two components for connecting the two F-CPUs to the fiber-optic cable, for example, OBT
- Non-redundant fail-safe signal modules and, if necessary, standard signal modules
- Safety protector (required for SIL3/Category 4/PLe applications only, if

  F-SMs and standard SMs are used together in an ET 200M)

Configuration Example of S7 FH Systems: Single-channel Switched I/O

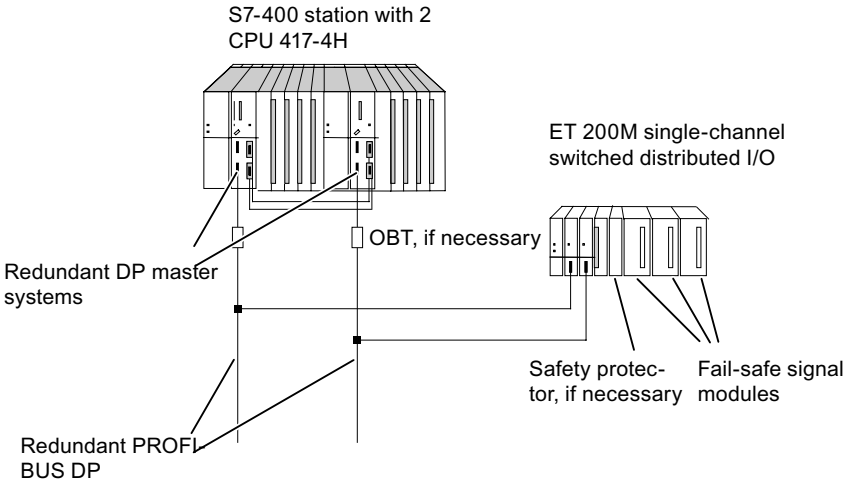


Figure 2-13 S7 FH Systems with Single-channel Switched I/O

Limits of Availability with Single-channel Switched I/O

Switched I/O are no longer available to the process in case of:

- Failure of the fail-safe signal module

  (relevant fail-safe signal module is passivated)
- Failure of the entire ET 200M

Switched I/O are still available to the process in case of:

- Failure of an IM153-2/-2 FO
- Failure of a PROFIBUS DP line
- Failure of an F-CPU

2.3.4 Redundant Switched I/O (S7 FH Systems Only)

Characteristics of Redundant Switched I/O

With redundant switched I/O, the F-I/O is redundant.

Only S7 FH Systems can have this configuration. F-I/O can only be used in ET 200M distributed I/O systems.

The two fail-safe signal modules are located either in different ET 200Ms or in one ET 200M. In the following example, the redundant signal modules are inserted in different ET 200Ms.

Required Hardware Components

Which hardware components are required depends on whether PROFIBUS DP is configured with copper cable or fiber-optic cable.

The fail-safe I/O are redundant.

S7 FH Systems and PROFIBUS DP with Copper Cable

The following are required to configure PROFIBUS DP with copper cable:

- Two CPU 412-3H, CPU 414-4H, or CPU 417-4H
- Two PROFIBUS DP lines
- Two ET 200M: each with two (redundant) IM153-2
- Six bus connectors for connecting the two F-CPUs and the four IM153-2 modules to PROFIBUS DP
- Redundant fail-safe signal modules and, if necessary, standard signal modules
- Two safety protectors (required for SIL3/Category 4/PLe applications only)

S7 FH Systems and PROFIBUS DP with Fiber-optic Cable

The following are required to configure PROFIBUS DP with fiber-optic cables:

- Two CPU 412-3H, CPU 414-4H, or CPU 417-4H
- Two PROFIBUS DP lines
- Two ET 200M: each with two IM153-2 FO
- Two components for connecting the two F-CPUs to the fiber-optic cable, for example, OBT
- Redundant fail-safe signal modules and, if necessary, standard signal modules
- Two safety protectors (required for SIL3/Category 4/PLe applications only if F-SMs and standard signal modules are used together in one ET 200M)

Configuration Example of S7 FH Systems: Redundant Switched I/O

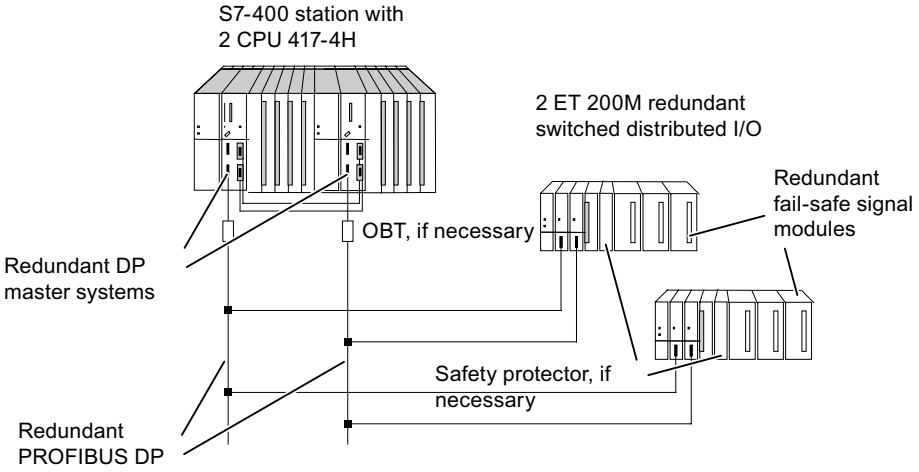


Figure 2-14 S7 FH Systems with Redundant Switched I/O

Availability with Redundant Switched I/O

The I/O are still available to the process in case of:

- Failure of a fail-safe redundant signal module
- Failure of an IM153-2/-2 FO in both ET 200Ms
- Failure of an entire ET 200M (requirement: the redundant F-SMs must be located in different ET 200Ms)
- Failure of a PROFIBUS DP line
- Failure of an F-CPU

2.4 S7 Distributed Safety or S7 F/FH Systems – Selection Guide

The Automation Task

The right solution for every automation task – for the user, this means achieving the optimum price-performance ratio.

S7 Distributed Safety or S7 F/FH Systems – Selection Criteria

The following table lists the principal F-System requirements that are critical for selection.

The last row of the table indicates which fail-safe system – S7 Distributed Safety, S7 F Systems, or S7 FH Systems – is best suited for the automation task at hand.

Table 2- 2 Selection Citeria for an F-System

Selection criteria			
Applicable F-I/O on PROFIBUS DP	• Fail-safe signal modules in ET 200M • Fail-safe signal modules in S7-300 station (centralized configuration with CPU 315F-2 DP, for example) • Fail-safe electronic modules in ET 200S • Fail-safe electronic modules in ET 200pro • ET 200eco fail-safe I/O module • Fail-safe DP standard slaves	• Fail-safe signal modules in ET 200M • Fail-safe electronic modules in ET 200S • Fail-safe electronic modules in ET 200pro • ET 200eco fail-safe I/O module • Fail-safe DP standard slaves	
Applicable F-I/O on PROFIBUS DP	-	• Fail-safe PA field devices	
Applicable F-I/O on PROFINET IO	• Fail-safe electronic modules in ET 200S • Fail-safe electronic modules in ET 200pro • Fail-safe I/O standard devices	-	
Requirement for typical response time of the F-System	100 ms to 200 ms	200 ms to 500 ms	
Integration in a control system	Integration not required	Integration in a PCS 7 process control system required	
Requirement for programming language	Standard programming languages (LAD, FBD) in *STEP 7* must be used	CFC must be used for programming (simple integration in a control system possible)	
Automatic generation of the safety program using the cause-effect matrix	-	Using the Safety Matrix	
Availability requirement for the F-System	Normal availability of the F-System is sufficient	Normal availability is sufficient	Increased availability or highest level of availability is required
Solution...	**S7 Distributed Safety**	**S7 F Systems**	**S7 FH Systems**

Requirements Satisfied by Both S7 Distributed Safety and S7 F/FH Systems

There is no difference in the F-Systems with regard to the following requirements. That is, S7 Distributed Safety and S7 F/FH Systems are equally applicable:

- Configuration is possible using copper or fiber-optic technology.

  (Fiber-optic technology should be used in standard automation systems if large distances are to be spanned or if the system will be subjected to strong electromagnetic interference.)

- Safety integrity levels SIL2/Cat.3/PLd and SIL3/Cat.4/PLe can be achieved.

System Configuration of F-System

The limits for the system configuration of a fail-safe system are determined mainly by the F-CPU used. The memory configuration for all applicable F-CPUs is listed in the "Memory Configuration of F-CPUs" table, chapter "Performance Characteristics of S7 Distributed Safety and S7 F/FH Systems" (Page 21). Additional values are listed in the technical data for the F-CPU in the manual and Product Information of the F-CPU.

For information about possible restrictions for S7 FH Systems, refer to the "S7-400H Automation System, Fault-tolerant Systems" (http://support.automation.siemens.com/WW/view/en/1186523/) Manual and to the readme file of the *S7 H Systems* optional package.

Communication Options

3

3.1 Introduction

Overview

This chapter presents the safety-related communication options in S7 Distributed Safety and S7 F/FH Systems and presents the similarities and differences between the two F-Systems.

Additional Information

Communication can take place between standard user programs exactly the same as in standard S7-300 and S7-400 automation systems and is not presented in this chapter. You will find a description in the *STEP 7* manuals and in the hardware manuals for each CPU.

The user employs fail-safe blocks to some extent for safety-related communication. F-blocks and their handling are described in detail in the following references:

- for S7 Distributed Safety in the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) manual
- for S7 F/FH Systems in the "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) manual

3.2 Overview of Safety-Related Communication

Communication Overview

The following figure illustrates the communication options for the F-Systems S7 Distributed Safety or S7 F/FH systems.

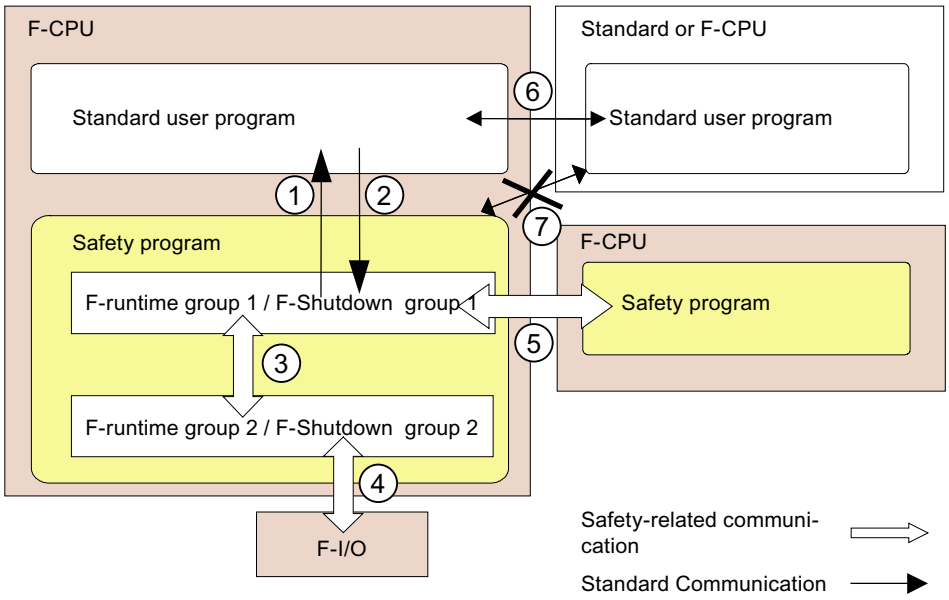


Figure 3-1 Overview of F-System Communication

Table 3- 1 Communication Options

No.	Communication Between ...	And ...	Safety-Related	See Section ...
1	Safety program in F-CPU	Standard user program in F-CPU	No	Chapter "Communication between Standard User Program and Safety Program" (Page 63)
2	Standard user program in F-CPU	Safety program in F-CPU	No	Chapter "Communication between Standard User Program and Safety Program" (Page 63)
3	F-runtime group F-shutdown group	F-runtime group F-shutdown group	Yes	Chapter "Communication between F-runtime groups or F-Shutdown groups" (Page 66)
4	Safety program in F-CPU	F-I/O	Yes	Chapter "Communication between F-CPU and F-I/O" (Page 68) Chapter "F I/O access and safety-related communication via WLAN" (Page 85)

No.	Communication Between ...	And ...	Safety-Related	See Section ...
5	Safety program in F-CPU	Safety program in F-CPU	Yes	Chapter "Safety-Related CPU-CPU Communication" (Page 75) Chapter "F I/O access and safety-related communication via WLAN" (Page 85)
6	Standard user program in standard or F-CPU	Standard user program in standard or F-CPU	No	*CPU manual*
7	Safety program in F-CPU	Standard user program in standard or F-CPU	Communication is not possible	-

3.3 Communication between Standard User Program and Safety Program

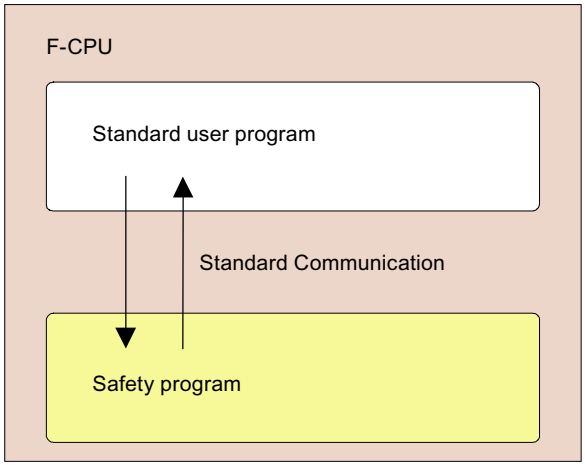


Figure 3-2 Communication between Standard User Program and Safety Program

Data

In the standard user program, all of the data in the safety program can be evaluated.

In the safety program, only fail-safe data or fail-safe signals of F-I/O and other safety programs (in other F-CPUs) can be processed. Data from the standard user program cannot be processed in the safety program unless they are subject to a validity check. The in-plant safety experts are responsible for ensuring this and implementing the validity check. In case of doubt, these data must be generated by a safety program.

Differences between S7 Distributed Safety and S7 F/FH Systems

In S7 Distributed Safety, data are exchanged between the safety program and the standard user program in the F-CPU using memory bits or by accessing the process image of the inputs and outputs of the standard I/O.

In addition, the standard user program can access F-shared DBs, F-DBs, and instance data blocks of the safety program.

In S7 F/FH systems, different data formats are used in the safety program and the standard user program of the F-CPU; special F-blocks must be used to convert these data formats for exchange of data between the safety program and the standard user program.

3.3.1 Communication between Standard User Program and Safety Program in S7 Distributed Safety

Data Transfer from the Safety Program to the Standard User Program

The standard user program can read out all of the data in the safety program directly, since the data exist in standard format in F-DBs, instance DBs, the F-shared DB, and the process image.

Memory bits can also be written in the safety program to enable intermediate results of the safety program to be used by the standard user program without having to pass through F-data blocks. However, these memory bits are only available for processing by the standard user program and cannot be read in the safety program itself.

The process output image (PIO) of the standard I/O can be written to, for example, for display purposes. These values cannot be read in the safety program, either.

Data Transfer from the Standard User Program to the Safety Program

To process data from the standard user program in the safety program, memory bits from the standard user program or signals from the standard I/O can be read using the process input image (PII). Because these data are unsafe, the user must perform additional process-specific validity checks in the safety program to ensure that no hazardous situations can arise.

To facilitate the validity check, all signals from the standard user program that are evaluated in the safety program are included when the safety program is printed out. Addresses in the safety program that come from the standard user program are highlighted.

3.3.2 Communication between Standard User Program and Safety Program in S7 F/FH Systems

Different Data Formats

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

In an F-CPU in S7 F/FH systems, the user employs special conversion blocks for the data exchange.

Data Transfer from the Safety Program to the Standard User Program

If data from the safety program are to be processed further in the standard user program, e.g., for monitoring, then an F_F*data type_data type* data conversion block must be connected between the two programs in CFC to convert F-data types to standard data types. These blocks can be found in the *S7 F Systems Lib* F-library.

The F_F*data type_data type* blocks must be called in the standard user program (CFC, standard runtime group).

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. The user must perform additional process-specific validity checks in the safety program to ensure that no hazardous conditions can arise.

To process data from the standard user program, safety-related F-data types must be generated from standard data types with the aid of F_*data type*_F*data type* data conversion blocks. These blocks can be found in the *S7 F Systems Lib* F-library.

The F_*data type*_F*data type* data conversion blocks must be called in the safety program (CFC, F-runtime group).

3.4 Communication between F-runtime groups or F-Shutdown groups

F-runtime Groups

S7 Distributed Safety: An F-runtime group is a logical construct made of several related F-blocks.

S7 F/FH Systems: Runtime groups containing fail-safe blocks are called F-runtime groups.

F-shutdown groups: S7 F/FH Systems

An F-shutdown group represents a self-contained entity of the safety program. It contains the user logic which is simultaneously executed or shut down. An F-shutdown group contains one or several F-runtime groups which are assigned to a shared task (OB).

Communication overview: Communication between F-runtime groups

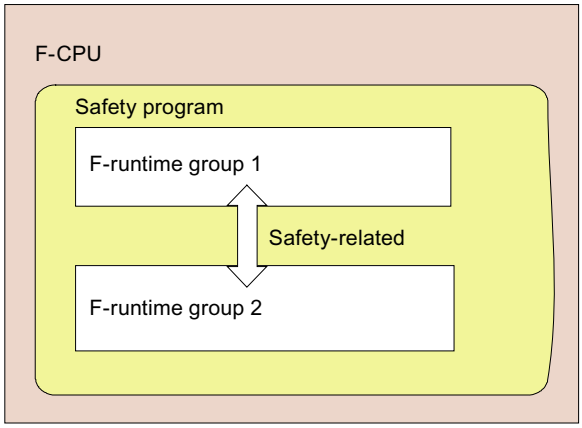


Figure 3-3 S7 Distributed Safety: Communication between F-runtime groups

Communication overview: Communication between F-Shutdown groups

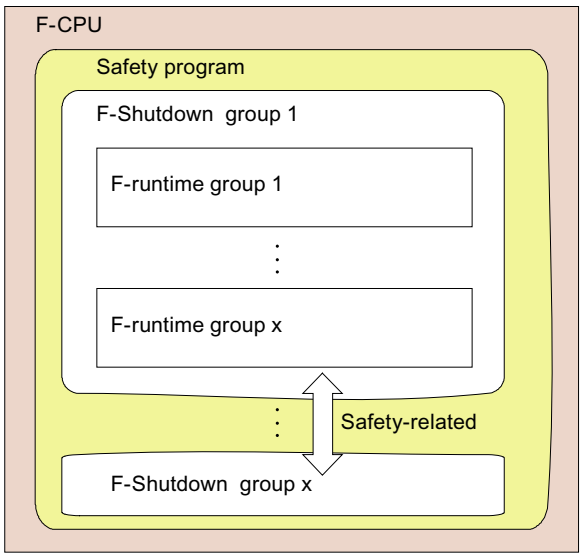


Figure 3-4 S7 F/FH Systems: Communication between F-Shutdown groups

Communication

Communication between the F-runtime groups or F-Shutdown groups of a safety program is safety-related.

S7 Distributed Safety: F-runtime group communication can take place between the two F-runtime groups of a safety program in S7 Distributed Safety. Communication takes place via the "DB for F-runtime group communication".

S7 F/FH Systems: Fail-safe blocks for F-Shutdown group communication are available in the *S7 F Systems Lib* F-library. These fail-safe blocks can be used to transfer a fixed number of parameters of the same F-Data type.

In S7 F Systems, it is not required to make any further provisions for communication between the F-runtime groups of a shared F-shutdown group. The F-blocks can be interconnected based on the assumption that they belong to the same F-runtime group.

3.5 Communication between F-CPU and F-I/O

Introduction

Both safety-related communication and - depending of the F-I/O used - standard communication can take place between the F-CPU and F-I/O. This section describes these two communication types.

3.5.1 Safety-Related Communication

Communication Overview

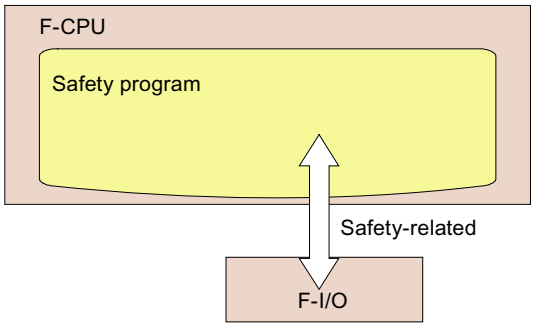


Figure 3-5 Safety-Related Communication between F-CPU and F-I/O

Differences in the F-I/O Connection between S7 Distributed Safety and S7 F/FH Systems

Connection of F-I/O differs in the two F-systems with respect to integration in the safety program and the associated user actions:

In S7 Distributed Safety, safety-related communication takes place the same as in standard automation systems via the process image (PII and PIO). The I/O cannot be accessed directly.

The process input image is updated at the beginning of the F-runtime group, before the F-program block is executed. The process output image is updated at the end of the F-runtime group, after the F-program block is executed.

The actual communication between the F-CPU (process image) and the F-I/O to update the process image occurs in the background using a special safety protocol in accordance with PROFIsafe.

In S7 F/FH Systems, safety-related communication takes place via inputs and outputs of F-driver blocks. The user must position and interconnect special F-driver blocks in the CFC charts of the F-runtime group.

Variables for F-I/O communication are made available **to both F-systems** for evaluation by the user. The difference lies in how the variables are made available. In S7 Distributed Safety, variables are provided in F-I/O DBs, while in S7 F/FH systems, variables are provided as inputs and outputs of F-driver blocks.

3.5.2 Accessing F-I/O in S7 Distributed Safety

Introduction

For the most part, the F-I/O is accessed in the background in S7 Distributed Safety.

What is to be done?

The following table presents the user actions required for F-I/O access and the effects of these actions on the F-System.

Table 3- 2 Accessing F-I/O in S7 Distributed Safety

Step	Action Required	Effect on F-I/O Connection
1.	Configure and assign parameters for F-I/O in *HW Config*	Required for connection of F-I/O
2.	Save and compile configuration in *HW Config*	*S7 Distributed Safety* generates one F-I/O DB and one symbol in in the symbol table for each F-I/O. (In the safety program, the user must have symbolic access to certain variables for F-I/O communication in the F-I/O DB.)
3.	Create the F-CALL (call block for safety program)	*S7 Distributed Safety* provides for the connection of the F-I/O to the safety program in the F-CALL. The F-CALL block cannot be edited by the user.
4	Create the safety program with accesses to the process image	*See section below*
5.	Call "Edit Safety Program" dialog in *SIMATIC Manager* and define the F-runtime group(s).	This dialog box displays all F-blocks of a safety program, including the F-I/O data blocks of the F-I/O.
6.	Compile safety program	Consistency check of the safety program with all valid F-blocks.
7.	Download safety program to F-CPU	Downloads the safety program to the F-CPU (including F-I/O data blocks).

Process Data of the F-I/O

Process data from/to the F-I/O can be found in the process image (PII and PIO) of the F-CPU.

The user uses the start addresses of the F-I/O to access the F-I/O in the process image (PII, PIO). The start addresses are automatically entered in the configuration table in *HW Config* (input/output addresses) and can be changed.

Variables for F-I/O Communication

Certain variables **must** be initialized by the user in the safety program in the F-I/O DB:

- Variables for acknowledging communication errors and F-I/O or channel faults for reintegration of F-I/O

In addition, certain variables **can** be initialized and evaluated in the F-I/O data block:

- Evaluation of whether the output value represents process data or a fail-safe value
- Setting for automatic or manual reintegration of process data
- Passivation of other F-I/O or channels, e.g., for group passivation of associated F-I/O
- Display of whether or not an acknowledgment is required for reintegration of F-I/O
- Display of service information (type of fault)

Additional Information

For a detailed description of the F-I/O DB variables and how to initialize and evaluate them, refer to the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) manual.

3.5.3 S7 Distributed Safety Safety-Related I-Slave-I-Slave Communication

Introduction

In S7 Distributed Safety, safety-related I-slave-slave communication between the safety program of the F-CPU of an I-slave and F-I/O of a slave is performed with direct data exchange – as it is in standard programs. The process input image is used to access the channels of the F-I/O in the safety program of the F-CPU of the I-slave (PII and PIO).

Restrictions

Note

Safety-related I-slave-slave communication with F-I/O is possible in a DP slave that supports safety-related I-slave-slave communication, e.g. with all ET 200S F-Modules and fail-safe S7-300 signal modules with IM 153-2, as of order no. 6ES7153-2BA01-0XB0, firmware > V4.0.0.

Communication Overview

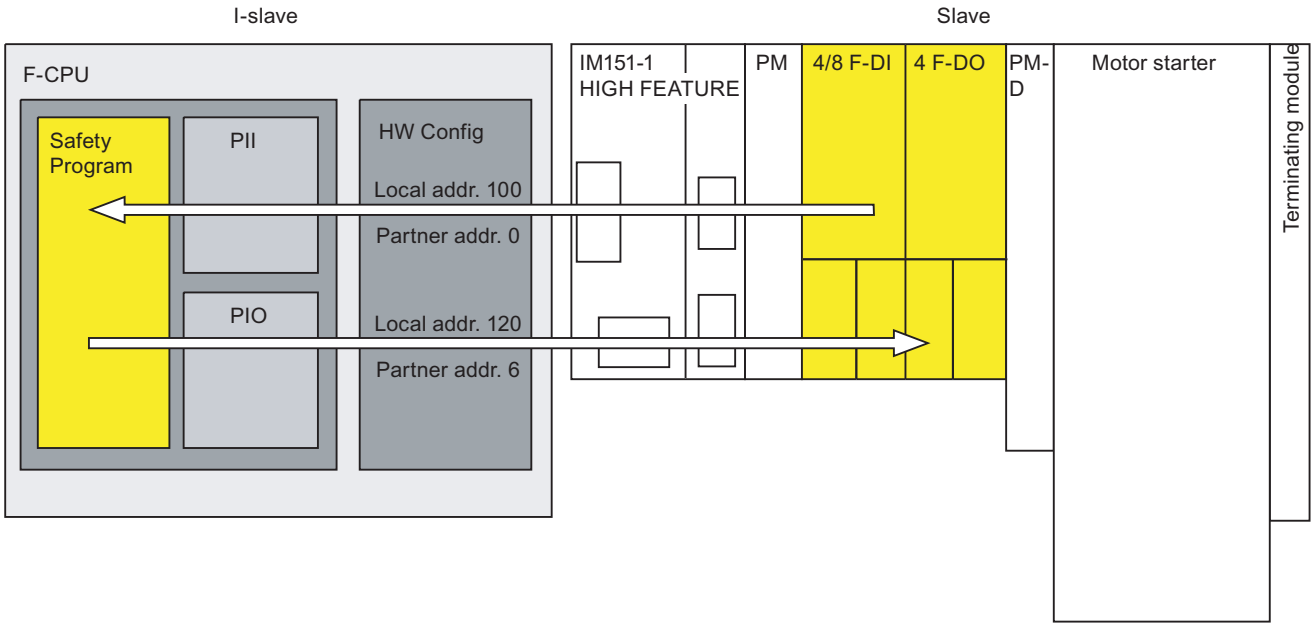


Figure 3-6 S7 Distributed Safety: Safety-related I-Slave-Slave Communication

I-Slave-Slave Communication

In safety-related I-slave-slave communication, F-I/O are accessed the same as standard I/O using the process image (PII and PIO). The I/O cannot be accessed directly. The channels of an F-I/O can only be accessed from one F-runtime group.

What is to be done?

The user performs the following steps for safety-related I-slave-slave communication:

1. Configure I-slave and slave in *HW Config*.
2. Configuring the DP master system in *HW Config*
3. Connect the I-slave to the slave.
4. Set the address areas for data exchange in *HW Config* in the "Object Properties" dialog of the I-slave.
5. Once the safety program has been created, generate and download it to the F-CPU of the I-slave.

Additional information

For detailed information on configuring
safety-related I-slave-slave communication, refer to the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) manual.

3.5.4 Accessing F-I/O in S7 F/FH Systems

Access via F-Driver Blocks

In S7 F/FH Systems, the F-I/O is accessed via F-Driver blocks, which must be positioned and interconnected by the user in some cases.
One fail-safe module driver per F-I/O and one fail-safe channel driver for each F-I/O input and output channel used are required.

Fail-safe module driver

The fail-safe module driver takes over the PROFIsafe communication between the safety program and the F-I/O. It is automatically positioned and interconnected in the safety program.

F-Channel Drivers

The fail-safe channel drivers in the safety program form the interface to a channel of the F-I/O and process signals. Different fail-safe channel drivers are available for different F-I/O (e.g. fail-safe DP standard slaves, PA field devices, Siemens F-modules and fail-safe modules) and data types. Users must install and interconnect the fail-safe channel drivers in the safety program.

What is to be done?

The user must perform the following steps to connect the F-I/O:

1. Configuring and parameterizing the F-I/O in *HW Config*.
2. Selecting appropriate fail-safe channel drivers from the *S7 F Systems Lib* F-library and installing them in the safety program.
3. Interconnect the fail-safe channel drivers.
4. Once the safety program has been created, compile and download it to the F-CPU.

Process Data of the F-I/O

Process data can be found as follows:

- Process data from the F-I/O (input channels), at an output of the associated fail-safe channel driver
- Process data to the F-I/O (output channels), at an input of the associated fail-safe channel driver

Parameters for F-I/O communication

Certain parameters **must** be set by the user at fail-safe channel drivers:

- Parameters for acknowledging communication errors and F-I/O / channel faults for reintegration of F-I/O

In addition, certain parameters **can** be set and evaluated by the user at fail-safe channel drivers:

- Evaluation of whether the output value represents process data or a fail-safe value
- Setting for automatic or manual reintegration of process data
- Passivation of other F-I/O or channels, e.g., for group passivation of associated F-I/O
- Display of whether or not an acknowledgment is required for reintegration of F-I/O
- Display of service information (type of fault)

Additional information

For a detailed description of the parameters and how to set and evaluate them, refer to the "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) manual.

3.5.5 Standard Communication

Communication overview

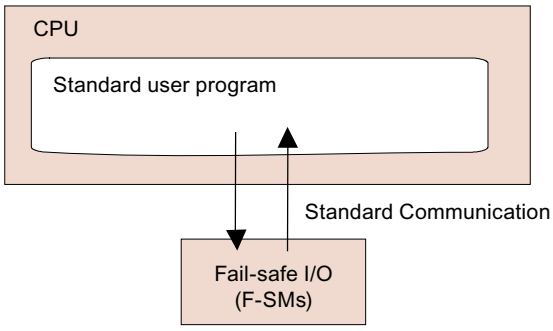


Figure 3-7 Standard Communication between CPU and F-I/O

Standard Communication (Standard Mode)

F-I/O can also be used in standard mode for standard applications. This is useful, for example, if the diagnostic functions provided by the F-I/O are relevant in the standard application or if flexibility is a priority (F-I/O can be used in both the standard system and the fail-safe system).

Whether or not standard mode is an option depends on the type of F-I/O used. Only the S7-300 fail-safe signal modules can be used in standard mode (exception: SM 326; DO 8 × DC 24V/2A and SM 336; F-AI 0/4 ... 20 mA HART). The ET 200S, ET 200pro, and ET 200eco fail-safe modules operate only in safety mode and never operate in standard mode.

Mechanisms in Standard Mode

The mechanisms commonly used in standard automation systems can be used for standard mode between the CPU and S7-300 fail-safe signal modules. These include:

- Direct access
- Access via the process image
- In CFC, access via channel drivers of the *PCS 7 Drivers* library (S7 F/FH Systems only)
- Reading out diagnostic data records

Reading Out Diagnostic Data as in Standard Mode

Diagnostic information from fail-safe signal modules ET 200S and ET 200pro, and the ET 200eco fail-safe I/O module is not relevant for safety. As in standard mode, diagnostic data record transfers are used to transfer this information to the F-CPU and enter it in the diagnostic buffer of the F-CPU and F-SMs acyclically.

Diagnostic data can be read out by the user with *STEP 7* as follows:

- From the diagnostic buffer of the F-CPU and F-SMs
- As slave diagnostics of the ET 200S, ET 200pro and ET 200eco fail-safe modules
- In the standard user program with SFC 59 (F-SMs only)

Reading Out Diagnostic Data in Safety Mode of F-SMs

When F-SMs are operated in safety mode, the diagnostic data records of the F-SMs can also be read out to the standard user program with SFC 59.

PCS 7 provides module diagnostics blocks. Those blocks generate automatic messages, e.g., to *WinCC* and also for the F-SMs.

3.6 Safety-Related CPU-CPU Communication

Introduction

S7 Distributed Safety and S7 F/FH Systems support safety-related communication between safety programs in different F-CPUs and between both F-Systems. However, the communication mechanisms for each are different:

Table 3- 3 Overview of Communication between F-CPUs

F-System	Communication via ...	Communication between ...
S7 Distributed Safety	PROFIBUS DP/PROFINET IO by means of IE/PB-Link	DP master/DP master
	PROFIBUS DP/PROFINET IO by means of IE/PB-Link	DP-master/I-slave
	PROFIBUS DP/PROFINET IO by means of IE/PB-Link	I-slave/I-slave
	PROFINET IO	IO Controller / IO Controller
	Industrial Ethernet (configured S7 connections)	Not relevant
S7 F/FH Systems	Via PROFIBUS, MPI, Industrial Ethernet, etc: Configured standard or fault-tolerant S7 connections	Not relevant

3.6.1 S7 Distributed Safety: Safety-related Master-Master Communication

DP/DP coupler

In S7 Distributed Safety, a DP/DP coupler (order number 6ES7 158-0AD01-0XA0) must be used for safety-related communication between the safety programs in different F-CPUs (DP masters).

Each F-CPU is linked to the DP/DP coupler via its PROFIBUS DP interface.

Communication overview

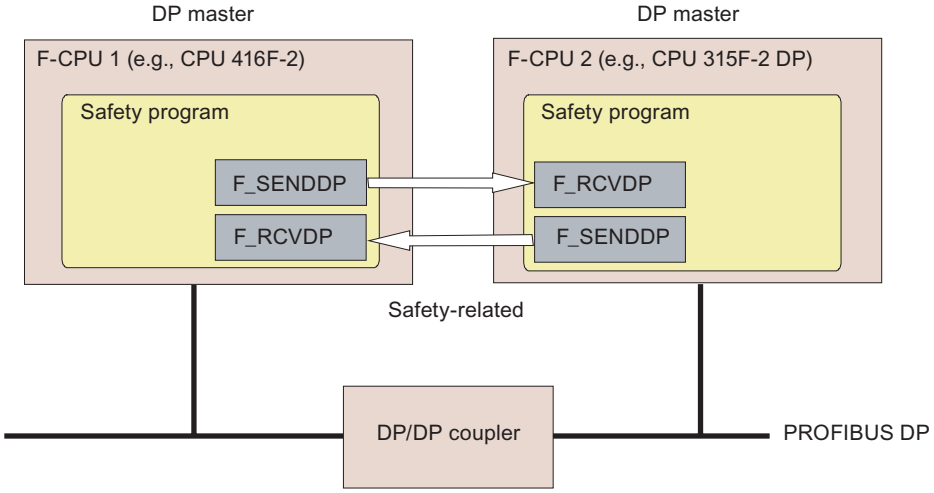


Figure 3-8 S7 Distributed Safety: Safety-related master-master communication

Master-master communication

Safety-related communication takes place with the aid of two fail-safe application blocks: the F_SENDDP block for sending data and the F_RCVDP block for receiving data. These blocks are called by the user in the respective safety program of the F-CPU. The blocks can be used for the fail-safe transfer of a fixed number of fail-safe data of data types BOOL and INT.

What is to be done?

The user performs the following steps for safety-related master-master communication:

1. Set up hardware with a DP/DP coupler
2. Configure the DP/DP coupler in *HW Config*
3. Call F_SENDDP and F_RCVDP from the *Distributed Safety* F-library in the safety program of the respective F-CPU
4. Assign parameters for F_SENDDPs and F_RCVDPs
5. Once the safety programs have been created, compile and download them to the appropriate F-CPU.

Additional information

For information on the DP/DP coupler, refer to its documentation and to the "SIMATIC NET, PROFIBUS Networks" (http://support.automation.siemens.com/WW/view/en/1971286) manual. For detailed information on configuring and programming safety-related master to master communication, refer to the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) manual.

3.6.2 S7 Distributed Safety: Safety-related Master-I-Slave Communication

Introduction

In S7 Distributed Safety, safety-related CPU-CPU communication between the safety program of the F-CPU for the DP master and the safety program(s) of the F-CPU(s) for one or more I-slaves takes place over master-slave connections, as in standard systems.

Communication Overview

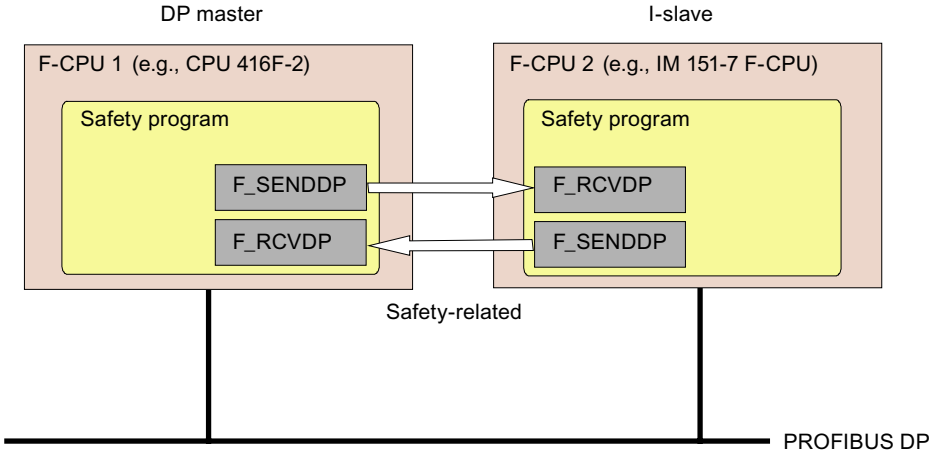


Figure 3-9 S7 Distributed Safety: Safety-related master-I-slave communication

Master-I-Slave Communication

Safety-related communication is handled using two fail-safe application blocks, i.e., the F_SENDDP block for sending data and the F_RCVDP block for receiving data. These blocks are called by the user in the respective safety program of the F-CPU. The blocks can be used for the fail-safe transfer of a fixed number of fail-safe data of data types BOOL and INT.

What is to be done?

The user should carry out the following steps for safety-related master-I-slave communication:

1. Configure I-slave in *HW Config*
2. Configuring the DP master system in *HW Config*
3. Connect the I-slave to the DP master
4. Set the address areas for data exchange in *HW Config*
5. Call F_SENDDP and F_RCVDP from the *Distributed Safety* F-library in the safety programs of the F-CPU for the DP master and I-slave
6. Assign parameters for F_SENDDPs and F_RCVDPs
7. Once the safety programs have been created, compile and download them to the appropriate F-CPU.

Additional information

For detailed information on configuring and programming safety-related master to I-slave communication, refer to the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) manual.

3.6.3 S7 Distributed Safety: Safety-Related I-Slave-I-Slave Communication

Introduction

In S7 Distributed Safety, safety-related CPU-CPU communication between the safety programs of the F-CPUs for I-slaves takes place in standard mode via data exchange.

Communication Overview

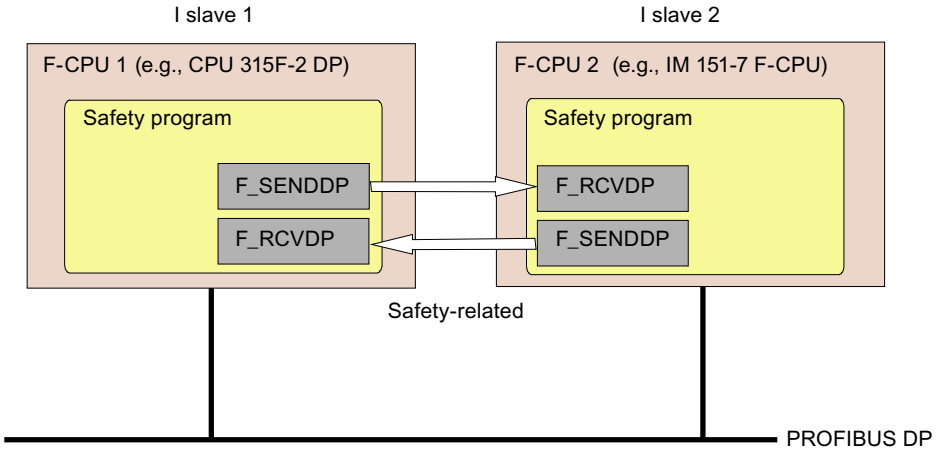


Figure 3-10 S7 Distributed Safety: Safety-Related I-Slave-I-Slave Communication

I-Slave-I-Slave Communication

Safety-related communication is handled using two fail-safe application blocks, i.e., the F_SENDDP block for sending data and the F_RCVDP block for receiving data. These blocks are called by the user in the respective safety program of the F-CPU. The blocks can be used for the fail-safe transfer of a fixed number of fail-safe data of data types BOOL and INT.

What is to be done?

The user performs the following steps for safety-related I-slave-I-slave communication:

1. Configure I-slaves in *HW Config*
2. Configuring the DP master system in *HW Config*
3. Connect the I-slaves to the DP master
4. Set the address areas for data exchange in *HW Config*
5. Call F_SENDDP and F_RCVDP from the *Distributed Safety* F-library in the safety programs of the F-CPUs for the relevant I-slaves
6. Assign parameters for F_SENDDPs and F_RCVDPs
7. Once the safety programs have been created, compile and download them to the appropriate F-CPU.

Additional information

For detailed information on configuring and programming safety-related I-slave to I-slave communication, refer to the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) manual.

3.6.4 S7 Distributed Safety: Safety-related communication between I/O controllers

Introduction

Safety-related communication between the safety-programs in the F-CPUs of IO controllers is handled by means of PN/PN Coupler (order no. 6ES7158-3AD00-0XA0) which interconnects both F-CPUs.

Reference

The information pertaining to safety-relevant master to master communication provided in chapter "S7 Distributed Safety: Safety-related Master-Master Communication (Page 75)" applies accordingly.

3.6.5 S7 Distributed Safety: Safety-Related Communication via S7 Connections

Introduction

Safety-related CPU to CPU communication via S7 connection between the safety programs of two F-CPUs is handled in **S7 Distributed Safety** similar to the standard by means of the configuration of connection tables in *NETPro*.

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

Communication overview

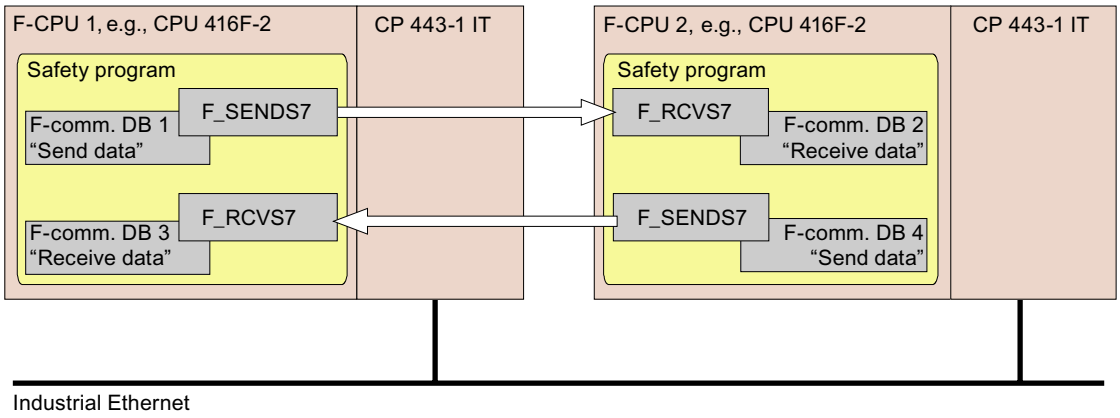


Figure 3-11 S7 Distributed Safety: Communication via S7 connections

Communication via S7 Connections

Safety-related communication takes place with the aid of two fail-safe application blocks: the F_SENDS7 block for sending data and the F_RCVS7 block for receiving data. These blocks are called by the user in the respective safety program of the F-CPU. Using these fail-safe application blocks, a user-defined amount of fail-safe data of data types BOOL, INT, WORD, or TIME can be transferred in a fail-safe manner. The fail-safe data are applied to F-DBs ("F-Communication DB") on the sending and receiving side.

What is to be done?

The user performs the following steps for safety-related communication via S7 connections:

1. Configure the S7 connection for each F-CPU in *STEP 7 NetPro*.
2. Create an F-Communication DB for both the send and receive data.
3. Initialize the variables of the F-Communication DB for sending with variables.
4. Call F_SENDS7 in the safety program from where data are to be sent.
5. Call F_RCVS7 in the safety program in which data are to be received.
6. Assign parameters to F_SENDS7 and F_RCVS7.
7. After having been created, compilation of the safety programs and their transfer to the corresponding F-CPU.

Limitations for S7 Distributed Safety

Note

In Distributed Safety, S7 connections are generally allowed via Industrial Ethernet only!

Safety-related communication via S7 connections can take place to and from the following CPUs:

- CPU 315F-2 PN/DP (only via PN interface of the CPU)
- CPU 317F-2 PN/DP (only via PN interface of the CPU)
- CPU 319F-3 PN/DP (only via PN interface of the CPU)
- CPU 416F-3 PN/DP
- CPU 416F-2 **as of firmware version V 4.0**

Additional information

You can find information on configuring S7 connections in the *STEP 7 online help*.

For detailed information on configuring and programming safety-related communication via S7 connections, refer to the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) manual.

3.6.6 S7 F/FH Systems: Safety-Related Communication via S7 Connections

Introduction

Safety-related CPU to CPU communication via S7 connection between the safety programs of two F-CPUs is handled in **S7 F/FH Systems** similar to the standard by means of the configuration of connection tables in *NETPro*.

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

Communication overview

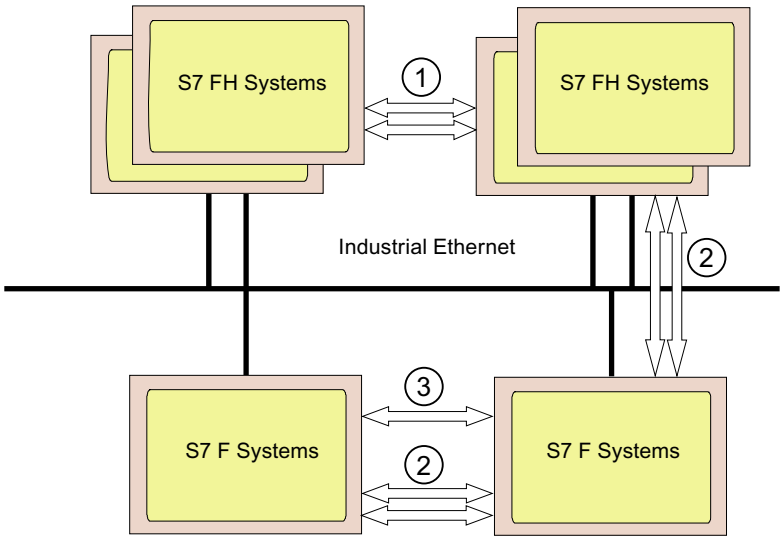


Figure 3-12 S7 F/FH Systems: Communication between F-CPUs

Table 3- 4 Safety-Related CPU-CPU Communication

Number	Communication From…	To…	Connection Type	Safety-Related
1	S7 FH Systems	S7 FH Systems	S7 connection, fault-tolerant	Yes
2	S7 F/FH Systems	S7 F Systems	S7 connection, fault-tolerant	Yes
3	S7 F Systems	S7 F Systems	S7 connection	Yes

Communication via S7 connections

Safety-related communication is handled using the fail-safe blocks F_SENDBO, F_SENDR and F_SDS_BO blocks for sending data, and F_RCVBO, F_RCVR and F_RDS_BO for receiving data. These blocks are called by users in the relevant safety program of the F-CPU. These F-blocks can be used to transfer a fixed volume of fail-safe data of the types BOOL and INT.

What is to be done?

Users carry out the following tasks to implement safety-related communication via S7 connections:

1. Configuring the S7 connection for each F-CPU in *STEP 7 NetPro*
2. Selecting, interconnecting and parameterizing fail-safe blocks from the *S7 F Systems Lib* F-library in the safety program of the corresponding F-CPU for CPU to CPU communication.
3. Once the safety programs have been created, compile and download them to the appropriate F-CPU.

F-CPUs for safety-related communication via S7 connections

Note

S7 F/FH Systems support safety-related communication via S7 connections with the following F-CPUs:

- CPU 412-3H
- CPU 414-4H
- CPU 417-4H

Additional information

You can find information on configuring the possible connection types in the *STEP 7 online help*.

For detailed information on configuring and programming safety-related communication via S7 connections, refer to the "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) manual.

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

Introduction

Safety-related CPU to CPU communication between S7 Distributed Safety and S7 F systems is possible via S7 connections by means of the configuration of connection tables in *NetPro,*.

Communication overview

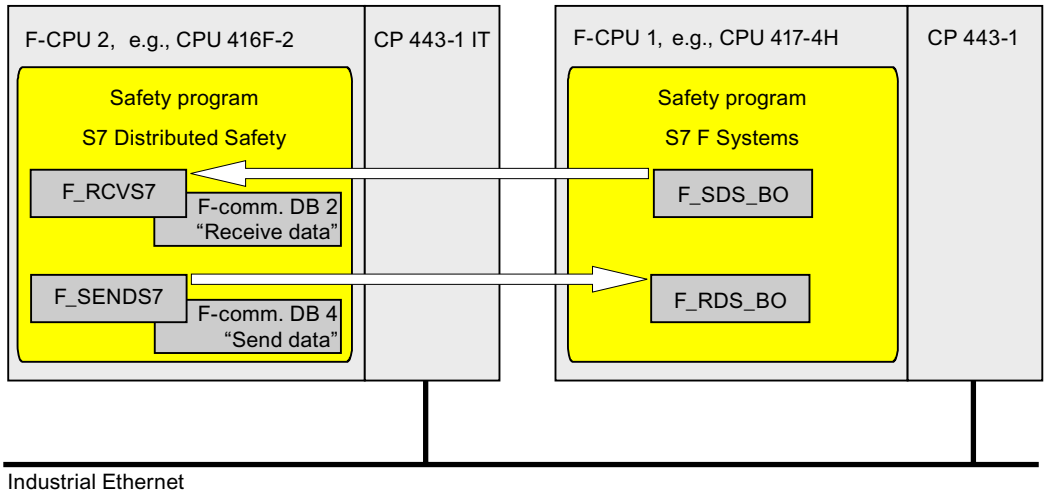


Figure 3-13 Safety-related communication between S7 Distributed Safety and S7 F-Systems

Communication via S7 connections

Safety-related communication is handled using fail-safe application blocks for sending data and receiving data which users call in the corresponding safety program of the F-CPU. Those F-application blocks can be used to exchange up to 32 data packets of the type BOOL.

What is to be done?

Users carry out the following tasks to implement safety-related communication between S7 Distributed Safety and S7 F Systems:

1. Configuring the S7 connection for each F-CPU in *STEP 7 NetPro*
2. in *S7 F Systems*: Installing, interconnecting and parameterizing the F-blocks F_SDS_BO/F_RDS_BO in the safety program of the F-CPU.
3. in *S7 Distributed Safety*: in the safety program of the F-CPU:
   - creating two F-communication DBs with precisely 32 data of the type BOOL
   - Installing, interconnecting and parameterizing the F-blocks F_SENDS7/F_RCVS7
4. After having created the program, generation / compilation of the safety programs and their transfer to the corresponding F-CPU.

Additional information

For information on configuring S7 connections, refer to the *STEP 7 Online help*.

3.7 F-I/O access and safety-related communication via WLAN to IEEE 802.11

Notes on configuring

Observer the following information on F-I/O access and safety-related CPU to CPU communication via WLAN to IEEE 802.11:

Users must configure the access points to meet security requirements defined in the 61784-3-3 standard "Digital data communications for measurement and control - Part 3: Profiles for functional safety communications in industrial networks", chapter 9.8 "Wireless transmission channels" are met.

Usually, purchase of the IEC 61784-3 standard is subject to charges. The standard can be purchased from Beuth Verlag (http://www.beuth.de), for example. Search the website for "IEC 61784-3". The website of this publisher is also available in English language.

S7 Distributed Safety: F-I/O access via WLAN

F-I/O access, including safety-related i-slave-slave communication via WLAN, is possible in the PROFINET IO environment (or in mixed configurations on PROFIBUS DP and PROFINET IO to IE/PB-Links) based on the following conditions:

- F-CPUs and F-I/O must support PROFIsafe V2-MODE.
- The safety program must be generated with *S7 Distributed Safety* V 5.4 or higher.

Based on a hardcopy of the safety program, the acceptance test of the safety program must include validation of PROFIsafe V2-MODE for each F-I/O that is addressed via WLAN.

S7 Distributed Safety: Safety-related CPU-CPU communication via WLAN

Safety-related CPU-CPU communication via WLAN is possible in *S7 Distributed Safety* using the fail-safe application blocks F_SENDDP/F_RCVDP or F_SENDS7/F_RCVS7 of the *Distributed Safety* F-library, e.g., with the following options of safety-related CPU-CPU communication:

- Safety-related master to master communication between the IO controller and the DP master via IE/PB-Link and DP/DP Coupler
- Safety-related master to I-slave communication between the IO controller and the I-slave via IE/PB-Link
- Safety-related I-slave to I-slave communication between the I-slaves downstream of a IE/PB-Link
- Safety-related communication between IO controllers via PN/PN Coupler
- Safety-related communication via S7 connections

S7 F Systems: Safety-related CPU-CPU communication via WLAN

Safety-related CPU-CPU communication via WLAN is possible in *S7 F Systems* using the F-blocks F_SENDBO/F_RCVBO, F_SENDR/F_RCVR or F_SDS_BO/F_RDS_BO of the *S7 F Systems Lib* F-library. Safety-related communication via S7 connections is possible.

Safety in F-Systems

4

4.1 Introduction

Overview

The safety mechanisms in S7 Distributed Safety and S7 F/FH Systems F-Systems are essentially the same. Safety mechanisms visible to the user are presented in this chapter, including:

- Safety Mode
- Fault reactions
- Restart of F-System
- Password protection for F-Systems

Differences between S7 Distributed Safety and S7 F/FH Systems are individually noted.

Chapters "Standards and Certification (Page 94)" and "Safety requirements (Page 95)" provide an overview of the standards, approvals and safety requirements met by S7 Distributed Safety and S7 F/FH Systems.

Additional information

The configuring and programming manuals for S7 Distributed Safety and S7 F/FH systems present information on working with the safety mechanisms and provide more detailed information, where applicable.

Standard behavior is described in the *STEP 7* manuals and hardware manuals and is not covered in this manual.

Safety in F-Systems

⚠WARNING

S7 Distributed Safety and S7 F/FH Systems F-Systems are used to control processes that can achieve a safe state immediately as a result of a shutdown.

S7 Distributed Safety and S7 F/FH Systems can only be used for controlling processes in which an immediate shutdown does not pose a danger to persons or the environment.

Safety in F-Systems is guaranteed through the following:

- Integrated safety functions for fault detection and fault reaction
- F-System access protection

Safety Functions

The safety functions for fault detection and fault reaction are contained mainly in the safety program and the F-I/O. These functions are implemented by suitable fail-safe blocks and supported by the hardware and operating system of the F-CPU.

Access protection

Access to F-Systems is protected by assigning passwords for the F-CPU and the safety program. Access protection is described in more detail in the following manuals:

- for S7 Distributed Safety in the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) Manual
- for S7 F/FH Systems in the "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) Manual

⚠ WARNING

To protect against unauthorized F-System hardware modifications, appropriate measures must be taken, such as:

- Installation in a locked cabinet
- Using an adhesive label to protect the Micro Memory card or Flash card of the F-CPU

4.2 Safety Mode

Safety mode

In safety mode, the safety functions for fault detection and fault reaction are activated in the following:

- Fail-safe I/O
- Safety program of the F-CPU

Safety Mode of F-I/O

The "Safety mode" parameter configuration for **S7-300 fail-safe signal modules** defined in *HW Config* determines whether the modules are operated in standard mode (implementation as S7-300 standard signal modules, except SM 326; DO 8 × DC 24V/2A and SM 336; F-AI 0/4 ... 20mA HART) or in safety mode.

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

Safety Mode of Safety Program

The safety program runs in the F-CPU in safety mode. This means that all safety mechanisms for fault detection and fault reaction are activated. The safety program cannot be modified during operation in safety mode.

Safety mode of the safety program in the F-CPU can be deactivated and reactivated occasionally. So-called "deactivated safety mode" enables the safety program to be tested online and changed as needed while the F-CPU is in RUN mode.

For S7 Distributed Safety, you can switch back to safety mode only after an operating mode change of the F-CPU from RUN to STOP to RUN.

For S7 F/FH systems, an operating mode change of the F-CPU is not needed to return to safety mode.

Safety message frame

In safety mode, data are transmitted consistently between the F-CPU and F-I/O in a safety message frame. The safety message frame in accordance with PROFIsafe consists of the following:

- Process data (user data)
- Status byte/control byte (coordination data for safety mode)
- Sequence number
- CRC signature

Safety-related CPU-CPU communication also takes place using a safety message frame similar to PROFIsafe. The following information on monitoring time, sequence number, and CRC signature is also applicable.

Monitoring Time and Sequence Number

The F-CPU assigns a sequence number to the F-I/O for time monitoring of the message frame update in the PROFIsafe protocol.

A valid, current safety message frame with a valid sequence number must be received by the F-CPU and the F-I/O within an assignable monitoring time.

If a valid sequence number is not detected within the monitoring time, the F-I/O is passivated.

CRC (Cyclic Redundancy Check) Signature

A CRC signature contained in the safety message frame protects the validity of the process data in the safety message frame, the accuracy of the assigned address references, and the safety-relevant parameters.

If a CRC signature error occurs during communication between the F-CPU and F-I/O, e.g., due to intermittent electromagnetic interference, the F-I/O is passivated.

See also

Configuring the Monitoring Times (Page 136)

4.3 Fault Reactions

Safe State

The basic principle behind the safety concept is the existence of a safe state for all process variables. The value "0" represents this safe state for digital F-I/O. This applies to both sensors and actuators.

Fault Reactions in the F-CPU and Operating System

The F-CPU and the operating system react to faults in S7 Distributed Safety and S7 F/FH Systems the same way as in standard S7-300 and S7-400 systems. In addition, fault reactions are triggered in the safety program in F-Systems.

Fault Reactions in the Safety Program

All of the fault reactions in the safety program cause the process variables to go to a safe state. Specifically, the fault reactions are:

- **S7 Distributed Safety:** F-CPU goes to STOP mode.

  This state can only be overridden by restarting the F-System.

- **in S7 F Systems:** Optional shutdown of all F-Shutdown groups of the F-CPU, or only of the F-Shutdown group in which a fault was detected (F-STOP). The F-CPU does not go to STOP mode. The standard user program is not affected by the shutdown.

  The safety program / F-Shutdown group must be restarted after all faults were eliminated. This restart is executed after user acknowledgment at F-block F_SHUTDN.

- **in S7 FH Systems:** The first reaction is a master to reserve changeover. An F-STOP is triggered if the fault persists (see above "in S7 F Systems").

- Passivation of F-I/O/Channels of an F-I/O.

  F-I/O / channel faults or communication errors lead to passivation of the corresponding F-I/O or F-I/O channels and the F-CPU does not go into STOP.

  Once faults are eliminated, the F-I/O or channels of the F-I/O must be reintegrated (depassivation). Reintegration (switchover from fail-safe values to process data) occurs automatically or, alternatively, after mandatory acknowledgment by the user.

Standard diagnostic and message functions can also be implemented in response to a detected fault.

Fault Reactions in F-I/O

After having detected an F-I/O / a channel fault, an F-I/O sets the safe state at the affected channel, or at all channels, that is, it passivates the channels of this F-I/O. The F-I/O signals the detected fault to the F-CPU. In addition, the fault is signaled to the safety program in the F-CPU via a safety message frame. Once the fault is eliminated, the F-I/O must be reintegrated (depassivation) (see "Fault Reactions in Safety Program").

4.4 Restart of F-System

F-System Operating Modes

The operating modes of S7 Distributed Safety and S7 F/FH Systems differ from those of standard systems only in terms of the restart characteristics and the behavior in HOLD mode.

Restart Characteristics

When an F-CPU is switched from STOP to RUN mode, the standard user program restarts in the usual way. When the safety program is restarted, the following data blocks are initialized with values from the load memory:

- For S7 Distributed Safety: all data blocks with the F-Attribute
- For S7 F/FH Systems: all data blocks with F-Attribute

This occurs analogously to a cold restart. As a result, saved error information is lost.

The F-System automatically reintegrates the F-I/O. In contrast to the standard user program, restart OBs (OB 100 to OB 102) cannot be used in the safety program.

Restart Protection

A data handling error or an internal fault can also trigger a safety program restart with the values from the load memory. 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. The process data output block must not be released until it is safe to do so and faults have been corrected.

HOLD Mode

HOLD mode is not supported for S7 Distributed Safety and S7 F/FH Systems. If a HOLD request stops execution of the user program, this state can only be overridden by a restart of the safety program.

At S7 F Systems, the safety program can be shut down and be restarted while the F-CPU remains in RUN mode (controlled by means of F-block F_SHUTDN). The F-I/O must be re-integrated manually in this case.

4.5 Password Protection for F-Systems

Two Passwords

In addition to the standard password for the F-CPU or CPU, F-Systems require a password for the safety program.

The password for the F-CPU protects the F-Systems from unauthorized downloads to the F-CPU from the engineering system (ES) or programming device (PG).

The password for the safety program prevents unauthorized users from making changes to the safety program. In S7 Distributed Safety it also prevents any unauthorized changes to the configuration and parameterization of the F-CPU and F-I/O.

Assigning Passwords

The user parameterizing the F-CPU assigns the password for the F-CPU in the "Protection" tab in *HW Config*.

The user assigns the password for the safety program when programming/configuring the safety program. Accordingly, a dialog box is displayed automatically when the safety program is compiled the first time.

4.6 Acceptance Test of System

Who Performs the Acceptance Test?

As a general rule, the acceptance test is performed by independent experts.

Support when Preparing for Acceptance Test

When a system undergoes an acceptance test, all standards relevant to the specific application must be checked for compliance.

The following special *STEP 7* functions are available in *SIMATIC Manager* to aid the user in checking for proper use of the F-system:

- Compare safety programs
- Print safety programs

All data relevant to the acceptance test of the F-system can be accessed in *SIMATIC Manager* and printed as needed.

User Actions

Actions that are undertaken by the user to prepare the system for the acceptance test depend on the F-system that is used. For this reason, the procedures are described in the relevant configuring and programming manuals for S7 Distributed Safety and S7 F/FH systems under "System Acceptance Test."

4.7 Standards and Certification

Safety Certificate

Copies of the Safety Certificate (TÜV Certificate) for the fail-safe components of S7 Distributed Safety and S7 F/FH Systems, of the certificate report, and of the annexes for the certificate report

"Safety-Related Programmable System
SIMATIC S7 Distributed Safety"
and

"Safety-Related Programmable Systems
SIMATIC S7 F/FH Systems (formerly S7-400F and S7-400FH)"
are available upon request from:

Ms. Petra Bleicher
A&D AS RD ST Type Test
Fax No. 49 9621 80 3146
e-mail: petra.bleicher@siemens.com

Note

The annexes of the certificate report contain the valid version numbers and signatures for fail-safe components of S7 Distributed Safety and S7 F/FH Systems which must be qualified within an acceptance test!

The certificate report contains the current operating requirements to be met for S7 Distributed Safety or S7 F/FH Systems.

Standards and Guidelines Regarding Functional Safety

S7 Distributed Safety and S7 F/FH Systems F-Systems are certified to standards and guidelines for functional safety; for information, refer to the relevant safety certificate (TÜV certificate) report and corresponding annex. The current TÜV documents are available for downloading on the Web at http://support.automation.siemens.com under "Product Support".

4.8 Safety requirements

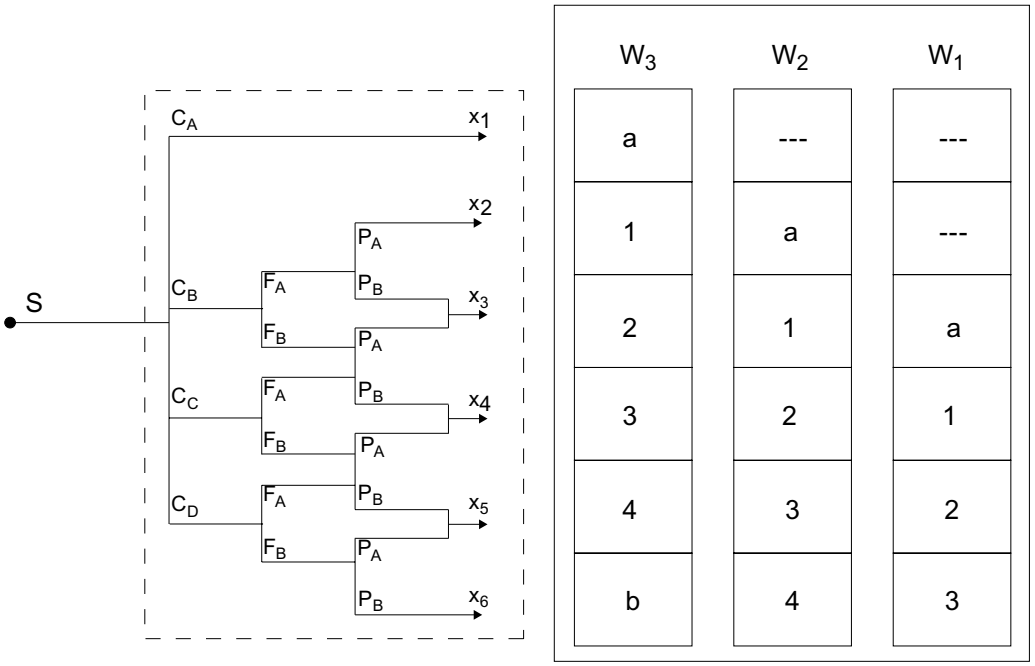
Standardized Safety Requirements

The following safety requirements can be met with S7 Distributed Safety and S7 F/FH Systems F-Systems:

- Safety class (Safety Integrity Level) SIL1 to SIL3 in accordance with IEC 61508
- Category 2 to Category 4 in accordance with EN 954-1

Determining the Safety Integrity Level in Accordance with IEC 61508-5

The qualitative methods of the risk graphs enable the safety integrity level for a safety-related system to be determined based on knowledge of the risk factors involved:



S	Starting point of the analysis for risk reduction
C	Risk parameter for the effect
F	Risk parameter for the frequency and exposure time
P	Risk parameter for possibility of avoiding dangerous occurrence
W	Probability of occurrence of undesirable event
---	No safety requirements
a	No special safety requirements
b	A single electrical/electronic/programmable electronic system is not sufficient.
1, 2, 3, 4	Safety integrity level

Figure 4-1 Risk Graphs in Accordance with IEC 61508-5

Risk parameters

Risk parameters have the following meaning in accordance with DIN V 61508-5:

Table 4- 1 Meaning of the risk parameters in accordance with IEC 61508-5

Parameter	Meaning
Effect (C)	
C_A	Minor injury
C_B	Major irreversible injury to one or more persons; fatality of a person
C_C	Multiple fatalities
C_D	Large number of fatalities
Frequency and exposure time in hazardous area (F)	
F_A	Exposed to hazardous area seldom to often
F_B	Exposed to hazardous area more often to continuous
Possibility of avoiding dangerous occurrence (P)	
P_A	Possible under certain circumstances
P_B	Almost impossible
Probability of the undesirable event (W)	
W_1	Very low
W_2	Low
W_3	Relatively high

Safety Integrity Level in Accordance with IEC 61508

For each "Safety Integrity Level“ (SIL), IEC 61508 defines the target measure to be the probability of failure of a safety function assigned to a fail-safe system.

Table 4- 2 Safety Integrity Level in Accordance with IEC 61508

Safety Integrity Level	Operation in Low Demand Mode low demand mode (average probability of failure on demand)	Operation in High Demand or Continuous Mode High demand/continuous mode (probability of a dangerous failure per hour)
4	≥ 10^{-5} to < 10^{-4}	≥ 10^{-9} to < 10^{-8}
3	≥ 10^{-4} to < 10^{-3}	≥ 10^{-8} to < 10^{-7}
2	≥ 10^{-3} to < 10^{-2}	≥ 10^{-7} to < 10^{-6}
1	≥ 10^{-2} to < 10^{-1}	≥ 10^{-6} to < 10^{-5}

Explanations for Table

In general, actuators and sensors are the largest contributor to the failure probabilities in the above table.

In all cases, the safety function encompasses the entire chain from information acquisition to information processing to the intended action.

The devices involved, such as an S7 F/FH Systems F-System, sensors, and actuators, must collectively comply with the, SIL, Category or PL determined during risk assessment.

If control functions and associated protection functions are implemented together in S7 Distributed Safety or S7 F/FH Systems, operation is in high demand mode or continuous mode.

Risk Analysis in Accordance with IEC 61508

As shown in the following figure, an F-System prevents potential dangers or reduces them to a tolerable level through appropriate organizational and technical measures.

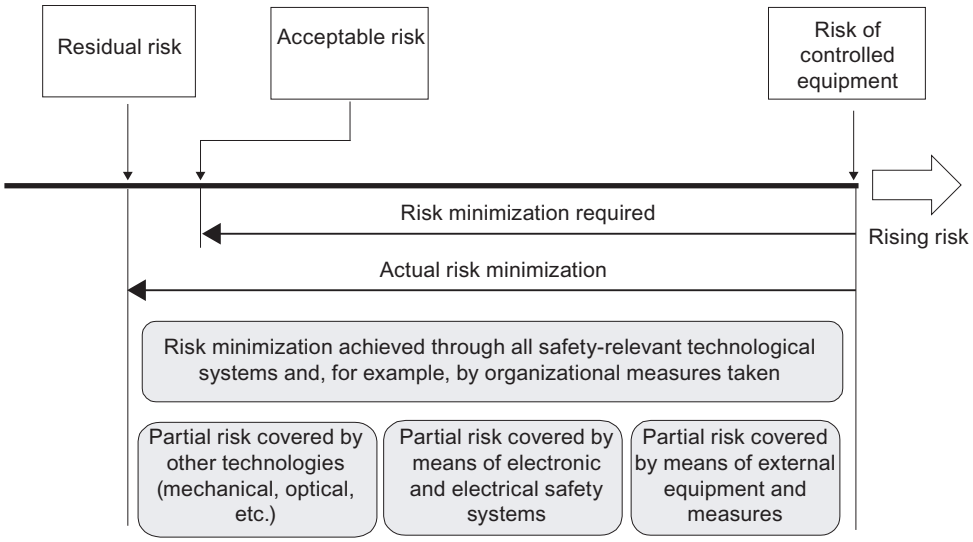


Figure 4-2 Risk Analysis in Accordance with IEC 61508

Performance Level to EN ISO 13849-1: 2006 and Correlation to the Safety Integrity Level

EN ISO 13849-1: 2006 defines a Performance Level (PL) that expresses the capability of safety-related components to execute a safety function. EN ISO 13849-1: 2006 describes the correlation between Performance Level (PL) and Safety Integrity Level (SIL).

Probability of failure values for specific components of S7 Distributed Safety and S7 F/FH Systems

The probability of failure for individual components of S7 Distributed Safety and S7 F/FH Systems is presented in the following table:

Table 4- 3 Probability Values for Individual Components of S7 Distributed Safety and S7 F/FH Systems

	Operation in Low Demand Mode low demand mode (average probability of failure on demand)	**Operation in High Demand or Continuous Mode** High demand/continuous mode (probability of a dangerous failure per hour)	**Proof-test interval**
F-Capable CPUs for S7 Distributed Safety:			
IM 151-7 F-CPU	1.59 E-05	3.62E-10	10 years
6ES7151-7FA20-0AB0	3.18E-05	3.62E-10	20 years
IM 151-8F PN/DP CPU	< 5E-05	< 2E-09	10 years
6ES7151-8FB00-0AB0	< 1E-04	< 2E-09	20 years
CPU 315F-2 DP	2.38 E-05	5.43E-10	10 years
6ES7315-6FF01-0AB0	4.76E-05	5.43E-10	20 years
CPU 315F-2 PN/DP	4.76E-05	1.09E-09	10 years
6ES7315-2FH13-0AB0	9.52E-05	1.09E-09	20 years
CPU 317F-2 DP	4.76E-05	1.09E-09	10 years
6ES7317-6FF03-0AB0	9.52E-05	1.09E-09	20 years
CPU 317F-2 PN/DP	4.76E-05	1.09E-09	10 years
6ES7317-2FK13-0AB0	9.52E-05	1.09E-09	20 years
CPU 319F-3 PN/DP	< 1E-04	< 3E-09	10 years
6ES7318-3FL00-0AB0	< 2E-04	< 3E-09	20 years
CPU 416-2	4.76E-05	1.09E-09	10 years
6ES7416-2FN05-0AB0	9.52E-05	1.09E-09	20 years
CPU 416F-3 PN/DP	4.76E-05	1.09E-09	10 years
6ES7416-3FR05-0AB0	9.52E-05	1.09E-09	20 years
F-Capable CPUs for S7 F/FH Systems:			
CPU 412-3H	1.9E-04	4.3E-09	10 years
6ES7412-3HJ14-0AB0	3.8E-04	4.3E-09	20 years
CPU 414-4H	1.9E-04	4.3E-09	10 years
6ES7414-4HM14-0AB0	3.8E-04	4.3E-09	20 years
CPU 417-4H	1.9E-04	4.3E-09	10 years
6ES7417-4HT14-0AB0	3.8E-04	4.3E-09	20 years
Safety-related communication	1.00E-05	1.00E-09	

	Operation in Low Demand Mode low demand mode (average probability of failure on demand)	**Operation in High Demand or Continuous Mode** High demand/continuous mode (probability of a dangerous failure per hour)	**Proof-test interval**
F-I/O, for example: • S7-300 F-SMs	See technical specifications in the following manuals: • "S7300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151)		
• ET 200S F-Modules	• "ET 200S Distributed I/O System - Fail-Safe Modules" (http://support.automation.siemens.com/WW/view/en/12490437)		
• ET 200pro fail-safe modules	• "ET 200pro Distributed I/O System, Fail-safe Modules" (http://support.automation.siemens.com/WW/view/en/22098524)		
• ET 200eco fail-safe I/O module	• "ET 200eco Distributed I/O Device, Fail-safe I/O Module" (http://support.automation.siemens.com/WW/view/en/19033850)		
• Fail-safe DP standard slaves	• For fail-safe DP standard slave		
• Fail-safe I/O standard devices	• To the fail-safe I/O standard devices		
• Fail-safe PA field devices	• To the fail-safe PA field device		

Determining Contribution of F-System to Probability of Failure

The contribution of the F-System to the probability of failure of a safety function is determined by summing the probabilities of failure for the F-CPUs and F-I/O involved. In so doing, redundant F-CPUs count once and redundant F-I/O twice.

(Redundant F-I/O with inputs count twice, because the input signals that are read redundantly via two addresses are internally ORed and, consequently, there are two causes of failure, that is, either one F-I/O or the other.

A redundant F-I/O with outputs counts twice, because the outputs for the two F-I/O that are activated redundantly via two addresses are ORed from the hardware point of view.)

The contribution of the safety-related communication is then added. More than one F-System can be involved with one safety function as well.

The failure probability of a safety function is calculated by adding the contribution of the F-System to the contribution of the sensors and actuators involved in the safety function.

Calculation Example

A safety function is implemented using an S7 FH Systems F-System. The F-CPUs and F-SMs indicated in the following table are involved in the safety function.

The F-CPU and F-SMs are set up redundantly. They have a proof-test interval of 10 years. The F-SMs operate in safety mode for SIL3/Cat.4/PLe. Operation is in high demand mode:

Table 4- 4 Calculation Example for the Contribution of the F-System to the Failure Probability of a Safety Function

F-CPUs, F-SMs, and Safety-Related Communication Involved in the Safety Function	**Number**	**Redundancy**	**Probability of a dangerous failure per hour** (probability of a dangerous failure per hour)
CPU 417-4H 6ES7417-4HT14-0AB0	1	Yes	4.3E-09
SM 326; DO 10 X DC 24V/2A 6ES7326-2BF01-0AB0	1	Yes	2.00E-09
SM 326; DI 24 X DC 24V 6ES7326-1BK01-0AB0	2	Yes	4.00E-09
Safety-related communication			1.00E-09
Total			**11.3E-09**

Achievable Safety Classes with F-I/O

5

5.1 Introduction

Overview

This chapter presents the options available for achieving safety classes SIL2/Cat.3/PLd and SIL3/Cat.4/PLe with fail-safe I/O in S7 Distributed Safety and S7 F/FH Systems. The information relates to the F-I/O of the SIMATIC S7 product family, that is, S7-300 F-SMs, F-Modules ET 200S and ET 200pro, and the ET 200eco fail-safe I/O module.

Additional Information

The F-I/O used determines whether the options described can be implemented in your application. This information is available in the following manuals:

- for S7 Distributed Safety, in the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) Manual
- for S7 F/FH Systems, in the "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) Manual
- for F-SMs S7-300, in the "S7300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151) Manual
- For ET 200S fail-safe modules, in the "ET 200S Distributed I/O System - Fail-Safe Modules" (http://support.automation.siemens.com/WW/view/en/12490437) Manual
- For ET 200pro fail-safe modules, in the "ET 200pro Distributed I/O System, Fail-safe Modules" (http://support.automation.siemens.com/WW/view/en/22098524) Manual
- for the fail-safe I/O module ET 200eco, in the "ET 200eco Distributed I/O Device, Fail-safe I/O Module" (http://support.automation.siemens.com/WW/view/en/19033850) Manual

Achieving the Safety Class for F-I/O with Inputs

The required safety class is achieved for F-I/O with inputs as follows:

- Internally, using test circuits and automatic tests
- Externally, by the type of sensor evaluation, that is, **the sensor wiring determines the safety class** SIL2/Cat.3/PLd or SIL3/Cat.4/PLe

  SIL3/Cat.4/PLe can also be reached by evaluating the blocks which execute a discrepancy analysis in the safety program.

Achieving the Safety Class for F-I/O with Outputs

The required safety class is achieved for F-I/O with outputs as follows:

- Internally, using test circuits and automatic tests
- Externally, by the prescribed interconnection of the actuator
  In addition, it may be necessary to have test signals from the process read by the F-I/O and evaluated by the safety program.

5.2 Safety Functions for Achieving Safety Classes for F-I/O with Inputs

Sensor Evaluation for F-I/O with Digital Inputs

For F-I/O with **digital inputs**, the required safety class is achieved through the type of sensor evaluation.

Table 5- 1 Achievable Safety Classes for F-I/O with Digital Inputs

Safety Class, Category, Performance Level, ...			... Sensor Evaluation Required	Evaluation is performed ...
In accordance with IEC 61508	In accordance with EN 954-1	In accordance with EN ISO 13849-1: 2006		
SIL2	Category 3	PLd	1oo1 evaluation	In the F-I/O
SIL3	Category 4	PLe	1oo2 evaluation	In the F-I/O; or in safety program with F-block
SIL3	Category 4	PLe	2oo3 evaluation	In safety program with F-block

Sensor Evaluation for F-I/O with Analog Inputs

For F-I/O with **analog inputs**, the required safety class is achieved through the type of sensor evaluation. The required safety class is achieved with or without redundancy of the sensors.

Table 5- 2 Achievable Safety Classes for F-I/O with Analog Inputs

Safety Class, Category, Performance Level, ...			... Sensor evaluation required	Evaluation is performed ...
In accordance with IEC 61508	In accordance with EN 954-1	In accordance with EN ISO 13849-1: 2006		
SIL3	Category 3	PLe	1oo1 evaluation	In the F-I/O (SM 336; F-AI 6 × 0/4 ... 20 mA HART only)
SIL3	Category 4	PLe	1oo2 evaluation	In the F-I/O; or in safety program with F-block
SIL3	Category 4	PLe	2oo3 evaluation	In safety program with F-block

Required User Steps

- Wire the sensor to the F-I/O according to the sensor evaluation and sensor supply requirements (1oo1 or 1oo2 evaluation, single-channel or two-channel sensor; sensor supply from the F-I/O or externally)
- Assign the following parameters using *STEP 7*:
  - Sensor evaluation (1oo1 or 1oo2)
  - Type of sensor interconnection (single-channel or two-channel)
  - Enable short-circuit test, if applicable
  - Define which F-I/O is to be redundant, if applicable (for S7 FH Systems only)
  - Define the discrepancy time, if applicable
- Call and interconnect F-blocks with discrepancy analysis (e.g., in *S7 F Systems* FB 317 "F_2oo3AI") in the safety program, if applicable

Effect of Sensor Quality on Safety Class

The achievable safety class is dependent on the quality of the sensor and the magnitude of the proof-test interval in accordance with IEC 61508.

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

5.2.1 1oo1 evaluation at F-I/O with inputs

Introduction

This chapter presents examples of sensor wiring to provide a better understanding of 1oo1 evaluation. The examples, taken from the "S7300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151) manual, show several options for wiring sensors to F-SMs.

1oo1 evaluation

For 1oo1 evaluation, a non-redundant sensor is connected via one channel to the F-Modules.

Burner Management Applications in Accordance with VDE 0116 and EN 298

If sensors which offer single-channel mode for safety to VDE 0116 and EN 298, S7-300 F-SMs, ET 200S and ET 200pro F-Modules, and ET 200eco I/O modules with digital inputs may be used **with 1oo1 sensor evaluation** for burner applications in accordance with VDE 0116 and EN 298.

Example: A single-channel sensor is interconnected via one channel with an F-DI (SIL2/Cat.3/PLd)

Below you see the wiring diagram for an SM 326, DI 24 × DC 24V with 1oo1 sensor evaluation. The sensor is supplied by the F-I/O. SIL2/Cat3/PLd can be achieved with this wiring. SIL2/Cat.3/PLd can only be achieved if a suitably qualified sensor is used

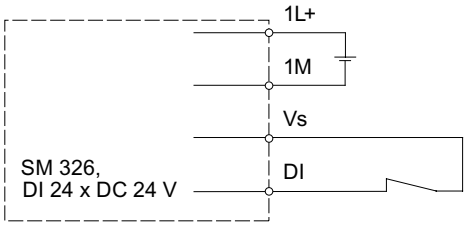


Figure 5-1 Example: Wiring diagram for a sensor with single-channel connection to an F-DI (1oo1)

1oo1 evaluation with high availability (only for S7 FH Systems)

To achieve high availability, one sensor can be connected to two redundant F-DI or two sensors can be connected redundantly to two F-DI in **S7 FH Systems**.

Example: One sensor with single-channel connection to two F-DIs (high availability; SIL2/Cat.3/PLd)

The following figure presents the wiring diagram for a 1oo1 evaluation of a sensor connected to two SM 326, DI 24 × DC 24 V modules. The sensor is supplied externally. SIL2/Cat.3/PLd and high availability can be achieved with this wiring. SIL2/Cat.3/PLd can only be achieved if a suitably qualified sensor is used

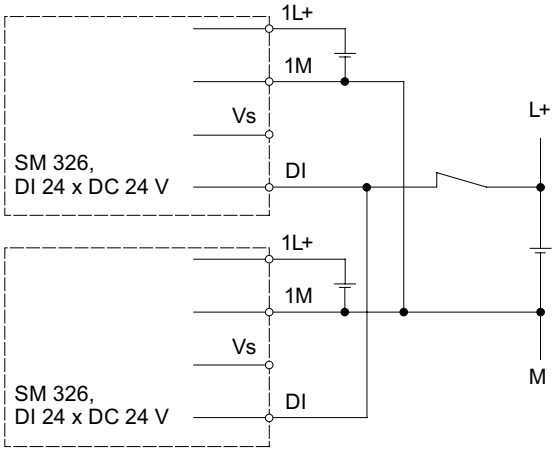


Figure 5-2 Example: Wiring diagram of a single-channel sensor connection to two F-DIs (1oo1, high availability)

Example: Single-channel connection of two redundant sensors to two F-DIs (high availability; SIL2/Cat.3/PLd)

The following figure presents the wiring diagram for a 1oo1 evaluation of two redundant sensors connected to two SM 326, DI 24 × DC 24 V modules. The sensor is supplied by the F-I/O. SIL2/Cat.3/PLd and high availability can be achieved with this wiring. SIL2/Cat.3/PLd can only be achieved if a suitably qualified sensor is used

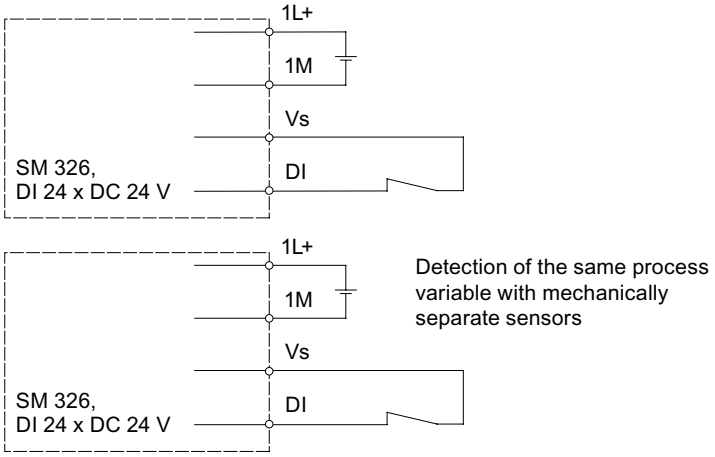


Figure 5-3 Example: Wiring diagram of a single-channel connection of two redundant sensors to two F-DIs (1oo1, high availability)

Example: Single-channel sensor connection to one F-AI (SIL2/Cat.3/PLe)

The wiring diagram below shows an SM 336; F-AI 6 x 0/4 ... 20 mA HART application for 4 mA to 20 mA current measurement range with 2-wire transducer. The sensor is supplied by the F-I/O. SIL3/Cat.3/PLe can be achieved with this wiring. SIL3/Cat.3/PLe can only be achieved if a suitably qualified sensor is used.

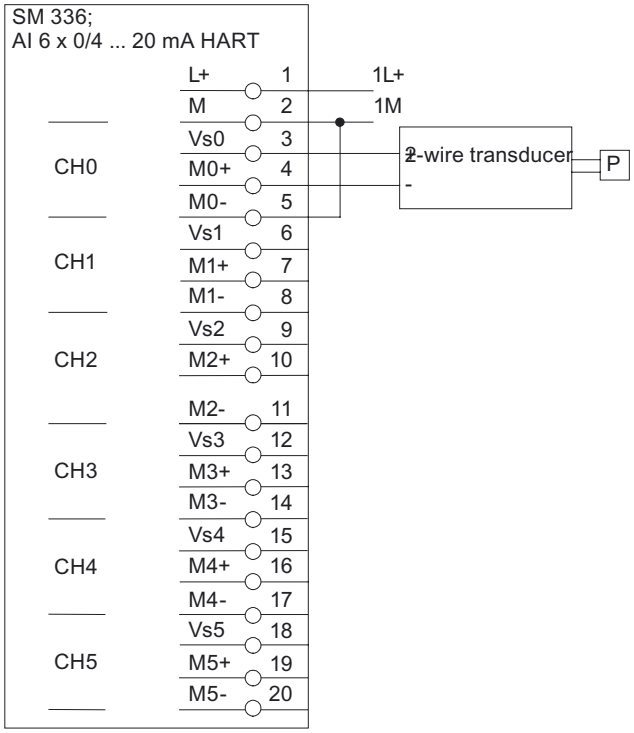


Figure 5-4 Example: Wiring diagram for single-channel sensor connection to an F-AI (1oo1)

5.2.2 1oo2 Evaluation for F-I/O with Inputs

Introduction

This section presents examples for wiring of sensors to provide a better understanding of 1oo2 evaluation. The examples, taken from the "S7300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151) manual, show several options for wiring sensors to F-SMs.

1oo2 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.

Discrepancy Analysis for 1oo2 Evaluation

To differentiate a hardware failure from a transient, random signal change, the safety-related input signals undergo an internal discrepancy analysis as part of 1oo2 sensor evaluation.

Discrepancy analysis is initiated when different levels are detected for two associated input signals (for non-equivalence testing, when the same levels are detected). After a programmable time, the so-called discrepancy time, has elapsed, a check is made to determine whether the difference has disappeared (for non-equivalence testing: whether the agreement has disappeared). If not, this means that a discrepancy error exists.

1oo2 Evaluation for F-I/O with Digital Inputs

In the case of 1oo2 evaluation, only the lower-order channel of the two channels involved in the 1oo2 sensor evaluation is available in the safety program.

The 1oo2 evaluation can be performed with one or two sensors. The sensors are connected to the F-I/O via one or two channels.

Example: One Single-channel Sensor Connected via One Channel to One F-DI (SIL3/Category 3/PLe)

The following figure presents the wiring diagram for an SM 326, DI 24 × 24 VDC with 1oo2 sensor evaluation. The sensor is supplied by the F-I/O. SIL3/Category 4/PLe can only be achieved if a suitably-qualified sensor is used.

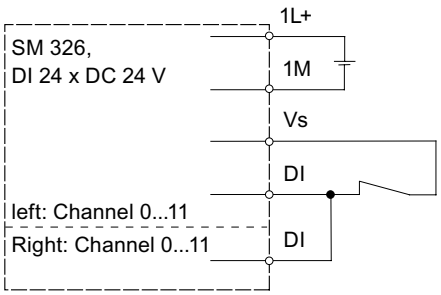


Figure 5-5 Example: Wiring Diagram for One Sensor Connected via One Channel to One F-DI (1oo2)

Example: One Two-channel Sensor Connected via Two Channels to One F-DI (SIL3/Category 4/PLe)

The following figure presents the wiring diagram for an SM 326, DI 24 × 24 VDC with 1oo2 evaluation of a two-channel sensor. SIL3/Cat.4/PLe can be achieved with this wiring. SIL3/Category 4/PLe can only be achieved if a suitably-qualified sensor is used.

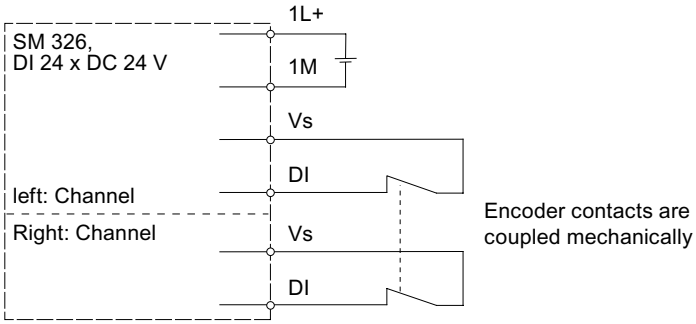


Figure 5-6 Example: Wiring Diagram for One Two-channel Sensor Connected via Two Channels to One F-DI (1oo2)

Example: One Non-equivalent Sensor Connected Non-equivalently via Two Channels to One F-DI (SIL3/Category 4/PLe)

The following figure presents the wiring diagram for an SM 326, DI 24 × 24 VDC with non-equivalent sensor (1oo2 evaluation). SIL3/Cat.4/PLe can be achieved with this wiring. The left channels of the module supply the useful signals. This means that when no faults are detected, these signals will be available in the I/O area for inputs on the F-CPU. SIL3/Category 4/PLe can only be achieved if a suitably-qualified sensor is used.

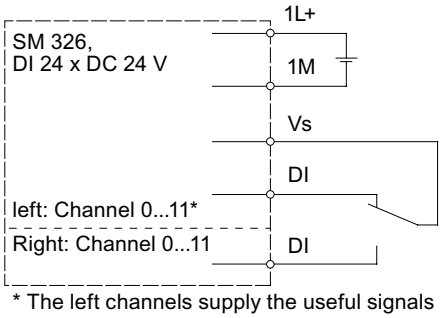


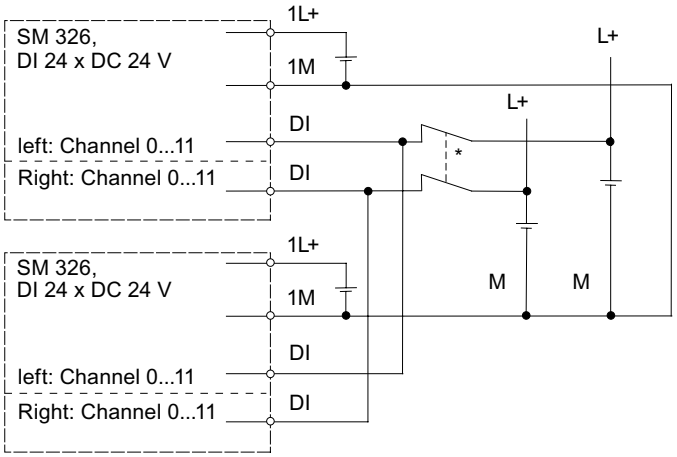
Figure 5-7 Example: Wiring Diagram for One Non-equivalent Sensor Connected Non-equivalently via Two Channels to One F-DI (1oo2)

1oo2 Evaluation with High Availability (for S7 FH Systems Only)

To achieve high availability, one sensor can be connected to two F-DI or two sensors can be connected redundantly to two F-DI in **S7 FH Systems**.

Example: One Two-channel Sensor Connected via Two Channels to Two F-DIs (High Availability; SIL3/Category 4/PLe)

The following figure presents the wiring diagram for a 1oo2 evaluation of a sensor connected to two SM 326, DI 24 × 24 VDC modules. The sensor is supplied externally. SIL3/Cat.4/PLe and high availability can be achieved with this wiring. SIL3/Category 4/PLe can only be achieved if a suitably-qualified sensor is used.



* Sensor contacts are coupled mechanically; you can also connect two single-channel sensors

Figure 5-8 Example: Wiring Diagram for One Two-channel Sensor Connected via Two Channels to Two F-DIs (1oo2, High Availability)

Example: Two Redundant Single-Channel Sensors Connected via One Channel to Two F-DIs (High Availability; SIL3/Category 4/PLe)

The following figure presents the wiring diagram for a 1oo2 evaluation of the sensors connected to two SM 326, DI 24 × 24 VDC modules. The sensor is supplied by the F-I/O. SIL3/Cat.4/PLe and high availability can be achieved with this wiring. SIL3/Category 4/PLe can only be achieved if a suitably-qualified sensor is used.

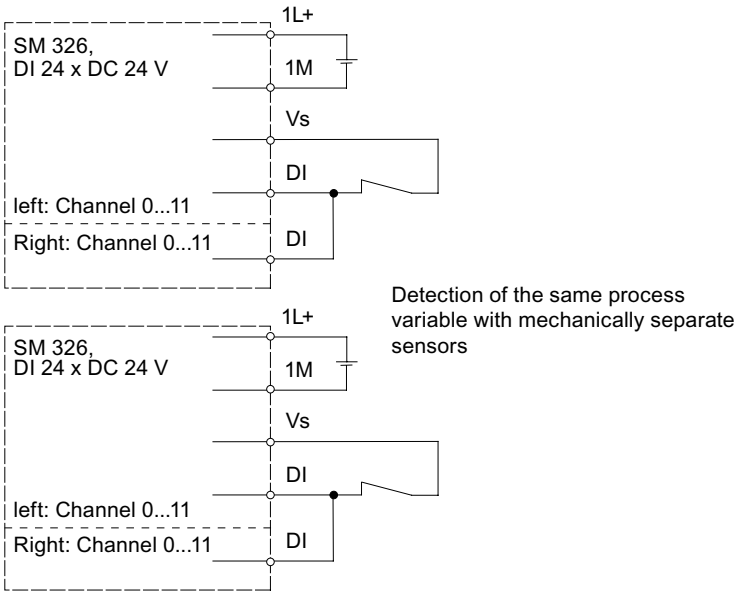


Figure 5-9 Example: Wiring Diagram for Two Redundant Single-channel Sensors Connected via One Channel to Two F-DIs (1oo2, High Availability)

1oo2 Evaluation for F-I/O with Analog Inputs

The 1oo2 evaluation for F-I/O with analog inputs can be performed with one or more sensors. The sensors are connected to the F-I/O via one or two channels.

Example: One Sensor Connected via One Channel to One F-AI (SIL2/Category 3/PLd)

The following figure presents the wiring diagram for an SM 336, AI 6 × 13 bit with 4 mA to 20 mA current measurement range and 2-wire transducer output. The sensor is supplied by the F-I/O. This wiring enables SIL2/Category 3/PLd to be achieved.

SIL3 can be achieved if a suitably-qualified sensor is used.

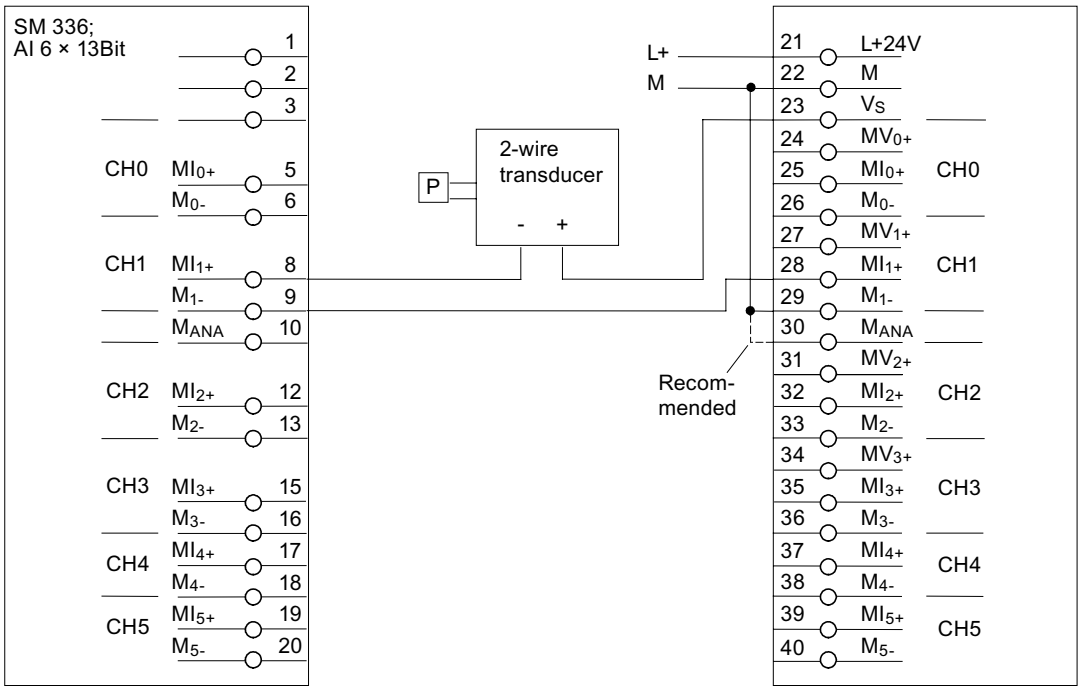


Figure 5-10 Example: Wiring Diagram for One Sensor Connected via One Channel to One F-AI (1oo2)

Example: Two Redundant Sensors Connected via Two Channels to One F-AI (SIL3/Category 4/PLe)

The following figure presents the wiring diagram for an SM 336, AI 6 × 13 bit with 4 mA to 20 mA current measurement range and 2-wire transducer output. The sensor is supplied by the F-I/O. This wiring enables SIL3/Category 4/PLe to be achieved.

SIL3/Category 4/PLe can only be achieved if suitably-qualified sensors are used.

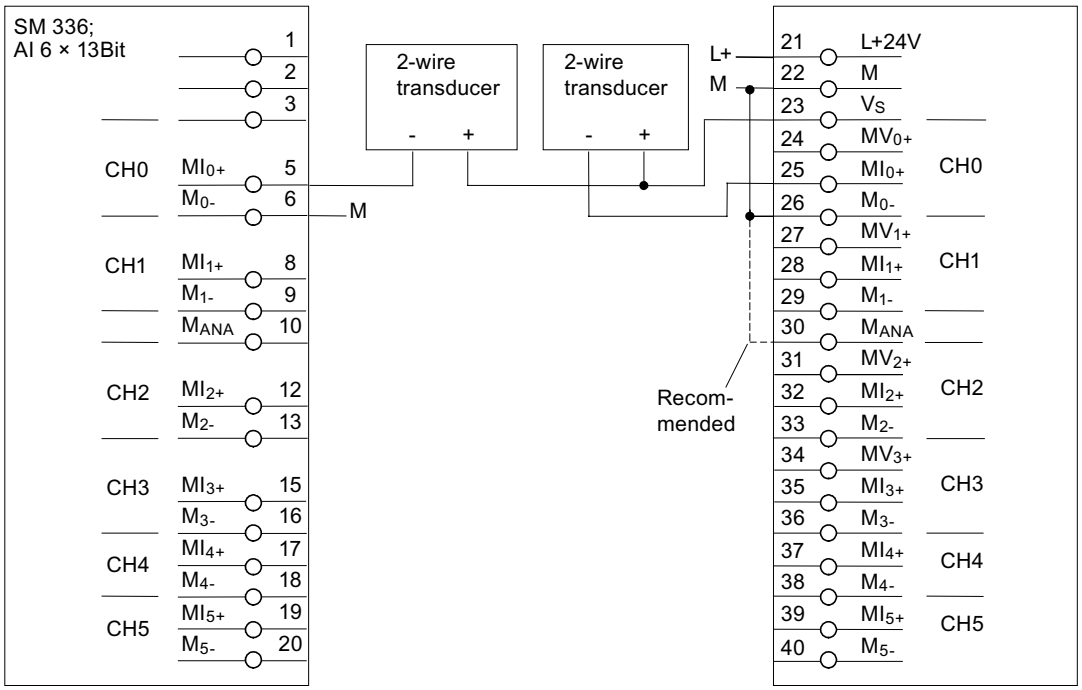


Figure 5-11 Example: Wiring Diagram for Two Redundant Sensors Connected via Two Channels to One F-AI (1oo2)

1oo2 Evaluation with High Availability (for S7 FH Systems Only)

To achieve high availability, four redundant sensors can be connected to two F-AI in **S7 FH Systems**.

Example: Four Redundant Sensors Connected via Two Channels to Two F-AIs (High Availability; SIL3/Category 4/PLe)

The following figure presents the wiring diagram for two SM 336, AI 6 × 13 bit modules with 4 mA to 20 mA current measurement range and 2-wire transducer output. The sensor is supplied by the F-I/O. This wiring enables SIL2/Category 4/PLe and high availability to be achieved.

SIL3/Category 4/PLe can only be achieved if suitably-qualified sensors are used.

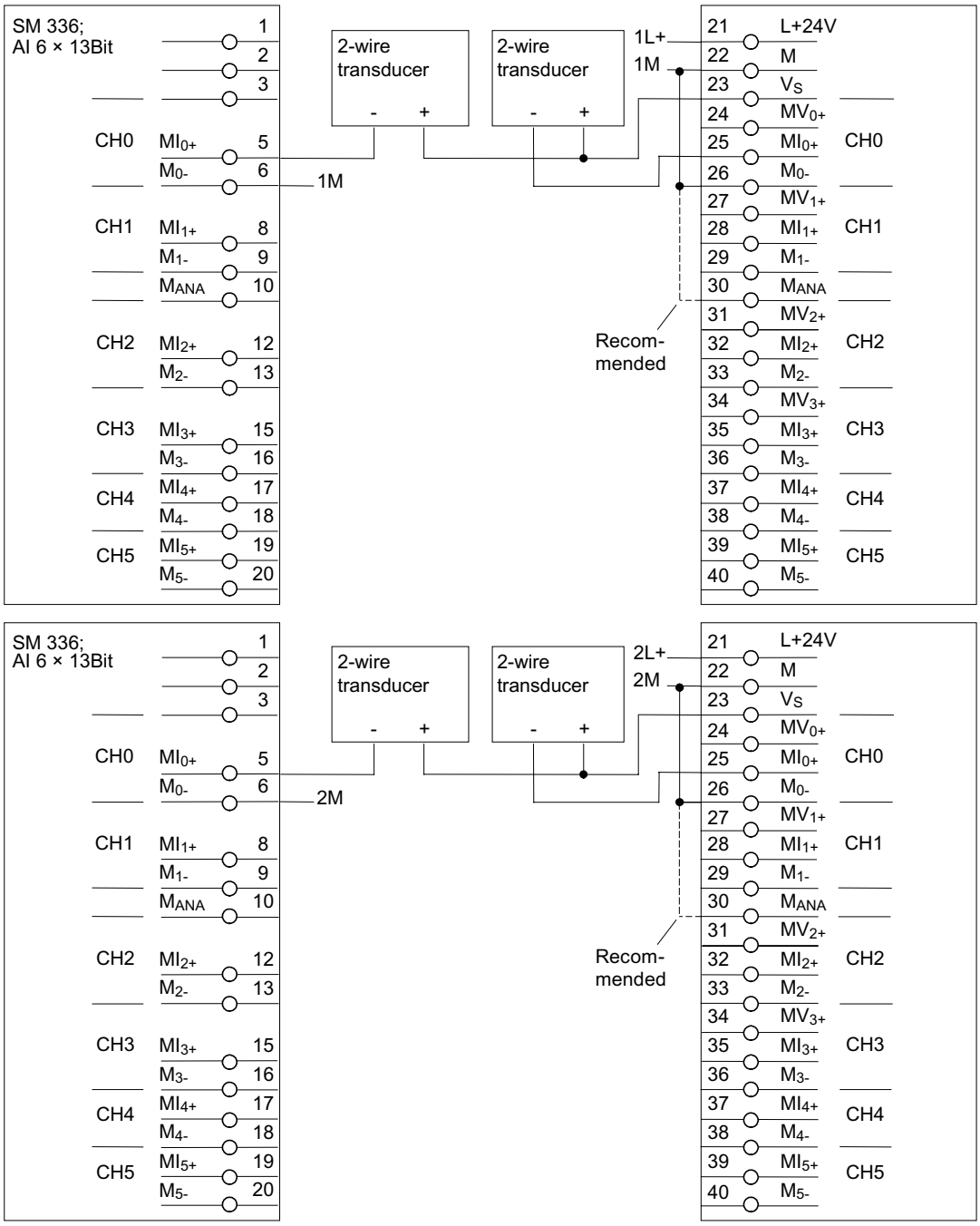


Figure 5-12 Example: Wiring Diagram for Four Redundant Sensors Connected via Two Channels to Two F-AIs (1oo2, High Availability)

5.2.3 2oo3 evaluation at F-I/O with analog inputs (only for S7 F/FH Systems)

Introduction

This chapter provides an example of sensor wiring for a better understanding of 2oo3 evaluation. The example is an extract from the "S7300 Automation System, ET 200M Distributed I/O Device, Fail-safe Signal Modules" (http://support.automation.siemens.com/WW/view/en/19026151) manual.

2oo3 evaluation

The three input channels required for 2oo3 evaluation are used by single-channel sensors. The safety program uses an F_2oo3AI block in *S7 F Systems* to perform a 2oo3 evaluation of the input signals.

2oo3 evaluation with high availability

You can wire three sensors to two F-AIs, or three sensors to three F-AIs to achieve high availability.

Example: Three single-channel sensors connected to three F-AI (high availability; SIL3/Cat.4/PLe)

The figure below shows the wiring diagram for 2oo3 -evaluations of the sensors at three SM 336; F-AI 6 x 0/4 ... 20 mA HART application for 0/4 mA to 20 mA current measurement range with 2-wire transducer. The sensor is supplied by the F-I/O. SIL3/Cat.4/PLe and high availability can be achieved with this wiring. SIL3/Cat.4/PLe can only be achieved if suitably qualified sensors are used. You will have to perform a discrepancy analysis in the safety program with 2oo3 evaluation (for example with the F block F_2oo3AI).

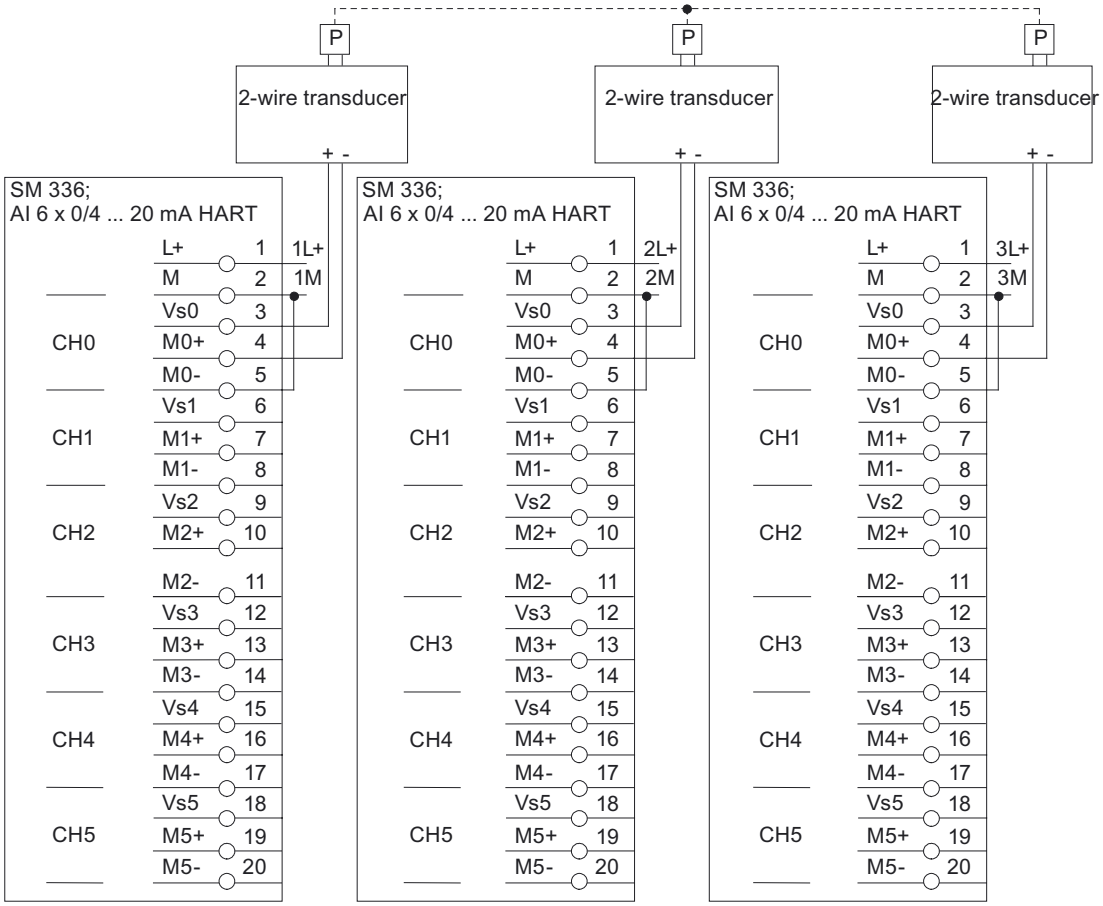


Figure 5-13 Example: Wiring diagram of three sensors with single-channel connection to three F-DIs (2oo3, high availability)

5.3 Safety Functions for Achieving Safety Classes for F-I/O with Outputs

Test Signal Injections for F-I/O with Outputs

For F-I/O with outputs, the necessary safety class is achieved by injecting test signals.

Table 5- 3 Achievable Safety Classes for F-I/O with Outputs

Safety Class, Category, Performance Level, ...			... Test Signal Injection Required
In accordance with IEC 61508	In accordance with EN 954-1	In accordance with EN ISO 13849-1: 2006	
SIL2	Category 3	PLd	• Dark period
SIL3	Category 4	PLe	• Light period • Dark period

Dark period

Dark periods occur during switch-off tests and during complete bit pattern tests. This involves test-related "0" signals being fed to the output by the F-I/O with outputs while the output is active. The output is then switched off briefly (dark period). A sufficiently slow actuator does not respond to this and remains switched on.

Light period

Light periods occur during complete bit pattern tests. This involves test-related "1" signals being fed to the output by the F-I/O with outputs while the output is deactivated (output signal "0"). The output is then switched on briefly (light period). A sufficiently slow actuator does not respond to this and remains deactivated.

Light periods occur with two-channel, single-pin activation of the outputs. Light periods do **not** occur with two-channel, two-pin activation of current sourcing and current sinking outputs (ET 200S, ET 200pro F-modules and SM 326; DO 8 × 24 VDC/2 A PM).

Required User Steps

For SM 326; DO 10 x DC 24V/2A assign the following parameters with *STEP 7*:

- "SIL2 safety mode" or "SIL3 safety mode" (this implicitly specifies the type of test signal injection)
- Enable or disable light test (if the signal changes daily or more frequently, SIL3/Kat.4/PLe can also be achieved without a light period)

For all other F-I/O with digital outputs, no settings are required, since they are usually designed for safety class SIL3/Category 4/PLe.

Configuring F-Systems

6

6.1 Introduction

Configuring as in the standard system

S7 Distributed Safety and S7 F/FH Systems fail-safe systems are configured in basically the same way as standard S7-300 and S7-400 stations. The only difference is that the object properties for the fail-safe components (F-CPU and F-I/O) include some special tabs.

F-Components Requiring Configuration by User

The following hardware components must be configured:

- F-Capable CPU, such as CPU 315F-2 DP
- F-I/O, such as:
  - ET 200S fail-safe modules
  - ET 200pro fail-safe modules
  - ET 200eco fail-safe I/O module
  - Fail-safe S7-300 signal modules (for centralized configuration next to the F-CPU, or for distributed configuration in ET 200M)
  - Fail-safe DP standard slaves/standard I/O devices
  - Fail-safe PA field devices

Overview

The overview provided in this chapter shows how to configure the components of an F-System. Minor differences between S7 Distributed Safety and S7 F/FH Systems are individually noted.

Additional information

You can find detailed information about configuring the hardware in the *STEP 7 online help*. For specific rules and examples with regard to configuring and programming of F-Systems, refer to:

- for S7 Distributed Safety, in the "Getting Started S7 Distributed Safety" (http://support.automation.siemens.com/WW/view/en/19810812)
- for S7 Distributed Safety, in the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) Manual
- for S7 F/FH Systems, in the "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) Manual

6.2 Configuring the F-CPU

Configuration

The F-CPU is listed in the hardware catalog of *HW Config* along with the other S7-300 and S7-400 CPUs.

The F-CPU is configured according to the same scheme used for standard CPUs. Once the F-CPU has been placed in the configuration table, you can access the configuration dialog by selecting the **Edit > Object Properties** menu command or by double-clicking the F-CPU.

Configure Protection Level 1, the CPU password and the "CPU contains safety program" option in the "Protection" tab.

The S7 Distributed Safety CPU also has a specific tab for F-properties called "F-parameters"; this tab is not included for S7 F/FH systems.

Example of Configuring an F-CPU for S7 Distributed Safety

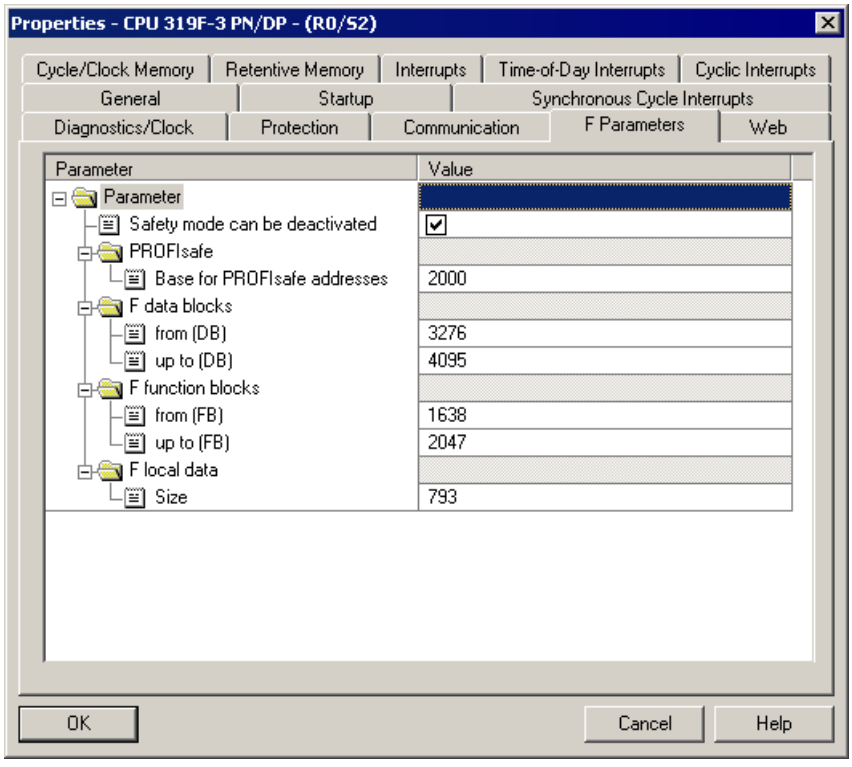
The picture below shows the F-relevant tab for a CPU 319F-3PN/DP.

You can enable / lock deactivation of the safety mode. Deactivation is generally prevented if this function is locked.

S7 Distributed Safety automatically assigns the PROFIsafe addresses. The "Base for PROFIsafe addresses" information is required for internal management of the PROFIsafe addresses of the F-System. PROFIsafe addresses are used to uniquely identify the source and destination.

Users also have to reserve CPU resources (fail-safe data areas, F-function blocks and F-local data) for the safety program.

For information on the parameters, refer to the *context-sensitive online help for the tab* and to the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) manual.



6.3 Configuring the F-I/O

Configuring as in the standard system

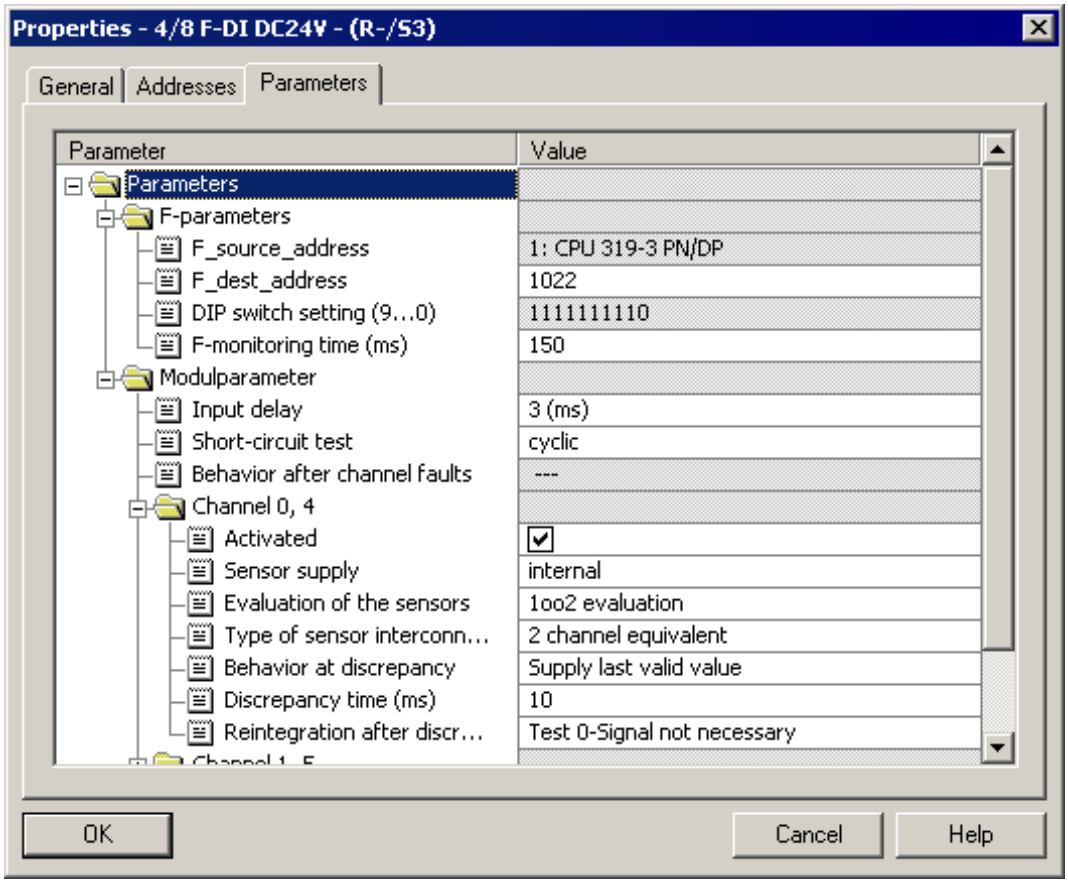
F-I/O are always configured according to the same scheme:

Once the F-I/O has been positioned in the station window of *HW Config*, you can access the configuration dialog by selecting the **Edit > Object Properties** menu command or by double-clicking the F-I/O.

Example of Configuring F-I/O

The Parameter tab for a 4/8 F-DI 24 VDC PROFIsafe fail-safe module is shown below. The values in the shaded fields are automatically assigned by the optional software. The values in the non-shaded fields can be changed by the user.

For information on the parameters, refer to the *context-sensitive online help for the tab* and to the "ET 200S Distributed I/O System - Fail-Safe Modules" (http://support.automation.siemens.com/WW/view/en/12490437) manual.



6.4 Configuring fail-safe DP standard slaves, fail-safe I/O standard devices and fail-safe PA field devices

Requirements

Fail-safe DP standard slaves to be implemented in S7 Distributed Safety and S7 F/FH Systems must be connected to PROFIBUS DP and support the PROFIsafe bus profile. Fail-safe DP standard slaves that are used in a mixed configurations on PROFIBUS DP and PROFINET IO after IE/PB links, must support the PROFIsafe bus profile in the V2 mode.

In order to use fail-safe standard I/O devices with S7 Distributed Safety, the standard devices must be on the PROFINET IO and support the PROFIsafe bus profile in V2 mode.

Fail-safe PA field devices to be implemented in S7 F/FH Systems must be connected to PROFIBUS PA and support the PROFIsafe bus profile.

Configuring with a GSD files

The device specification provided in the GSD file (**G**eneric **S**tation **D**escription) forms the basis for configuring fail-safe DP standard slaves / I/O standard devices / PA field devices, similar to procedures for standard systems.

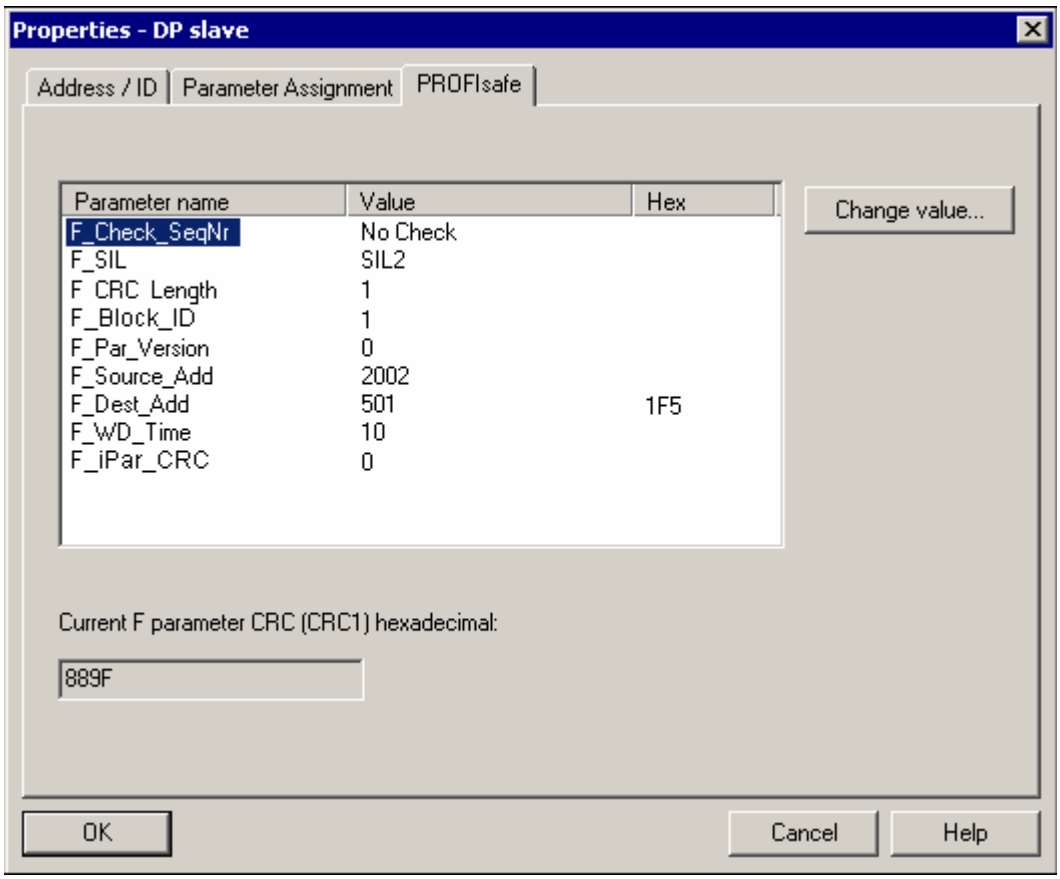
A GSD file contains all the properties of DP standard slaves / I/O standard devices / PA field devices. Certain elements of the specification for DP standard slaves / I/O standard devices / PA field devices are qualified by means of CRC.

The GSD files are supplied by the device manufacturers. Users import the GSD files to their current project (refer to the *STEP 7 Online Help*). After having completed the import, you can select the fail-safe DP standard slaves / fail-safe I/O standard devices / PA field devices from the hardware catalog of *HW Config*.

Example of Configuring Fail-safe DP Standard Slaves

The fail-safe relevant tab for a fail-safe DP standard slave is shown below as an example. The parameter texts specified in the GSD file are contained in the "PROFIsafe" tab under "Parameter name," and the current value for each parameter is included under "Value." This value can be modified by clicking "Change value...."

For information on the parameters, refer to the *context-sensitive online help for the tab* in the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) manual and to the "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) manual.



Programming F-Systems

7

7.1 Introduction

Programming with Standard Programming Languages

S7 Distributed Safety and S7 F/FH Systems fail-safe systems are programmed using standard programming languages of *STEP 7*.

Overview

This chapter describes the program structure and the elements of the safety program.

The structure of the safety programs is described separately for S7 Distributed Safety and S7 F/FH Systems since there are fundamental differences in programming of the two systems.

Additional information

The procedure for programming the safety program is described in detail in the following manuals:

- for S7 Distributed Safety, in the "S7 Distributed Safety, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/22099875) Manual
- for S7 F/FH Systems, in the "S7 F/FH Systems, Configuring and Programming" (http://support.automation.siemens.com/WW/view/en/2201072) Manual

Schematic Structure of a Project with Standard User Program and Safety Program

The figure below presents the schematic structure of a *STEP 7* project in the programming device or engineering system with a standard user program and a safety program for S7 Distributed Safety and S7 F/FH Systems.

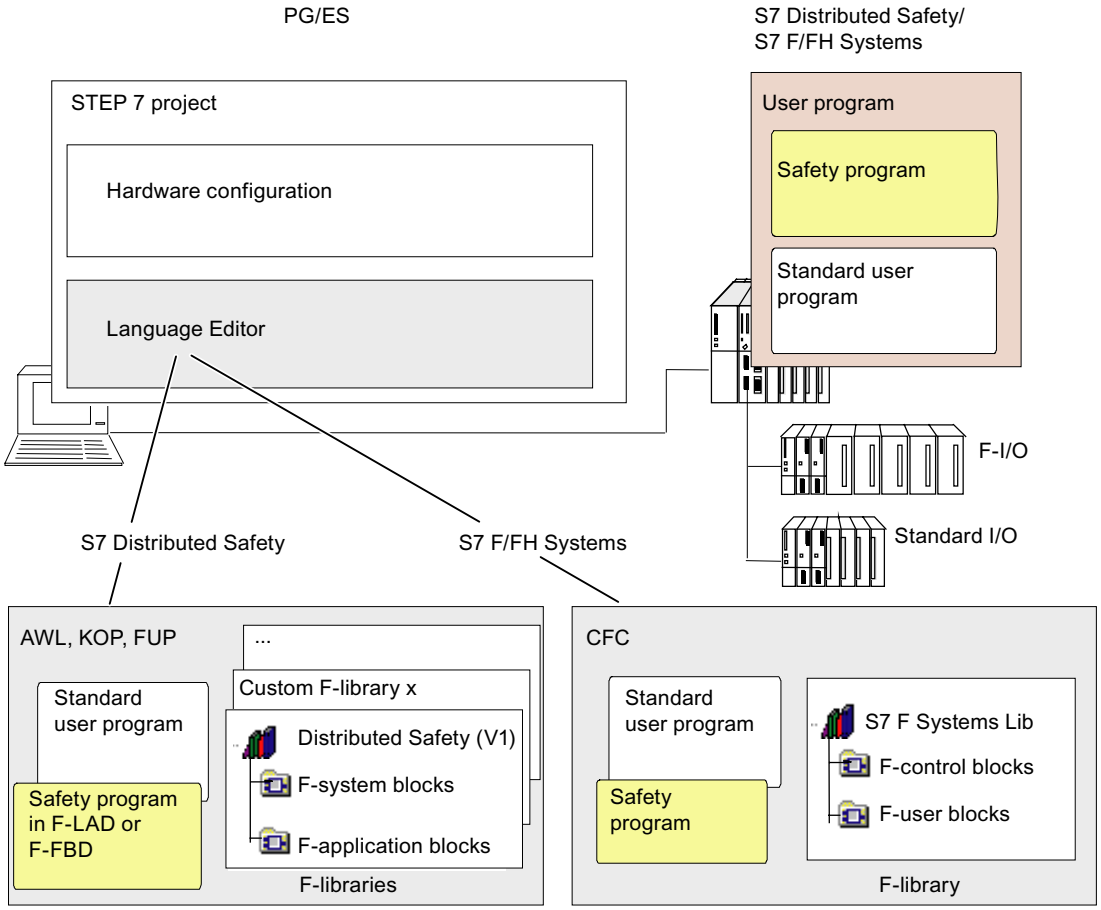


Figure 7-1 Schematic Structure of a STEP 7 Project

Differences between S7 Distributed Safety and S7 F/FH Systems

Programming of S7 Distributed Safety and S7 F/FH Systems differs in the available programming languages and the integration of fail-safe blocks from F-libraries in the safety program.

7.2 Programming Languages for F-Systems

User Program in the F-CPU

The user program in the F-CPU typically consists of a standard user program and a safety program. The standard user program is created in *STEP 7* using standard programming languages such as STL, LAD, or FBD or the CFC programming language.

For S7 Distributed Safety, the safety program is programmed in F-FBD or F-LAD. **For S7 F/FH systems**, fail-safe blocks of an F-library are interconnected in CFC.

The safety program also includes fail-safe blocks for error detection and error response that are automatically amended by the add-on software. This ensures that failures and faults are detected and an appropriate response is triggered so that the F-System either stops in the safe state or goes to a safe state.

S7 Distributed Safety: F-FBD and F-LAD Programming Languages

The F-FBD and F-LAD programming languages correspond in principle to the standard FBD/LAD languages. The standard *FBD/LAD Editor* in *STEP 7* is used for programming.

The primary difference between the F-FBD and F-LAD programming languages and their standard counterparts lies in the limitations in the instruction set and data types and in the address areas that can be used.

S7 F/FH Systems: Programming Language CFC

The safety program is created in individual Continuous Function Charts (CFC) from fail-safe blocks that are supplied in an F-library with the *S7 F-Systems* optional package.

F-libraries

The *S7 Distributed Safety* and *S7 F Systems* optional packages include the following for programming F-Systems:

- For S7 Distributed Safety: *Distributed Safety* F-library (V1)
- For S7 F/FH Systems, F-library *S7 F Systems Lib* V1_3

The F-libraries are located in the *step7/s7libs* directory.

7.3 Structure of the Safety Program in S7 Distributed Safety

Representation of Program Structure

The figure below shows the schematic structure of a safety program for S7 Distributed Safety. For structuring purposes, a safety program consists of one or two F-runtime groups. The safety program has the following components:

- F-blocks that are created by the user or selected from F-libraries (e.g., *Distributed Safety* F-library (V1)).
- F-blocks that are automatically added (F-SBs, automatically generated F-blocks, and the F-shared DB)

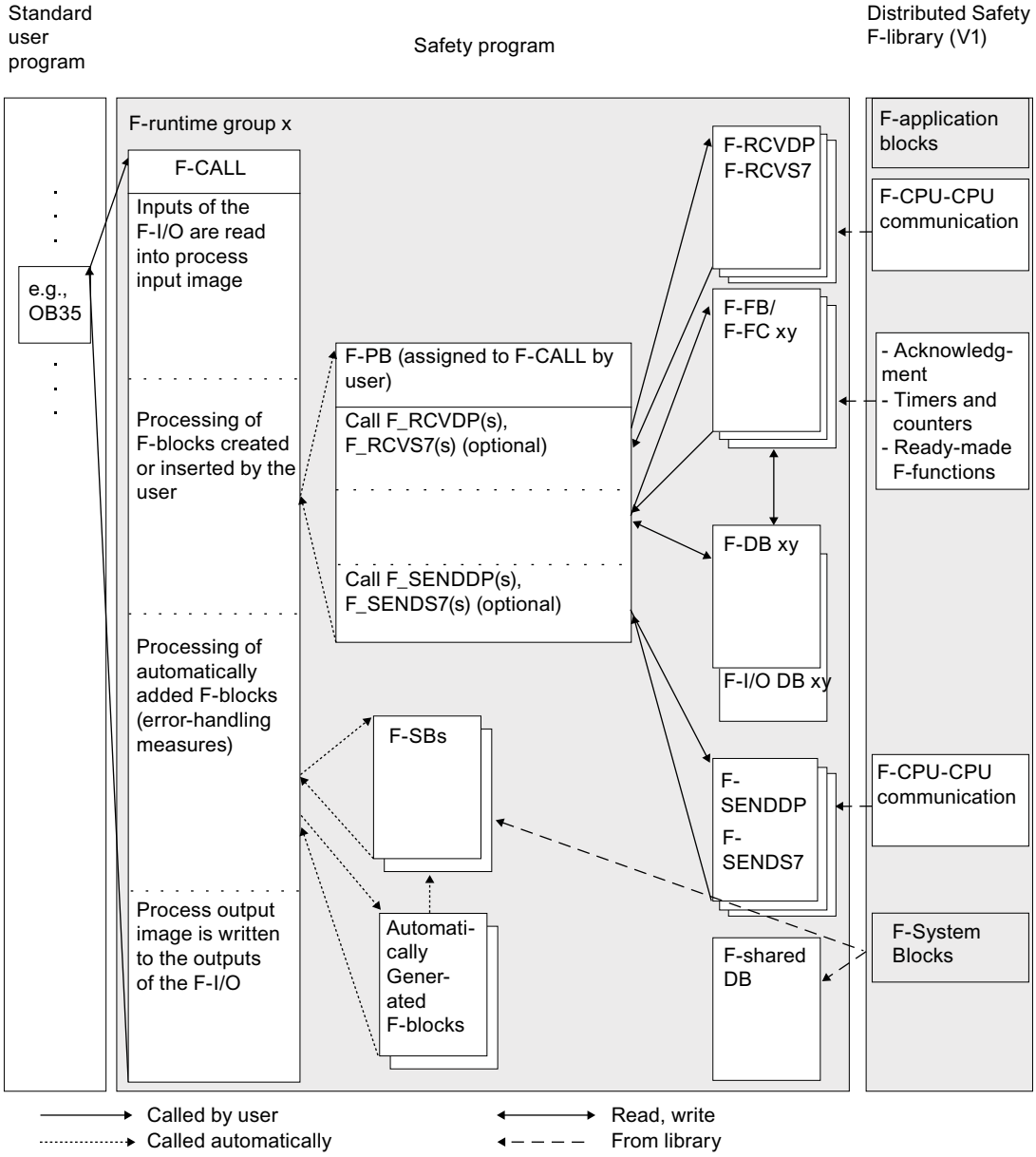


Figure 7-2 Components of the Safety Program in S7 Distributed Safety

Description of Program Structure

The safety program is accessed by calling F-CALL from the standard user program. F-CALL is called in an OB, preferably in a time interrupt OB (e.g., OB 35).

The advantage of time interrupt OBs is that they interrupt the cyclic program execution in OB 1 of the standard user program at fixed time intervals. That is, the safety program is called and run at fixed time intervals in a time interrupt OB.

Once the safety program is executed, the standard user program resumes.

Structure of the Safety Program in F-runtime Groups

To make it easier to handle, a safety program is formed from one or two "F-runtime groups." An F-runtime group is a logical construct made of several related F-blocks.

An F-runtime group in the safety program for S7 Distributed Safety consists of:

- One F-CALL F-Call block
- One F-Program block (an F-FB/F-FC assigned to the F-CALL)
- Additional F-FBs or F-FCs programmed using F-FBD or F-LAD, as needed
- One or more F-DBs, as needed
- F-I/O DBs
- F-blocks of the *Distributed Safety* F-library (V1)
- F-blocks from custom F-libraries
- F-System blocks
- Automatically generated F-blocks

If the user divides his safety program into two F-runtime groups, portions of the safety program (one F-runtime group) can be executed in a faster priority class, thereby achieving faster safety circuits with short response times.

F-blocks of an F-runtime Group

The F-blocks that the user employs in an F-runtime group are shown in the table below:

Table 7- 1 Fail-safe Blocks of an F-runtime Group

F-block	Function	Programming Language
F-CALL	F-block for calling the F-runtime group from the standard user program. The F-CALL contains the call for the F-Program block and the calls for the automatically added F-blocks of the F-runtime group. The F-CALL is created by the user and cannot be edited.	F-CALL
F-FB/F-FC, F-PB	The user programs the actual safety function using F-FBD or F-LAD. The starting point for F-programming is the F-Program block. The F-PB is an F-FC or F-FB (with instance DB) that becomes the F-PB when assigned to the F-CALL. The user can perform the following in the F-PB: • Program the safety program with F-FBD or F-LAD • Call other created F-FBs/F-FCs for structuring the safety program • Insert F-blocks of the *F-Application Blocks* block container from the *Distributed Safety* F-library (V1) • Insert F-blocks from "custom F-libraries" The user defines the call sequence of the F-blocks within the F-PB.	F-FBD/F-LAD
F-DB	Optional fail-safe data blocks that that can be read/write-accessed from anywhere in the safety program	F-DB
F-I/O DB	An F-I/O DB is automatically generated for each F-I/O when the program is compiled in *HW Config*. The user can or must access the variables of the F-I/O DB in conjunction with F-I/O accesses.	-

F-blocks of the *Distributed Safety* F-Library (V1)

The *Distributed Safety* F-library (V1) contains:

- F-application blocks in the *F-Application Blocks*\|*Blocks* block container
- F-System blocks and the F-shared DB in the *F-System Blocks*\|*Blocks* block container

The F-blocks contained in the block containers are shown in the table below:

Table 7- 2 Fail-safe Blocks of the Distributed Safety F-Library (V1)

Block containers	... Contains F-blocks for	Function/F-blocks
F-application blocks		Block container containing the F-application blocks that can be called by the user in the F-PB/F-FBs/F-FCs
	Safety-related CPU-CPU communication	F-application blocks for safety-related CPU-CPU communication: • F_RCVDP and F_RCVS7 for receiving data in safety-related CPU-CPU communication • F_SENDDP and F_SENDS7 for sending data in safety-related CPU-CPU communication
	Acknowledgment	F-application block F_ACK_OP for a fail-safe acknowledgment using an operator control and monitoring system F-application block F_ACK_GL for global acknowledgment of all F-I/O of an F-runtime group
	Timers and counters	F-application blocks F_TP, F_TON, F_TOF; F-blocks F_CTU, F_CTD, F_CTUD
	Scaling	F-application block F_SCA_I
	1oo2) evaluation with discrepancy analysis	F-application block F_1oo2DI
	Ready-made F-functions	F-application blocks for such functions as two-hand monitoring, muting, EMERGENCY STOP, protective door monitoring, feedback loop monitoring, etc.
	Data conversion	F-application blocks F_BO_W, F_W_BO
	Copy	F-application blocks F_INT_WR, F_INT_RD
	Shift operations	F-application blocks F_SHL_W, F_SHR_W

Block containers	... Contains F-blocks for	Function/F-blocks
F-System blocks		Block container containing the F-System blocks (F-SBs) and F-shared DB that are automatically inserted in the safety program
	F-System blocks	The F-System blocks (F-SBs) are automatically inserted by the *S7 Distributed Safety* optional software when the safety program is compiled in order to create an executable safety program from the user's safety program. The user must not insert F-System blocks from the *F-System Blocks* block container in an F-PB/F-FB/F-FC. Likewise, the user must not modify (rename) or delete the F-System blocks in the *Distributed Safety* F-library (V1) or the block container of the user project.
	F-shared DB	Fail-safe data block that contains all of the global data of the safety program and additional information needed by the F-System. The F-shared DB is automatically inserted and expanded when the safety program is compiled. The user can evaluate certain data of the safety program in the standard user program using the symbolic name of the F-shared DB (F_GLOBDB).

7.4 Structure of Safety Program in S7 F/FH Systems

Representation of Program Structure

The block diagram below shows the structure of a safety program for S7 F/FH Systems. A safety program consists of CFC charts with fail-safe blocks that are assigned to F-runtime groups.

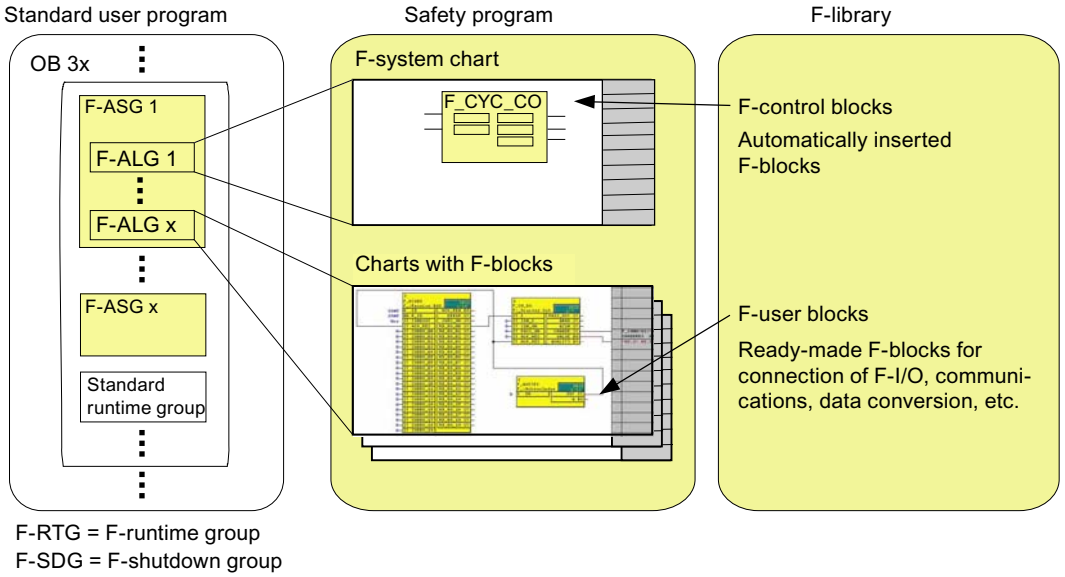


Figure 7-3 Components of Safety Program in S7 F/FH Systems

Description of 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.

Users install the F-runtime groups at the beginning of a task (watchdog interrupt OBs: OB 30 to OB 38). Unless programmed otherwise by users, all F-runtime groups of a task are assigned to a shared F-Shutdown group.

The advantage of time interrupt OBs is that they interrupt the cyclic program execution in OB 1 of the standard user program at fixed time intervals. That is, the safety program is called and run at fixed time intervals in a time interrupt OB.

The watchdog interrupt OB can also contain standard runtime groups.

F-runtime groups

Users must no install any F-blocks directly in the tasks (OBs) when programming the safety program. Instead, users should initially generate an F-runtime group for insertion of the F-blocks. An F-runtime group does not appear as such unless F-blocks are called within this group. An empty F-runtime group always appears as a standard runtime group. The safety program consists of several F-runtime groups.

F-Shutdown groups

An F-Shutdown group represents a self-contained entity of the safety program. An F-Shutdown group contains the user logic which is simultaneously executed or shut down. The F-Shutdown group contains one or several F-runtime groups which are assigned to a shared task (OB). Users can select whether to shut down the entire safety program (full shutdown) after a fault was detected in its execution, or whether to initiate a partial shutdown, that is, shutdown only of the F-runtime group in which the fault occurred. All fail-safe channel drivers of an F-I/O must be located in the same F-Shutdown group.

Fail-safe blocks of F-library *S7 F Systems Lib* V1_3

F-library *S7 F Systems Lib* V1_3 includes the following block containers:

- F-user blocks
- F-control blocks

The block containers include the F-block listed in the table below:

Table 7- 3 Fail-safe blocks of F-library *S7 F Systems Lib* V1_3

Block containers	... Contains F-blocks	Function
F-user blocks		Block container containing the F-blocks that the user can place in the CFC, assign parameters for, and interconnect.
	F-Channel Drivers for F-I/O	
	F_CH_BI, F_CH_BO, F_PA_AI, F_PA_DI, F_CH_DI, F_CH_DO, F_CH_AI	Channel drivers for the input and output signals of the F-I/O
	Conversion	F-blocks for data conversion within the safety program, and for activation of data entered by users in the safety program.
	F_BO_FBO, F_I_FI, F_R_FR, F_TI_FTI	Conversion of standard data types to F-Data types
	F_FBO_BO, F_FI_I, F_FR_R, F_FTI_TI	Conversion of F-Data types to standard data types
	F_FR_FI, F_FI_FR	Conversion of F-Data type to F-Data type
	F_CHG_R, F_CHG_BO	Safety Data Write
	F_QUITES	Fail-safe acknowledgment via an operator control and monitoring system

Block containers	... Contains F-blocks	Function
F-user blocks	**F-System blocks**	
	F_S_BO, F_S_R, F_R_BO, F_R_R	Communication between F-Shutdown groups
	F_START	F-startup detection
	F_PSG_M	Flag block for F-Shutdown groups
	Pulse and count blocks	
	F_CTUD, F_TP, F_TON, F_TOF	IEC pulse and count blocks
	F_REPCYC, F_ROT, F_LIM_TI, F_R_TRIG, F_F_TRIG	Pulse blocks
	Communication	
	F_SENDBO, F_SENDR, F_SDS_BO, F_RCVBO, F_RCVR, F_RDS_BO	F-blocks for safety-related CPU-CPU communication
	Compare	
	F_CMP_R, F_LIM_HL, F_LIM_LL	F-blocks for comparing two input values of the same type
	Voter blocks	
	F_2oo3DI, F_2oo3AI, F_1oo2AI	2oo3 or 1oo2 evaluation with discrepancy analysis
	Mathematical standard functions	F-blocks for mathematical standard functions such as arithmetic, logic, multiplexing, etc.
F-control blocks	F_MOVRWS, F_DIAG, F_CYC_CO, F_PLK, F_PLK_O, F_TEST, F_TESTC, F_TESTM, F_SHUTDN, RTGLOGIC, F_PS_12, F_CHG_WS, ...	Block container containing F-blocks that are called and inserted by *S7 F Systems* when the safety program is compiled, in order to generate an executable safety program from the user's safety program. Users are not allowed to insert any F-blocks of the F-control block in the safety program, or to modify (rename) / delete such blocks in the F-library or in the block container of the user project!

Monitoring and Response Times of F-Systems

A

A.1 Introduction

Overview

This chapter provides the following information for S7 Distributed Safety and S7 F/FH Systems:

- F-related monitoring times that must be configured
- Rules to be followed when specifying monitoring times
- Location where F-related monitoring times are to be entered
- Rule to be followed with regard to the max. response time of a safety function.

Support for Calculations

An Excel file is available for each F-System for calculating the approximate runtime of the F-Shutdown groups, F-specific minimum monitoring times and the maximum response times of your F-System:

- For S7 Distributed Safety *s7fcotia.xls* on the Internet at http://support.automation.siemens.com/WW/view/eng/11669702/133100
- For S7 F/FH Systems *s7ftimea.xls* on the Internet at http://support.automation.siemens.com/WW/view/eng/26091594/133100

Additional Information

The monitoring and response times for the standard portion are calculated in S7 Distributed Safety and S7 F/FH Systems in exactly the same way as for standard S7-300 and S7-400 automation systems and are not addressed here. For a description of this calculation, refer to the hardware manuals for the CPUs.

A.2 Configuring the Monitoring Times

Configuring the Monitoring Times for F-Systems

Monitoring times for the safety program are configured similarly in S7 Distributed Safety and S7 F/FH Systems. That is, in some cases you enter the monitoring times as F-block parameters and in *STEP 7* dialogs, as described in the following sections. Configure the PROFIsafe monitoring times for communication between the F-CPU and F-I/O in *HW Config*, in the object properties dialogs of the corresponding F-I/O.

Rules for Configuring Monitoring Times

When configuring monitoring times, you must take into account the availability as well as the safety of the F-System as follows:

- Availability: To ensure that the temporal monitoring is not triggered when there is no error, the monitoring times selected must be sufficiently long.
- Safety: Observe the maximum length when selecting monitoring times in order to prevent the process safety time from being exceeded.

⚠ WARNING
In order for pulses to be **reliably** detected, the time interval between two signal changes (pulse duration) must be greater than the corresponding monitoring time.

General Procedure for Configuring Monitoring Times

Use the following procedure for configuring monitoring times:

1. Configure the standard or H-system.
   Refer to the applicable hardware manuals and online help systems for needed information.
2. Configure the specific monitoring times of the F-System with respect to availability.
   Calculate the approximate minimum monitoring time using an Excel file. This Excel file is available:
   - For S7 Distributed Safety on the Internet at http://support.automation.siemens.com/WW/view/eng/11669702/133100.
   - For S7 F/FH Systems on the Internet at http://support.automation.siemens.com/WW/view/eng/26091594/133100
3. Using the Excel files, calculate the maximum response time and then verify that the process safety time is not exceeded. If necessary, reduce the specific monitoring times of the F-System.

A.3 F-Related Monitoring Times for S7 Distributed Safety

Monitoring Times to be Configured

The following monitoring times must be configured for S7 Distributed Safety:

Monitoring ...	F-block/ in *STEP 7*	Parameter	Reference
F-cycle time of the F-runtime groups that contain the safety program	"Edit F-runtime Groups“ dialog	Maximum cycle time	Minimum Monitoring Time for F-Cycle Time (Page 137)
Safety-related communication between F-CPU and F-I/O via PROFIsafe (PROFIsafe monitoring time)	Object properties dialog of the F-I/O in *HW Config*.	F_monitoring_time	Minimum monitoring time for safety-related communication between F-CPU and F-I/O (Page 138)
of safety-related CPU-CPU communication	F_SENDDP F_RCVDP F_SENDS7 F_RCVS7	TIMEOUT	Minimum monitoring time of safety-related CPU-CPU communication (Page 138)

The user does not have to configure the monitoring time for safety-related communication between
F-runtime groups.

A.3.1 Minimum Monitoring Time for F-Cycle Time

Maximum Cycle Time Parameter

The monitoring time for the F-cycle time can be specified in the "Edit F-runtime Groups" dialog.

Set a sufficiently high value at the "max. cycle time" parameter to prevent F-cycle time monitoring from being triggered in faultless state and causing the F-CPU to go into STOP.

Use the Excel file provided for S7 Distributed Safety to calculate the minimum value for F-cycle time monitoring. The Excel file is available on the Internet at http://support.automation.siemens.com/WW/view/eng/11669702/133100. Observe the comments in the Excel file.

A.3.2 Minimum monitoring time for safety-related communication between F-CPU and F-I/O

PROFIsafe monitoring time T_{PSTO}

Select a sufficiently high value for the PROFIsafe monitoring time T_{PSTO} to prevent its triggering in faultless state.

Use the Excel file provided for S7 Distributed Safety to calculate the minimum monitoring time for communication between the F-CPU and F-I/O. The Excel file is available on the Internet at http://support.automation.siemens.com/WW/view/eng/11669702/133100. Read also the comments in the Excel file.

Check to Determine If Configured PROFIsafe Monitoring Time Is Too Short

Observe the corresponding information on S7 F/FH Systems provided in chapter "Minimum Monitoring Time for Safety-Related Communication between F-CPU and F-I/O (Page 140)".

A.3.3 Minimum monitoring time of safety-related CPU-CPU communication

Parameter TIMEOUT at F_SENDDP and F_RCVDP, or F_SENDS7 and F_RCVS7

Timeout is monitored in the F-application blocks F_SENDDP and F_RCVDP, or F_SENDS7 and F_RCVS7, based on the same monitoring time. This time must be set a parameter TIMEOUT in both F-application blocks.

Select a sufficiently high TIMEOUT monitoring time to prevent the monitoring function from being triggered in faultless state.

Use the Excel file provided for S7 Distributed Safety to calculate the minimum TIMEOUT value. The Excel file is available on the Internet at http://support.automation.siemens.com/WW/view/eng/11669702/133100. Observe the comments in the Excel file.

A.3.4 Monitoring Time for Safety-Related Communication between F-Runtime Groups

The monitoring time for safety-related communication between F-runtime groups is determined automatically from the values for the "maximum cycle time" ("Edit F-Runtime Groups" dialog).

Monitoring time = Maximum cycle time of the 1st F-runtime group + maximum cycle time of the 2nd F-runtime group

A.4 F-Related Monitoring Times for S7 F/FH Systems

Monitoring Times to be Configured

The following monitoring times must be configured for S7 F/FH Systems:

Monitoring ...	F-block/ in *HW Config*	Parameter	Reference ...
The F-cycle time of any watchdog interrupt OB that contains F-runtime groups	F_CYC_CO	MAX_CYC	"Minimum Monitoring Time for F-Cycle Time (Page 139)"
Safety-related communication between the F-CPU and F-I/O via PROFIsafe (PROFIsafe monitoring time)	Object properties dialog of the F-I/O in *HW Config*.	F_monitoring_time	"Minimum Monitoring Time for Safety-Related Communication between F-CPU and F-I/O (Page 140)"
Safety-related communication between F-CPUs	F_RCVR, F_RCVBO, F_RDS_BO F_SENDR, F_SENDBO, F_SDS_BO	TIMEOUT	"Minimum Monitoring Time for Safety-Related Communication between F-CPUs (Page 141)"
Safety-related communication between F-Shutdown groups	F_R_R F_R_BO	TIMEOUT	"Minimum monitoring time for safety-related communication between F-Shutdown groups (Page 141)"

A.4.1 Minimum Monitoring Time for F-Cycle Time

MAX_CYC Parameter in F_CYC_CO

F-cycle time monitoring is parameterized at input parameter MAX_CYC of F-block F_CYC_CO. In the course of initial compilation of the S7 program, you are requested to enter a value for the maximum cycle time "MAX_CYC" which may expire between between two block calls.

If you have to modify the maximum cycle time, parameterize the F-cycle time at parameter MAX_CYC of F-lock F_CYC_CO-OB3x in the @F_CycCo-OB3x chart for the OBx monitoring time.

Set a sufficiently high value at parameter MAX_CYC to prevent the F-cycle time monitoring function from being triggered in faultless state.

Use the Excel file provided for S7 F/FH Systems to calculate the minimum MAX_CYC value. The Excel file is available on the Internet at http://support.automation.siemens.com/WW/view/eng/13711209/133100. Observe the comments in the Excel file.

A.4.2 Minimum Monitoring Time for Safety-Related Communication between F-CPU and F-I/O

PROFIsafe monitoring time T_{PSTO}

Select a sufficiently high value for the PROFIsafe monitoring time T_{PSTO} to prevent its triggering in faultless state.

Use the Excel file provided for S7 F/FH Systems to calculate the minimum monitoring time for safety-related communication between the F-CPU and F-I/O. The Excel file is available on the Internet at http://support.automation.siemens.com/WW/view/eng/13711209/133100. Observe the comments in the Excel file.

Check to Determine If Configured PROFIsafe Monitoring Time Is Too Short

Note

During commissioning of the F-System, you can perform a check in safety mode to determine whether the configured PROFIsafe monitoring time is too short.
This check is useful if you want to ensure that the configured monitoring time exceeds the minimum monitoring time by a sufficient amount. In this way, you can avoid any sporadic monitoring time errors.

Procedure:

1. Insert an F-I/O (one that will not be needed later for system operation).
2. Assign a shorter monitoring time for this F-I/O than for the F-I/O of the system.
3. If the added F-I/O fails and the "monitoring time for safety message frame exceeded" diagnostic is signaled, you have fallen below the minimum possible PROFIsafe monitoring time.
4. Increase the monitoring time for the added F-I/O just to the point where it no longer fails. This monitoring time corresponds approximately to the minimum possible monitoring time.

Conditions:

The F-I/O to be inserted and the F-I/O whose PROFIsafe monitoring time is to be checked must have the following properties in common:

- They must be inserted in the same rack
- All nodes must be on the same subnet
- They must be addressed by F-Driver blocks in the same F-Shutdown group

Tip:

It may be useful to leave the added F-I/O in place for systems that will be modified or expanded during operation after commissioning. This F-I/O will then provide an early warning in the event of changes in the time behavior, enabling you to avoid a process shutdown triggered by the F-I/O in the process.

A.4.3 Minimum Monitoring Time for Safety-Related Communication between F-CPUs

Parameter TIMEOUT at F_SENDR/F_RCVR, F_SENDBO/F_RCVBO, or F_SDS_BO/F_RDS_BO

Timeout is monitored in the F-blocks F_SENDR/F_RCVR, F_SENDBO/F_RCVBO or F_SDS_BO/F_RDS_BO, based on the same monitoring time. This time must be set a parameter TIMEOUT in both F-blocks.

Select a sufficiently high TIMEOUT monitoring time to prevent the monitoring function from being triggered in faultless state.

Use the Excel file provided for S7 F/FH Systems to calculate the minimum monitoring time for safety-related communication between the F-CPUs. The Excel file is available on the Internet at http://support.automation.siemens.com/WW/view/eng/13711209/133100. Observe the comments in the Excel file.

A.4.4 Minimum monitoring time for safety-related communication between F-Shutdown groups

TIMEOUT Parameter in F_R_BO or F_R_R

Time monitoring takes place in F-blocks F_R_BO or F_R_R and is assigned in the TIMEOUT input parameter.

Select a sufficiently high TIMEOUT monitoring time to prevent the monitoring function F_R_BO or F_R_R from being triggered in faultless state.

Use the Excel file provided for S7 F/FH Systems to calculate the minimum monitoring time for safety-related communication between the F-Shutdown groups. The Excel file is available on the Internet at http://support.automation.siemens.com/WW/view/eng/13711209/133100. Observe the comments in the Excel file.

A.5 Response Times of Safety Functions

Definition of Response Time

The response time starts with the detection of an input signal and ends with the modification of a gated output signal.

Fluctuation Range

The actual response time lies between a minimum and maximum response time. You must always take the maximum response time into account in your system configuration.

Rules for Maximum Response Time of a Safety Function

The maximum response time of a safety function must be less than the process safety time of the process.

Definition of Process Safety Time

The process safety time is the time interval during which the process can be left on its own without causing injury to 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 of a process depends on the process type and must be determined on a case-by-case basis.

Procedure for Response Time Calculation

An Excel file for calculating the maximum response time of a safety function is available for each F-System:

- For S7 Distributed Safety on the Internet at http://support.automation.siemens.com/WW/view/eng/11669702/133100.
- For S7 F/FH Systems on the Internet at http://support.automation.siemens.com/WW/view/eng/13711209/133100

Using the Excel file, calculate the approximate maximum response time of the safety function and then verify that the process safety time is not exceeded.
You may have to reduce the specific F-System monitoring times (refer to the chapters "F-specific monitoring times for S7 Distributed Safety (Page 137)" and "F-specific monitoring times for S7 F/FH Systems (Page 139)").

Glossary

1oo1 evaluation

Type of -> Sensor evaluation - 1oo1 evaluation covers a single sensor with single-channel connection to the -> F-I/O.

1oo2 evaluation

Type of -> sensor evaluation - 1oo2 evaluation covers two input channels which are interconnected either with a single dual-channel sensor, or with two single-channel sensors. The input signals are compared internally for equivalence or non-equivalence.

2oo3 evaluation

Type of -> Sensor evaluation - 2oo3 evaluation covers three input channels which are interconnected with single-channel sensors. The safety program uses an F_2ooAI block in S7 F Systems for 2oo3 evaluation of the input signals.

Access Protection

-> Fail-safe systems must be protected from dangerous, unauthorized access. Access protection for -> F-Systems is implemented through assignment of two passwords (for the -> F-CPU and the -> safety program).

Actuators

Actuators can be power relays or contactors for switching on loads, or they can be loads themselves (for example, directly controlled solenoid valves).

Automatically Generated F-blocks

S7 Distributed Safety: These -> F-blocks are generated automatically when the -> safety program is compiled and are called, if necessary, to generate an executable safety program from the user's safety program.

Availability

Availability is the probability that a system is functional at a specific point in time. Availability can be increased through -> redundancy (for example, by using redundant F-I/O and/or by using multiple -> sensors at the same measuring point).

Category

Category in accordance with EN 954-01

-> S7 Distributed Safety and S7 F/FH Systems fail-safe systems can be used in-> safety mode up to Category 4.

CFC

Continuous Function Chart

1. CFC is a function chart with graphical interconnection of technological functions (blocks).
2. CFC provides a software package (CFC editor) for technology-oriented, graphics-based configuration of an automation task. CFC is used to create an overall software structure (continuous function chart) from ready-made blocks.

Channel Fault

A channel fault is a channel-related fault, such as a wire break or a short circuit.

Channel-selective Passivation

With this type of passivation, only the affected channel is passivated when a -> channel fault occurs. If a fault occurs in the -> F-I/O, all channels of the F-I/O are passivated.

CiR

CiR (Configuration in RUN) refers to a system modification during operation. A system modification in RUN mode by means of CiR enables configuration changes to be made in RUN mode in portions of the system with distributed I/O. The process is thereby halted for a brief, assignable time period. The process inputs retain their last value during this time period.

Continuous Function Chart (CFC)

A continuous function chart consists of up to 26 subcharts containing 6 pages each. Functions (blocks) are interconnected and parameterized on a continous function chart.

Control System

A control system is a system that combines and displays higher-level functions of individual distributed control systems.

CRC

Cyclic Redundancy Check -> CRC signature

CRC Signature

The validity of the process data in the -> safety message frame, the accuracy of the assigned address references, and the safety-related parameters are protected via a CRC signature contained in the safety message frame.

Custom F-Libraries

S7 Distributed Safety: F-libraries created by the users; contain F-FBs, F-FCs and application templates (network templates).

Dark Period

Dark periods occur during switch-off tests and during complete bit pattern tests. Test-related 0 signals are switched from the fail-safe output module to the output bit while the output is active. The output is then switched off briefly (dark period). A sufficiently slow actuator does not respond to this and remains switched on.

DB for F-runtime Group Communication

S7 Distributed Safety: -> F-DB for safety-related communication between F-runtime groups of a safety program.

Deactivated Safety Mode

Deactivated safety mode refers to the temporary deactivation of -> safety mode for test purposes, commissioning, etc.

Whenever safety mode is deactivated, the safety of the system must be ensured by other organizational measures, such as operational monitoring and manual safety shutdown.

Depassivation

-> Reintegration

Discrepancy Analysis

Discrepancy analysis for equivalence or non-equivalence is used for fail-safe inputs to detect errors based on the timing of two signals with the same functionality. Discrepancy analysis is initiated when different levels are detected for two associated input signals (for non-equivalence testing, when the same levels are detected). A check is made to determine whether the difference (when checking for non-equivalence: the match) has disappeared after expiration of a specified time known as the discrepancy time. If not, this means that a discrepancy error exists.

There are two types of discrepancy analyses for fail-safe input modules:

- For -> 1oo2 evaluation:

  The discrepancy analysis of the two input signals is executed for -> 1oo2 evaluation in the fail-safe input modules.

- In the case of redundant I/O (S7 FH systems only):

The discrepancy analysis is carried out between the two input signals of the redundant input modules by the fail-safe driver blocks of the *S7 F Systems* optional software.

Discrepancy Time

Discrepancy time is a period of time assigned for the -> discrepancy analysis. If the discrepancy time is set too high, the error detection time and the -> 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.

DP/DP Coupler

The DP/DP coupler is a device for coupling two PROFIBUS DP subnets required for -> safety-related master-master communication between -> safety programs in different -> F-CPUs in S7 Distributed Safety.

Two (or more) F-CPUs are involved in safety-related master-master communication via a DP/DP coupler. Each F-CPU is linked to the DP/DP coupler via its PROFIBUS DP interface.

ES

Engineering **S**ystem (ES): An engineering system is a PC-based configuration system that enables convenient, visual adaptation of the process control system to the task at hand.

Expert

A system is generally approved, that is, the safety acceptance test of the system is usually carried out by an independent expert (for example, from TÜV).

Fail-safe DP Standard Slaves

Fail-safe DP standard slaves are standard slaves that are operated on PROFIBUS with the DP protocol. Their behavior must comply with IEC 61784-1:2002 Ed1 CP 3/1 and the PROFIsafe bus profile. A GSD file is used to configure your devices.

Fail-safe I/O Module

A fail-safe I/O module is an ET 200eco I/O module that can be used for safety-related operation (in -> safety mode) in S7 Distributed Safety or S7 F/FH Systems fail-safe systems. This I/O module is equipped with integrated -> safety functions.

These modules are equipped with integrated -> safety functions.

Fail-safe I/O standard devices

Fail-safe I/O standard devices are standard devices that are operated on PROFINET with the IO protocol. They respond according to the standard IEC 61784-1:2002 Ed1 CP 3/3 and the PROFIsafe bus profile in V2 mode. A GSD file is used to configure your devices.

Fail-safe module driver

S7 F/FH Systems: The fail-safe module driver ensures -> PROFIsafe communication between the -> safety program and the -> F-I/O. It is automatically positioned and interconnected in the safety program.

Fail-safe Modules

ET 200S and und ET 200pro modules that can be used for safety-related operation (-> safety mode) in the ET 200S distributed I/O system or the ET 200pro distributed I/O device. These modules are equipped with integrated -> safety functions.

Fail-safe PA field devices

Fail-safe PA field devices are operated on PROFIBUS with PA protocol. Their behavior must comply with IEC 61784-1:2002 Ed1 CP 3/2 and the PROFIsafe bus profile. A GSD file is used to configure your devices.

Fail-safe Systems

Fail-safe systems (F-Systems) are systems that remain in a safe state or immediately switch to another safe state when certain failures occur.

F-Application blocks

S7 Distributed Safety: Block container of the *Distributed Safety* F-library; contains the F-Application blocks.

F-Application Blocks

F-blocks (F-FBs, F-FCs) with ready made functions in the Distributed Safety F-library. The F-Application blocks can be called by the user in the -> F-PB and in additional -> F-FBs and -> F-FCs.

F-Attribute

S7 Distributed Safety: All -> F-blocks associated with the -> safety program have an F-Attribute (identified in the "Safety Program" dialog by an "F" in the F-block symbol). Once the -> safety program has been generated successfully, only the blocks of the -> safety program have an F-Attribute.

Fault Reaction Function

-> User safety function

Fault Reaction Time

The maximum fault reaction time for an F-System is the time between the occurrence of any fault and a safe reaction at all affected fail-safe outputs. For the overall F-System: The maximum fault reaction time is the time between the occurrence of any fault in any F-I/O and a safe reaction at the associated fail-safe output.

For inputs: The maximum fault reaction time is the time between the occurrence of the fault and the safe response on the backplane bus.

For digital outputs: The maximum fault reaction time is the time between the occurrence of the fault and the safe response at the digital output.

F-blocks

Fail-safe blocks of the -> safety program

F-CALL

S7 Distributed Safety: "F-Call block" for the -> safety program. The F-CALL is created by the user as an FC in the "F-CALL" programming language; "F-CALL" cannot be edited. The F-CALL calls the -> F-runtime group from the -> standard user program. It contains the call for the -> F-PB and the calls for the automatically added F-blocks (-> F-SBs, -> automatically generated F-blocks, -> F-shared DB) of the F-runtime group.

F-Channel Drivers

S7 F/FH Systems: F-Channel Drivers provide process data in a safe format. The user must position and interconnect the fail-safe channel drivers in the -> safety program.

F-Communication DBs

S7 Distributed Safety: Fail-safe data blocks used for safety-related CPU-CPU communication via S7 connections.

F-Control Blocks

S7 F/FH Systems: Block container of the F-library; contains the -> F-blocks that are automatically called / inserted during compilation of the -> safety program in order to generate an executable safety program from the safety program created by the user.

F-CPU

An F-CPU is a central processing unit with fail-safe capability that is permitted for use in S7 Distributed Safety/S7 F/FH Systems. The S7 F Systems RT License (Copy License) for S7 F/FH Systems allows users to operate the central processing unit as an F-CPU, that is, to run a -> safety program on this CPU. An F-Runtime license is not required for S7 Distributed Safety. A -> standard user program can also be run in the F-CPU.

F-Data Type

S7 F/FH Systems: A -> standard user program and -> safety program use different data formats. Safety-related F-Data types are used in the safety program.

F-DBs

S7 Distributed Safety: Optional fail-safe data blocks that can be read and written to within the entire -> safety program.

F-Driver Block

Block used for the input/output of values from/to the -> F-I/O. It forms the software interface to the process, converts the physical values to process data (and vice-versa), and also provides information about the availability of the hardware addressed.

In S7 F/FH Systems, -> safety-related communication takes place using inputs and outputs of F-Driver blocks. The user must position and interconnect special F-Driver blocks in -> continuous function charts (CFC) of the -> F-runtime group.

F-FBD

Programming language for -> safety programs in S7 Distributed Safety. The standard FBD/LAD Editor in *STEP 7* is used for programming.

F-FBs

S7 Distributed Safety: Fail-safe function blocks (with instance DBs), in which the user programs the -> safety program in -> F-FBD or -> F-LAD.

F-FCs

S7 Distributed Safety: Fail-safe FCs, in which the user programs the -> safety program in -> F-FBD or -> F-LAD.

F-I/O

F-I/O is a group designation for fail-safe inputs and outputs available in SIMATIC S7 for integration in S7 Distributed Safety and S7 F/FH Systems fail-safe systems. The following F-I/O are available:

- -> ET 200eco fail-safe I/O module
- S7-300 fail-safe signal modules (-> F-SMs)
- -> fail-safe modules ET 200S and ET 200pro
- -> fail-safe DP standard slaves
- -> fail-safe I/O standard devices (for S7 Distributed Safety only)
- -> fail-safe PA field devices (only for S7 F/FH Systems)

F-I/O DB

S7 Distributed Safety: Fail-safe data block for -> F-I/O in an -> F-CPU in S7 Distributed Safety. An F-I/O DB is automatically generated for each F-I/O when the program is compiled in *HW Config*. The F-I/O DB contains variables that the user can evaluate in the -> safety program, or that he can or must write to:

- For reintegration of the F-I/O following communication errors, F-I/O faults, or channel faults
- If the F-I/O must be passivated as a result of particular states of the safety program (for example, group passivation)
- In order to evaluate whether fail-safe values or process data are output

F-LAD

-> F-FBD

F-Modules

-> Fail-safe modules

F-PB

S7 Distributed Safety: "Introductory F-block" for fail-safe programming of the -> safety program. The F-PB is an
-> F-FB or -> F-FC that the user assigns to the -> F-CALL of the
-> F-runtime group.

The F-PB contains the F-FBD or F-LAD safety program, any calls of additional -> F-FBs/F-FCs for program structuring, and any F-Application blocks from the
-> F-Application Blocks block container of the *Distributed Safety* F-library.

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 one or two (S7 Distributed Safety), or of several F-runtime groups (S7 F/FH systems).

F-SBs

S7 Distributed Safety: Fail-safe system blocks that are automatically called/inserted when the -> safety program is compiled in order to create an executable safety program from the user's safety program.

F-Shared DB

S7 Distributed Safety: Fail-safe data block that contains all of the global data of the -> safety program and additional information needed by the F-System. When the -> safety program is generated, the F-shared DB is automatically inserted and expanded. Using the symbolic name of the F-shared DB (F_GLOBDB), the user can evaluate certain data from the -> safety program in the -> standard user program.

F-Shutdown group

S7 F/FH Systems: An F-Shutdown group represents a self-contained entity of the safety program. It contains the user logic which is simultaneously executed or shut down. The F-Shutdown group contains one or several F-runtime groups which are assigned to a shared task (OB). Users can select whether to shut down the entire safety program (full shutdown) after a fault was detected in its execution, or whether to initiate a partial shutdown, that is, shutdown only of the F-runtime group in which the fault occurred.

F-SMs

F-SMs are signal modules of S7-300 that can be used for safety-related operation (in -> safety mode) in S7 Distributed Safety or S7 F/FH Systems fail-safe systems. These modules are equipped with integrated -> safety functions.

F-System Blocks F-System Blocks

S7 Distributed Safety: Block container of the *Distributed Safety* library containing the -> F-SBs and the -> F-shared DB.

-> F-SB

F-System Blocks F-System Blocks

S7 Distributed Safety: Block container of the *Distributed Safety* library containing the -> F-SBs and the -> F-shared DB.

-> F-SB

F-Systems

-> Fail-safe systems

F-User Blocks

S7 F/FH Systems: Block container of F-library *S7 F Systems Lib;* contains the -> F-blocks which can be placed, parameterized and interconnected in -> CFC charts by the users.

Light Period

Light periods occur during complete bit pattern tests. Test-related "1" signals are switched from the fail-safe output module to the output bit while the output is deactivated (output signal "0"). The output is then switched on briefly (light period). A sufficiently slow actuator does not respond to this and remains switched off.

MSR

Instrumentation and control technology

Non-equivalent Sensor

An non-equivalent sensor is a changeover switch that is wired in -> fail-safe systems (dual-channel connection) to two inputs of an -> F-I/O (for -> 1oo2 evaluation of sensor signals).

OBT

Optical **B**us **T**erminal (OBT): Equipment used to connect an individual PROFIBUS DP device without an integrated optical interface or an RS 485 segment to the optical PROFIBUS DP.

OP

Operator **P**anel (OP): A programmable HMI device used to operate and monitor machines and systems.

OS

Operator **S**tation (OS): A configurable operator station used to operate and monitor machines and systems.

Passivation

If an -> F-I/O detects a fault, it switches either the affected channel or all channels to a -> safe state; that is, the channels of this F-I/O are passivated. The F-I/O reports the detected fault to the -> CPU via the slave diagnostics.

For an F-I/O with inputs, if passivation occurs, the F-System provides fail-safe values for the -> safety program instead of the process data pending at the fail-safe inputs.

For an I/O with outputs, if passivation occurs, the F-System transfers fail-safe values (0) to the fail-safe outputs instead of the output values provided by the safety program.

PCS 7

PCS 7 is a process control system based on selected SIMATIC components that have been optimized for use in a control system. In addition, there are functional enhancements to ensure availability of control-system-specific system behavior and functions required in a process and instrumentation control system from engineering to operation.

Performance Level

Performance Level (PL) to EN ISO 13849-1: 2006

Process Safety Time

The process safety time is the time interval during which the process can be left on its own without causing injury to 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.

PROFINET IO

Within the framework of PROFINET, PROFINET IO is a communication concept for the implementation of modular, distributed applications.

PROFINET IO allows you to create automation solutions familiar from PROFIBUS.

PROFINET IO is implemented based on both the PROFINET standard for automation devices and the *STEP 7* engineering tool.

This means that you have the same application view in *STEP 7*, regardless of whether you are configuring PROFINET or PROFIBUS devices. Programming your user program is essentially the same for PROFINET IO and PROFIBUS DP if you use the expanded blocks and system status lists for PROFINET IO.

PROFINET IO Controller

A PROFINET IO controller is a device that is addressed via the connected IO device. That is: that the IO controller exchanges input and output signals with assigned field devices. The IO controller is often the controller on which the automation program runs.

PROFINET IO Device

A PROFINET IO device is a decentralized field device that is assigned to one of the IO controllers (e.g., remote IO, valve terminals, frequency converters, switches)

PROFINET IO Supervisor

A PG/PC or HMI device used for commissioning and diagnostics.

PROFINET IO controller with assigned PROFINET IO devices.

PROFIsafe

Safety-related PROFIBUS DP/PA and PROFINET IO bus profile for communication between the -> safety program and the -> F-I/O in an -> F-System.

PROFIsafe Address

Every -> F-I/O has a PROFIsafe address. The PROFIsafe address must be configured in *STEP 7 HW Config* and set via a switch on the fail-safe I/O.

PROFIsafe Monitoring Time

Minimum monitoring time for safety-related communication between F-CPU and F-I/O

Programming Device (PG)

Programmng**D**evice (PG): Programming devices (PGs) are compact personal computers especially made for use in an industrial setting. A programming device (PG) is fully equipped for programming SIMATIC automation systems.

Proof-test Interval

The proof-test interval is the time period after which a component must be put into fail-safe state. That is, it is replaced by an unused component or it is proven to be completely fault-free.

Redundancy, Availability-enhancing

Availability-enhancing redundancy refers to redundancy of components with the aim of ensuring that components continue to function even in the event of hardware faults.

Redundancy, Safety-enhancing

Redundant component configuration with the focus set on the disclosure of hardware faults by comparison, e.g., by means of -> 1oo2 evaluation in -> F-I/O.

Redundant Switched I/O

Configuration variant of S7 FH Systems in -> safety mode to increase availability. -> F-CPU, PROFIBUS DP, and -> F-I/O are redundant. In the event of a fault, the F-I/O is no longer available.

Reintegration

Once a fault has been eliminated, the -> F-I/O must be reintegrated (depassivated). The reintegration (switching from fail-safe values to process data) is performed automatically or, alternatively, only after a mandatory user acknowledgment in the safety program.

For an F-I/O with inputs, the process data pending at the fail-safe inputs are provided again for the -> safety program after reintegration. For an F-I/O with outputs, the F-System transfers the output values provided in the safety program to the fail-safe outputs again.

Restart of F-System

When an -> F-CPU transitions from STOP to RUN, the -> standard user program restarts as usual. When the -> safety program restarts, data blocks are initialized with values from the load memory as follows:

- for S7 Distributed Safety: all data blocks with -> F-Attribute
- for S7 F/FH Systems: all data blocks with -> F-Attribute
- This occurs analogously to a cold restart. As a result, saved error information is lost. The -> F-System performs an automatic -> reintegration of the -> F-I/O.
  In contrast to the standard user program, the startup OBs (OB 100 to 102) cannot be used in the safety program.

S7 F Systems RT License (Copy License)

-> F-CPU

S7-PLCSIM

S7-PLCSIM allows you to test and edit your program in a simulated automation system on your programming device or PC. Since the simulation takes place completely in STEP 7, you do not need any hardware (CPU, I/O).

Safe State

The basic principle of the safety concept in an -> F-System is the existence of a safe state for all process variables. The value "0" always represents the safe state for digital -> F-I/O.

Safety Class

Safety Integrity Level (SIL) to IEC 61508 and EN 50129. Higher Safety Integrity Levels imply that more stringent measures have to be taken to prevent and handle systematic faults and hardware failures.

-> S7 Distributed Safety and S7 F/FH Systems fail-safe systems can be used in -> safety mode up to SIL3.

Safety Function

Safety function is a mechanism built into the -> F-CPU and -> F-I/O that allows them to be used in -> S7 Distributed Safety or S7 F/FH Systems fail-safe systems.

In accordance with IEC 61508: Function 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 (-> user safety function).

Safety Message Frame

In -> safety mode, data are 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. Safety mode is the operating mode of the -> F-I/O that allows -> safety-related communication using -> safety message frames. -> Fail-safe modules ET 200S, ET 200pro und ET 200eco are designed for safety mode only. -> F-SMs S7-300 can be operated in -> standard mode or safety mode (except SM 326; DO 8 × DC 24V/2A and SM 336; F-AI 6 × 4 ... 20 mA HART).
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. The safety program cannot be modified during operation in safety mode. Safety mode can be deactivated by the user (-> deactivated safety mode).

Safety Program

The safety program is a safety-related user program.

Safety Protector

The safety protector protects the -> F-SMs from possible overvoltages in the event of a fault. The safety protector must be used for SIL3/Cat.4/PLe applications:

- Generally, when PROFIBUS DP is configured with copper cable
- When PROFIBUS DP is configured with fiber-optic cable and combined operation of standard signal modules and -> F-SMs in one ET 200M is required

Safety-related Communication

Safety-related communication is communication used to exchange fail-safe data.

Sensor Evaluation

There are two types of sensor evaluation:

- -> 1oo1 evaluation – sensor signal is read once
- -> 1oo2 evaluation – sensor signal is read twice by the same -> F-I/O and is then either compared internally, or is evaluated in the safety program by means of an F-block that executes a -> discrepancy analysis.

Sensors

Sensors are used for exact measurement of paths, positions, velocities, rotational speeds, masses, etc.

Sequence Number

Time-monitoring of the message-frame update in the PROFIsafe protocol is performed through the transfer of a sequence number from the -> F-CPU to the -> F-I/O. A valid, current -> safety message frame with a valid sequence number must be received by the F-CPU and the F-I/O within an assignable monitoring time. If a valid sequence number is not detected within the monitoring time, the F-I/O is passivated.

Single-channel I/O

Single-channel I/O is a configuration variant of S7 Distributed Safety/S7 F Systems in -> safety mode. The -> F-CPU and -> F-I/O are not redundant. In the event of a fault, the F-I/O is no longer available.

Single-channel Switched I/O

Configuration variant of S7 FH Systems in -> safety mode to increase availability. The -> F-CPU is redundant and the -> F-I/O is not redundant; in the event of a fault, the system switches over to the other F-CPU. In the event of a fault, the F-I/O is no longer available.

Standard Communication

Standard communication is communication used to exchange non-safety-related data.

Standard Mode

In standard mode of -> F-I/O, -> safety-related communication using -> safety message frames is not possible; only -> standard communication is possible in this operating mode.

-> S7-300 F-SMs can be used in standard mode or -> safety mode. -> Fail-safe modules ET 200S, ET 200pro und ET 200eco are designed for safety mode only.

Standard User Program

The standard user program is a non-safety-related user program.

Test Signals

For -> F-I/O with outputs, the required -> safety class is achieved by injecting test signals (-> light period, -> dark period).

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 programs the user safety function. If the -> F-System can no longer execute its actual user safety function, it executes the fault reaction function; for example, the associated outputs are deactivated, and the -> F-CPU switches to STOP mode, if necessary.

Validity Check

The validity check checks the signals for validity.
It must be ensured that a process data element lies within the limits specified by the user.

In -> F-Systems: The user must perform a validity check in the -> safety program to ensure that dangerous conditions cannot arise when data are transferred from a -> standard user program to a safety program.

WinCC

WinCC is an industry and technology-neutral system for visualization and control tasks in production and process automation.

WinCC offers industry-standard function modules for graphics representation, messaging, archiving, and logging functions. WinCC ensures high availability with its powerful process interfacing, rapid image updating, and reliable data archiving.

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

SIEMENS

Siemens AG

A&D AS SM ID
Postfach 1963
D-92209 Amberg

mailto:doku.automation@siemens.com

Your Address:

Name:
Company:
Position:
Street:
Postal code / Place:
Email:
Phone:
Fax:

Your Feedback as regards the S7 Distributed Safety

Dear SIMATIC user,

Our goal is to provide you information with a high degree of quality and usability, and to continuously improve the SIMATIC documentation for you. To achieve this goal, we require your feedback and suggestions. Please take a few minutes to fill out this questionnaire and return it to me by Fax, e-mail or by post.

We are giving out three presents every month in a raffle among the senders. Which present would you like to have?

☐ **SIMATIC Manual Collection** ☐ **Automation Value Card** ☐ **Laser pointer**

Dr. Thomas Rubach,
Head of Information & Documentation

General Questions

1. Are you familiar with the SIMATIC Manual Collection?

☐ yes ☐ no

2. Have you ever downloaded manuals from the internet?

☐ yes ☐ no

3. Do you use Getting Starteds?

☐ yes ☐ no

if yes, which:

4. How much experience do you have with the S7 Distributed Safety?

☐ Expert
☐ Experienced user
☐ Advanced user
☐ Beginner

Please specify the documents, for which you want to answer the questions below:

- ☐ **A: Manual S7 Distributed Safety, Configuring and Programming**
- ☐ **B: Manual S7-300, Fail-Safe Signal Modules**
- ☐ **C: Manual ET 200S, Distributed I/O System Fail-Safe Modules**
- ☐ **D: Manual ET 200eco, Distributed I/O Fail-Safe I/O Module**
- ☐ **E: System Description Safety Engineering in SIMATIC S7**
- ☐ **F: Getting Started S7 Distributed Safety**
- ☐ **G: ET 200pro Distributed I/O Device - Fail-Safe Modules**

1. **In which project phase do you use this document frequently?**

☐ Information ☐ Assembly
☐ Planning ☐ Commissioning
☐ Configuration ☐ Maintenance & Service
☐ Programming ☐ others:

2. **Finding the required information in the document:**

- How quickly can you find the desired information in the document?

☐ immediately ☐ not at all
☐ after a brief search ☐ after a long search

- Which search method do you prefer?

☐ Table of contents ☐ Index
☐ Full-text search ☐ others:

- Which supplements/improvements would you like in order to help you find the required information quickly?

3. **Your judgement of the document as regards content.**

- How satisfied are you with this document

☐ Totally satisfied ☐ not very satisfied
☐ Very satisfied ☐ not satisfied
☐ Satisfied

- Were able to find the required information?

☐ yes ☐ no

which was not:

4. **What is the scope of the information?**

☐ Just right
☐ Not enough - which topic:
☐ Too detailed – which topic:

5. **Is the information easy to understand (texts, figures, tables)?**

☐ yes ☐ no

if no, which was not:

6. **Are examples important to you?**

☐ no, of less importance
☐ yes, important –were the examples enough?

☐ yes ☐ no

if no, on which topic:

7. **What are your suggestions as regards the contents of the document?**

Thank you for your cooperation