

MANUFACTURER DOCUMENT PACKAGE

Manufacturer's Manual

Selected official pages for procurement and maintenance review

PRODUCT BRAND

Siemens

PRODUCT MODEL

6ES7138-4CF02-0AB0

Fail-Safe Power and Output Module. Source PDF pages: manual pp. 2-3,5,36-37,61-68,80-83; safety-update pp. 9,13,15. Adjacent model text on shared pages is outside this product reference.

OFFICIAL SOURCE

ET 200S Distributed I/O System - Fail-Safe Modules; 07/2005, A5E00103686-04

Siemens original documentation and product reference

Siemens 10/2015, A5E03310062-AE; safety-update source pp. 9,13,15

Product and rating excerpt, not a complete commissioning manual. Read historical safety figures with the appended 10/2015 update. Wiring, configuration and diagnostics require the full manufacturer documentation.

AMIKON PRODUCT SUPPORT

+86-18020776786

INFO@AMIKON.CN

AMIKONG.COM

Amikon Limited prepared this independent reference package. Selected manufacturer pages follow with their original content and pagination visible.

Safety Guidelines

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.

Prescribed Usage

Note the following:



Warning

This device may only be used for the applications described in the catalog or the technical description and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens. Correct, reliable operation of the product requires proper transport, storage, positioning and assembly as well as careful operation and maintenance.

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.

Preface

Purpose of this Manual

The information in this manual is a reference source for operations, function descriptions, and technical specifications of the fail-safe modules of the ET 200S distributed I/O system.

Basic Knowledge Requirements

This manual is a supplement to the ET 200S Distributed I/O System manual. Working with this manual requires general knowledge of automation engineering. You also require experience of using the *STEP 7* basic software and the ET 200S distributed I/O system.

Scope of this Manual

Module	Order Number	Release Number and Higher
PM-E F pm DC24V PROFIsafe Power Module	6ES7 138-4CF02-0AB0	01
PM-E F pp DC24V PROFIsafe power module	6ES7 138-4CF41-0AB0	01
PM-D F DC24V PROFIsafe power module	3RK1 903-3BA01	01
4/8 F-DI DC24 V PROFIsafe Digital Electronic Module	6ES7 138-4FA02-0AB0	01
4 F-DO DC24V/2A PROFIsafe digital electronic module	6ES7 138-4FB02-0AB0	01

What's New

Compared with the previous version, this manual includes the following major changes/additions:

- Ability to connect ET 200S to PROFINET I/O (with modules as of order numbers above)
- New parameter "Behavior after channel faults"

Position in the Information Landscape

When working with ET 200S fail-safe modules and depending on your particular application, you will need to consult the additional documentation listed below.

References to additional documentation are included in this manual where appropriate.

Documentation	Brief Description of Relevant Contents
<i>ET 200S Distributed I/O system</i> manual	Describes all generally applicable topics related to the ET 200S hardware (including configuration, installing, and wiring of the ET 200S) and the IM 151 interface module.
<i>Safety Engineering in SIMATIC S7</i> system description	- Provides an overview of the implementation, configuration, and method of operation of S7 Distributed Safety and S7 F/FH fail-safe automation systems - Contains a summary of detailed technical information concerning fail-safe engineering in S7-300 and S7-400 - Includes monitoring and response time calculations for S7 Distributed Safety and S7 F/FH F-systems
For integration in the S7 F/FH F-systems	The <i>S7 F/FH Automation Systems</i> manual describes the tasks that must be performed to commission an S7 F/FH F-system. - The <i>S7-400, M7-400 Programmable Controllers Hardware and Installation</i> manual describes the installation and assembly of S7-400 systems. - The <i>S7-400H Programmable Controllers, Fault-Tolerant Systems</i> manual describes the CPU 41x-H central modules and the tasks involved in setting up and commissioning an S7-400H fault-tolerant system. - The <i>CFC for S7 Continuous Function Chart</i> manual/online help provides a description of programming with CFC.
For integration in the S7 Distributed Safety F-system	The following elements are described in the <i>S7 Distributed Safety, Configuring and Programming</i> manual and online help: - Configuration of the fail-safe CPU and the fail-safe I/O - Programming of the fail-safe CPU in fail-safe FBD or LAD Depending on which F-CPU you use, you will need the following documentation: - The operating manual <i>S7-300, CPU 31xC and CPU 31x: Configuration</i> describes the configuration, installation, addressing and commissioning of S7-300 systems. - The <i>CPU 31xC and CPU 31x, Technical Data</i> product manual describes the standard functions of the CPU 315F-2 DP and PN/DP and the CPU 317F-2 DP and PN/DP. - The <i>Automation System S7-400 CPU Specifications</i> manual describes the standard functions of the CPU 416F-2. - The <i>ET 200S IM 151-7 CPU Interface Module</i> manual describes the standard IM 151-7 CPU. - A separate product information bulletin is available for each applicable F-CPU. The product information bulletins describe only the deviations from the corresponding standard CPUs.
<i>STEP 7</i> manuals	- The <i>Configuring Hardware and Communication Connections with STEP 7 V5.x</i> manual describes the operation of the standard tools of STEP 7. - The <i>System Software for S7-300/400 System and Standard Functions</i> reference manual describes functions for distributed I/O access and diagnostics.
<i>STEP 7</i> online help	- Describes the operation of <i>STEP 7</i> standard tools - Contains information about how to configure and assign parameters for modules and intelligent slaves with <i>HW Config</i> - Contains a description of the programming languages FBD and LAD
<i>PCS 7</i> manuals	Describe how to operate the <i>PCS 7</i> process control system (required when ET 200S with fail-safe modules is integrated in a higher-level control system).

The entire SIMATIC S7 documentation is available on CD-ROM.

4.5 Requirements for Sensors and Actuators

General Requirements for Sensors and Actuators

Note the following important information for safety-related use of sensors and actuators:



Warning

The use of sensors and actuators is outside of our sphere of influence. We have equipped our electronics with such safety engineering features as to leave 85% of the maximum permissible probability of hazardous faults for sensors and actuators up to you (This corresponds to the recommended load division in safety engineering between sensing devices, actuating devices, and electronic switching for input, processing, and output).

Note, therefore, that instrumentation with sensors and actuators bears a considerable **safety responsibility**. Consider, too, that sensors and actuators do not generally withstand proof-test intervals of 10 years (the interval for an external function test according to IEC 61508) without considerable loss of safety.

The probability of hazardous faults and the rate of occurrence of hazardous faults of a safety function must comply with an upper limit determined by a safety integrity level (SIL). You will find a listing of values achieved by F-modules under "Fail-Safe Performance Characteristics" in the technical specifications for F-modules in Chapter 9.

To achieve SIL3 (AK6/Category 4), suitably qualified sensors are necessary.

Requirements for the Duration of Sensor Signals



Warning

Observe the following requirements for sensor signals:

- In order to guarantee accurate detection of the sensor signal by the F-DI module, you must ensure that the sensor signals have a particular minimum duration.
- In order for pulses to be detected with certainty, the time between two signal changes (pulse duration) must be greater than the PROFIsafe monitoring time.

Reliable acquisition by the F-DI module

The following table lists the minimum duration of the sensor signals for the F-DI module. This depends on the parameter settings for the short-circuit test and the input delay in *STEP 7*.

Table 4-2 Minimum Duration of the Sensor Signals to Allow Correct Acquisition by the F-DI Module

Short-Circuit Test Parameter	Assigned Input Delay		
	0.5 ms	3 ms	15 ms
Deactivated	7 ms	9 ms	23 ms
Activated	7 ms	12 ms	37 ms

Reliable acquisition by the safety program on the F-CPU

You will find information on the times necessary for correct acquisition of the sensor signals in the safety program in *"Fail-Safe Modules"* in the system description *Safety Engineering in SIMATIC S7*.

Additional Requirements for Actuators

Fail-safe modules test the outputs in regular intervals. To do so, the F-module briefly switches off activated outputs. The test pulses have the following duration:

- Dark period < 1 ms

Rapid response actuators can drop out briefly during the test. If your process does not tolerate this, you must use actuators with a sufficient lag (> 1 ms).



Warning

If the actuators are operated at voltages higher than 24 VDC (for example, 230 VDC) or if the actuators clear higher voltages, safe isolation must be ensured between the outputs of a fail-safe output module and the components carrying a higher voltage (in accordance with EN 50178).

This is generally the case for relays and contactors. Particular attention must be paid to this aspect for semiconductor switching devices.

Fail-Safe Modules

7.1 Introduction

Overview

Fail-safe power modules and fail-safe digital modules are available for connecting digital sensors or encoders and actuators or loads to ET 200S. This chapter provides the following information for each fail-safe module:

- Properties and special features
- Front view, terminal assignment for terminal modules, and block diagram
- Wiring diagram and programmable parameters
- Diagnostic functions, including corrective measures
- Technical specifications



Warning

The safety characteristics in the Technical Specifications apply for a proof-test interval of 10 years and a repair time of 100 hours.

Description of Usable Standard Power Modules and Terminal Modules

The applicable standard power modules and terminal modules are described in the *ET 200S Distributed I/O System* manual.

7.2 PM-E F pm DC24V PROFIsafe Power Module

7.2.1 Properties of the PM-E F pm DC24V PROFIsafe Power Module

Order Number

6ES7 138-4CF02-0AB0

Properties

The PM-E F pm DC24V PROFIsafe power module has the following properties:

- Two relays for switching voltage buses P1 and P2, 10 A output current
- 2 fail-safe digital outputs, P/M-switching, output current 2 A
- 24 VDC rated load voltage
- Suitable for solenoid valves, DC contactors, and indicator lights
- Group fault display (SF; red LED)
- Status display for each output (green LED)
- Status display for load current power supply (PWR; green LED)
- Assignable diagnostics
- For achievable safety classes (safety integrity level), see following table

Table 7-1 Overview of Achievable Safety Classes (Safety Integrity Levels) with PM-E F pm DC24V PROFIsafe

PM-E F pm DC24V PROFIsafe			Maximum Safety Level That Can Be Achieved
Relay outputs P1 and P2	Without standard DO modules	Signal switches daily or more often	AK6/ SIL3/Category 4
		Signal switches less than once a day	AK4/ SIL2/ Category 3
	with standard DO modules		AK4/ SIL2/ Category 3
DO 0 and DO 1 electronic outputs	without standard DO modules on P1 and P2		AK6/ SIL3/Category 4
	with standard DO modules on P1 and P2		AK4/ SIL2/ Category 3

Switching of Voltage Buses P1 and P2

The power module can be used for fail-safe connection of voltage buses P1 and P2 by means of relay contacts in accordance with AK4/SIL2/Category 3.

Two fail-safe digital outputs

In addition to the P1 and P2 voltage buses the power module has two fail-safe digital outputs, DO 0 and DO 1. AK6/SIL3/Category 4 can be achieved with these outputs if standard DO modules are not connected to P1 and P2.

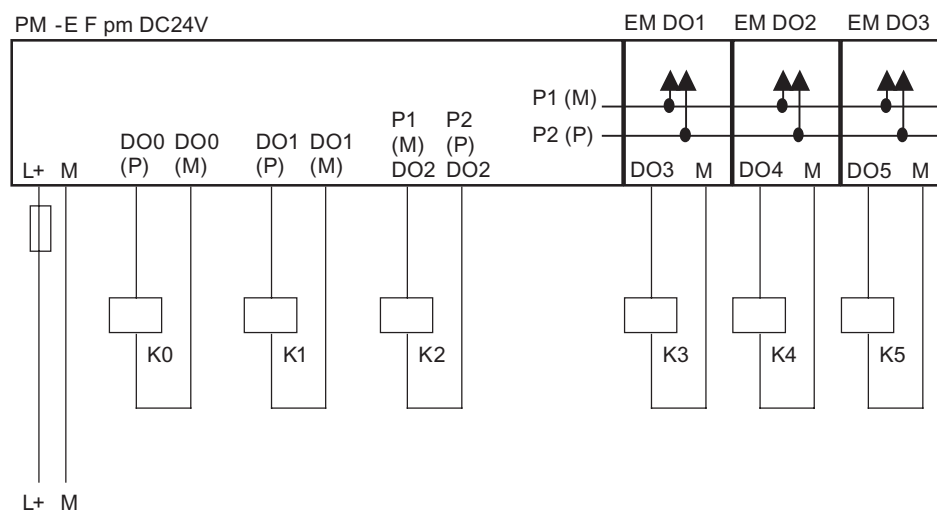


Figure 7-1 Wiring diagram of the PM-E F pm DC24V PROFIsafe

Conditions for Achieving Safety Class

The conditions for achieving the respective safety classes are summarized in the following table.

Table 7-2 PM-E F pm DC24V PROFIsafe: Conditions for AK/SIL/Category

Condition	Achievable AK/SIL/Category
ET 200S standard modules supplied by means of P1 and P2	AK4/SIL2/Category 3 on P1 and P2 and at DO 0 and DO 1
DO 0 and DO 1 used, modules not supplied by means of P1 and P2	AK6/SIL3/Category 4 on DO 0 and DO 1

Power Module Supplies for Standard ET 200S Modules



Warning

Always connect the 24 VDC supply for the standard ET 200S modules on the PM-E F pm DC24V PROFIsafe. Otherwise, the outputs of DO modules may exhibit safety critical behavior.



Warning

When supplying standard DO modules, always use the terminal modules to supply the sensors or actuators (actuator feedback on the DO module). Otherwise, the power module signals a short circuit and the load voltage of this voltage group is interrupted.

Safety-Related Shutdown of Standard DO Modules



Warning

The following ET 200S standard modules are approved for safety-related shutdown in accordance with SIL2:

- 2DO DC24V/0.5A (order number 6ES7 132-4BB01-0AA0 or higher)
 - 2DO DC24V/2A (order number 6ES7 132-4BB31-0AA0 or higher)
 - 2DO DC24V/0.5A HIGH FEATURE (order number 6ES7 132-4BB01-0AB0 or higher)
 - 2DO DC24V/2A HIGH FEATURE (order number 6ES7 132-4BB31-0AB0 or higher)
 - 4DO DC24V/0.5A (order number 6ES7 132-4BD00-0AA0 or higher)
 - 4DO DC24V/2A (order number 6ES7 132-4BD31-0AA0 or higher)
-



Warning

Safety-related activation of outputs of standard DO modules is not possible; rather, only safety-related **shutdown** is possible. You must therefore take the following effects into account:

In the worst case you must consider all possible faults of the standard DO modules and the programs controlling them for which the faults cannot be found directly. For example, the PM-E F pm DC24V PROFIsafe does not detect external short-circuits as per L+ at the standard DO module outputs. All faults of the standard DO modules influence the process via final controlling elements. The process must be made known to the F-CPU via sensors and a suitable safety program.

The safety program must react in a safety-related and logically suitable fashion to unwanted or potentially dangerous states in the process via the PM-E F pm DC24V PROFIsafe and fail-safe output modules.

If you want to avoid the problems described above completely, we recommend that you use P/M switching fail-safe electronic modules 4 F-DO DC24V/2A PROFIsafe with standard ET 200S power modules (see *"4 F-DO DC24V/2A PROFIsafe Digital Electronic Module"* and *Table "Assignment of Power Modules to Electronic Modules/Motor Starters and Safety Class"*) instead of standard DO modules.

Property of the safety-related shutdown of standard DO modules by the PM-E F pm DC24V PROFIsafe:

With this cost-effective solution, when a fault is discovered in the process or on the PM-E F pm DC24V PROFIsafe, there is a comprehensive and simultaneous shutdown of all outputs involved.

Property of individual shutdown of F-modules with fail-safe outputs:

If a fault is discovered, the extent of the shutdown is kept to a minimum. It is also possible to react to critical process states staggered over time or to perform safety-related shutdown of individual outputs. This solution is expensive compared with the safety-related shutdown by the PM-E F pm DC24V PROFIsafe.

Switching grounded loads

If the PM-E F pm DC24V PROFIsafe switches loads that have a connection between chassis and ground (for example to improve the EMC properties) **and** if chassis and ground are connected in the power supply being used, a "short circuit" will be detected.

From the perspective of the F-module, the M switch is bridged by the chassis-ground connection (refer to the following figure as an example of a PM-E F pm DC24V PROFIsafe).

Remedy:

- Use the PM-E F pp DC24V PROFIsafe
- The value of the resistance between chassis and ground at the load end must be greater than 100 k Ω

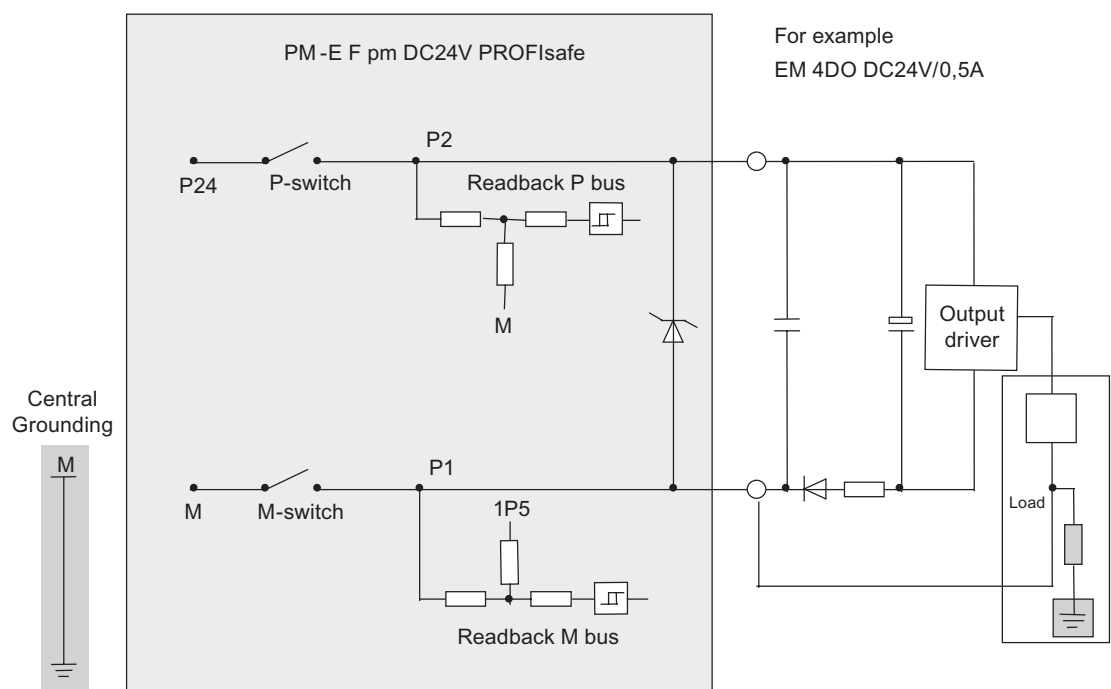


Figure 7-2 Connecting Grounded Loads (resistance exists between chassis and ground)

Capacitive Crosstalk of Digital Input/Output Signals

When fail-safe digital output signals and fail-safe digital input signals are routed through one cable, readback errors can occur on the PM E-F pm DC24V PROFIsafe power module or the F-DO modules. The module then signals a short-circuit.

Cause

During the sensor supply tests of the 4/8 F-DI DC24V PROFIsafe module, the steep switching edge of the output driver can cause crosstalk with other inactive output channels due to the coupling capacitance of the wire, for example on the PM E F pm DC24V PROFIsafe power module. In these channels, this can lead to a response in the readback circuit. A short is detected leading to a safety-related shutdown.

Remedy

- Use separate cables for F-DI modules and F-DO modules or standard DO modules driven by a PM-E F pm DC24V PROFIsafe
- Coupling relay or diodes in the outputs
- Turn off the sensor supply test if this is permitted by the required safety class (safety integrity level).

See also

Assigning Modules of an ET 200S (Page 2-4)

Properties of the 4 F-DO DC24V/2A PROFIsafe digital electronic module (Page 7-80)

7.2.2 Terminal assignment of the PM-E F pm DC24V PROFIsafe

Incoming Supply of the 24 VDC Supply for Electronic Modules with Process-Related Functions

Depending on whether the electronic and load current supplies are electrically isolated in the electronic modules with process-related functions (positioning, counting), you must adhere to the following wiring instructions:

- If electrically isolated, provide an external 24 VDC feed for the electronic module.
- If electrical isolation is not implemented, you must supply the electronic module from the voltage bus P1 of the PM-E F pm 24 VDC PROFIsafe power module.

AK4/SIL2/Category 3 is attainable in both cases.

Front View

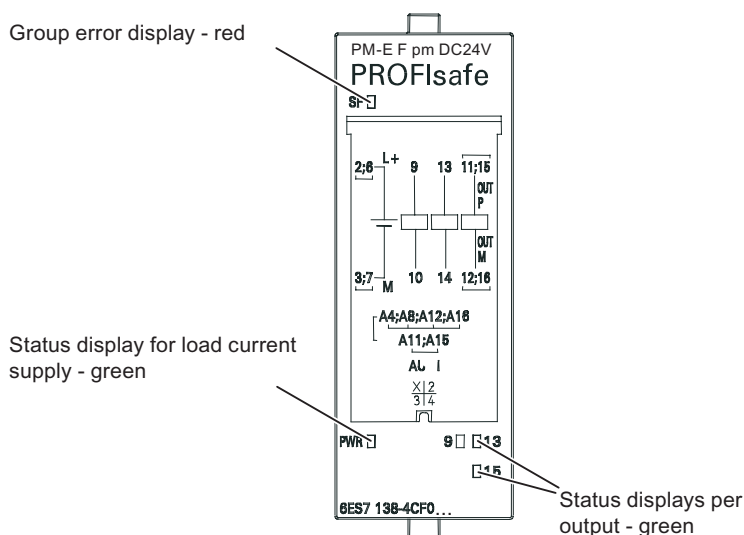


Figure 7-3 Front view of the PM-E F pm DC24V PROFIsafe



Warning

The SF LED and the status displays of the outputs must not be evaluated for safety-related activities.

7.2.6 Technical Specifications for PM-E F pm 24 VDC PROFIsafe

Overview

Technical Specifications	
Dimensions and Weight	
Dimensions W x H x D (mm)	30 x 81 x 52
Weight	Approx. 88 g
Data for Specific Module	
Number of outputs	
• Semiconductor outputs (P-M switching)	2
• Relay outputs (P-M switching)	1
Assigned address area	
• In the I/O area for inputs	5 Byte
• In the I/O area for outputs	5 Byte
Length of cable*	
• Unshielded	200 m, maximum
• Shielded	200 m, maximum
Maximum achievable safety class	
• In accordance with IEC 61508, DIN VDE 0801, and EN 954	Max. SIL3, AK6, Category 4 (for conditions see "PM-E F pm DC24V PROFIsafe Power Module")
Fail-safe performance characteristics	SIL3
• Low demand mode (average probability of failure on demand)	< 1,00E-05
• High demand/continuous mode (probability of a dangerous failure per hour)	< 1,00E-05
Voltages, Currents, Potentials	
Rated supply voltage L+	24 VDC
• Permissible range	20.4 V to 28.8 V
• Power loss ride-through of L+	None
• Power loss ride-through of internal P5	5 ms
• Reverse polarity protection	No
Aggregate current	
• Horizontal installation	
– Up to 40 °C	10 A
– Up to 55 °C	7 A
– Up to 60 °C	6 A
• Vertical installation	
– Up to 40 °C	6 A
Electrical isolation	
• Between channels and backplane bus	Yes
• Between channels and power supply	No
• Between channels	No
• Between channels/power supply and shield	Yes

Technical Specifications	
Permissible potential difference between	
• Shield and ET 200S bus connection	75 VDC/60 VAC
• Shield and I/O (DOs, P1/P2 buses)	75 VDC/60 VAC
• ET 200S bus connection and I/O (DOs, P1/P2 buses)	250 VAC
Isolation in the series tested with	
• Shield and ET 200S bus connection	500 VDC/1 min or 600 VDC/1 s
• Shield and I/O (DOs, P1/P2 buses)	500 VDC/1 min or 600 VDC/1 s
• ET 200S bus connection and I/O (DOs, P1/P2 buses)	1500 VAC/1 min or 2545 VDC/1 s
Isolation in the type test tested with	
• Shield and ET 200S bus connection	350 VAC/1 min
• Shield and I/O (DOs, P1/P2 buses)	350 VAC/1 min
• ET 200S bus connection and I/O (DOs, P1/P2 buses)	2830 VAC/1 min
• Impulse current test between ET 200S bus connection and I/O (DOs, P1/P2 buses)	6000 VDC/5 positive and 5 negative pulses
Current consumption	
• From backplane bus	28 mA, maximum
• From load voltage L+ (without load)	100 mA, typical
Power dissipation of the module	4 W, typical
Status, Interrupts, Diagnostics	
Status display	• Green LED per channel • Green LED for the load voltage
Diagnostic functions	
• Group fault display	Red LED (SF)
• Diagnostic information can be displayed	Possible
Data for Selecting an Actuator for the Semiconductor Outputs**	
Output voltage	
• For "1" signal	• Minimum L+ (-2.0 V) • P-switch: minimum L+ (-1.5 V), voltage drop in M-switch: 0.5 V, maximum
Output current for "1" signal	
• Rated value	2 A
• Permissible range	20 mA to 2.4 A
For "0" signal (residual current)	0.5 mA, maximum
Indirect control of load by means of interface relay:	
Residual current for "0" signal	
• P-Switch	0.5 mA, maximum
• M-Switch	4 mA, maximum
Load resistance range	12 Ω to 1 k Ω
Lamp load	10 W, maximum

Technical Specifications		
Wire break monitoring (open load detection) and overload monitoring		
• Response threshold	I < 4 to 19 mA	
• Fault detection time	Depending on the selected readback time (see <i>Response Times</i>)	
Parallel connection of 2 outputs		Not possible
Control of a digital input		Not possible
Switching frequency		
• With resistive load	30 Hz symmetrical, maximum	
• With inductive load in accordance with IEC 947-5-1, DC13	0.1 Hz symmetrical, maximum	
• With lamp load	10 Hz symmetrical, maximum	
Voltage induced on current interruption limited to		
• Semiconductor outputs	L+ (-2x 47 V)	
• Relay outputs	P1/P2 (1 V)	
Short-circuit protection of semiconductor outputs		Yes, electronic
• Response threshold of short circuit	5 A to 12 A	
• Response threshold (external M-short circuit)	5 A to 12 A	
• Response threshold (external P-short circuit)	25 A to 45 A	
Overload protection of semiconductor outputs		Yes
• Response threshold	I >2.6 A to 2.8 A	
Data for Selecting an Actuator for the Relay Outputs**		
Switching capacity and service life of contacts (voltage 24 VDC)		
• Mechanical endurance (without load)	Current	Number of switching cycles (typ.)
	0 A	10 million
• For resistive load	Current	Number of switching cycles (typ.)
	10 A	0.23 million
	8 A	0.3 million
	6 A	0.38 million
	4 A	0.5 million
	2 A	1.0 million
	1 A	2.0 million
• For inductive load in accordance with IEC 947-5-1, DC13	Current	Number of switching cycles (typ.)
	10 A	0.1 million
	8 A	0.15 million
	6 A	0.2 million
	4 A	0.3 million
	2 A	0.5 million
	1 A	1.0 million
• For lamp load	Power	Number of switching cycles (typ.)
	100 W	0.12 million

Technical Specifications	
Contact protection (internal)	Internal readback circuit
• Between P and M relay output	39 V suppressor diode
Wire break monitoring	No
Parallel connection of 2 outputs	Not possible
Control of a digital input	Not possible
Switching frequency	
• With resistive load	2 Hz, maximum
• With inductive load in accordance with IEC 947-5-1, DC13	0.1 Hz, maximum
• With lamp load	2 Hz, maximum
Short-circuit protection of output	No, external miniature circuit breaker, "B" characteristic (in accordance with IEC 947-5-1), 10 A required
Time, Frequency	
Internal preparation times	See <i>Response Times</i>
Acknowledgment time in safety mode	4 ms minimum/8 ms maximum
Protection against Overvoltage	
Protection of supply voltage L+ from surge in accordance with IEC 61000-4-5 with external protection elements only	
• Symmetrical (L+ to M)	+ 1 kV; 1,2/50 µs
• Asymmetrical (L+ to PE, M to PE)	+2 kV; 1,2/50 µs
Protection of outputs from surge in accordance with IEC 61000-4-5 with external protection elements only	
Symmetrical (DO to M)	+ 1 kV; 1,2/50 µs
Asymmetrical (DO to PE, M to PE)	+ 1 kV; 1,2/50 µs
*: In order to achieve the specified cable length, you must route the P- and M-signal lines in a cable or a non-metallic sheathed cable.	
**: For more information on the requirements for sensors and actuators see <i>Wiring and Installing Modules</i> .	

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. You can find more information about industrial security on the Internet (<http://www.siemens.com/industrialsecurity>).

To stay informed about product updates as they occur, sign up for a product-specific newsletter. You can find more information on the Internet (<http://support.automation.siemens.com>).

PFDavg and PFH values for components with use in SIMATIC Safety, Distributed Safety and F/FH Systems

This product information contains **important information on the F-systems SIMATIC Safety, Distributed Safety and F/FH Systems**. The Product Information is part of the product supplied.

PFDavg and PFH values

The following tables contain the PFDavg and PFH values for individual components with use in SIMATIC Safety (S), Distributed Safety (D) and F/FH Systems (F) with a repair time of 100 hours:

F-CPU S7-1200/1500	Operation in low demand mode low demand mode According to IEC 61508:2010: PFDavg = Average probability of a dangerous failure on demand	Operation in high demand or continuous mode high demand/continuous mode According to IEC 61508:2010: PFH = Average frequency of a dangerous failure [h ⁻¹]	With a mission time of	S	D	F
For all F-CPU S	< 2E-05	< 1E-09	20 years	x	-	-

F-I/O ET 200SP	Article number	Operation in low demand mode low demand mode According to IEC 61508:2010: PFD_{avg} = Average probability of a dangerous failure on demand	Operation in high demand or continuous mode high demand/continuous mode According to IEC 61508:2010: PFH = Average frequency of a dangerous failure [h⁻¹]	With a mission time of	S	D	F
F-DI 8x24VDC HF	6ES7136-6BA00-0CA0	SIL 3: < 2E-05	SIL 3: < 1E-09	20 years	x	x	-
F-DQ 4x24VDC/2A PM HF	6ES7136-6DB00-0CA0	SIL 3: < 2E-05	SIL 3: < 1E-09	20 years	x	x	-
F-PM-E 24VDC/8A PPM ST	6ES7136-6PA00-0BC0	SIL 3: < 2E-05	SIL 3: < 1E-09	20 years	x	x	-
F-RQ 1x24VDC/24..230V AC/5A	6ES7136-6RA00-0BF0	SIL 2: < 1E-04, with function test 1x per year	SIL 2: < 1E-08, with function test 1x per year	20 years	x	x	-
		SIL 3: < 1E-05, with function test 1x per month	SIL 3: < 6E-09, with function test 1x per month	20 years	x	x	-

F-I/O ET 200S	Article number	Operation in low demand mode low demand mode (PFD = average probability of failure on demand)	Operation in high demand or continuous mode high demand/continuous mode (PFH = probability of a dangerous failure per hour)	With a mission time of	S	D	F
4/8 F-DI DC24V PROFIsafe	6ES7138-4FA03-0AB0	SIL 2: < 1E-03 SIL 3: < 1E-05	SIL 2: < 1E-08 SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4FA04-0AB0	SIL 2: < 1E-03 SIL 3: < 1E-05	SIL 2: < 1E-08 SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4FA05-0AB0	SIL 2: < 1E-03 SIL 3: < 1E-05	SIL 2: < 1E-08 SIL 3: < 1E-10	20 years	x	x	x
4 F-DO DC24V/2A PROFIsafe	6ES7138-4FB02-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4FB03-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4FB04-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
4 F-DI/3 F-DO DC24V PROFIsafe	6ES7138-4FC00-0AB0	SIL 2: < 1E-04	SIL 2: < 1E-08	20 years	x	x	x
	6ES7138-4FC01-0AB0	SIL 2: < 1E-04	SIL 2: < 1E-08	20 years	x	x	x
PM-E F pm DC24V PROFIsafe	6ES7138-4CF02-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4CF03-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
PM-E F pp DC24V PROFIsafe	6ES7138-4CF41-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4CF42-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
1 F-RO DC24V/AC24..230V /5A	6ES7138-4FR00-0AA0	SIL 3: < 1E-05	SIL 3: < 1E-09	20 years	x	x	x

Fail-safe GSD based DP slaves Fail-safe GSD based IO devices Fail-safe PA field devices Fail-safe HMI devices	Operation in low demand mode low demand mode According to IEC 61508:2010: PFD_{avg} = Average probability of a dangerous failure on demand	Operation in high demand or continuous mode high demand/continuous mode According to IEC 61508:2010: PFH = Average frequency of a dangerous failure [h⁻¹]	With a mission time of	S	D	F
Fail-safe GSD based DP slaves: See Technical Data for fail-safe GSD based DP slave						
Fail-safe GSD based IO devices: See Technical Data for fail-safe GSD based IO device						
Fail-safe PA field devices: See Technical Data for fail-safe PA field device						
Fail-safe HMI devices: See technical specifications on the fail-safe HMI device						
Other fail-safe devices: See technical specifications on the fail-safe device						

Determine the contribution of the F-system to the PFD_{avg} and PFH values

The contribution of the fail-safe system to the PFD_{avg} and PFH values of a safety function is determined by adding the PFD_{avg}- and PFH values of the F-CPU and F-I/Os involved.

The contribution of the safety-related communication is added to this. Please note that several F-systems can be involved in a safety function.

You determine the PFD_{avg} and PFH values of a safety function by adding the contribution of the fail-safe system to the contribution of the encoders and actuators involved in the safety function.

Calculation example

A safety function is implemented with a SIMATIC Safety F-system. The F-CPU and F-I/O listed in the following table are involved in the safety function.

20 years was selected as the mission time. The fail-safe signal modules operate in safety mode for SIL3/Kat.4/PL_e. Operation is in high demand mode:

F-CPU, F-SMs and safety-related communication involved in the safety function	Quantity	Probability of a dangerous failure per hour
CPU 319F-3 PN/DP 6ES7318-3FL01-0AB0	1	3E-09
SM 326; DO 10 × DC 24V/2A 6ES7326-2BF01-0AB0	1	1E-09
SM 326; DI 24 × DC 24V 6ES7326-1BK02-0AB0	2	2E-09
Safety-related communication		1E-09
Total		7E-09

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG

PFD_{avg} and PFH values for components with use in SIMATIC Safety, Distributed Safety and F/FH Systems
A5E03310062-AE, 10/2015