SIEMENS

SIMATIC

ET 200SP
ET 200SP distributed I/O system

Product Information

Translation of original operating instructions

07/2013

A5E32288220-AA

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E32288220-AA
℗ 08/2013 Technical data subject to change

Preface

Scope of the product information

This product information amends the ET 200SP Distributed I/O System System Manual (http://support.automation.siemens.com/WW/view/en/58649293) to include ET 200SP fail-safe modules.

Table of contents

Product overview

1

1.1 What are fail-safe automation systems and fail-safe modules?

Fail-safe automation systems

Fail-safe automation systems (F-systems) are used in systems with higher-level safety requirements. F-systems serve to control processes and ensure that they are in a safe state immediately after shutdown. In other words, F-systems control processes in which an immediate shutdown does not endanger persons or the environment.

Fail-safe modules

The key difference between fail-safe modules (F-modules) and standard ET 200SP modules is that they have an internal two-channel design. The two integrated processors monitor each other, automatically test the input and output circuits, and switch the F-I/O module to a safe state in the event of a fault.

The F-CPU communicates with the fail-safe modules via the fail-safe PROFIsafe bus profile.

Fail-safe power modules, together with the respective BaseUnit, serve the load voltage supply of the potential group and the safety-oriented tripping of the load voltage for standard output modules.

Fail-safe digital input modules detect the signal states of safety-oriented sensors and send the relevant safety message frames to the F-CPU.

Fail-safe digital output modules are suitable for safety-related shutdown procedures with short circuit and cross-circuit protection up to the actuator.

Possible uses of ET 200SP with fail-safe modules

The use of ET 200SP with fail-safe modules allows conventional configurations in safety engineering to be replaced with PROFNET IO components. This includes the replacement of switching devices for emergency STOP, protective door monitors, two-hand operation, etc.

ET 200SP fail-safe modules are supported with the STEP 7 Safety Advanced optional package V12 including HSP 54 or higher.

ET 200SP fail-safe modules are supported with IM155-6PN ST as of firmware V1.1.

Achievable safety classes

Fail-safe modules are equipped with integrated safety functions for safety mode.

The following safety classes can be achieved through appropriate parameter assignment of the safety functions in STEP 7 Professional V12 SP1 or higher with STEP 7 Safety Advanced optional package V12 or higher, through a specific combination of fail-safe and standard modules, and through a specific arrangement and wiring of sensors and actuators:

Safety class in safety mode		
According to IEC 61508	According to ISO 13849-1:2006	
SIL2	Category 3	(PL) Performance Level d
SIL3	Category 3	(PL) Performance Level e
SIL3	Category 4	(PL) Performance Level e

Use in SIMATIC Safety F-systems

ET 200SP fail-safe modules can be used with the STEP 7 Safety Advanced optional package, V12 or higher under PROFINET IO, together with an F-CPU.

SIMATIC Safety F-system with ET 200SP

The following figure shows a sample configuration for a SIMATIC Safety F-system with, among other things, an ET 200SP on a PROFINET IO. The PROFINET IO lines can be set up with copper cable, with fiber-optic cable or WLAN.

You will find further information on the Internet at Application planning (Page 13).

Tasks of the fail-safe IO controller (F-CPU) include the exchange of safety-related and non-safety-related data with fail-safe and standard ET 200SP modules.

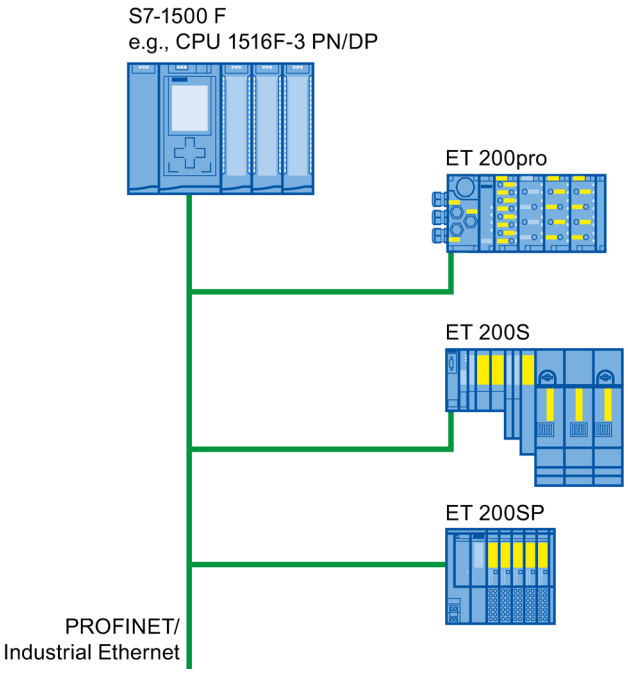


Figure 1-1 Fail-safe SIMATIC Safety automation system (sample configuration)

Use in safety mode only

Fail-safe modules can only be used in fail-safe mode. They cannot be used in non-fail-safe mode In this context, fail-safe mode/non-fail-safe mode refers to the operating mode of the F-I/O module, which either does or doesn't support safety-related communication via safety message frames.

Fail-safe modules and non-fail-safe modules can be combined within an ET 200SP.

1.2 Fault reactions with fail-safe modules

Safe state (safety concept)

The basic principle behind the safety concept is the existence of a safe state for all process variables.

Note

For digital F-modules, this safe state is the value "0". This applies to both sensors and actuators.

Fault reactions and startup of the F-system

The safety function requires that fail-safe values (safe state) be applied to the fail-safe module instead of process values (**passivation of the fail-safe module**) in the following situations:

- When the F-system is started up
- If errors are detected during safety-related communication between the F-CPU and the F-module via the PROFIsafe safety protocol (communication error)
- If F-I/O faults or channel faults are detected (e.g., wire break, discrepancy error)

Detected faults are written to the diagnostic buffer of the F-CPU and communicated to the safety program in the F-CPU.

F-modules cannot save errors as retentive data. When the system is powered down and then restarted, any faults still existing are detected again during startup. However, you have the option of saving faults in your safety program.

⚠ WARNING

For channels that you set to "deactivated" in *STEP 7*, no diagnostic response or error handling is triggered when a channel fault occurs, not even when such a channel is affected indirectly by a channel group fault ("Channel activated/deactivated" parameter).

Remedying faults in the F-system

To remedy faults in your F-system, follow the procedure described in IEC 61508-1:2010 section 7.15.2.4 and IEC 61508-2:2010 section 7.6.2.1 e.

The following steps must be performed:

1. Diagnostic and repair of the fault
2. Revalidation of the safety function
3. Recording in the service report

Fail-safe value output for F-modules

In the case of F-modules with inputs, the F-system provides fail-safe values (0) for the safety program instead of the process data pending at the fail-safe inputs in case of passivation.

In the case of F-modules with outputs, the F-system transfers fail-safe values (0) to the fail-safe outputs instead of the output values provided by the safety program in case of passivation. The output channels are de-energized. This also applies when the F-CPU goes into STOP mode. The parameter assignment of fail-safe values is not possible.

Depending on which F-system you are using and the type of fault that occurred (F-I/O fault, channel fault or communication error), fail-safe values are used either for the relevant channel only or for all channels of the relevant fail-safe module.

Reintegration of a fail-safe module

The system changes from fail-safe to process values (reintegration of an F-module) either automatically or only after user acknowledgment in the safety program. If channel faults occur, it may be necessary to remove and reinsert the F-module. A detailed listing of faults requiring removal and insertion of the F-module can be found in the section Diagnostic messages of the respective F-module.

After reintegration, the following occurs:

- In the case of an F-module with inputs, the process data pending at the fail-safe inputs are provided to the safety program
- In the case of an F-module with outputs, the output values provided in the safety program are again transferred to the fail-safe outputs

Additional information on passivation and reintegration

For additional information on passivation and reintegration of F-I/O, refer to the SIMATIC Safety, Configuring and Programming (http://support.automation.siemens.com/WW/view/en/54110126) manual.

Reaction of the F-module with inputs to communication errors

F-modules with inputs respond differently to communication errors compared to other errors.

If a communication error is detected, the current process values remain set at the inputs of the F-module. There is no passivation of the channels. The current process values are passivated in the F-CPU.

Application planning

2

2.1 Forming potential groups with fail-safe modules

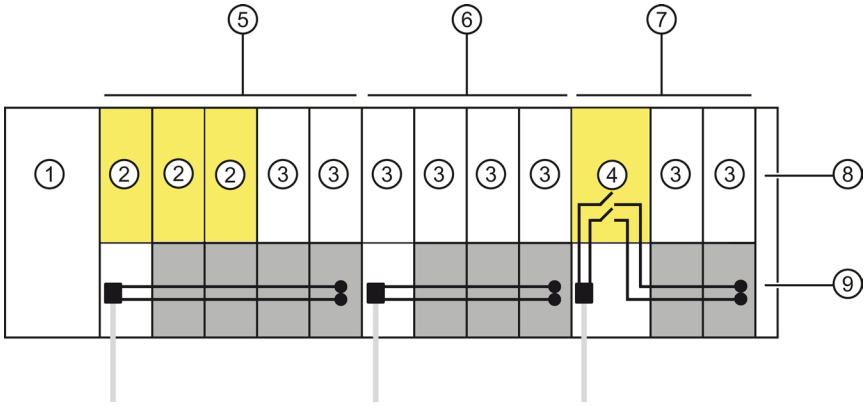
Introduction

ET 200SP distributed I/O systems can be configured using fail-safe and non-fail-safe modules. This chapter provides an example of a mixed configuration comprising fail-safe and non-fails-safe modules.

Assembly example for ET 200SP with fail-safe and non-fail-safe modules

Generally speaking, it is not necessary to operate fail-safe and non-fail-safe modules in separate potential groups. You can divide the modules into fail-safe and non-fail-safe potential groups and mount them.

The following diagram shows an assembly example with fail-safe and non-fail-safe modules within a single ET 200SP.



① Interface module IM 155-6 PN HF
② F-module
③ Non-fail-safe module
④ Power module F-PM-E 24VDC/8A PPM ST
⑤ Mixed fail-safe and non-fail-safe potential group with BaseUnits BU15..D and BU15..B.
You achieve SIL3/Cat.4/PLe for the fail-safe modules.
⑥ Non-fail-safe potential group with BaseUnits BU15..D and BU15..B.
⑦ Fail-safe potential group with BaseUnits BU20..D and BU15..B.
Through disconnection of the power bus, and thus of the non-fail-safe modules, up to SIL2/Cat.3/PLd is possible.
⑧ Server module
⑨ P1/P2 power buses

Figure 2-1 ET 200SP assembly example with fail-safe modules

Installation

3

3.1 Basics

The following applies to ET 200SP fail-safe modules:

⚠ WARNING
Protection from conductive contaminants In consideration of the environmental conditions, the devices must be protected from conductive contaminants. One way to accomplish this is by installing the devices in a control cabinet with an appropriate degree of protection.

Connecting

4

4.1 Additional rules and provisions for operation of the ET 200SP with fail-safe modules

4.1.1 Safe functional extra-low voltage (SELV) for fail-safe modules

⚠ WARNING

The fail-safe modules must be operated with safe functional extra low voltage (SELV, PELV).

You can find more information on safe functional extra-low voltage in the data sheets, for example, of the applicable power supplies.

The fail-safe modules work with a rated voltage of 24 V DC. The tolerance range is 20.4 V DC to 28.8 V DC.

Within the overvoltage range from 32 V DC to 36 V DC, the F-modules react in a fail-safe manner and the inputs and outputs are passivated. For overvoltages greater than 36 V DC, the F-modules are permanently de-energized.

Use a power supply unit that does not exceed U_m = 36 V DC even in the event of a fault. For more on this, refer to the information in the data sheet on overvoltage protection in the case of an internal error. Or implement appropriate measures to limit the voltage, e.g., use of an overvoltage protector.

All system components that can supply electrical energy in any form whatsoever must fulfill this condition.

Each additional circuit (24 V DC) used in the system must have a safe functional extra low voltage (SELV, PELV). Refer to the relevant data sheets or contact the manufacturer.

Sensors and actuators with an external power supply can also be connected to F-modules. Make sure that power is supplied to these components from safe functional extra-low voltage as well. The process signal of a 24 V DC digital module may not exceed a fault voltage U_m in the event of a fault.

⚠ WARNING

Even when a fault occurs, the permissible potential difference between the supply of the interface module (bus voltage) and the load voltage must not be exceeded.

An external direct electrical connection is one way to meet this requirement. This also prevents potential differences from causing voltage additions at the individual voltage sources, which would cause the
fault voltage U_m to be exceeded.

Power supply requirements for compliance with NAMUR recommendations

Note

To ensure adherence to the NAMUR recommendation NE 21, IEC 61131-2 and EN 298, only use power packs/power supply units (230 V AC → 24 V DC) with a mains buffering time of at least **20 ms**. The latest up-to-date information on PS components is available on the Internet (http://mall.automation.siemens.com).

It goes without saying that these requirements also apply to power packs/power supply units not constructed using ET 200SP / S7-300/-400/-1500 technology.

4.1.2 Requirements of sensors and actuators for fail-safe modules

General requirements for sensors and actuators

Note the following important warning regarding safety-related use of sensors and actuators:

⚠ WARNING

Note that instrumentation with sensors and actuators bears a considerable **safety responsibility**. Also bear in mind that sensors and actuators generally do not have proof-test intervals of 20 years as defined in IEC 61508:2010 without considerable loss of safety.

The probability of hazardous faults and the rate of hazardous faults of safety functions must comply with an SIL-defined high limit. A listing of values achieved by F-modules in the technical specifications of the F-modules is available under "Fail-safe performance characteristics".

To achieve the respective safety class, suitably qualified sensors and actuators are necessary.

Additional sensor requirements

General rule: To achieve SIL3/Cat.3/PLe, a single-channel sensor is all you need. However, to achieve SIL3/Cat.3/PLe with a single-channel sensor, the sensor itself must be SIL3/Cat.3/PLe-capable; otherwise the sensor must be connected by two channels to achieve this safety level.

To achieve SIL3/Cat.4/PLe, sensors must be connected by two channels.

⚠ WARNING

In the case of fail-safe input modules, a "0" value is output to the F-CPU after detection of faults. You therefore need to make sure that the sensors are implemented in such a way as to ensure the reliable reaction of the safety program when the sensor is in the "0" state.

Example: In its safety program, an EMERGENCY-STOP sensor must achieve the shutdown of the respective actuator when it is in the "0" state (EMERGENCY-STOP button pressed).

Duration requirements for sensor signals

⚠ WARNING

Observe the following requirements for sensor signals:

- In order to ensure the correct detection of the sensor signals via fail-safe modules with inputs, you need to make sure that the sensor signals are output for a 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 detection by F-modules with inputs

The minimum duration of sensor signals for F-modules with inputs depends on the configured input delay, the parameters of the short circuit test of the sensor supplies, and the configured discrepancy behavior for 1oo2 evaluation. The signal must be greater than the maximum response time of the configured application. Information on calculating the maximum response time can be found in section "Response times" of the respective F-module.

The maximum permitted switching frequency of the sensor signals results from the minimum duration.

Additional requirements for actuators

The fail-safe output modules test the outputs at regular intervals. The F-module briefly switches off the activated outputs and, if necessary, switches on the deactivated outputs. You can assign the maximum duration of the test pulses (dark and light period) with parameters.

High-speed actuators may briefly drop out or be activated during this test. If your process does not tolerate this, set the pulse duration of the light or dark test correspondingly or use actuators that have sufficient lag.

⚠ WARNING

If the actuators switch voltages greater than 24 V DC (e.g., 230 V DC), the outputs of a fail-safe output module and the parts carrying a higher voltage must be electrically isolated (according to IEC 60664-1).

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

Technical specifications of sensors and actuators

Refer to the manuals of the fail-safe modules for technical specifications to assist you in selecting sensors and actuators.

4.1.3 Capacitive crosstalk of digital input/output signals

When fail-safe digital output and input signals are in a single cable, F-DQ modules and F-PM-E modules may experience readback errors.

Cause: Capacitive crosstalk

During the bit pattern test of the outputs or the sensor supply of the inputs, the steep switching edge of the output drivers caused by the coupling capacitance of the line may result in crosstalk to other non-activated output or input channels. This may then lead to a response of the readback circuit in these channels. The module detects a cross circuit/short circuit and performs a safety-related shutdown.

Remedy:

- Separate cables for F-DI modules, F-DQ modules, and F-PM-E modules or non-fail-safe DQ modules
- Separate cables for F-DQ channel and F-DI channels for the F-PM-E module
- Coupling relay or diodes in the outputs
- Disable the sensor supply test if safety class requirements allow it

Cause: magnetic crosstalk

Note that an inductive load connected to the F-DQ channels can induce capacitive coupling of a strong magnetic field.

Remedy:

- Spatially disconnect the inductive loads or shield against the magnetic field.
- Configure the readback time to 50 ms or higher.

Configuring

5

5.1 Assigning the F-destination address for fail-safe modules

5.1.1 Assigning the F-destination address

The F-destination address is saved permanently on the coding element of the ET 200SP fail-safe modules.

Note

During assignment of the F-destination address, the F-modules must be supplied with supply voltage L+.

Note

Note the following in conjunction with configuration control:

Before you can use configuration control together with F-modules, you must assign the F-destination address to the F-modules at the designated slots. For this, each F-module must be inserted in the slot configured for it. The actual configuration can then differ from the specified configuration.

For additional information on assigning the F-destination address, refer to the SIMATIC Safety - Configuring and Programming (http://support.automation.siemens.com/WW/view/en/54110126) programming and operating manual.

Maintenance 6

6.1 Firmware update

Introduction

It may be necessary to update the firmware during operation (e.g. function expansions).

Update the firmware of the interface module and I/O modules using firmware files.

Options for the firmware update

Online via PROFINET IO/PROFIBUS DP (with STEP 7)

Requirements

The ET 200SP is accessible online via PROFINET IO/PROFIBUS DP.

Additional requirement for fail-safe modules

⚠ WARNING

Check of the firmware version for F-validity

When using a new firmware version, you must check whether the employed firmware version is approved for use in the respective module.

The approved firmware version is specified in the appendices of the Certificate for SIMATIC Safety.

Procedure

Connect the programming device or PC to the PROFINET IO or PROFIBUS DP interface of the ET 200SP.

Note

Firmware update of analog I/O modules

For analog I/O modules, L+ supply voltage must be present on the module at the start of and during the firmware update.

You can find additional information on the procedure in the online help for STEP 7.

See also

Certificate (http://support.automation.siemens.com/WW/view/en/49368678/134200)

Technical specifications

7

7.1 Electromagnetic compatibility of fail-safe modules

Protecting ET 200SP with fail-safe modules against overvoltages

If your equipment requires protection from overvoltage, we recommend that you use an external protective circuit (surge filter) between the load voltage power supply and the load voltage input of the BaseUnits to ensure surge immunity for the ET 200SP with fail-safe modules.

Note

Lightning protection measures always require a case-by-case examination of the entire system. An almost complete protection from overvoltages, however, can only be achieved if the entire building surroundings have been designed for overvoltage protection. In particular, this involves structural measures in the building design phase.

For detailed information regarding overvoltage protection, we recommend that you contact your Siemens representative or a company specializing in lightning protection.

The following figure shows an example configuration with fail-safe modules. Voltage is supplied by 1 power supply unit. Note, however, that the total current of the modules fed by the power supply unit must not exceed the permissible limits. You can also use multiple power supply units.

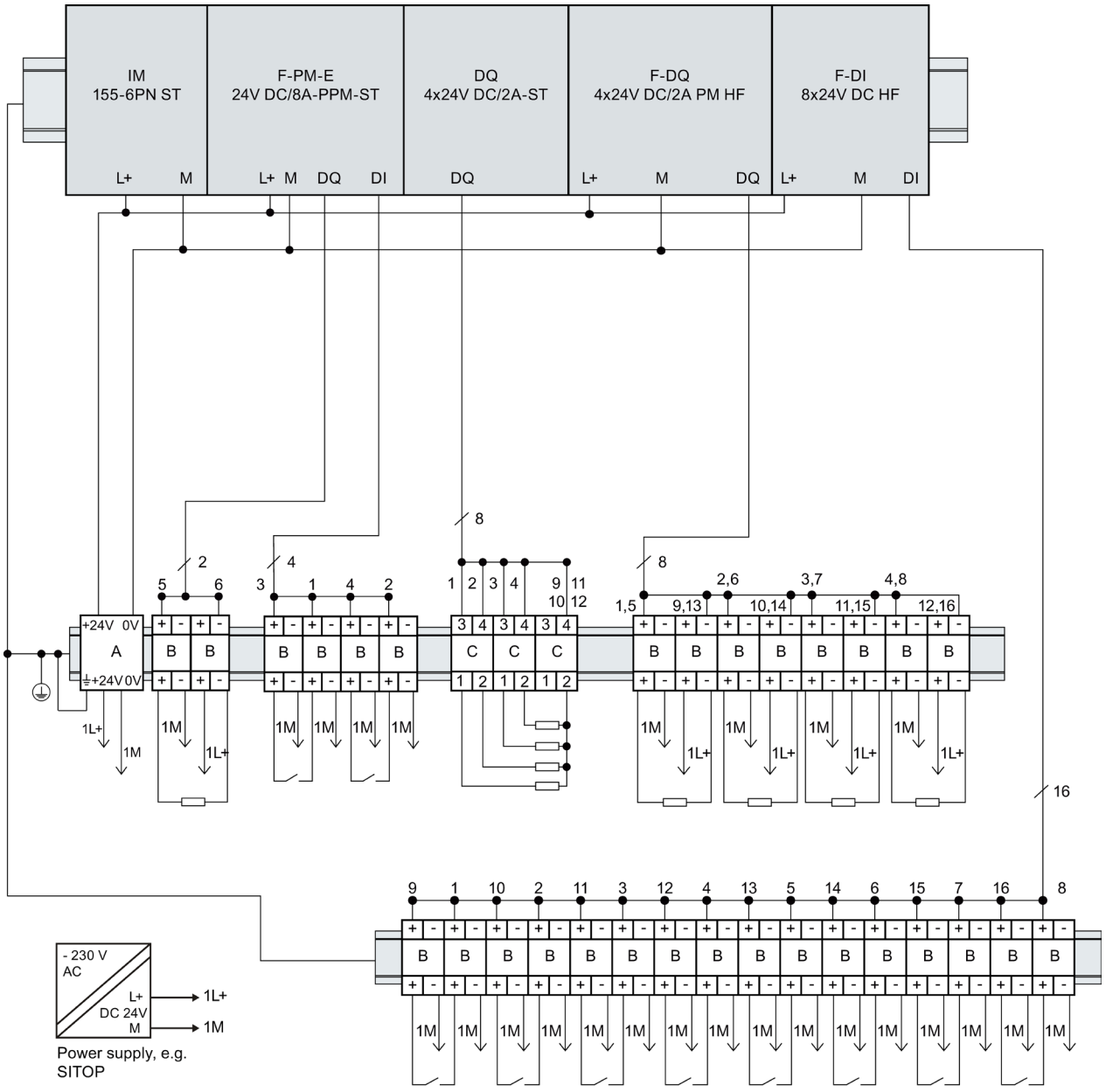


Figure 7-1 External protective circuit (surge filter) for ET 200SP with fail-safe modules

Name	Order number of Dehn Co.
A = BVT AD 24	918 402
B = DCO RK D 5 24	919 986
C = DEHNconnect DCO RK E 60	919 990

7.2 Standards and approvals

CE mark

The ET 200SP F distributed I/O system meets the requirements and safety objectives of the following EC directives and satisfies the harmonized European Standards (EN) for programmable logic controllers published in the official journals of the European Community:

- 2006/42/EC "Directive on Machinery" (Machinery Directive)
- 2006/95/EC "Electrical Equipment Designed for Use within Certain Voltage Limits" (Low-Voltage Directive)
- 2004/108/EC "Electromagnetic Compatibility" (EMC Directive)
- 94/9/EC "Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres" (Explosion Protection Directive)

The EC declarations of conformity are kept available for the relevant authorities at:

Siemens Aktiengesellschaft
Industry Sector
I IA AS FA DH AMB
PO Box 1963
D-92209 Amberg, Germany

These are also available for download on the Customer Support web page, keyword "Declaration of Conformity".

Accessories/spare parts

8

8.1 Lightning protection and overvoltage protection for fail-safe modules

Overvoltage suppressors for fail-safe electronic modules

Note

This section lists only those overvoltage suppressors that may be used for the protection of fail-safe modules.

Be sure to observe the detailed information on lightning protection and overvoltage protection of the ET 200SP distributed I/O device in ET 200SP distributed I/O system (http://support.automation.siemens.com/WW/view/en/58649293).

Components for overvoltage protection of fail-safe modules (lightning protection zone transition 0_B to 1)

The table below lists overvoltage arresters you can use for fail-safe modules:

Table 8- 1 Components for the overvoltage protection (only for unshielded lines)

Fail-safe modules	Connecting of the lines to interface 0_B to 1 with:	Article number
Supply voltage 1L+, L+ (24 V DC)	BLITZDUCTOR BVT AD 24	918 402
Inputs/outputs of the F-modules (24 V DC)	DEHNconnect RK DCO RK D 5 24	919 986
Direct ordering of the components from: DEHN + SÖHNE GmbH + CO. KG. Hans-Dehn-Str. 1 D-92318 Neumarkt, Germany Phone +49 (0)9181-906-730		

Glossary

1oo1 evaluation

Type of → sensor evaluation – in the case of the 1oo1 evaluation, there → is one sensor with a 1-channel connection to the F module.

1oo2 evaluation

Type of → sensor evaluation – in the case of 1oo2 evaluation , two input channels are assigned one two-channel sensor or two one-channel sensors. The input signals are compared internally for equivalence or nonequivalence.

Acknowledgment time

During the acknowledgment time, the → F-I/O acknowledge the sign of life specified by the → F-CPU. The acknowledgment time is included in the calculation of the → monitoring time and → response time of the overall fail-safe system.

Actuator

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

Availability

Availability is the probability that a system is functional at a specific point in time. Availability can be increased by redundancy, e.g., by using multiple -> sensors at thesame measuring point.

Channel fault

Channel-specific fault, such as a wire break or short circuit.

In channel-specific passivation, the affected channel is either automatically reintegrated or the fail-safe module must be removed and reinserted after the fault has been eliminated.

Channel group

The channels of a module are grouped together in a channel group. Certain parameters in STEP 7 can only be assigned to channel groups, rather than to individual channels.

Channel number

Channel numbers are used to uniquely identify the inputs and outputs of a module and to assign channel-specific diagnostic messages.

Channel-specific passivation

With this type of passivation, only the affected channel is passivated in the event of a → channel fault. In the event of a → module fault, all channels of the → fail-safe module are passivated.

CRC

Cyclic Redundancy Check

CRC signature

The validity of the process values in the safety message frame, the accuracy of the assigned address references, and the safety-related parameters are validated by means of the CRC signature in the safety message frame.

Dark period

Dark periods occur during shutdown tests and complete bit pattern tests. The fail-safe output module switches test-related zero signals to the active output. This output is then briefly disabled (= dark period). An adequate carrier → actuator will not respond to this and will remain activated.

Derating

See temperature characteristics

Discrepancy analysis

The discrepancy analysis for equivalence/non-equivalence is used for fail-safe applications to prevent errors from time differences between two signals for the same function. The discrepancy analysis is initiated when different levels are detected in two associated input signals (when testing for non-equivalence: the same levels). A check is performed to determine whether the difference (for nonequivalence testing: the same levels) has disappeared after an assignable time period, the so-called discrepancy time. If not, this means that a discrepancy error exists.

The discrepancy analysis compares the two input signals of the 1oo2 sensor evaluation in the fail-safe input module.

Discrepancy time

Configurable time for the → discrepancy analysis. If the discrepancy time is set too high, the fault detection time and → fault reaction time are extended unnecessarily. If the discrepancy time is set too low, availability is decreased unnecessarily since a discrepancy error is detected when, in reality, no error exists.

Fail-safe modules

ET 200SP modules with integrated safety functions that can be used for safety-related operation (safety mode).

Fail-safe systems

Fail-safe systems (F-systems) remain in a safe state or immediately assume another safe state as soon as particular failures occur.

Fault response time

The maximum fault response time of an F-system defines the interval between the occurrence of any fault and a safe reaction at all affected fail-safe outputs.

For → F-systems overall: The maximum fault response time defines the interval between the occurrence of any fault at any → F-I/O and the safe reaction at the corresponding fail-safe output.

For digital inputs: The maximum fault response time defines the interval between the occurrence of the fault and the safe reaction at the backplane bus.

For digital outputs: The maximum fault response time defines the interval between the occurrence of the fault and the safe reaction at the digital output.

Fault tolerance time

The fault tolerance time of a process is the time a process can be left unattended without risk to life and limb of the operating personnel, or damage to the environment.

Any type of F-system control is tolerated within this fault tolerance time, i.e. the → F-system can control its processes incorrectly or even not at all. The fault tolerance time depends on the type of process and must be determined on a case-by-case basis.

F-CPU

An F-CPU is a central processing unit with fail-safe capability that is permitted for use in SIMATIC Safety. A standard user program can also be run on the F-CPU.

F-I/O

Collective name for fail-safe inputs and outputs available in SIMATIC S7 for integration into the SIMATIC Safety F-system. Available F-I/O modules:

- Fail-safe I/O module for ET 200eco
- Fail-safe signal modules S7-300 (F-SMs)
- Fail-safe modules for ET 200S
- Fail-safe modules for ET 200SP
- Fail-safe DP standard slaves
- Fail-safe PA field devices
- Fail-safe IO devices

F-monitoring time

→ PROFIsafe monitoring time

F-Systems

→ fail-safe systems

Module fault

Module faults can be external faults (e.g. missing load voltage) or internal faults (e.g. processor failure). Internal faults always require module replacement.

Monitoring time

→ PROFIsafe monitoring time

M-switch

Each fail-safe digital output of ET 200SP F-modules consists of a P-switch DO-P_x (current sourcing) and an M-switch DO-M_x (current sinking). The load is connected between the P-switch and M-switch. The two switches are always activated so that voltage is applied to the load.

Nonequivalent sensor

A nonequivalent → sensor is a two-way switch that is connected to two inputs of an → F-I/O (via 2 channels) in → fail-safe systems (for → 1oo2 evaluation of sensor signals).

Passivation

If an → F-I/O module detects a fault it switches either the affected channel or all channels to a → safe state, i.e. the channels of this F-I/O module are passivated. The F-I/O module signals the detected faults to the → F-CPU.

When passivating channels at F-I/O with inputs, the → F-System provides fail-safe values for the → safety program instead of the process values pending at the fail-safe inputs.

When passivating channels at F-I/O with outputs, the F-system returns fail-safe values (0) to the fail-safe outputs instead of the output values provided by the safety program.

Performance Level

Performance Level (PL) according to ISO 13849-1:2006 or EN ISO 13849-1:2008

PROFIsafe

Safety-oriented PROFINET I/O bus profile for communication between the → safety program and the → F-I/O module in a → fail-safe system.

PROFIsafe address

Every → fail-safe module has a PROFIsafe address. You have to configure the PROFIsafe address.

PROFIsafe monitoring time

Monitoring time for safety-related communication between the F-CPU and F-I/O

Proof-test interval

Period after which a component must be forced to fail-safe state, that is, it is either replaced with an unused component, or is proven faultless.

P-switch

→ M-switch

Redundancy, availability-enhancing

Multiple instances of components with the objective of maintaining component functionality in the event of hardware faults.

Redundancy, safety-enhancing

Multiple availability of components with the aim of exposing hardware faults based on comparison; such as → 1oo2 evaluation in → fail-safe modules.

Reintegration

After the elimination of a fault, it is necessary to ensure the reintegration (depassivation) of the → F-I/O. Reintegration (switchover from fail-safe values to process values) occurs either automatically or only after a user acknowledgment in the safety program.

In the case of a fail-safe input module, the process values pending at the fail-safe inputs are made available to thesafety program again after reintegration. In the case of a fail-safe output module, the → fail-safe system transfers the output values in the safety program to the fail-safe outputs again.

Safe state

The basic principle of the safety concept in F-systems is the existence of a safe state for all process variables. For the digital F-I/O, for example, the safe state is the value "0".

Safety class

Safety level (Safety Integrity Level) SIL according to IEC 61508:2010. The higher the Safety Integrity Level, the more rigid the measures for prevention of systematic faults and for management of systematic faults and hardware failures.

The fail-safe modules support operation in safety mode up to safety class SIL3.

Safety function

A mechanism integrated in the → F-CPU and → F-I/O that enables their use in → the fail-safe system SIMATIC Safety.

According to IEC 61508:2010 A safety function is implemented by a safety system in order to maintain or force a system safe state in the event of a specific fault.

Safety message frame

In safety mode, data are transferred between the → F-CPU and → F-I/O in a safety message frame.

Safety mode

Operating mode of → F-I/O that enables → safety-related communication via → safety message frames.

→ ET 200SP fail-safe modules can only used in safety mode.

Safety program

Safety-related user program

Safety-related communication

Communication used to exchange fail-safe data.

Sensor evaluation

There are two types of sensor evaluation:

→ 1oo1 evaluation – sensor signal is read once

→ 1oo2 evaluation – sensor signal is read in twice by the same F-module and compared internally

Sensors

Sensors are used for accurate detection of digital and analog signals as well as routes, positions, velocities, rotational speeds, masses, etc.

SIL

Safety Integrated Level → safety class

Standard mode

Operating mode of F-I/O in which standard communication is possible by means of → safety message frames, but not → safety-related communication.

Fail-safe ET 200SP modules can only be operated in safety mode.

Value status

The value status is the binary additional information of a digital signal. The value status is entered in the process image of the input and provides information on the validity of the signal.