SIEMENS

SIMATIC

S7
S7-1200 Functional Safety Manual

Manual

02/2015

A5E03470344-AA

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E03470344-AA
Ⓟ 04/2015 Subject to change

Preface

Purpose of the manual

The S7-1200 series is a line of programmable logic controllers (PLCs) that can control a variety of automation applications. Compact design, low cost, and a powerful instruction set make the S7-1200 a perfect solution for controlling a wide variety of applications. The S7-1200 models and Windows-based programming tools give you the flexibility you need to solve your automation problems.

This manual provides information about using, installing, and programming the S7-1200 Fail-Safe PLCs and is designed for engineers, programmers, installers, and electricians who have a general knowledge of programmable logic controllers.

Required basic knowledge

To understand this manual, it is necessary to have a general knowledge of automation and programmable logic controllers.

Scope of the manual

This manual describes or references the following products:

- STEP 7 Basic V13 SP1 or later with:
  - STEP 7 Safety Basic V13 SP1 or later
  - STEP 7 Safety Advanced V13 SP1 or later
- STEP 7 Professional V13 SP1 or later with:
  - STEP 7 Safety Advanced V13 SP1 or later
- S7-1200 fail-safe CPU firmware release V4.1 or later
- S7-1200 fail-safe signal modules (SM) firmware release V2.0 or later

For a complete list of the S7-1200 products described in this manual, refer to the technical specifications article numbers for fail-safe CPUs (Page 193) and fail-safe SMs (Page 193).

> **WARNING**
>
> **The "SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual" in the current version is the authoritative source for Functional Safety-related information concerning configuring and programming.**
>
> Siemens identifies the "SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual" (http://support.automation.siemens.com/WW/view/en/54110126/0/en) as the authoritative and/or original source in the case of discrepancies between the manuals.
>
> All warnings in the "SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual" have to be observed.

Certification, CE label, C-Tick, and other standards

Refer to the technical specifications (Page 144) for more information.

Glossary

The definitions in the glossary are provided to give the reader an easy first reference for understanding the terms as used in this manual. Some terms have detailed formal definitions in IEC 61508, ISO EN 13849, IEC 61784-3-3, and associated standards, and must be understood in terms of broad safety concepts detailed in these standards.

Another reference for more exact definitions is the "SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual" (http://support.automation.siemens.com/WW/view/en/54110126/0/en).

Service and support

In addition to our documentation, we offer our technical expertise on the Internet on the customer support web site (http://www.siemens.com/automation/).

Contact your Siemens distributor or sales office for assistance in answering any technical questions, for training, or for ordering S7 products. Because your sales representatives are technically trained and have specific knowledge about your operations, processes, and industry, as well as the individual Siemens products that you are using, they can provide the fastest and most efficient answers to any problems you might encounter.

Documentation and information

S7-1200 and STEP 7 provide a variety of documentation and other resources for finding the technical information that you require.

- The *S7-1200 Functional Safety Manual* presents an overview of the Siemens Safety software and fail-safe CPUs and SMs and a Getting Started configuration and programming example. However, the focus of the manual is the S7-1200 fail-safe SMs. SM installation, configuration, diagnostics, applications, and technical specifications are emphasized.

  The English version of the *S7-1200 Functional Safety Manual* is the authoritative (original) language for Functional Safety-related information. All translated manuals refer back to the English manual as the authoritative and/or original source. Siemens identifies the English manual as the authoritative and/or original source in the case of discrepancies between the translated manuals.
- The *Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual* provides information that enables you to configure and program SIMATIC Safety fail-safe systems. In addition, you will obtain information on acceptance testing of a SIMATIC Safety fail-safe system. Before configuring and programming an actual live fail-safe operation, it is essential that you refer to this manual.
- The *S7-1200 Programmable Controller System Manual* provides specific information about the operation, programming, and the specifications for the complete S7-1200 product family. In addition to the system manual, the *S7-1200 Easy Book* provides a more general overview to the capabilities of the S7-1200 family.
- The *S7-1200 Functional Safety Manual; SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual; S7-1200 Programmable Controller System Manual*, and the *S7-1200 Easy Book* are available as electronic (PDF) manuals. The electronic manuals can be downloaded from the customer support web site and can also be found on the companion disk that ships with every S7-1200 CPU.
- The TIA portal STEP 7 online help information system provides immediate access to the conceptual information, specific instructions, and error code event IDs that describe the operation and functionality of the programming package and basic operation of SIMATIC CPUs.
- My Documentation Manager accesses the electronic (PDF) versions of the SIMATIC documentation set, including the system manual, the Easy Book, and the information system of STEP 7. With My Documentation Manager, you can drag and drop topics from various documents to create your own custom manual.

  The customer support entry portal (http://support.automation.siemens.com) provides a link to My Documentation Manager under mySupport.
- Siemens also provides online comprehensive support for your use of safety technology. A Safety Evaluation Tool assists you in determining required safety levels, Functional Examples guide you in your safety applications, and SITRAIN classes offer training in safety standards and products. Visit the following web sites to access these support activities:
  - Safety Evaluation Tool (http://www.siemens.com/safety-evaluation-tool)
  - Functional examples (http://www.siemens.com/safety-functional-examples)
  - SITRAIN (http://www.siemens.com/sitrain-safetyintegrated)

- The customer support web site also provides podcasts, FAQs, and other helpful documents for S7-1200 and STEP 7. The podcasts utilize short educational video presentations that focus on specific features or scenarios in order to demonstrate the interactions, convenience and efficiency provided by STEP 7. Visit the following web sites to access the collection of podcasts:
  - STEP 7 Basic web page (http://www.automation.siemens.com/mcms/simatic-controller-software/en/step7/step7-basic/Pages/Default.aspx)
  - STEP 7 Professional web page (http://www.automation.siemens.com/mcms/simatic-controller-software/en/step7/step7-professional/Pages/Default.aspx)
- You can also follow or join product discussions on the Service & Support technical forum (https://www.automation.siemens.com/WW/forum/guests/Conferences.aspx?Language=en&siteid=csius&treeLang=en&groupid=4000002&extranet=standard&viewreg=WW&nodeid0=34612486). These forums allow you to interact with various product experts.
  - Forum for S7-1200 (https://www.automation.siemens.com/WW/forum/guests/Conference.aspx?SortField=LastPostDate&SortOrder=Descending&ForumID=258&Language=en&onlyInternet=False)
  - Forum for STEP 7 Basic and Professional (https://www.automation.siemens.com/WW/forum/guests/Conference.aspx?SortField=LastPostDate&SortOrder=Descending&ForumID=265&Language=en&onlyInternet=False)

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).

Table of contents

Product overview 1

1.1 Overview

SIMATIC Safety fail-safe system

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. The SIMATIC Safety fail-safe system is available to implement safety concepts in the area of machine and personnel protection (for example, for emergency STOP devices for machining and processing equipment).

What are fail-safe automation systems?

Fail-safe automation systems control processes that can achieve a safe state immediately as a result of an unexpected operation or failure. These are fail-safe control processes where an immediate shutdown to safe state 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. You use fail-safe systems in applications with advanced safety requirements. You can resume production quickly following a safety-related interruption, using the improved fault detection and localization provided in fail-safe systems through detailed diagnostic information.

Achievable safety requirements

SIMATIC Safety fail-safe systems can satisfy the following safety requirements:

- Safety class (Safety Integrity Level) SIL 1 to SIL 3 in accordance with IEC 61508:2010
- Category 2 to 4, Performance Level (PL) a to e in accordance with EN ISO 13849-1:2008/AC:2009 (ISO 13849-1:2006)

Principles of safety functions in SIMATIC Safety

You implement functional safety using the hardware and firmware of the fail-safe CPUs and signal modules (SM) in conjunction with the safety program downloaded by the software (ES). The SIMATIC Safety system executes the safety function to bring the system to a safe state or maintain a safe state in case of a dangerous event.

The fail-safe SMs ensure the safe processing of field information (for example, sensors for emergency OFF pushbuttons and light barriers and actuators for motor control). The fail-safe SMs have the required hardware and software components for safe processing, in accordance with the required Safety Integrity Level (SIL).

You provide the safety function for the process through the application program that you create or by the reaction of the fail-safe system to a fault. In the event of an error, if the fail-safe system can no longer execute its actual user safety function, it executes the fault reaction function (for example, the fail-safe system shuts down the associated outputs).

Example of user safety function

If an object interrupts the beam of a light curtain, the fail-safe system stops the motion in the area protected by the light curtain (user safety function):

- The light curtain provides a "1" signal, perhaps redundantly, to say the light beam is not broken or "0" to say the light beam is broken.
- The fail-safe digital input signal module (SM) acquires the signal from the light curtain and provides the state to the fail-safe CPU through a safe communication protocol. Redundant processors with mutual diagnostics in the fail-safe digital input SM provide a high assurance that a "1" is provided only when correct and faults result in a "0" being provided.
- The fail-safe CPU executes your user program for normal control of the motion and includes your programmed safety logic that says a "1" from the light curtain is required to enable the motion. Your programmed safety logic is encoded by the Engineering System in redundant logic steps that gives a high assurance that any fault in CPU execution results in an identified discrepancy and an output of "0". If the CPU fails to receive verifiable communication from the fail-safe digital input SM in a required time, the fail-safe CPU replaces the signal from the fail-safe digital input SM with "0".
- The fail-safe CPU delivers the results of the safety logic to the fail-safe digital output SM through the safe communication protocol. A "1" signal from your safety logic enables motion by turning an output channel ON, or a "0" turns the output channel OFF. Redundant processors with mutual diagnostics in the fail-safe digital output SM provide a high assurance that redundant output switches (series relay contacts or P/M 24VDC solid state switches) are turned ON only when this is correct and at least one output switch turns OFF if a fault occurs. If the fail-safe digital output SM fails to receive verifiable communication from the fail-safe CPU in a required time, the fail-safe digital output SM replaces the signal from the fail-safe CPU with "0" and turns outputs OFF.

1.2 Hardware and software components

S7-1200 Fail-Safe CPUs and SMs

There are four fail-safe CPUs and three fail-safe signal modules (SM) in conjunction with the S7-1200 V4.1 or later release:

- CPU 1214FC DC/DC/DC
- CPU 1214FC DC/DC/RLY
- CPU 1215FC DC/DC/DC
- CPU 1215FC DC/DC/RLY
- SM 1226 F-DI 16 x 24 VDC
- SM 1226 F-DQ 4 x 24 VDC
- SM 1226 F-DQ 2 x Relay

An S7-1200 fail-safe system requires a fail-safe CPU and fail-safe SMs. The integrated I/O on the CPU is not fail-safe, but can be used to complete other control functions.

The S7-1200 standard signal modules (SM), communication modules (CM), and signal boards (SB) can be used in the same system with fail-safe SMs to complete your application control functions that do not require a rated Safety Integrity Level (SIL). Standard SMs that are supported for use with fail-safe SMs have the article numbers (6ES7 --- ---32 0XB0) or later.

The S7-1200 fail-safe CPUs do not support PROFIBUS or PROFINET distributed fail-safe I/O.

Required software components

You require one of the following software combinations:

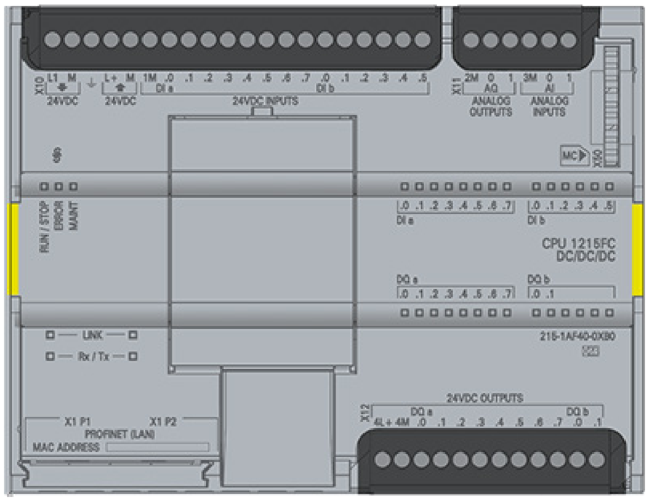
- STEP 7 Basic V13 SP1 or later with STEP 7 Safety Basic V13 SP1 or later
- STEP 7 Professional V13 SP1 or later with STEP 7 Safety Advanced V13 SP1 or later

STEP 7 Safety Advanced V13 SP1 or later and STEP 7 Safety Basic V13 SP1 or later are the configuration and programming software packages for the SIMATIC Safety fail-safe system. In both software packages, you receive the following:

- Support for configuring the fail-safe CPUs and SMs in the hardware and network editor of the TIA portal
- Support for creating the safety program using LAD and FBD and integrating error detection functions into the safety program
- Instructions for programming your safety program in LAD and FBD, which you are familiar with from the standard user programs
- Instructions for programming your safety program in LAD and FBD with special safety functions

1.3 S7-1200 Fail-Safe CPUs

The fail-safe CPU executes your safety program along with standard applications programs. Communication between the fail-safe CPU and the fail-safe signal modules is verified using the PROFIsafe protocol.



Safety program

You can create a safety program using the program editor. You can program fail-safe function blocks (FB) and functions (FC) in the Function Block Diagram (FBD) or Ladder Logic (LAD) programming languages and create fail-safe data blocks (DB).

The fail-safe system performs a dual execution using coded processing. The fail-safe system automatically performs safety checks and inserts additional fail-safe logic for error detection and error response when the safety program compilation occurs. This ensures the detection of failures and faults and appropriate execution of reactions to maintain the fail-safe system in the safe state or bring it to a safe state.

In addition to the safety program, you can run a standard user program on the fail-safe CPU. A standard program can coexist with a safety program in a fail-safe CPU. The fail-safe CPU protects the safety-related data of the safety program from the unintentional effects of the data of the standard user program.

WARNING

You cannot put an S7-1200 Fail-Safe system that provides safety-related functions into operation after installation or modification until after you successfully commission the safety-related functionality.

Death or serious personal injury and damage to machines and equipment may result if proper precautions are not taken.

An S7-1200 Fail-Safe system that provides both safety-related functions and standard (non safety-related) functions must not be put into operation in order to use the standard functions before you successfully commission the safety-related functions, even if all fail-safe signal modules go to the error state and thus remain safe.

You can exchange data between the safety program and the standard user program in the fail-safe CPU by means of bit memory or data of a standard DB.

1.3.1 Behavior differences between standard and fail-safe CPUs

1.3.1.1 Safety mode

Safety mode

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

- Safety program of the fail-safe CPU
- Fail-safe signal modules (SM)

Safety mode of safety program

The safety program runs in the fail-safe CPU in safety mode. The safety program activates all safety mechanisms for fault detection and fault reaction. You cannot modify the safety program during operation in safety mode.

You can deactivate and reactivate the safety mode of the safety program. "Deactivated safety mode" enables the safety program for online tests and changes as needed while the fail-safe CPU is in RUN mode.

For SIMATIC Safety, you can switch back to safety mode only after an operating mode change of the fail-safe CPU from RUN to STOP to RUN.

Safety message frame

In safety mode, the fail-safe CPU and fail-safe SMs consistently transmit data between them in a safety message frame. The safety message frame in accordance with PROFIsafe standards consists of the following:

- Process data (user data)
- Status byte/control byte (coordination data for safety mode)
- Virtual Monitoring Number (encoded in CRC signature, provides keep-alive mechanism and detection of out-of-sequence messages)
- CRC signature

1.3.1.2 Fault reactions

Safe state

The fail-safe concept depends on the identification of a safe state for all process variables. The value "0" (de-energized) represents this safe state for digital fail-safe signal modules (SM). This applies to both sensors and actuators.

Passivation

Passivation applies safe state values to the fail-safe SM or channel(s) instead of process values when the fail-safe system detects faults. The safety function requires passivation of the fail-safe SM or channel(s) in the following situations:

- When the fail-safe system starts up
- If the fail-safe system detects overall module faults, such as RAM or Processor failures
- If the fail-safe system detects errors during safety-related communication between the fail-safe CPU and the fail-safe SM through the PROFIsafe safety protocol (communication error)
- If fail-safe channel faults occur (for example, short-circuit and discrepancy errors or internal faults of fail-safe input or output channels)

When passivation occurs in a digital input fail-safe SM, SIMATIC Safety provides the safety program with safe state values (0) instead of the process data pending at the fail-safe inputs in the input process image.

When passivation occurs in a digital output fail-safe SM, the SM sets the passivated channel(s) to a value of (0).

Reintegration

Reintegration returns the process from passivation to a normal state after successful diagnostics determine that the fault has cleared. After reintegration of a fail-safe digital input, SIMATIC Safety again provides the process data pending at the inputs to the safety program. For a fail-safe digital output , SIMATIC Safety again transfers the output values provided by the safety program to the fail-safe outputs. Reintegration from safe state values to process data can be automatic or require acknowledgement by your safety program. See "Reactions to faults" (Page 115) for steps to reintegrate.

Detection and response to faults

SIMATIC Safety systems detect and respond to faults in several different conditions:

- Faults in the fail-safe CPU hardware and firmware
- Faults in the fail-safe user program
- PROFIsafe communication errors caused by conditions in either the fail-safe CPU or SMs
- Fail-safe SM-wide errors such as microprocessor errors or memory errors
- Fail-safe SM channel errors such as discrepancy errors, wiring shorts, or internal channel faults

Fail-safe CPU faults and fail-safe user program faults often result in the CPU operating mode being set to STOP. You can reintegrate PROFIsafe communication faults once communication is successfully restored. In most cases, you cannot reintegrate SM-wide faults because these faults require the fail-safe SM to be power-cycled. You can often reintegrate and return channel faults to proper operation by removing the fault and reintegrating the channel.

Virtual monitoring number, cyclic interrupt time, and F-monitoring time

The following parameters are integral to fault reactions:

- Virtual monitoring number: The PROFIsafe protocol provides time monitoring and detection of message sequence errors by means of a periodically-updated monitoring number.
- Cyclic interrrupt time: The cyclic interrupt time is the interval by which the F-runtime group executes and determines how often the fail-safe CPU sends the PROFIsafe frame to the fail-safe SMs. When you add a fail-safe CPU to your project, STEP 7 creates Functional Safety Organization Block 1 (FOB_1) (OB123 by default). FOB_1 contains the cyclic time interrupt time, and you can configure the cyclic interrupt time (100ms by default).
- F-monitoring time: The F-monitoring time is the amount of time an SM or CPU waits for an error-free communication including a new Virtual Monitoring Number before passivating channels. You can configure the F-monitoring time. The fail-safe CPU and SMs must receive a valid, current safety message frame with a valid monitoring number within the configured F-monitoring time.

If the fail-safe system fails to detect a valid monitoring number within the F-monitoring time, the fail-safe system passivates the fail-safe SM. Expiration of an SM's F-monitoring time causes a transition to safe state for all F-inputs or F-outputs of the SM.

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 fail-safe CPU and fail-safe SMs, the fail-safe system passivates the fail-safe SMs.

1.3.1.3 Restart of fail-safe system

The operating modes of the SIMATIC Safety system differ from those of the standard system only in terms of the restart characteristics.

Restart characteristics

When you switch a fail-safe CPU from STOP to RUN mode, the standard user program restarts in the usual way. When you restart the safety program, the fail-safe system initializes all data blocks with the F-Attribute with values from load memory. This is comparable to a cold restart.

The fail-safe system attempts to reintegrate each fail-safe SM at restart. In contrast to the standard user program, you cannot use startup OBs in the safety program.

1.3.1.4 Firmware update

Note

Fail-safe SM firmware (FW) updates

If 24 VDC power to the fail-safe SM is interrupted during the FW update, then the FW update must be started again with a memory card.

You cannot complete re-started FW updates from a web server or the TIA Portal.

Refer to the S7-1200 Programmable Controller System Manual (http://support.automation.siemens.com/WW/view/en/91696622) for firmware update procedures.

1.4 S7-1200 Fail-Safe signal modules (SM)

1.4.1 Overview

Siemens intends for the S7-1200 fail-safe products to be used to help solve functional safety in machine applications.

There are three fail-safe SMs in conjunction with the S7-1200 V4.1 or later release:

- SM 1226 F-DI 16 x 24 VDC
- SM 1226 F-DQ 4 x 24 VDC
- SM 1226 F-DQ 2 x Relay

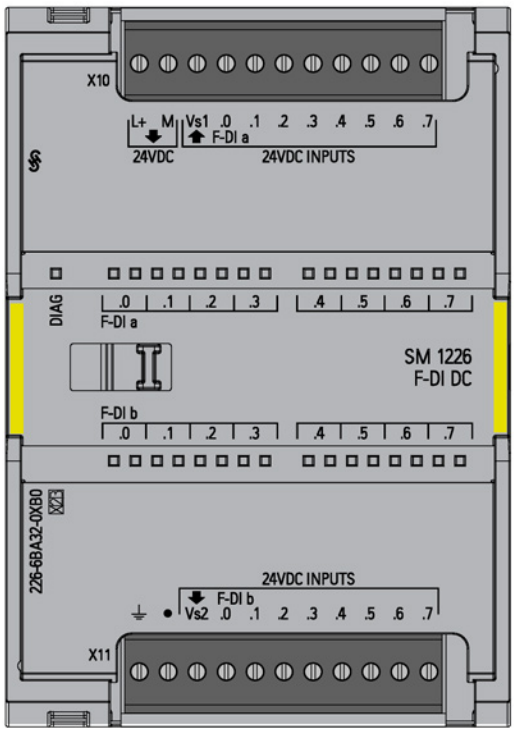
Redundant two-processor functional safety design

The major difference between S7-1200 fail-safe and standard SMs is that failsafe SMs use redundancy to achieve functional safety, including two processors that control fail-safe operation. Both processors monitor each other and verify that they are executing the same code at the same time, automatically test the I/O circuits, and set the fail-safe SMs to safe state in the event of a fault. Each processor monitors internal and external power supplies and module internal temperature and can passivate the module if an abnormal condition is detected.

Safety-related input and output signals form the interface to the process. This enables direct connection of single-channel and two-channel input signals from devices such as emergency STOP buttons or light barriers. The fail-safe SM redundantly combines the safety-related signals internally and passes the unified result on to the CPU in a fail-safe manner for further processing.

The fail-safe CPU sends the safety-related outputs from the CPU to the fail-safe SM for each individual output channel. Each output then sets two independent switches for each channel, a P and M solid-state switch, or two independent relays.

1.4.2 SM 1226 F-DI 16 x 24 VDC



The SM 1226 F-DI 16 x 24 VDC is an S7-1200 signal module (SM) for use in fail-safe applications. The inputs are rated for connection to 24V DC sensors/switches and 3/4-wire proximity switches (for example, BEROs: Siemens line of no-touch sensors) and have an EN61131-2 type 1 input rating.

The module has two sensor supply outputs that can each power eight external sensors (inputs).

Inputs and test circuit

The F-DI consists of 16 input channels (F-DI a.0..a.7, F-DI b.0...b.7). You can configure these inputs as sixteen one-out-of-one (1oo1) inputs (SIL 2/Category 3/PL d), eight one-out-of-two (1oo2) inputs (SIL 3/Category 3 or Category 4/PL e), or combinations of 1oo1 and 1oo2 channels. One microcomputer monitors inputs a.0 to a.7, and the other microcomputer monitors inputs b.0 to b.7. The corresponding channels from a and b (a.0, b.0), (a.1, b.1)...(a.7,b.7) form a 1oo2 channel group . The "a" input, the first of the two inputs, conveys the signal in a 1oo2 configuration. For example, if you wire I8.0 and I9.0 in a 1oo2 configuration and configure STEP 7 to use 1oo2 sensor evaluation, the signal appears at only the I8.0 input when you close or open the circuit for both.

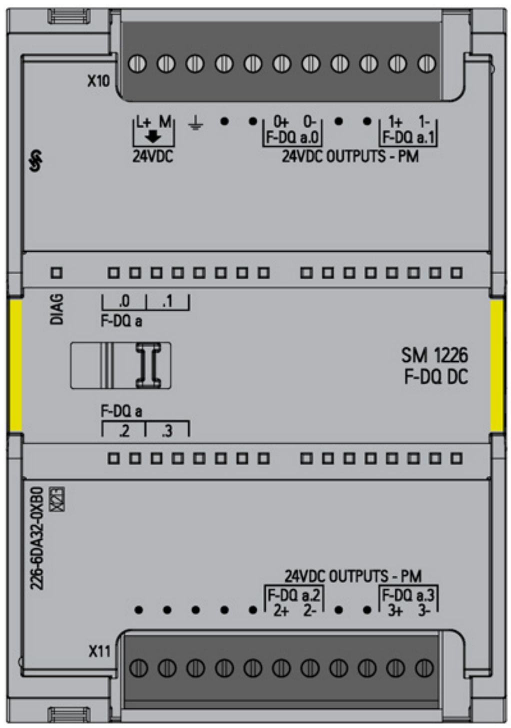
When you configure a channel group as 1oo2, the two controllers must sense the same input change within a configured time. Otherwise, the two controllers detect a discrepancy error. The F-DI reports the 1oo2 input back to the fail-safe CPU as a single input.

If you use a sensor supply output to provide power to a sensor, you can enable short-circuit testing. The short-circuit test checks for shorts to plus voltage by periodically pulsing the sensor output off and verifying that the associated input is off. This short-circuit test also checks for shorts to the other circuit in a 1oo2 paired input because the test pulses the two sensor outputs off at different times. The short-circuit test does not detect shorts between inputs in the same sensor group.

The processors cooperate in providing internal test pulses to each others process input circuits, after the initial field interface, to verify that sensing electronics are responsive to "1" and "0" inputs.

You can achieve Category 4 in 1oo2 configurations if you diagnose external wiring faults or exclude them according to standards.

1.4.3 SM 1226 F-DQ 4 x 24 VDC



The SM 1226 F-DQ 4 x 24 VDC is an S7-1200 signal module (SM) for use in fail-safe applications and is suitable for solenoid valves, DC contactors, and indicator LEDs. It has four outputs with P- and M-switching that are rated for connection to 24 VDC actuators with up to a 2.0 A rating.

Outputs

The F-DQ DC consists of four output channels (F-DQ a.0...F-DQ a.3). You can use each output for SIL 3 applications. Each output consists of two switches:

- A P-switch connects 24V positive (L+) to the load.
- An M-switch connects the load to M or 24V return.

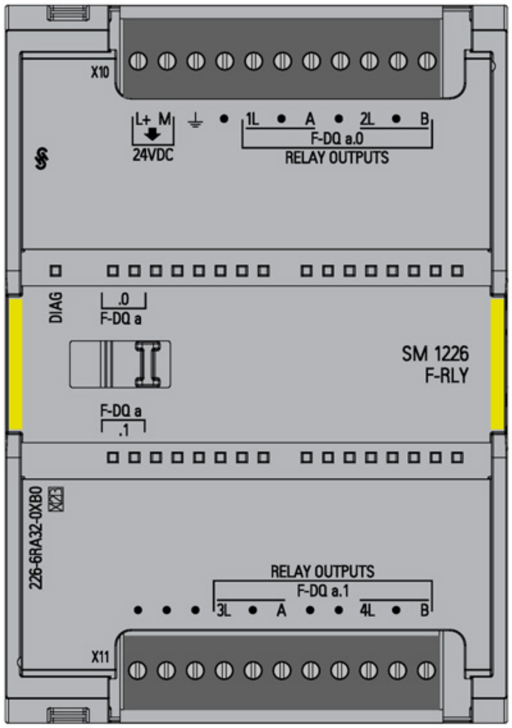
Both switches must be turned ON for current to flow to the load.

The F-DQ DC uses two microcomputers to implement the safety function. One microcomputer controls the P-switch while the other microcomputer controls the M-switch. There is feedback from the P-switch output to the other microcomputer that is controlling the M-switch. Likewise, there is feedback from the M-switch output to the other microcomputer that is controlling the P-switch. The feedback verifies that the output switches are operating properly and in the commanded state.

You must configure a "Maximum readback time" that specifies the allowed delay for the output voltage to respond to the switch change.

The F-DQ DC regularly tests each "OFF" switch "ON" briefly, and each "ON" switch "OFF" briefly, to verify that each switch is still functional and under independent control. Your configured "Maximum readback time" also sets the duration of the "OFF" test pulse. You must configure a "Maximum readback time switch on test" which sets the duration of the "ON" test pulse. You should choose these durations short enough to not affect your load.

1.4.4 SM 1226 F-DQ 2 x Relay

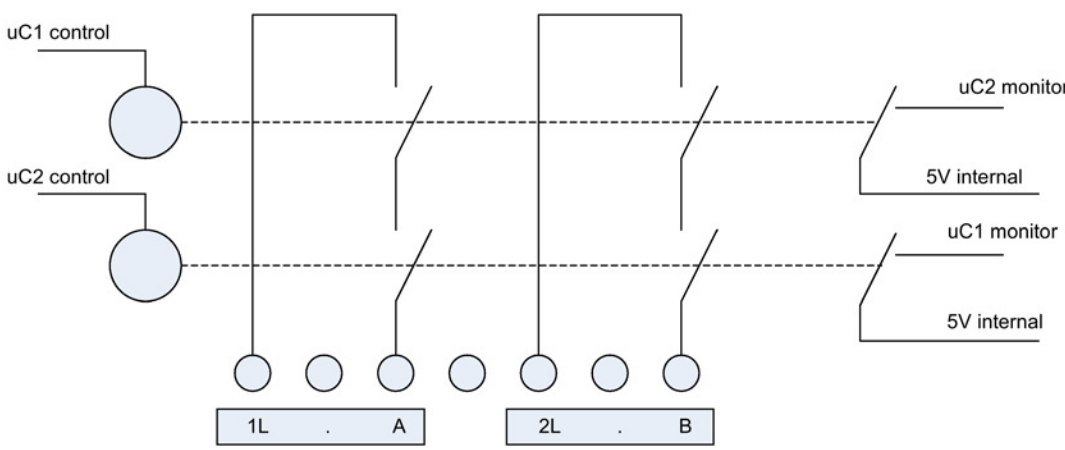


The SM 1226 F-DQ 2 x Relay is an S7-1200 signal module (SM) for use in fail-safe applications. The F-RLY has two output channels (F-DQ a.0 and F-DQ a.1). Each channel includes two circuits that switch mechanically-linked contacts at the same time. Each circuit has two contacts in series controlled by independent relay coils.

Each circuit can directly control an actuator in SIL 3 applications. You can use the two circuits together to control redundant contactors or relays for SIL 3 applications with interposing relays.

The F-RLY uses two microcomputers to implement the safety function. Different microcomputers control the two series relay contacts in each circuit. Control of each relay coil by one microcomputer is verified by the other microcomputer monitoring the mechanically-linked sense contact.

The series contacts in each circuit are switched in sequence to avoid common mode failure by the welding of both contacts.



Output channel a.0: Two circuits controlled as one process output channel.

Refer to the isolation description in the SM 1226 F-DQ 2 x Relay (Page 185) Specifications, Digital outputs table.

Outputs

You can use each of the two relay output channels for SIL 3 applications.

Note

Relay contacts of the SM 1226 F-DQ 2 x Relay are designed to Overvoltage Category III. You can use them in AC mains circuits without further overvoltage protection.

Relay contact outputs on the following products do not meet requirements for Overvoltage Category III, the requirement for EN 50156-1 conforming equipment:

- CPU 1214FC DC/DC/RLY CPU (6ES7 214-1HF40-0XB0)
- CPU 1215FC DC/DC/RLY CPU (6ES7 215-1HF40-0XB0)
- SM 1222 DQ 8 x Relay (6ES7 222-1HF32-0XB0)
- SM 1222 DQ 16 x Relay (6ES7 222-1HH32-0XB0)
- SM 1223 DI 8 x 120/230 VAC In / DQ 8 x Relay (6ES7 223 1QH32 0XB0)

When using the SM 1226 F-DQ 2 x Relay in safety critical circuits of burner applications, you can use the relays on any of the products listed above, but only if used in one of the following:

- SELV/PELV circuits
- Circuits connected to the electrical mains with permanent, recognized protection that reduces transients to Overvoltage Category II

Otherwise, the CPU and I/O system, including the SM 1226 F-DQ 2 x Relay, will not meet the Overvoltage Category III requirement for burner applications.

WARNING

Adjacent relay contacts in the same channel of the SM 1226 F DQ 2 x Relay are not rated to separate AC line from SELV / PELV.

Death or serious personal injury and damage to machines and equipment can result if SELV/PELV circuits are wired adjacent to high voltage circuits on this module.

The A and B circuits of each output must either be both AC line or both SELV.

Getting started 2

2.1 Introduction to example

2.1.1 Instructive, interactive animation files

The "Getting Started" chapter contains two animation files:

- "Procedure" (Page 28) shows a wiring overview of the S7-1200 Fail-Safe application example.
- "Step 13: Downloading the complete safety program to the fail-safe CPU and activating safety mode" (Page 61) shows the end result of the LAD programming ste

Nine animation videos take you step-by-step through many of the configuring and programming tasks. These animation videos show the completed task at the beginning of the video, with a fadeout to a step-by-step tutorial that demonstrates all of the required sub-tasks. You can find animation videos at the following locations:

- "Step 1: Configuring the S7-1200 CPU 1214FC or CPU 1215FC" (Page 31)
- "Step 6: Creating an F-FB" (Page 51)
- "Step 7: Programming the safety door function" (Page 52)
- "Step 8: Programming the emergency stop function" (Page 54)
- "Step 9: Programming the feedback monitoring" (Page 56)
- "Step 10: Programming the user acknowledgment for reintegration of the fail-safe SM" (Page 58)
- "Step 11: Programming of the main safety block" (Page 59)
- "Step 12: Compiling the safety program" (Page 60)
- "Step 13: Downloading the complete safety program to the fail-safe CPU and activating safety mode" (Page 61)

2.1.2 Requirements for configuring and programming

These instructions will guide you step-by-step through a specific example for configuring and programming with STEP 7 Safety V13 SP1 or later.

You will become acquainted with the basic functions and special features of STEP 7 Safety V13 SP1 or later.

It should take one or two hours to work through this example, depending on your experience.

Requirements for the example

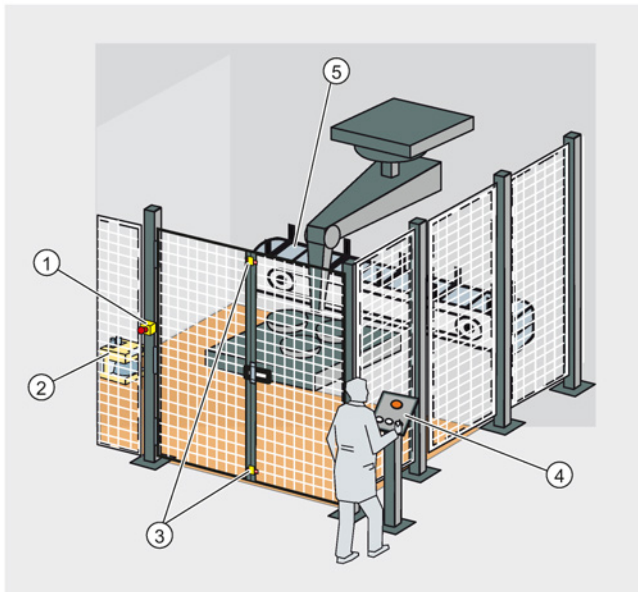
The following requirements must be met:

- You must have "Adobe Reader Version 9" or higher and "Adobe Flash Player 11 Active X" software loaded on your computer in order to operate the multi-media content.
- In order to understand these Getting Started instructions, you need general knowledge of automation technology. You also need to be familiar with STEP 7 V13 SP1 or later and STEP 7 Safety V13 SP1 or later.
- You need an S7-1200 station consisting of the following components:
  - Fail-safe CPU (CPU 1214FC or CPU 1215FC)
  - Fail-safe digital input signal module: SM 1226 F-DI 16 x 24 VDC
  - Fail-safe digital output signal module: SM 1226 F-DQ 4 x 24 VDC
- STEP 7 V13 SP1 or later and STEP 7 Safety V13 SP1 or later must be correctly installed on your Windows-based programming device with an Ethernet interface.
- The programming device must be connected to the fail-safe CPU through the PROFINET interface.
- The CPU 1214FC or CPU 1215FC and other hardware must be fully installed and wired. Instructions for this can be found in the "S7-1200 Programmable Controller System Manual" (http://support.automation.siemens.com/WW/view/en/91696622).

> **WARNING**
>
> **As a component in plants and systems, the S7-1200 is subject to specific standards and regulations depending on the area of application. Please note the applicable safety and accident prevention regulations (for example, IEC 60204-1 (General Requirements for Safety of Machinery)).**
>
> The example in these Getting Started instructions serves as an introduction to configuring and programming of STEP 7 Safety Advanced V13 SP1 or later. It does not lead to actual live operation in every case. Before you do this, it is essential that you refer to the current version of the "SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual" (http://support.automation.siemens.com/WW/view/en/54110126/0/en). The warnings and other notes contained in that manual must be heeded at all times even if they are not repeated in this document!
>
> Serious injury and damage to machines and equipment may result if these regulations are ignored.

2.1.3 Example structure and task definition

Production cell with access protection



① Emergency stop (E-STOP)
② Laser scanner
③ Safety door
④ Control panel with start and acknowledgement pushbuttons
⑤ Conveyor motor

A laser scanner monitors the entry to the production area. A safety door secures the service area.

Entering the production area or opening the safety door results in a stop or shutdown of the production cell similar to an emergency stop.

The system can only be restarted when the emergency stop is cancelled, the safety door is closed, and the laser scanner detects no one in the protected area. The user must acknowledge that conditions have returned to a safe state before production can be restarted.

2.1.4 Procedure

The example in these Getting Started instructions consists of the following sections:

Configuring

For this example, you must configure the following S7-1200 fail-safe CPUs and SMs:

- Fail-safe CPU (CPU 1214FC or CPU 1215FC)
- Fail-safe CPU standard digital inputs for user acknowledgement, feedback loop, and start pushbutton
- SM 1226 F-DI 16 x 24 VDC for connecting an emergency stop switch, the position switches for monitoring a safety door, and the laser scanner for monitoring the entry area
- SM 1226 F-DQ 4 x 24 VDC for connecting a motor

The configuration is described in the "Configuring" (Page 30) section.

Programming

Once the configuration is successfully completed, you can program your safety program.

In our example, a fail-safe block is programmed with an emergency stop, a safety door function, a feedback loop (as restart protection, when an incorrect load exists), and a user acknowledgement for reintegration. The block is then compiled to form a safety program.

The programming is described in the "Programming" (Page 46) section.

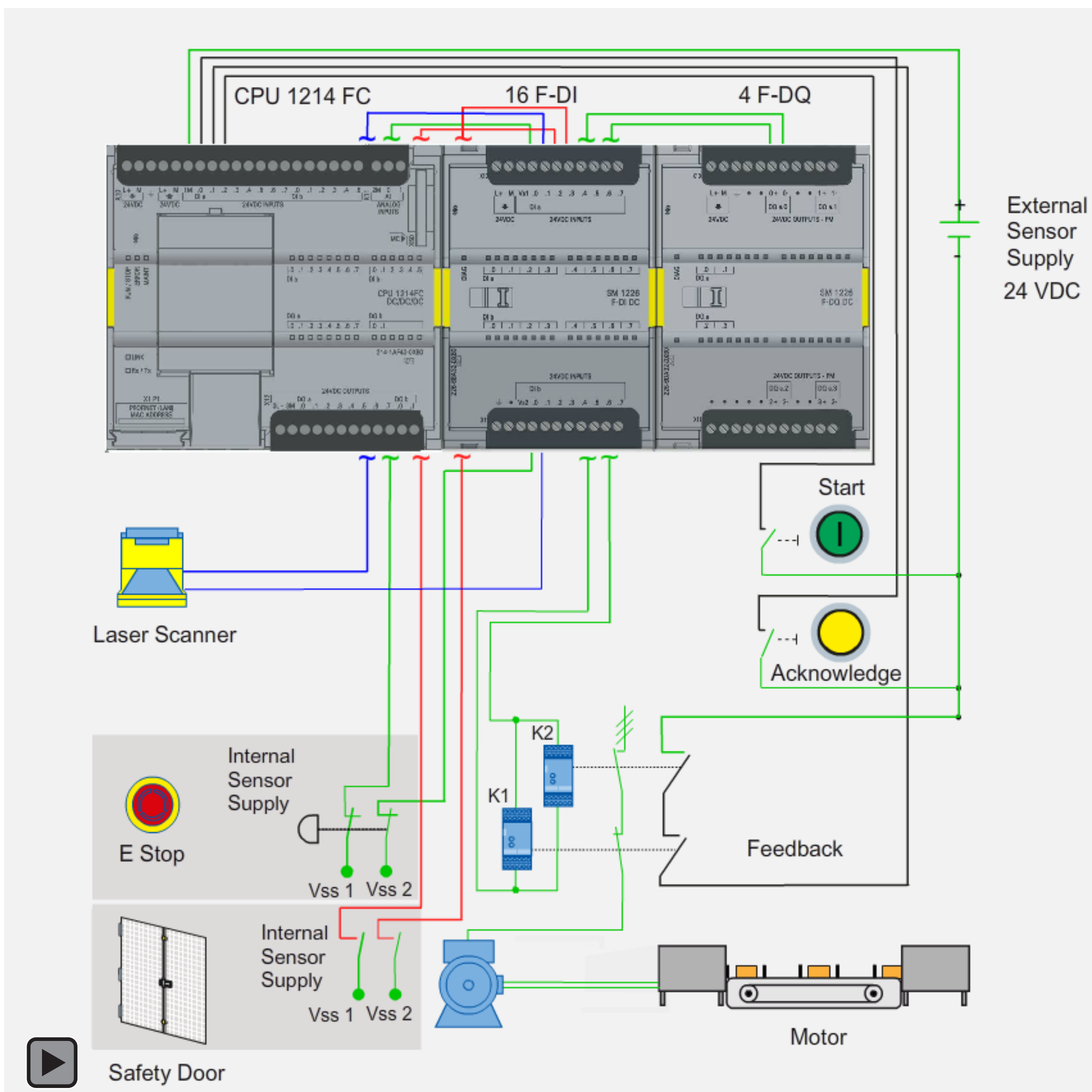
Operating the Getting Started example

This interactive graphic gives you the opportunity to become familiar with how the example functions in this Getting Started.

Note

Before you try to operate the example, ensure that you have loaded the required Adobe software (Page 26) on your computer.

Click the "Play" button to start the animation file and the control elements to operate the example. You can switch the Laser Scanner, E Stop, or Safety Door on and off to simulate an unsafe condition. However, you must press the "Acknowledge" button to notify the system that you have returned to a safe state. Then, you can press the "Start" button to operate the system again.



2.2 Configuring

2.2.1 Introduction

⚠ WARNING
You may come into contact with live electrical wires connected to the main power supply. Only wire the S7-1200 fail-safe CPU control system when the input power is turned OFF. Death or serious personal injury and damage to machines and equipment may result if proper precautions are not taken.

The installation and wiring of the S7-1200 fail-safe CPU is described in the S7-1200 Programmable Controller System Manual (http://support.automation.siemens.com/WW/view/en/91696622).

Configuring the Hardware

In STEP 7 Safety, you configure the following S7-1200 components:

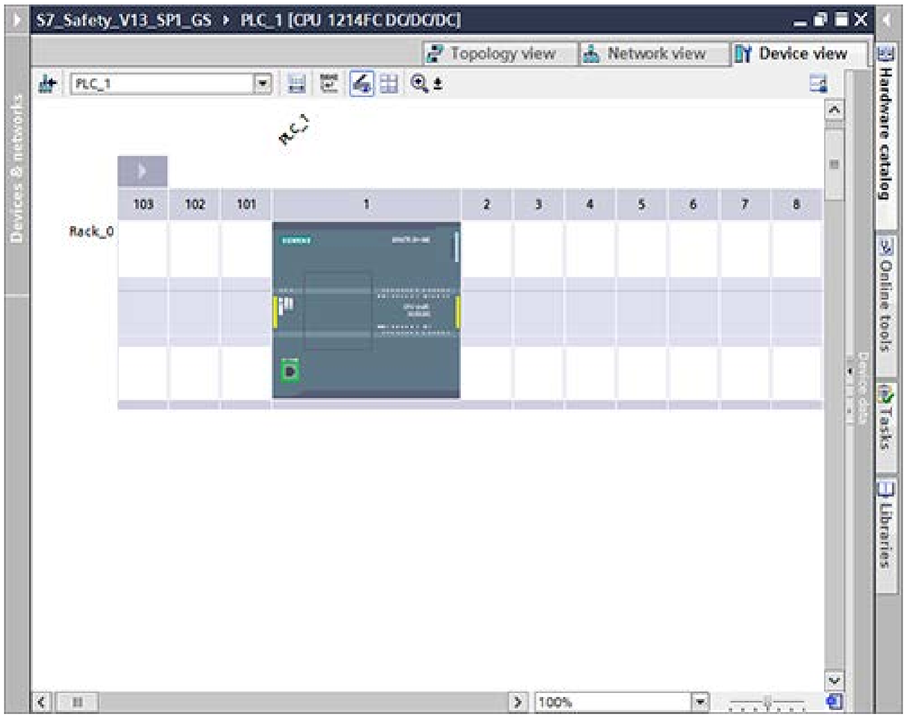
- Fail-safe CPU
- Fail-safe CPU standard digital inputs for user acknowledgement, feedback loop, and start pushbutton
- Fail-safe digital input SM for connecting an emergency stop switch and position switches for monitoring a safety door and the laser scanner
- Fail-safe digital output SM for connecting a motor

2.2.2 Step 1: Configuring the S7-1200 CPU 1214FC or CPU 1215FC

In this step, you create a new project, add a fail-safe CPU, and assign parameters.

Click the "Play" button to start the animation file. Click the other control elements to rewind, pause, go back, or go forward.

Procedure



1. In the portal view of STEP 7 Safety, create a new project named "S7_Safety_V13_SP1_GS"
2. Use "Add new device" to add a CPU 1214FC.

Note

Any of the four available fail-safe CPUs (1214FC DC/DC/DC, 1214FC DC/DC/Relay, 1215FC DC/DC/DC, 1215FC DC/DC/Relay) may be used in this example.

Result: The Device View containing the CPU 1214FC opens.

3. Locate the "Fail-safe: F-parameters" area.

   You can change the following parameters or accept the default setting:

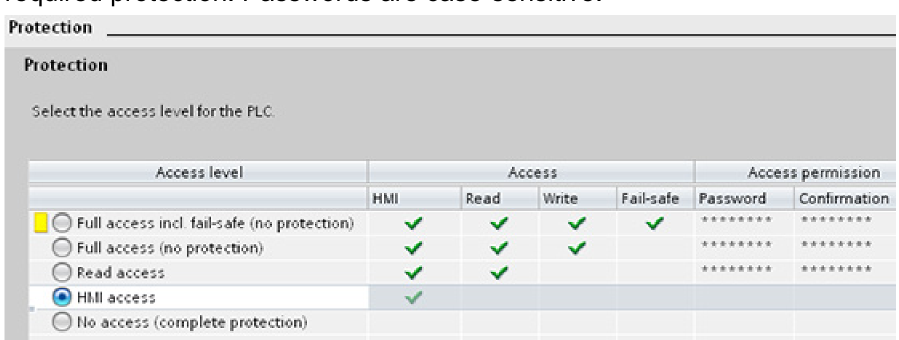
   – "Basis for PROFIsafe addresses": Any value is suitable for a stand-alone fail-safe S7-1200 CPU with local fail-safe SMs.

   – "Default F-monitoring time for central F-I/O": A valid current safety message frame must be received from the fail-safe CPU to a fail-safe SM within the F-monitoring time. Otherwise, the fail-safe SM goes to safe state. The F-monitoring time must be set high enough so that message frame delays are tolerated and, at the same time, low enough that the process can react as quickly as possible when a fault occurs. By default, the F-monitoring time for each fail-safe SM is taken from the "Default F-monitoring time for central F-I/O" parameter of the fail-safe CPU. However, you can configure the F-monitoring time individually for each fail-safe SM. Refer to Section 5.2: "Configuring common F-parameters" (Page 106) for further information.

   Leave the default values unchanged for this example.

4. Move to the "Protection" area.

   Select the "Protection" property to select the protection level and enter passwords. "Full access incl. fail-safe (no protection)" protection level with a fail-safe write protection password is the lowest level for a fail-safe CPU. Enter and confirm a password for the required protection. Passwords are case-sensitive.



   When you download this configuration to the fail-safe CPU, the user has HMI access and can access HMI functions without a password. To read data, the user must enter the configured password for "Read access", the password for "Full access (no protection)", or the password for "Full access incl. fail-safe (no protection)". To write data, the user must enter the configured password for "Full access (no protection)" or the password for "Full access incl. fail-safe (no protection)".

Access protection for the fail-safe CPU

The fail-safe CPU provides five levels of security for restricting access to specific functions. When you configure the security level and password for a fail-safe CPU, you limit the functions and memory areas that can be accessed without entering a password.

Each level allows certain functions to be accessible without a password. The default condition for the fail-safe CPU is to have no restriction and no password-protection. To restrict access to a fail-safe CPU, you configure the properties of the fail-safe CPU, and enter and confirm the password.

Table 2- 1 Security levels for the CPU

Security level	Access restrictions
Full access incl. fail-safe (no protection)	Allows full access without password. This is the lowest level of protection for a fail-safe CPU.
Full access (no protection)	Allows full access, except write access to fail-safe blocks. Password is required for modifying (writing to) fail-safe blocks and for changing the CPU mode (RUN/STOP).
Read access	Allows HMI access and all forms of PLC-to-PLC communications without password protection. Password is required for modifying (writing to) the CPU and for changing the CPU mode (RUN/STOP).
HMI access	Allows HMI access and all forms of PLC-to-PLC communications without password protection. Password is required for reading the data in the CPU, for modifying (writing to) the CPU, and for changing the CPU mode (RUN/STOP).
No access (complete protection)	Allows no access without password protection. Password is required for HMI access, reading the data in the CPU, for modifying (writing to) the CPU, and for changing the CPU mode (RUN/STOP)

Result

The new project has been created and the configuration of the fail-safe CPU is complete.

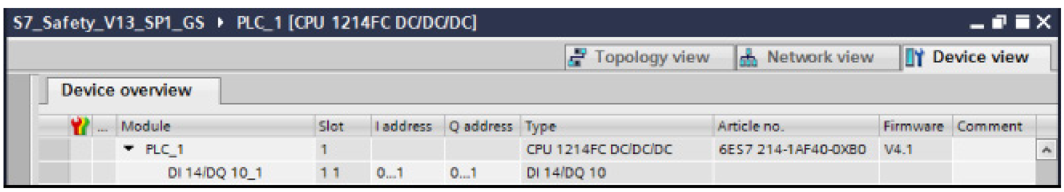
2.2.3 Step 2: Configuring fail-safe CPU standard digital inputs for user acknowledgement, feedback circuit, and start pushbutton

In this step, you assign parameters of fail-safe CPU standard digital inputs for the non-fail-safe signals (user acknowledgement, feedback loop, and start pushbutton).

Procedure

1. Assign the input address of the fail-safe CPU standard digital inputs to "0" for this example. Assign the output address of the fail-safe CPU standard digital outputs to "0" as well. You can assign these addresses in the CPU device configuration under "DI 14/DQ 10", "I/O addresses".

   Refer to the "CPU 1214FC Device view" information from the TIA Portal shown below:



Result

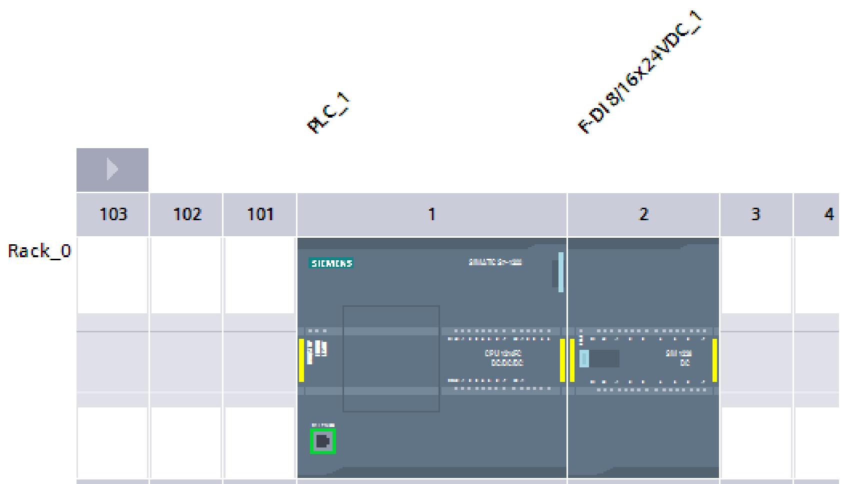
The configuration of the fail-safe CPU standard digital inputs is now complete.

2.2.4 Step 3: Configuring an SM1226 F-DI 16 x 24 VDC for connecting an emergency stop switch, position switches, and the laser scanner

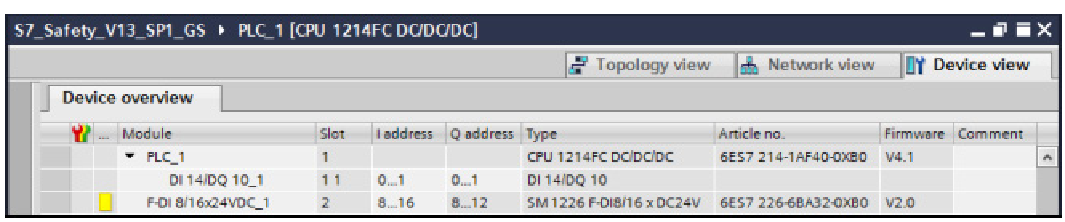
In this step, you configure an F-DI for connecting an emergency stop switch, the position switches for monitoring a safety door, and the laser scanner for monitoring the entry area.

Procedure

1. In the Device View of the S7-1200, use drag-and-drop to add an F-DI 8/16x24VDC_1 digital electronic module from the hardware catalog to slot 2.



2. Open "Device data" to display the "Device overview" area. Here, you can change the starting addresses for the inputs and outputs of your fail-safe module. Use the module default I/O addresses of "8" and "8" for this example (inputs begin at byte 8, and outputs begin at byte 8).



Module	Slot	I address	Q address	Type	Article no.	Firmware	Comment
PLC_1	1			CPU 1214FC DC/DC/DC	6ES7 214-1AF40-0XB0	V4.1	
DI 14/DQ 10_1	1 1	0...1	0...1	DI 14/DQ 10			
F-DI 8/16x24VDC_1	2	8...16	8...12	SM 1226 F-DI8/16 x DC24V	6ES7 226-6BA32-0XB0	V2.0	

Note

The fail-safe SMs each use both Is and Qs, even though they may physically only have input channels or only have output channels.

The F-DI can have 8 - 16 input channels; however, the SM requires 9 input (I) bytes and 5 output (Q) bytes.

3. Return to the "Device view" and select the F-DI 8/16x24VDC_1. Under the "Properties" tab, select the "IO tags" tab. This action displays the "Process value" and "Quality" bits for the fail-safe module. Here, you can define tags for each channel:

F-DI 8/16x24VDC_1 [Module] | Properties | Info | Diagnostics

General | IO tags | System constants | Texts

Name	Type	Address	Tag table	Comment
	Bool	%I8.0		
	Bool	%I8.1		
	Bool	%I8.2		
	Bool	%I8.3		
	Bool	%I8.4		
	Bool	%I8.5		
	Bool	%I8.6		
	Bool	%I8.7		
	Bool	%I9.0		
	Bool	%I9.1		
	Bool	%I9.2		
	Bool	%I9.3		
	Bool	%I9.4		
	Bool	%I9.5		
	Bool	%I9.6		
	Bool	%I9.7		
	Bool	%I10.0		
	Bool	%I10.1		
	Bool	%I10.2		
	Bool	%I10.3		
	Bool	%I10.4		
	Bool	%I10.5		
	Bool	%I10.6		
	Bool	%I10.7		
	Bool	%I11.0		
	Bool	%I11.1		
	Bool	%I11.2		
	Bool	%I11.3		
	Bool	%I11.4		
	Bool	%I11.5		
	Bool	%I11.6		
	Bool	%I11.7		

Each Process value bit has an associated Quality bit that reports whether the corresponding process value is valid or passivated. Quality bits are "ON" for valid data and "OFF" for data associated with passivated channels.. If an entire module or a single channel is passivated, the associated Quality bits are "OFF".

To check the Process value bits and the Quality bits, you must know where these bits are mapped in the module. For an F-DI 8/16x24VDC_1, the first two bytes of the input (I) image register are the Process value bits, and the next two bytes of the input (I) image register are the Quality bits. For example, if the module starting address is I8.0 and Q8.0 for the F-DI 8/16x24VDC_1 and you have a 1oo1 configuration, then the Process value bits and corresponding Quality bits are allocated as shown in the following table:

Process value	Quality bit
I8.0	I10.0
I8.1	I10.1
I8.2	I10.2
I8.3	I10.3
I8.4	I10.4
I8.5	I10.5
I8.6	I10.6
I8.7	I10.7
I9.0	I11.0
I9.1	I11.1
I9.2	I11.2
I9.3	I11.3
I9.4	I11.4
I9.5	I11.5
I9.6	I11.6
I9.7	I11.7

If you have a 1oo2 configuration, then the Process value bits and corresponding Quality bits are allocated as shown in the following table:

Process value	Quality bit
I8.0	I10.0
I8.1	I10.1
I8.2	I10.2
I8.3	I10.3
I8.4	I10.4
I8.5	I10.5
I8.6	I10.6
I8.7	I10.7
-	-
-	-
-	-
-	-
-	-
-	-
-	-
-	-

4. Under the "Properties" tab, select the "General" tab, and then select the "F-parameters" area. Here, you can change the following parameters or apply the default settings:
   - "F-monitoring time": A valid current safety message frame must be received from the fail-safe CPU to the F-DI within the F-monitoring time. Otherwise, the F-DI goes to safe state. The F-monitoring time must be set high enough so that message frame delays are tolerated and, at the same time, low enough that the process can react as quickly as possible when a fault occurs and run without impairment. By default, the F-DI's F-monitoring time is taken from the "Default F-monitoring time for central F-I/O" parameter of the fail-safe CPU.

     Note

     The "cyclic interrupt time" is a closely-related parameter to the F-monitoring time. The cyclic interrupt time is the interval by which the F-runtime group executes and determines how often the fail-safe CPU sends the PROFIsafe frame to the fail-safe SMs.

     When you add a fail-safe CPU to your project, STEP 7 creates Functional Safety Organization Block 1 (FOB_1) (OB123 by default). FOB_1 contains the cyclic interrupt time.

   - "F-destination address": A unique PROFIsafe address is critical for every F-IO used in a safety system (network and CPU-wide). Refer to the "SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual" (http://support.automation.siemens.com/WW/view/en/54110126/0/en) for procedures to set and verify unique PROFIsafe addresses in networked systems.

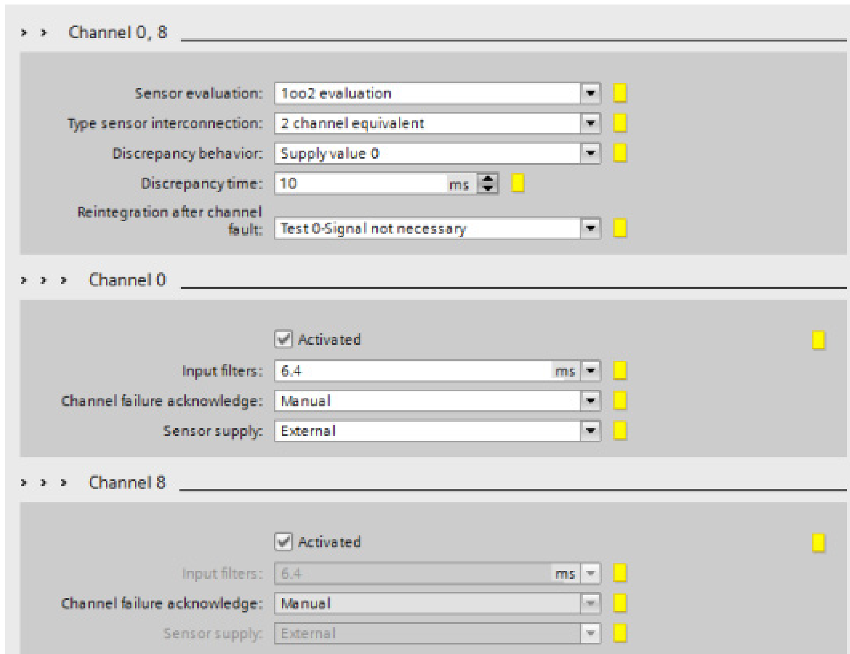
   Leave the settings unchanged for the F-parameters for this example.
5. Select the "DI parameters" area.

   Deactivate (uncheck the box) the "Short-circuit test" parameter for this example.

6. In this example, a two-channel emergency stop switch (emergency stop) is connected to channels 0 and 8.

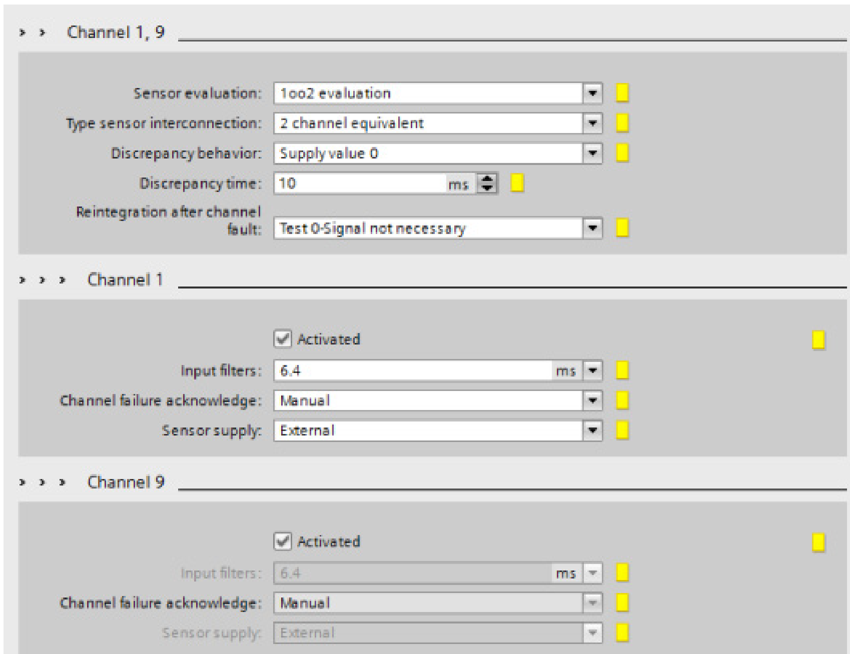
   In our example, these channels are wired to Process value bits I8.0 and I9.0. The first of the two inputs, I8.0, conveys the signal in this 1oo2 configuration. Expand "DI parameters" and "Channel parameters" and select "Channel 0, 8".

   Enter the settings as shown in the following figure:



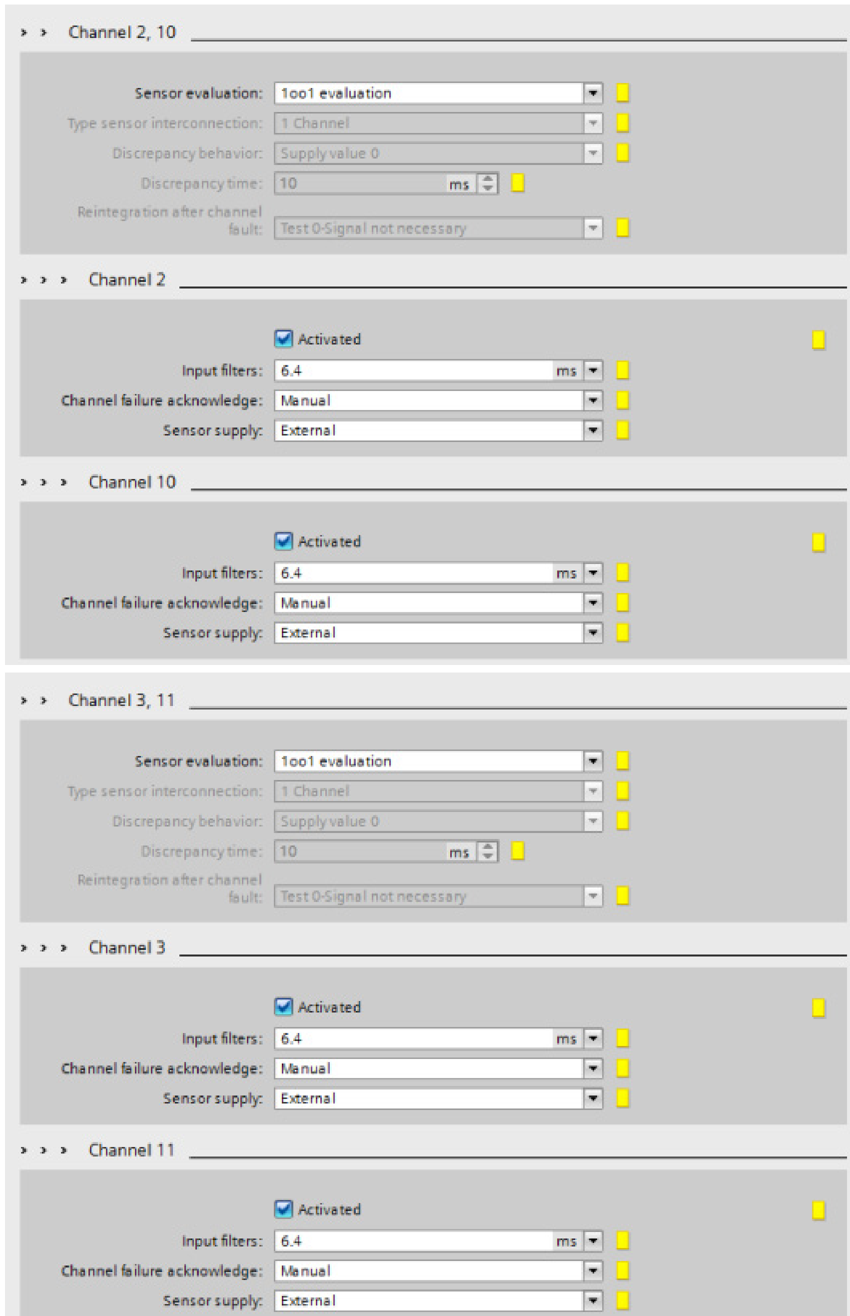
7. In this example, the laser scanner for monitoring the accessible entry area is connected to channels 1 and 9.

   Make the settings as shown in the following figure:



8. In this example, the position switches for monitoring a two-channel safety door are connected to channels 2 and 3.

   Make the settings as shown in the following figure:



9. Disable the following unused DI channels by clearing the "Activated" check box:

-
-
- 4
- 5
- 6
- 7
- 10
- 11
- 12
- 13
- 14
- 15

Result

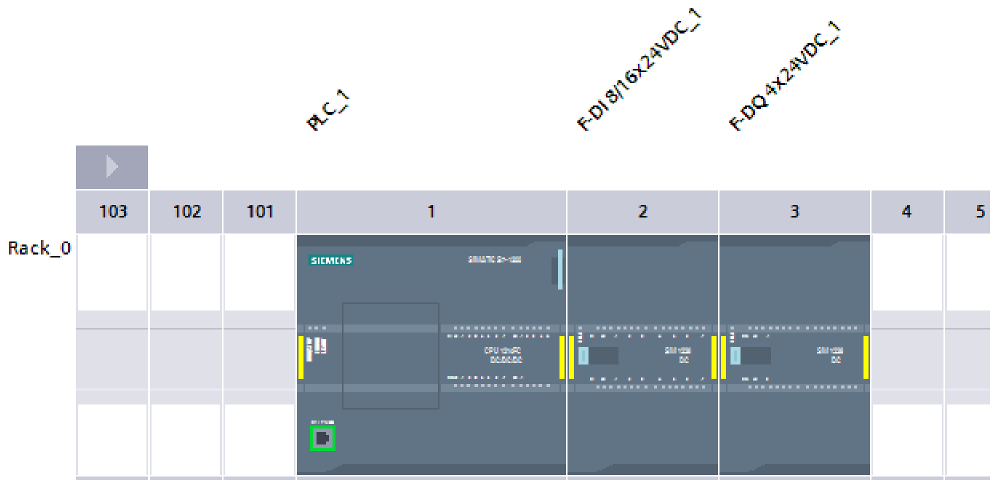
The configuration of the F-DI is now complete.

2.2.5 Step 4: Configuring an SM 1226 F-DQ 4 x 24 VDC for connecting a motor

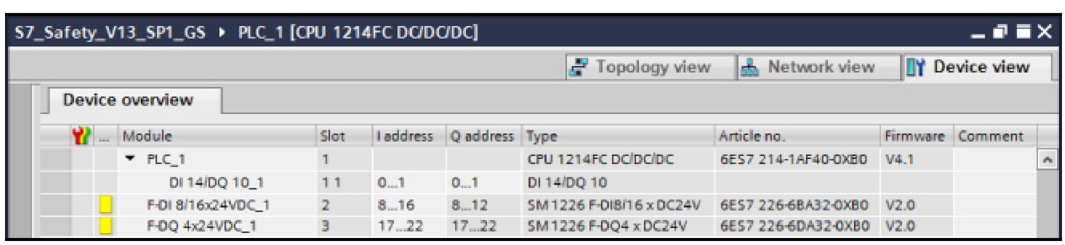
In this step, you configure an F-DQ DC for indirect connection of a motor to channel 0, using 2 contactors.

Procedure

1. In the Device View of the S7-1200, use drag-and-drop to add an F-DQ 4x24VDC_1 digital electronic module from the hardware catalog to slot 3.



2. Open "Device data" to display the "Device overview" area. Here, you can change the start addresses for the inputs and outputs of your fail-safe module. Use the module default I/O addresses of "17" and "17" for this example (inputs begin at byte 17, and outputs begin at byte 17).


S7_Safety_V13_SP1_GS ▸ PLC_1 [CPU 1214FC DC/DC/DC]

Topology view | Network view | Device view

Device overview

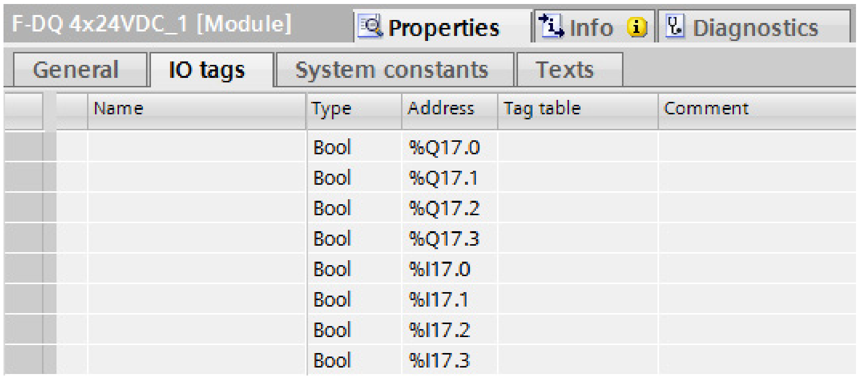
Module	Slot	I address	Q address	Type	Article no.	Firmware	Comment
PLC_1	1			CPU 1214FC DC/DC/DC	6ES7 214-1AF40-0XB0	V4.1	
DI 14/DQ 10_1	1 1	0...1	0...1	DI 14/DQ 10			
F-DI 8/16x24VDC_1	2	8...16	8...12	SM 1226 F-DI8/16 x DC24V	6ES7 226-6BA32-0XB0	V2.0	
F-DQ 4x24VDC_1	3	17...22	17...22	SM 1226 F-DQ4 x DC24V	6ES7 226-6DA32-0XB0	V2.0	

Note

The fail-safe SMs each use both Is and Qs, even though they may physically only have input channels or only have output channels.

The F-DQ DC has 4 output channels; however, the SM requires 6 input (I) bytes and 6 output (Q) bytes.

3. Return to the "Device view" and select the F-DQ 4x24VDC_1. Under the "Properties" tab, select the "IO tags" tab. This action displays the "Process value" and "Quality" bits for the fail-safe module. Here, you can define tags for each channel:



F-DQ 4x24VDC_1 [Module] | Properties | Info | Diagnostics

General | IO tags | System constants | Texts

Name	Type	Address	Tag table	Comment
	Bool	%Q17.0		
	Bool	%Q17.1		
	Bool	%Q17.2		
	Bool	%Q17.3		
	Bool	%I17.0		
	Bool	%I17.1		
	Bool	%I17.2		
	Bool	%I17.3		

Each Process value bit has an associated Quality bit that reports whether the corresponding process value is good. Quality bits are ON for good quality and OFF for bad quality. If an entire module or channel is passivated, the associated Quallity bits are OFF.

To check the Process value bits and the Quality bits, you must know where these bits are mapped in the module. For an F-DQ 4x24VDC_1, the first four bits of the output (Q) image register are the Process value bits, and the first four bits of the input (I) image register are the Quality bits. For example, if the module starting address is I17.0 and Q17.0 for the F-DQ 4x24VDC_1, then the Process value bits and corresponding Quality bits are allocated as shown in the following table:

Process value	Quality bit
Q17.0	I17.0
Q17.1	I17.1
Q17.2	I17.2
Q17.3	I17.3

4. Under the "Properties" tab, select the "General" tab, and then select the "F-parameters" area. Here, you can change the following parameters or accept the default settings:

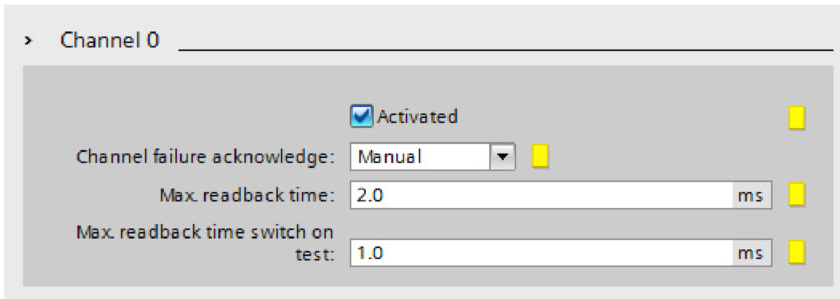
   – "F-monitoring time": A valid current safety message frame must be received from the fail-safe CPU to the F-DQ DC within the F-monitoring time. Otherwise, the F-DQ DC goes to safe state. The F-monitoring time must be set high enough so that message frame delays are tolerated and, at the same time, low enough that the process can react as quickly as possible when a fault occurs and run without impairment. By default, the F-DQ DC's F-monitoring time is taken from the "Default F-monitoring time for central F-I/O" parameter of the fail-safe CPU.

   – "F-destination address": A unique PROFIsafe address is critical for every F-IO used in a safety system (network and CPU-wide). Refer to the "SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual" (http://support.automation.siemens.com/WW/view/en/54110126/0/en) for procedures to set and verify unique PROFIsafe addresses in networked systems.

   Leave the settings unchanged for the F-parameters for this example.

5. Select the "DQ parameters" area. Here, you can change channel-specific parameters or apply the default settings.

   Enter the settings for the example as shown in the following figure:



6. Disable the unused DQ channels 1, 2, and 3 by clearing the "Activated" check box.

Result

The configuration of the F-DQ DC is now complete.

2.2.6 Summary: Configuring the Hardware

Summary

So far, you have configured the following S7-1200 components according to the task definition for the example:

- Fail-safe CPU
- Fail-safe CPU standard digital inputs for user acknowledgment, feedback loop, and start pushbutton:

  - Starting byte addresses of the input and output data areas: IB0 and QB0
  - Input channel (bit) 0 for re-integration acknowledgement (I0.0)
  - Input channel (bit) 1 for feedback (I0.1)
  - Input channel (bit) 2 for start (I0.2)
- Fail-safe digital input SM (F-DI 8/16x24VDC_1) for connecting an emergency stop switch, position switches for monitoring a safety door, and the laser scanner for monitoring the accessible production area:

  - Starting byte addresses of the input and output data areas: IB8 and QB8
  - Input channel (bits) 0 and 8 for the emergency stop (I8.0)
  - Input channel (bits) 1 and 9 for the laser scanner (I8.1)
  - Input channel (bit) 2 for one safety door position switch (I8.2)
  - Input channel (bit) 3 for other safety door position switch (I8.3)
- Fail-safe digital output SM (F-DQ 4x24VDC_1) for connecting a motor:

  - Starting byte addresses of the input and output data areas: IB17 and QB17
  - Output channel (bit) 0 for indirect switching of a motor using 2 contactors (Q17.0)

You can now continue with programming the safety program.

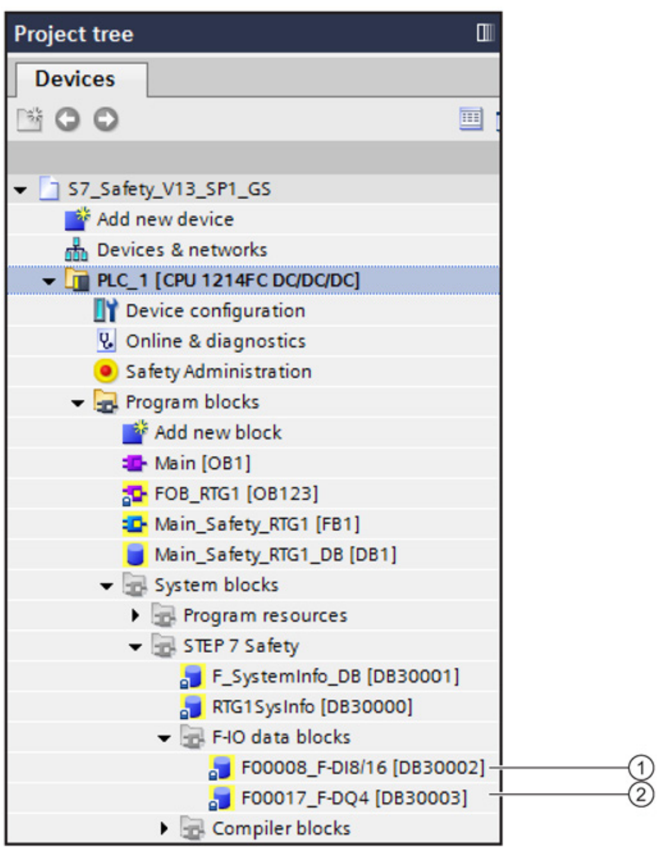
2.3 Programming

2.3.1 Introduction

In this example, a fail-safe function block (F-FB) will be programmed with a safety door function, an emergency stop function (safety circuit for switch-off in case of emergency stop, open safety door, or someone entering the protected area monitored by the laser scanner), a feedback circuit (as protection against reclosing in case of faulty load), a user acknowledgement for reintegration, and indirect switching of a motor using two contactors. The programmed F-FB will then be compiled to form a safety program and downloaded to the fail-safe CPU.

Fail-Safe SM data blocks (F-IO DBs)

An F-IO DB is automatically generated when you add a fail-safe SM to your configuration. The F-I/O DBs generated for the example I/O are located in the "Project tree" in the "Program blocks", "System blocks" folder:



① "F00008 F-DI16 [DB30002]": Fail-safe digital input SM 1226 F-DI 16 x 24 VDC data block (DB)

② "F000016 F-DQ4 [DB30003]": Fail-safe digital output SM 1226 F-DQ 4 x 24 VDC data block (DB)

The default name of the F-I/O DB is formed from the fixed prefix "F", the start input address of the fail-safe SM, and the names entered in the properties for the fail-safe SM in the hardware and network editor.

You can access the tags of the F-I/O DB with a fully qualified DB access (that is, by specifying the name of the F-I/O DB and the name of the tag).

Programming

You can program the safety program in LAD and FBD. In so doing, the instructions, data types, and operand areas you can use are subject to certain restrictions (see the "Programming" chapter, "Overview of programming" section of the SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual (http://support.automation.siemens.com/WW/view/en/54110126/0/en)).

The FBD programming language is used in this example.

Note

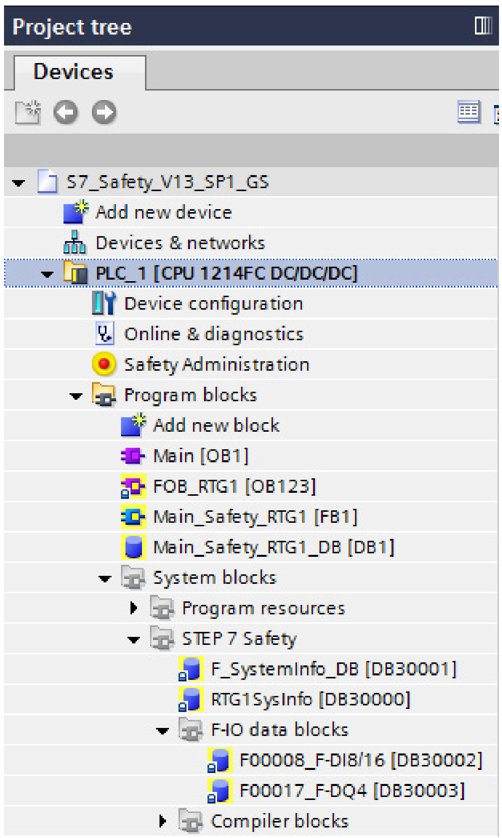
Fail-safe signals are shown in yellow in the "LAD/FBD Editor".

Note

Note the rules for the program structure in the "Programming" chapter, "Defining F-runtime groups" section of the SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual (http://support.automation.siemens.com/WW/view/en/54110126/0/en).

2.3.2 Step 5: Specifying the centralized settings for the safety program

When the fail-safe CPU is inserted, an F-runtime group and the associated main safety block are created by default and assigned to the CPU. An F-runtime group consists of an F-OB (cyclic interrupt OB) that calls a main safety block FB. Additional user-specific safety functions must then be called from this main safety block:



The first step in programming of the safety program is the main safety block. The main safety block is an F-FB (with instance DB) that is called from the "Fail-Safe Organization Block" (cyclic interrupt OB) assigned in each F-runtime group.

F-blocks created by the user are called from the main safety block. You can change the calling block and the called block at any time.

After the safety program is executed, the standard user program will resume.

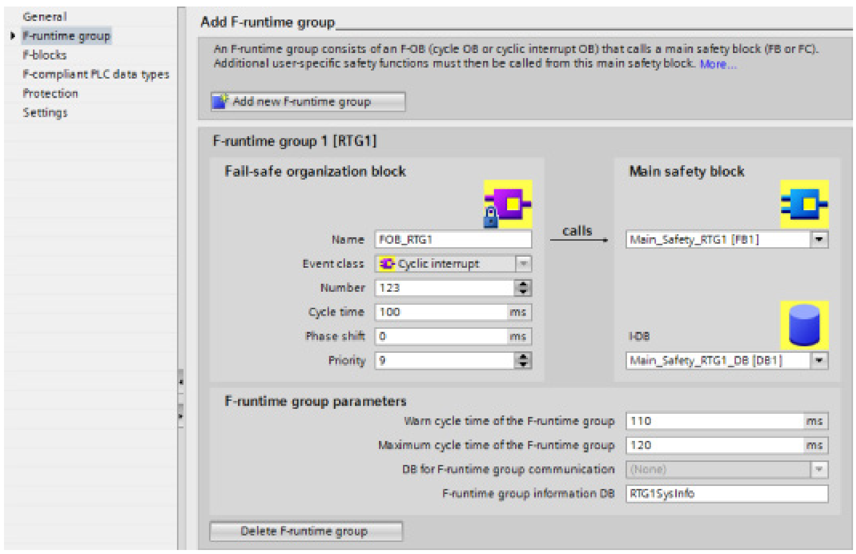
Opening the Safety Administration editor

1. In the "Project tree" of the fail-safe CPU, double-click on "Safety Administration".

   Result: The "Safety Administration" editor opens.

   You make central settings for the safety program in the Safety Administration editor.

2. In the area navigation of the Safety Administration editor, click "Safety runtime group". The F-runtime group is created automatically when the fail-safe CPU is created and the associated main safety block is displayed:



The cyclic interrupt OB (FOB_1 [OB123]) calls the main safety block (Main_Safety [FB1]) by default. The F-blocks created by the user are called from the main safety block. You can change the calling block and the called block at any time.

Leave the preset blocks for this example.

For additional information on the Safety Administration editor, refer to the SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual (http://support.automation.siemens.com/WW/view/en/54110126/0/en).

Numbering ranges of fail-safe system blocks

When the safety program is compiled, F-blocks are automatically added in order to generate an executable safety program.

By default, the system automatically manages the numbering range, which is displayed in the Safety Administration editor under "Settings".

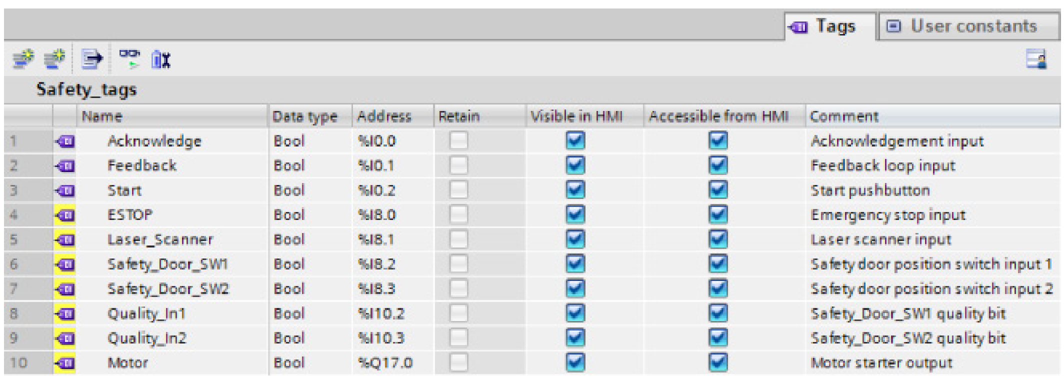
Keep the pre-assigned settings for this example.

Specifying inputs and outputs for the safety program

After configuring the hardware as described in Steps 1 to 4, the following fail-safe CPU and SM DBs are available for programming the example:

Configured hardware	Start input address	Symbolic name
Fail-safe CPU standard digital inputs CPU 1214FC	IB0	PLC_1 [CPU 1214FC DC/DC/DC]
Fail-safe digital input module SM 1226 F-DI 16 x 24 VDC	IB8	F00008_SM 1226 F-DI 16 x 24 VDC
Fail-safe digital output module SM 1226 F-DQ 4 x 24 VDC	IB16	F00016_SM 1226 F-DQ 4 x 24 VDC

Assign the following symbolic names for the fail-safe inputs and outputs:



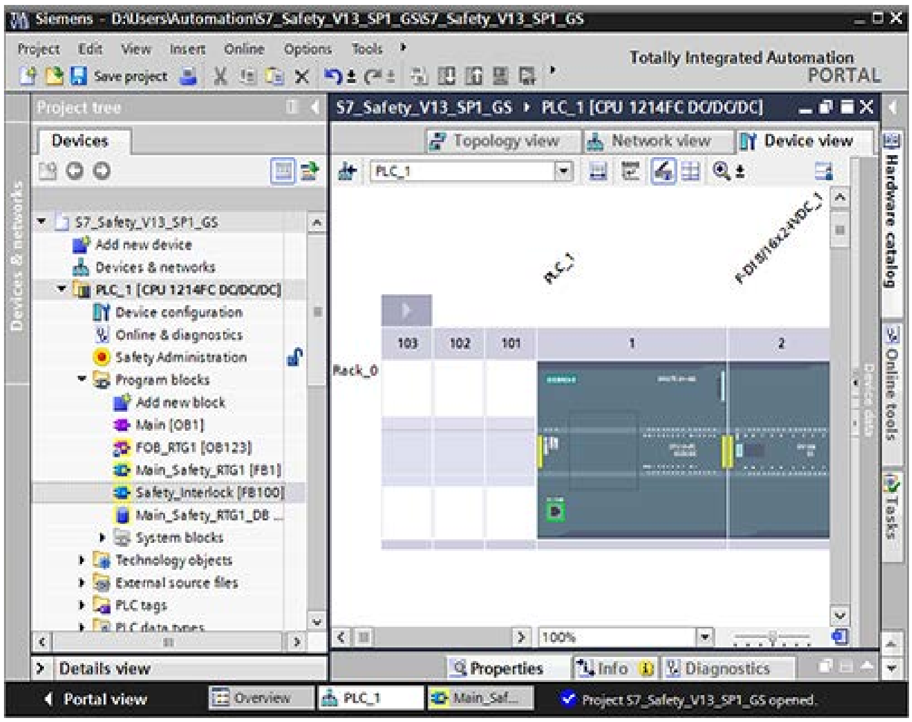
	Name	Data type	Address	Retain	Visible in HMI	Accessible from HMI	Comment
1	Acknowledge	Bool	%I0.0	☐	☑	☑	Acknowledgement input
2	Feedback	Bool	%I0.1	☐	☑	☑	Feedback loop input
3	Start	Bool	%I0.2	☐	☑	☑	Start pushbutton
4	ESTOP	Bool	%I8.0	☐	☑	☑	Emergency stop input
5	Laser_Scanner	Bool	%I8.1	☐	☑	☑	Laser scanner input
6	Safety_Door_SW1	Bool	%I8.2	☐	☑	☑	Safety door position switch input 1
7	Safety_Door_SW2	Bool	%I8.3	☐	☑	☑	Safety door position switch input 2
8	Quality_In1	Bool	%I10.2	☐	☑	☑	Safety_Door_SW1 quality bit
9	Quality_In2	Bool	%I10.3	☐	☑	☑	Safety_Door_SW2 quality bit
10	Motor	Bool	%Q17.0	☐	☑	☑	Motor starter output

2.3.3 Step 6: Creating an F-FB

In this step, you create the F-FB where you will program the safety functions for this example.

Click the "Play" button to start the animation file. Click the other control elements to rewind, pause, go back, or go forward.

Procedure



1. Insert an F-FB. Go to the "Program blocks" folder of the fail-safe CPU and double-click "Add new block".

   The "Add new block" dialog opens.
2. Under "Name" enter "Safety_Interlock" for the name of the F-FB.
3. Click the "Function block" button on the left.
4. Select "FBD" as the language for the F-FB.
5. Under "Number" choose the "Manual" option, and enter 100.
6. Ensure that you select the "Create F-block" check box so that a fail-safe function block is created.
7. Close the dialog box with "OK"

Result

The F-FB "Safety_Interlock" is created in the "Program blocks" folder and opens automatically in the "FBD Editor".

You can now continue with programming the safety functions in the next step.

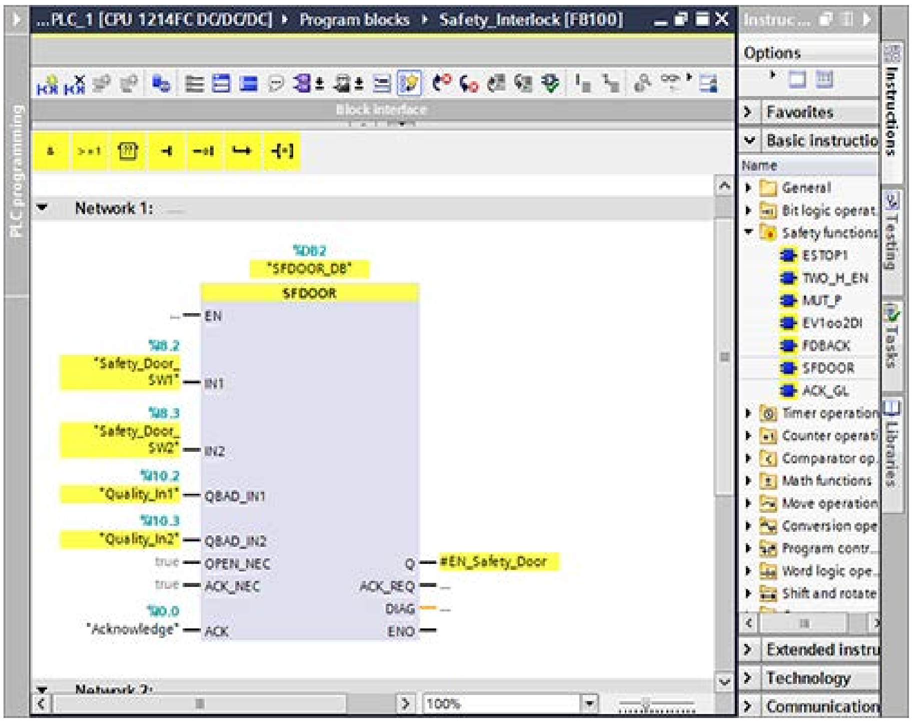
2.3.4 Step 7: Programming the safety door function

In this step, you program the safety door function for this example.

The safety door secures the application's service area. Opening the safety door results in a stop or shutdown of the production cell similar to an emergency stop.

Click the "Play" button to start the animation file. Click the other control elements to rewind, pause, go back, or go forward.

Procedure



1. In the interface of the "Safety_Interlock" F-FB, create a static tag of data type "Bool" named "EN_Safety_Door" (Enable safety door).
2. Insert the "SFDOOR" instruction from the "Safety functions" subfolder of the "Instructions" task card.
3. Click "OK" to confirm the "Call options" dialog.
4. Initialize the inputs and outputs with parameters as described in the table below.

Result

The programming of the safety door function is now complete.

Parameter assignment of the "SFDOOR" instruction

Inputs/outputs	Parameter	Data type	Description	Default
"Safety_Door_SW1" (I8.2)	IN1	Bool	Input 1	FALSE
"Safety_Door_SW2" (I8.3)	IN2	Bool	Input 2	FALSE
"Quality_In1" (I10.2)	QBAD_ IN1	Bool	Quality bit signal for input IN1 [1]	TRUE
"Quality_In2" (I10.3)	QBAD_ IN2	Bool	Quality bit signal for input IN2 [1]	TRUE
TRUE	OPEN_NEC	Bool	TRUE = Opening required on startup	TRUE
TRUE	ACK_NEC	Bool	TRUE = Acknowledgment required	TRUE
"Acknowledge" (I0.0)	ACK	Bool	User acknowledgement (Pushbutton)	FALSE
#EN_Safety_Door	Q	Bool	Output (Enable safety door)	FALSE
—	ACK_REQ	Bool	Acknowledgement prompt	FALSE
—	DIAG	Byte	Service information	B#16#0

[1] The two inputs QBAD_ IN1 and QBAD_ IN2 must be interconnected. In this example, both safety door position switches are connected through the SFDOOR and ESTOP1 program logic with the QBAD signal of the F-I/O DB of the SM 1226 F-DQ 4 x 24 VDC in the FDBACK program logic.

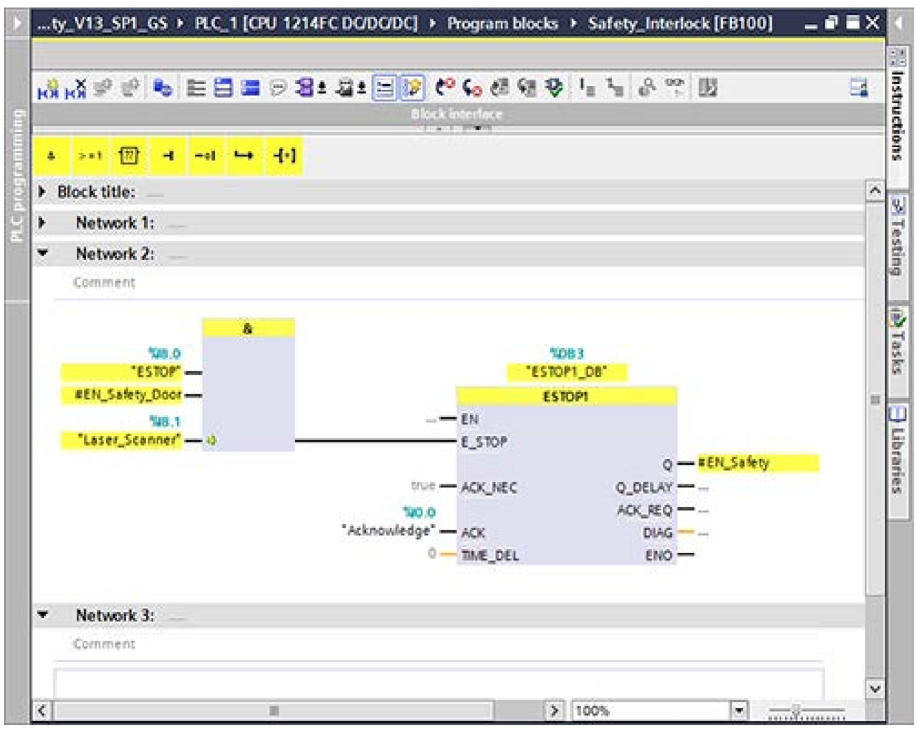
2.3.5 Step 8: Programming the emergency stop function

In this step, you program the emergency stop function for this example.

Used for emergencies only, the emergency stop button is a safety measure to immediately shut down all machine functions. An emergency stop button must be highly visible in color and shape and must be easy to operate in emergency situations. In this example, the emergency stop is a manual push button attached next to the safety door entrance to the service area enclosure. The emergency stop function provides shutdown in the case of an emergency stop, an open safety door, or someone entering the protected area monitored by the laser scanner.

Click the "Play" button to start the animation file. Click the other control elements to rewind, pause, go back, or go forward.

Procedure



1. In the interface of the "Safety_Interlock" F-FB, create a static tag of data type "Bool" named "EN_Safety" (Enable safety circuit).

   Note

   If the emergency stop is off, the safety door is closed, and the protected area laser scanner is not triggered, the inputs from the emergency stop, safety door, and the laser scanner are all true. All three inputs must be true, before the ESTOP1 instruction can power "EN_Safety". When "EN_Safety" is true, then the user knows that his operation is back to normal and that he can startup safely.

2. Insert a new network.
3. Insert the "AND logic operation" instruction from the "Bit logic operations" subfolder of the "Instructions" task card.

4. Insert a third input to the "AND logic operation" instruction and initialize the inputs of the instruction with parameters as described in the table below.
5. Insert the "ESTOP1" instruction from the "Safety functions" subfolder of the "Instructions" task card.
6. Click "OK" to confirm the "Call options" dialog.
7. Initialize the inputs and outputs of the instruction with parameters as described in the table below.
8. Connect the output of the "AND logic operation" instruction to the "ESTOP" input of the "ESTOP1" instruction.

Result

The programming of the emergency stop function is now complete.

Parameter assignment of the "AND logic operation" instruction

Inputs	Parameter	Data type	Description	Default
"ESTOP" (I8.0)	Input 1	Bool	Emergency STOP	FALSE
#EN_Safety_Door	Input 2	Bool	Enable safety door	FALSE
"Laser_scanner" (I8.1)	Input 3	Bool	Laser scanner	FALSE

Parameter assignment of the "ESTOP1" instruction

Inputs/outputs	Parameter	Data type	Description	Default
TRUE	ACK_NEC	Bool	TRUE = Acknowledgment required	TRUE
"Acknowledge" (I0.0)	ACK	Bool	User acknowledgement (using a pushbutton)	FALSE
T#0MS	TIME_DEL	Time	Time delay	T#0MS
#EN_Safety	Q	Bool	Enable safety circuit	FALSE
—	Q_DELAY	Bool	Enable is OFF delayed	FALSE
—	ACK_REQ	Bool	Acknowledgement prompt	FALSE
—	DIAG	Byte	Service information	B#16#0

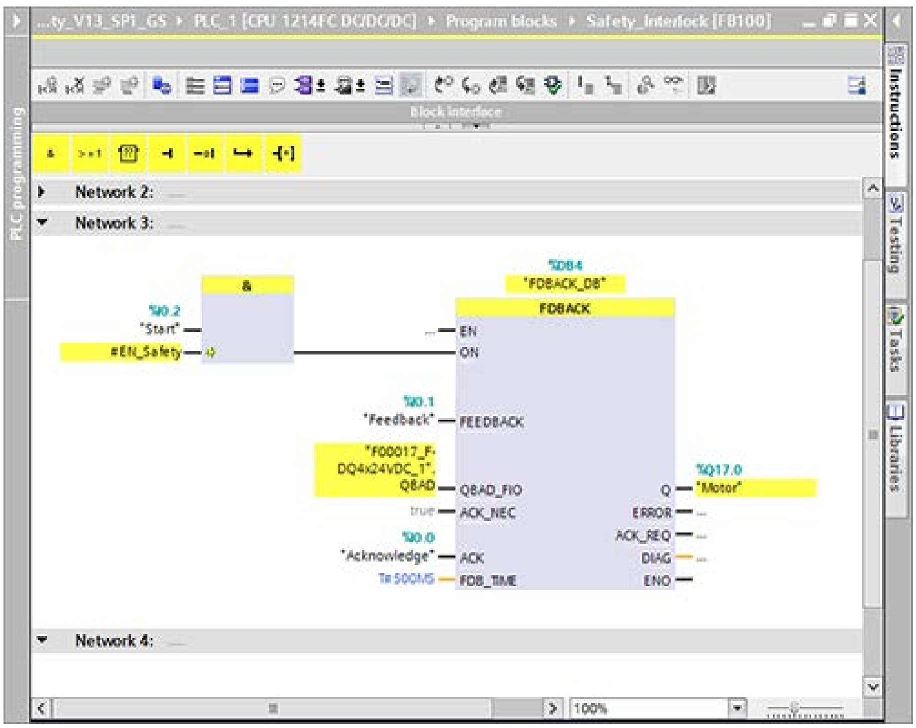
2.3.6 Step 9: Programming the feedback monitoring

In this step, you program the feedback circuit monitoring for this example.

The feedback circuit provides protection against restarting normal operations while unsafe conditions still exist. The system can only be restarted when the emergency stop is cancelled, the safety door is closed, and the laser scanner detects no one in the protected area.

Click the "Play" button to start the animation file. Click the other control elements to rewind, pause, go back, or go forward.

Procedure



1. Insert a new network.
2. Insert the "AND logic operation" instruction from the "Bit logic operations" subfolder of the "Instructions" task card.
3. Initialize the inputs of the instruction with parameters as described in the table below
4. Insert the "FDBACK" instruction from the "Safety functions" subfolder of the "Instructions" task card.
5. Click "OK" to confirm the "Call options" dialog.
6. Initialize the inputs and outputs of the instruction with parameters as described in the table below.
7. Connect the output of the "AND logic operation" instruction to the "ON" input of the "FDBACK" instruction.

Result

The programming of the feedback monitoring is now complete.

Parameter assignment of the "AND logic operation" instruction

Inputs	Parameter	Data type	Description	Default
"Start" (I0.2)	Input 1	Bool	TRUE = Switch on output	FALSE
#EN_Safety	Input 2	Bool	Enable safety circuit	FALSE

Parameter assignment of the "FDBACK" instruction

Inputs/outputs	Parameter	Data type	Description	Default
"Feedback" (I0.1)	FEEDBACK	Bool	Readback input	TRUE (No error detected)
"F00016_F-DQ4".QBAD	QBAD_FIO	Bool	QBAD signal from the fail-safe signal module DB of output Q [1]	FALSE (No error detected)
TRUE	ACK_NEC	Bool	TRUE = Acknowledgment required	TRUE
"Acknowledge" (I0.0)	ACK	Bool	User acknowledgement (via pushbutton)	FALSE
T#500MS	FDB_TIME	Time	Readback time	T#0MS
"Motor" (Q16.0)	Q	Bool	Output	FALSE
—	ERROR	Bool	Readback error	FALSE
—	ACK_REQ	Bool	Acknowledgement prompt	FALSE
—	DIAG	Byte	Service information	B#16#0

[1] In this example, this is the QBAD signal from the F-I/O DB of the SM 1226 F-DQ 4 x 24 VDC.

2.3.7 Step 10: Programming the user acknowledgment for reintegration of the fail-safe SM

In this step, you program the user acknowledgement for reintegration of the fail-safe signal module I/O for this example.

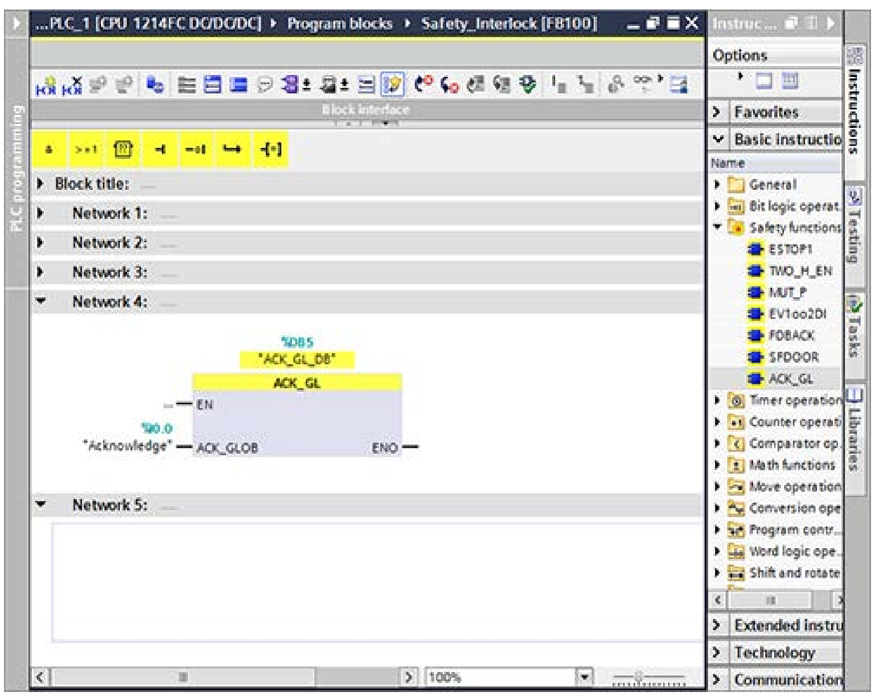
The user must acknowledge that conditions have returned to a safe state before production operations can be restarted.

Click the "Play" button to start the animation file. Click the other control elements to rewind, pause, go back, or go forward.

Procedure

In your safety program, you must provide a user acknowledgment for the reintegration of the fail-safe signal module I/O. In order to acknowledge in the event of passivated F-I/O, the acknowledgement pushbutton is evaluated using a standard input. In this example, this is the "Acknowledge" input.

You can use the ACK_GL instruction to reintegrate all F-I/O of an F-runtime group.



1. Insert a new network.
2. Insert the "ACK_GL" instruction from the "Safety functions" subfolder of the "Instructions" task card.
3. Click "OK" to confirm the "Call options" dialog.
4. Initialize the input with parameters as described in the table below.

Result

The programming of the user acknowledgment is now complete.

Parameter assignment of the "ACK_GL" instruction

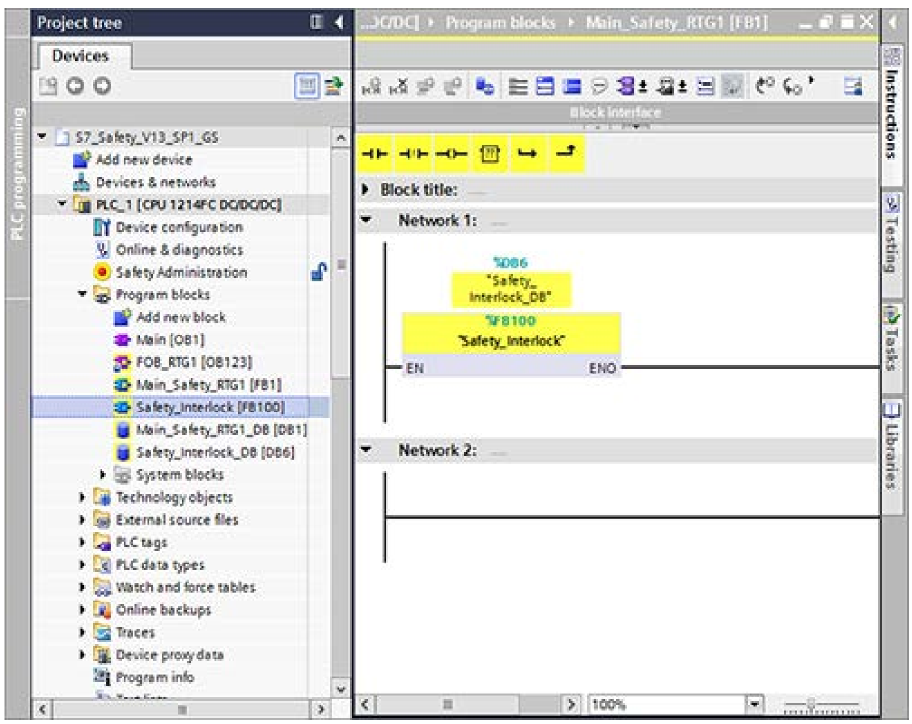
Input	Parameter	Data type	Description	Default
"Acknowledge" (I0.0)	ACK_GLOB	Bool	Acknowledgement for reintegration	FALSE

2.3.8 Step 11: Programming of the main safety block

In this step, you program the main safety block for this example.

Click the "Play" button to start the animation file. Click the other control elements to rewind, pause, go back, or go forward.

Procedure



1. Double-click in the project navigation to open the main safety block "Main_Safety".
2. Use drag-and-drop to insert the F-FB "Safety_Interlock" in Network 1 of the main safety block.
3. Click "OK" to confirm the "Call options" dialog.

Result

The F-FB "Safety_Interlock" will now be called cyclically by the main safety block.

You have now programmed the functionality according to the task definition of the example. You can now proceed with the next steps to compile the safety program, assign device names, and download the safety program along with the hardware configuration to the fail-safe CPU.

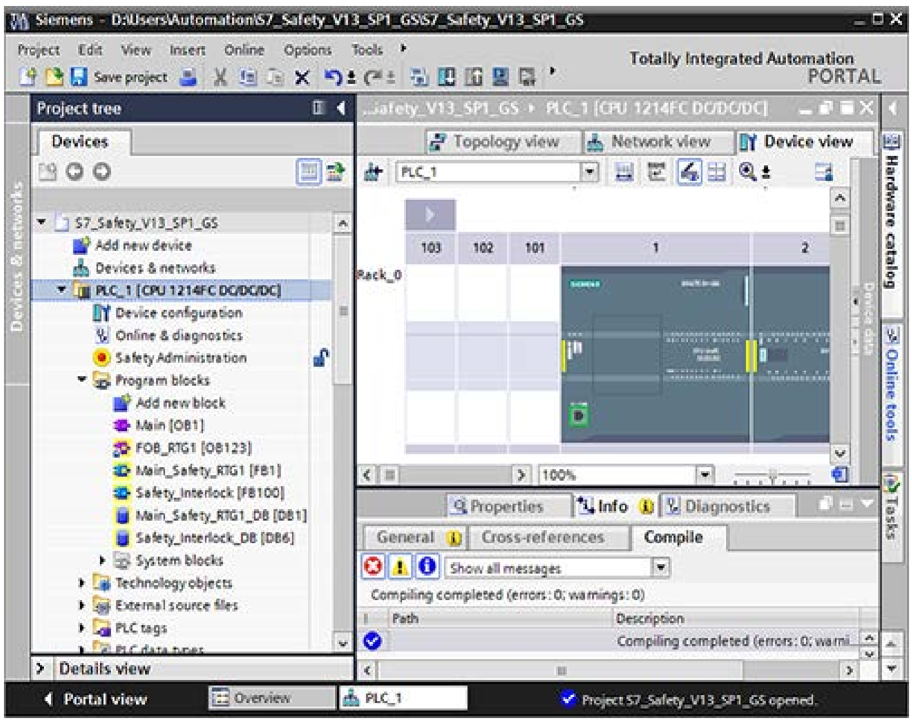
2.3.9 Step 12: Compiling the safety program

In this step, you compile the safety program and the hardware configuration.

A consistency check is performed on the execution-relevant F-blocks when the safety program is compiled, that is, the safety program is checked for errors. Any error messages are output in an error window. After a successful consistency check, the additionally required F-blocks are generated automatically and added to the F-runtime group in order to generate an executable safety program.

Click the "Play" button to start the animation file. Click the other control elements to rewind, pause, go back, or go forward.

Procedure



1. Select the fail-safe CPU in the project tree.
2. In the shortcut menu for the fail-safe CPU, select "Hardware and software (only changes)".

   The safety program is now compiled.

Result

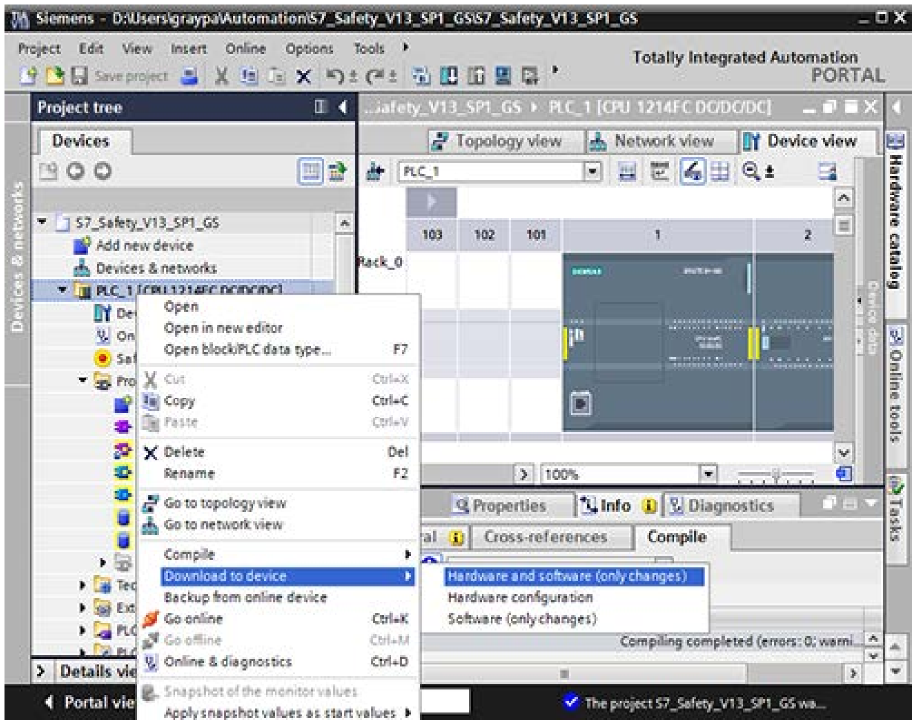
If compilation is successful, the result is always a consistent and executable safety program comprising all F-blocks with F-attributes. You are notified of this with the message "Safety program is consistent".

2.3.10 Step 13: Downloading the complete safety program to the fail-safe CPU and activating safety mode

In this step, you download the hardware configuration and the safety program to the fail-safe CPU.

Click the "Play" button to start the animation file. Click the other control elements to rewind, pause, go back, or go forward.

Procedure



1. In the "Project tree", select the fail-safe CPU.
2. In the shortcut menu for the fail-safe CPU, select "Hardware and software (only changes)". If an online connection to the fail-safe CPU does not yet exist, you will be prompted to establish this connection.
3. Select "Consistent download" in the "Action" column in each case.

Note

To download the entire safety program, the fail-safe CPU must be in STOP mode.

---

4. Click the "Load" button.

   Result: The "Load results" dialog is displayed.
5. Click the "Finish" button.
6. In the "Project tree", double-click "Safety Administration".
7. In the "Safety Administration" editor, check to see if the F-collective signatures of all F-blocks with F-attributes match online and offline to confirm whether your offline safety program blocks match what is in your connected CPU. You must be online in order to perform the signature comparison.
8. To activate safety mode, switch the fail-safe CPU from STOP to RUN mode.

   The Safety Administration editor displays the current safety mode status in the "General" area under "Safety Mode Status".

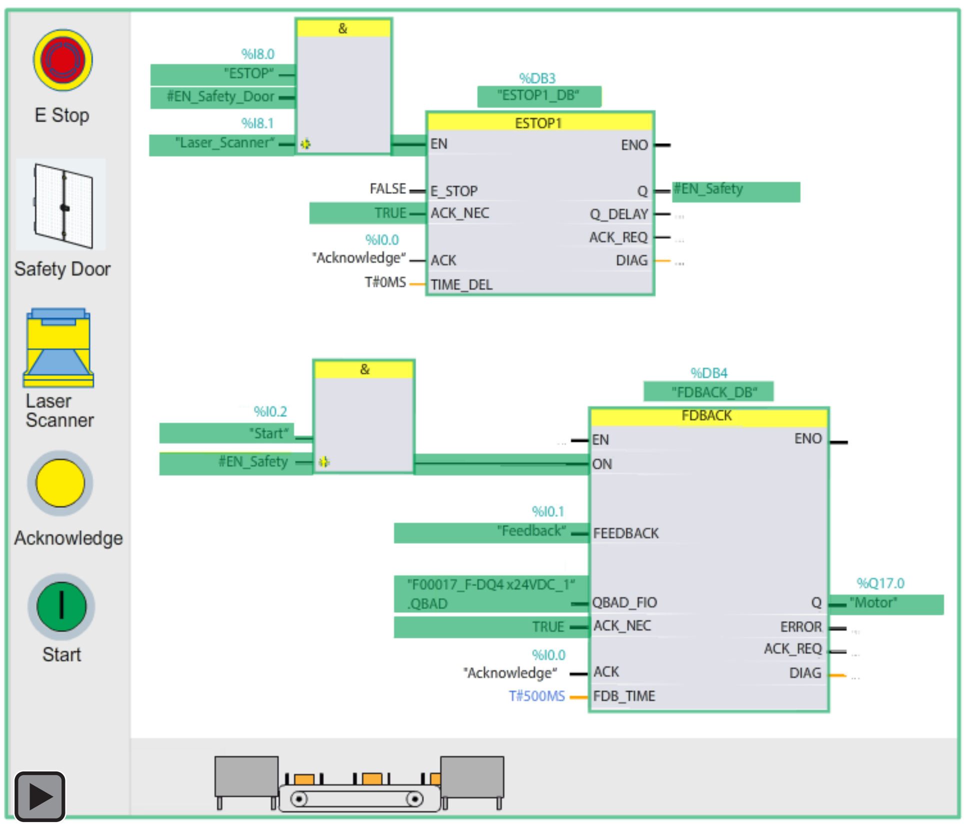
Note

Once a safety program has been created, you must perform a full function test according to your automation task (see SIMATIC Safety Configuring and Programming Manual (http://support.automation.siemens.com/WW/view/en/54110126/0/en)).

Result of programming

You have now finished creating the safety program according to the task definition of the example. In this interactive graphic, you can become familiar with the functions you just programmed.

Click the "Play" button to start the animation file and the control elements to operate the example. You can switch the Laser Scanner, E Stop, or Safety Door on and off to simulate an unsafe condition. However, you must press the "Acknowledge" button to notify the system that you have returned to a safe state. Then, you can press the "Start" button to operate the system again.



Fail-Safe signal module (SM) applications 3

This chapter presents typical application examples for connection of functional safety input and output channels, with a statement of the safety performance (SIL/Category/PL) that is possible for each example.

The PLC system typically contributes only a small part of the total probability of dangerous failure. The probability of dangerous failures of the sensors and actuators will typically be far larger than the PFH/PFD of the PLC system. Faults in the wiring system can also be a substantial contributor.

To achieve a targeted level of safety performance for each safety function, you must:

- Choose an appropriate architecture
- Choose sensors and actuators that are appropriately rated
- Provide a safety program that meets the requirements of the safety function
- Provide diagnostics and proof tests to maintain the ratings of the sensors and actuators
- Use wiring installation practices, diagnostics, and proof tests to assure wiring integrity
- Control operating and maintenance procedures for the lifetime of the installation

The S7-1200 Fail-Safe system provides a high level of internal diagnostic coverage. Diagnostic coverage of your external circuits, sensors, and actuators depends on your design choices using features of the PLC system and other measures.

The PFH/PFD of each S7-1200 fail-safe component is stated assuming no field proof test within the lifetime of the product. Sensors and actuators typically require regular proof tests to maintain an expected level of safety performance.

The reaction time of each safety function depends on the reaction time of each component, including the sensor, the PLC system, and the actuator. "Fail-Safe response times" (Page 197) gives further information on delay times through the PLC components. You must choose PLC parameters and external component reaction times to achieve a total safety reaction time goal.

In addition to total delay from safety demand input to safe actuator response, you must consider these additional time-related factors. Refer to "Fail-Safe response times" (Page 197) for exact information:

- To be assured of a safety response, a safety demand signal from the input sensor must last long enough to be seen by the safety program. Your configured filter time, discrepancy resolution time, short circuit test duration, and F-monitoring times all contribute to this time.

- The SM 1226 F-DQ 4 x 24 VDC provides ON test pulses to OFF switches, and OFF test pulses to ON switches, to test that the P and M switches respond. The OFF test pulse duration can be as long as your configured "Maximum readback time". The ON test pulse duration can be as long as your configured "Maximum readback time switch on test". The ON test pulse is only provided to one of the P or M switches at a time, but in the presence of single fault this could apply energy to your load. Your actuator should not respond to an OFF signal up to the "Maximum readback time" duration, or to an ON signal up to the "Maximum readback time switch on test" duration.
- Both the SM 1226 F-DQ 4 x 24 VDC and SM 1226 F-DQ 2 x Relay expect to complete and confirm any commanded transition from ON to OFF output state. After your program changes process output value from "1" to "0", you should not change the "0" back to a "1" until the F-DQ DC readback time or the F-RLY response time has completed. The affected output passivates on commanded "0" states that are too short to confirm.

WARNING

The safety performance of your installation depends on your design and continued maintenance of each complete safety function.

The S7-1200 fail-safe CPU and fail-safe signal modules provide components for logic processing with a certified level of safety integrity when used in accordance with ratings, specifications, and instructions.

Failure to comply with these guidelines could cause damage or unpredictable operation which could result in death or severe personal injury and/or property damage.

You must choose all components of your installation and complete your design and maintenance according to accepted safety standards and practices to achieve your required level of safety.

3.1 Digital input applications

You should consider the application modes presented here along with the features of the SM 1226 F-DI 16 x 24VDC as described in the overview. Refer to "SM 1226 F-DI 16 x 24 VDC" (Page 20).

These are the main features to keep in mind:

- You configure each channel as a 1oo1 or part of a 1oo2 evaluation pair.
- The corresponding channels from input bytes "a" and "b" (a.0, b.0), (a.1, b.1)...(a.7, b.7) form a 1oo2 channel group.
- Within this restriction, you can assign 1oo1 and 1oo2 in any order.
- Short-circuit testing requires use of the internal sensor supply. VS1 must be used with inputs a.0...a.7, and VS2 must be used with inputs b.0...b.7.
- If you enable the short-circuit test, both Vs1 and Vs2 are configured with the same parameters. All channels you configured for internal sensor supply will be subject to the same short-circuit test. You configure a test duration (length of dark time) and test interval (time between dark tests).
- The sensor supply is monitored to detect short-circuit or overload. It is cycled once on each power up to assure control and readback are working, and the readback is monitored during input short circuit tests.
- You configure a discrepancy time to identify unacceptable differences between 1oo2 inputs.
- You configure a filter time for each channel or each 1oo2 pair.

You can achieve Category 3 in 1oo1 configurations if you diagnose external wiring faults or exclude them according to standards by proper routing, protection, and proof testing of conductors:

- Each F-DI input includes sufficient diagnostics and redundant components such that no single internal fault can cause a dangerous failure.
- An appropriately-rated, single sensor can reach Category 3 by internal fault tolerance.
- The external wiring of a single sensor to a single input is vulnerable to single fault dangerous failure unless additional measures are applied.

You can achieve Category 4 in 1oo2 configurations if you diagnose external wiring faults or exclude them according to standards by proper routing, protection, and proof testing of conductors:

- With 1oo2 evaluation, a pair of F-DI inputs is not subject to dangerous internal failure within a reasonable number of accumulated internal faults.
- Appropriately-rated, external-paired sensors or equivalent redundancy can achieve Category 4.
- The duplicated external wiring of 2 sensors to 2 input points is vulnerable to accumulated fault dangerous failure unless additional measures are applied.

The F-DI is recommended for SIL 3/PL e only when 1oo2 evaluation is selected. A single high-integrity sensor can be rated up to SIL 3/PL e, but it should be wired and configured for 1oo2 evaluation for the channel to achieve SIL 3/PL e.

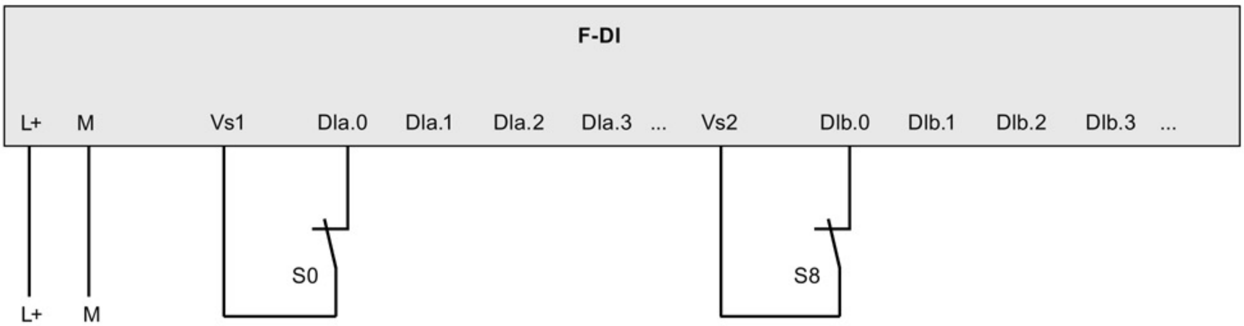
3.1.1 Selecting the digital input application

Input architectures for achieving Safety Integrity Level (SIL)/Category/Performance Level (PL)

Table 3- 1 Safety Integrity Level (SIL)/Category/Performance Level (PL) requirements

Application	Sensor supply	Sensor evaluation	Channel connection	Type of sensor connection	Achievable SIL/Category/PL	
					Without short-circuit detection	With short-circuit detection
1 and 2	Internal or External	1oo1 evaluation	Single input	1 channel	2/3/d	
3 and 4	Internal or External	1oo2 evaluation	Two inputs	2 channel equivalent	3/3/e	
5	Internal			2 channel equivalent	3/3/e	3/4/e
6	External				3/3/e	
7	Internal			2 channel - 3 wire non-equivalent	3/3/e	3/4/e
8	External				3/3/e	
9	Internal			2 channel - 4 wire non-equivalent	3/3/e	3/4/e
10	External				3/3/e	

3.1.2 Applications 1 and 2: 1oo1 evaluation of a single sensor



If short circuit detection is used, VS1 must be used with a.x inputs and VS2 must be used with b.x inputs.

Figure 3-1 F-DI Application mode 1: Internal sensor supply

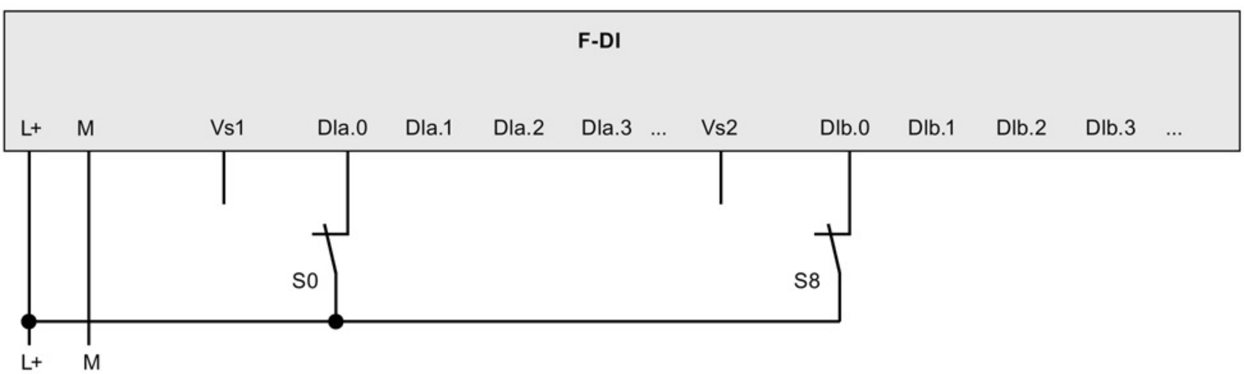


Figure 3-2 F-DI Application mode 2: External sensor supply

3.1.3 Applications 3 and 4: 1oo2 evaluation of a single sensor

You cannot configure short-circuit detection for this type of connection. Vs1 testing causes F-DI b.x inputs to fail.

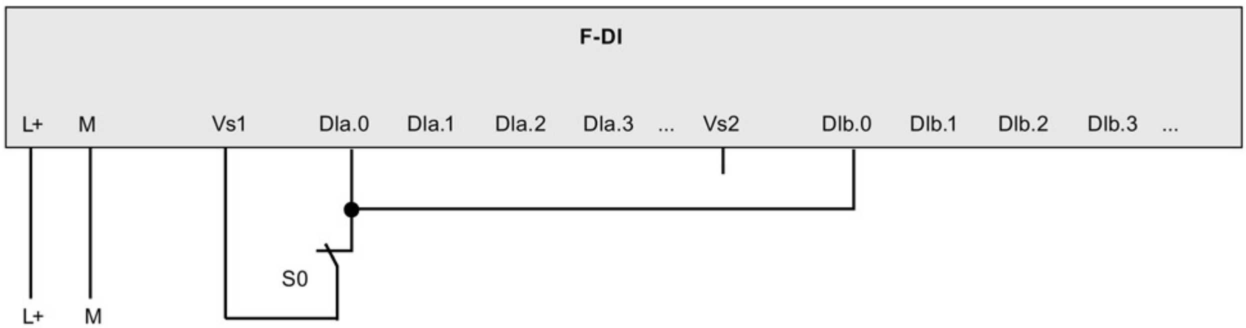


Figure 3-3 F-DI Application mode 3: Internal sensor supply

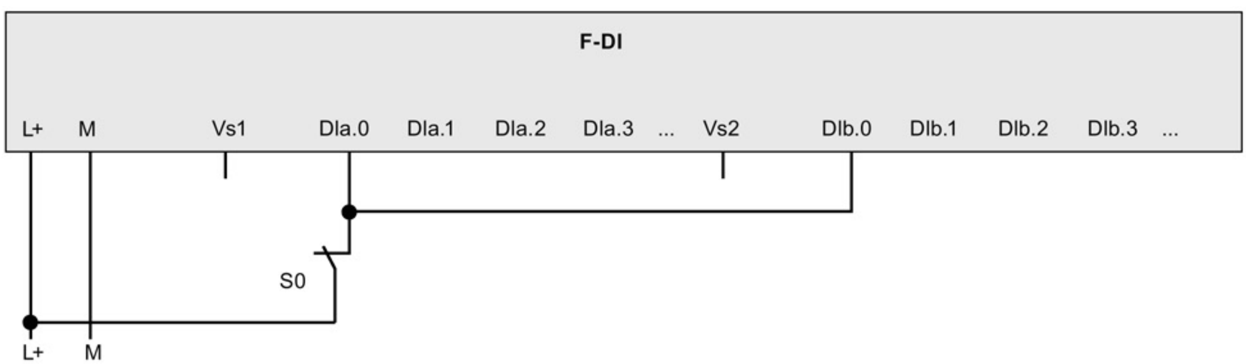


Figure 3-4 F-DI Application mode 4: External sensor supply

3.1.4 Applications 5 and 6: 1oo2 evaluation of independent equivalent sensors

S0 and S8 can be dual contacts of a single sensor.

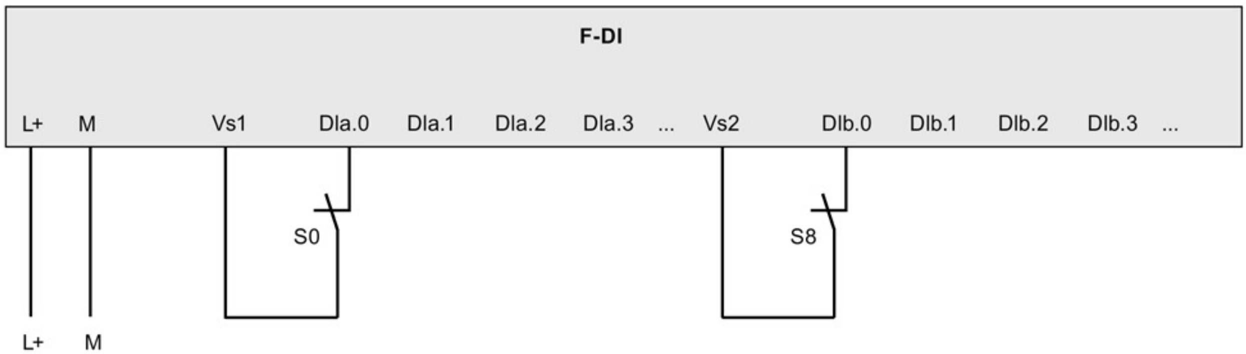


Figure 3-5 F-DI Application mode 5: Internal sensor supply

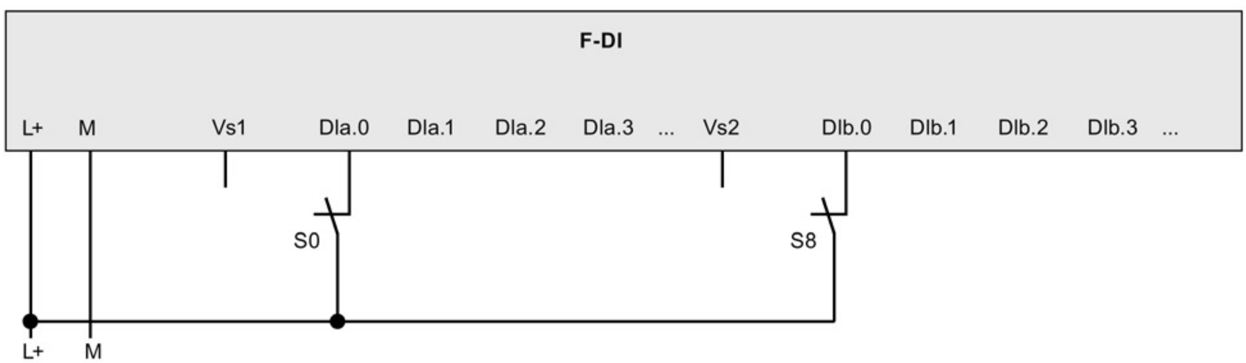


Figure 3-6 F-DI Application mode 6: External sensor supply

3.1.5 Applications 7 and 8: 1oo2 evaluation of 3-wire, non-equivalent sensor circuit

In non-equivalent mode, short-circuit testing can be enabled on a 3-wire circuit. The module expects that the logic "0" circuit will not change with the sensor dark test.

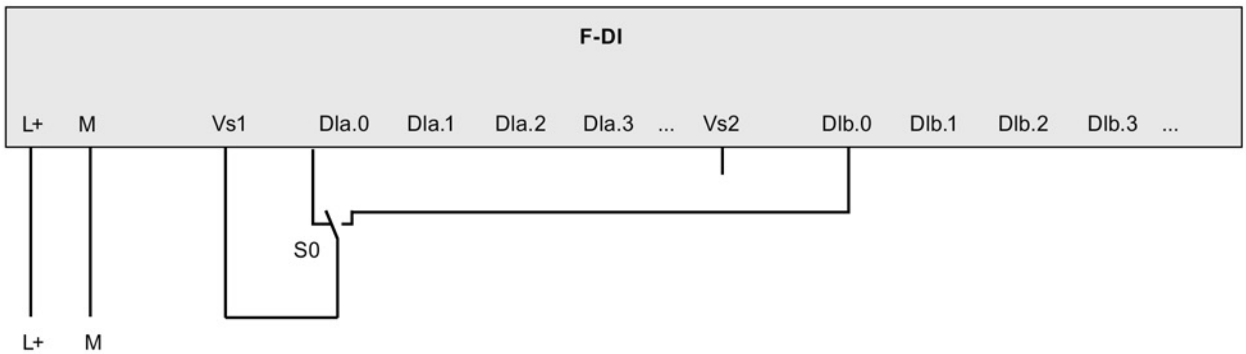


Figure 3-7 F-DI Application mode 7: Internal sensor supply

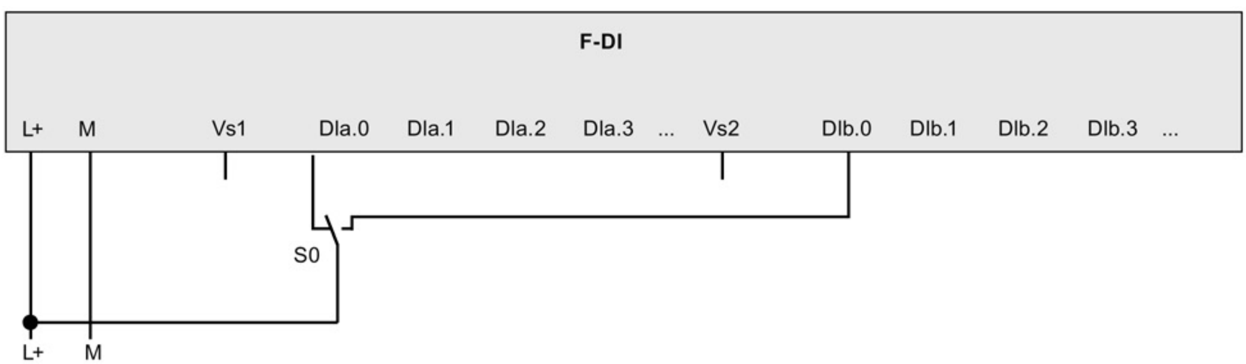


Figure 3-8 F-DI Application mode 8: External sensor supply

3.1.6 Applications 9 and 10: 1oo2 evaluation of 4-wire non-equivalent sensor circuit

S0 and S8 can be dual contacts of a single sensor.

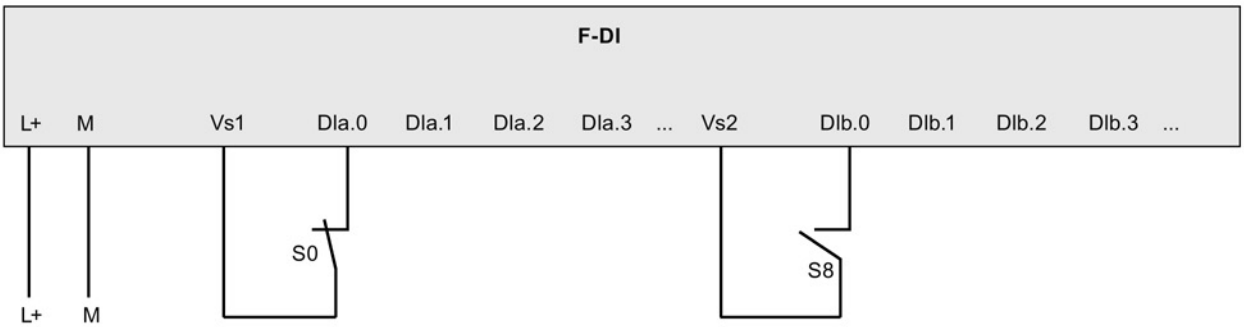


Figure 3-9 F-DI Application mode 9: Internal sensor supply

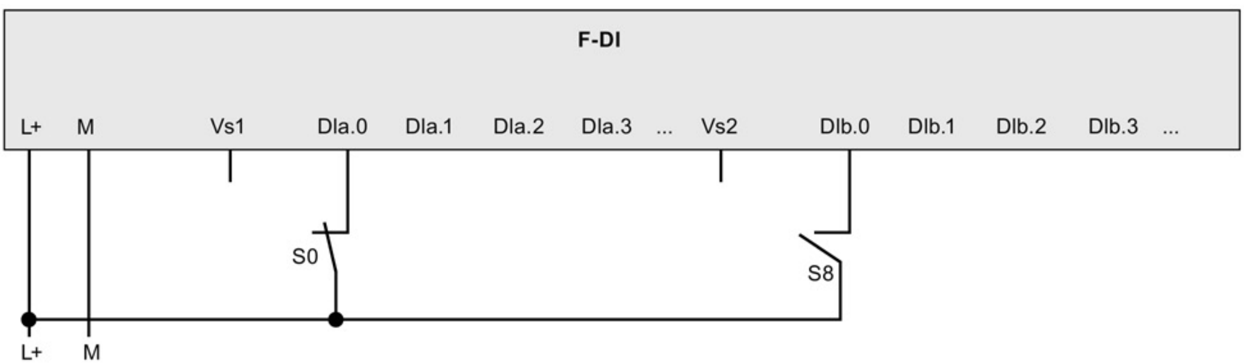


Figure 3-10 F-DI Application mode 10: External sensor supply

3.2 Digital output applications

You should consider the application modes presented here along with the features of the SM 1226 F-DQ 4 x 24 VDC and SM1226 F-DQ 2 x Relay as described in the overview. Refer to "SM 1226 F-DQ 4 x 24 VDC" (Page 21) and "SM 1226 F-DQ 2 x Relay" (Page 23).

These are the main features to keep in mind for the SM1226 F-DQ 4 x 24 VDC:

- The F-DQ DC separately controls current flow in the P (24 V to load) and M (load to common) sides of the circuit.
- The voltage at P and M outputs is read back to confirm proper state.
- The P and M switches are regularly tested with short ON and OFF pulses to confirm control.
- You must configure readback times that allow the external voltage to respond but do not cause your load to physically respond.
- Internal current limiting as described in the data sheet may be sufficient in combination with your 24 VDC supply, but you must consider whether additional current limits or fuses are necessary. Refer to Appendix A.3.3.3: "Specifications" (Page 178) (SM1226 F-DQ 4 x 24 VDC).

These are the main features to keep in mind for the SM1226 F-DQ 2 x Relay:

- The F-RLY controls each circuit with two independently-controlled series contacts.
- The series contacts are sequenced to avoid welding as a common cause failure.
- All internal relays include mechanically-linked sense contacts with read back.
- You must configure a maximum ON time for each channel, effectively the time between tests that the channel can be turned OFF. For SIL 3 applications, this time must be 30 days or less.
- There are two complete circuits for each process channel.
- The two circuits on each channel must be the same voltage category: both SELV/PELV or both line voltage
- Each circuit must be protected by an external fuse as defined in the data sheet.

All output channels are controlled as 1oo2 with cross-diagnostics.

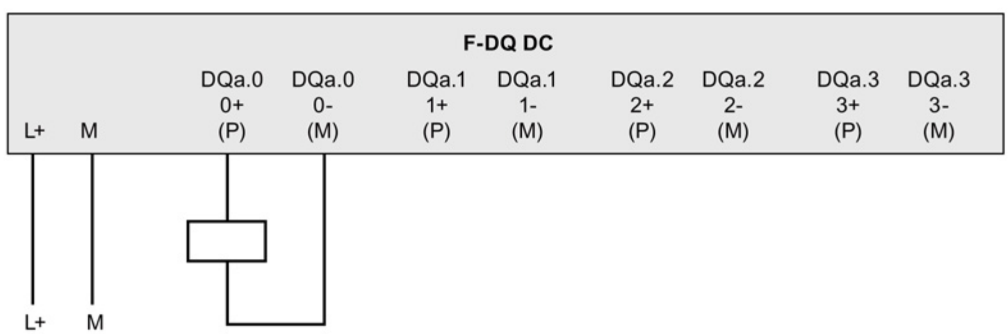
All applications shown are capable of reaching SIL 3/Category 4/PL e.

To reach Category 4, external contactors must be SIL-rated with sense contacts. You must read the sense contacts back and confirm the external relay response in your program. Siemens recommends using an F-DI input for sense contact and other safety diagnostic inputs.

3.2.1 Selecting the digital output application

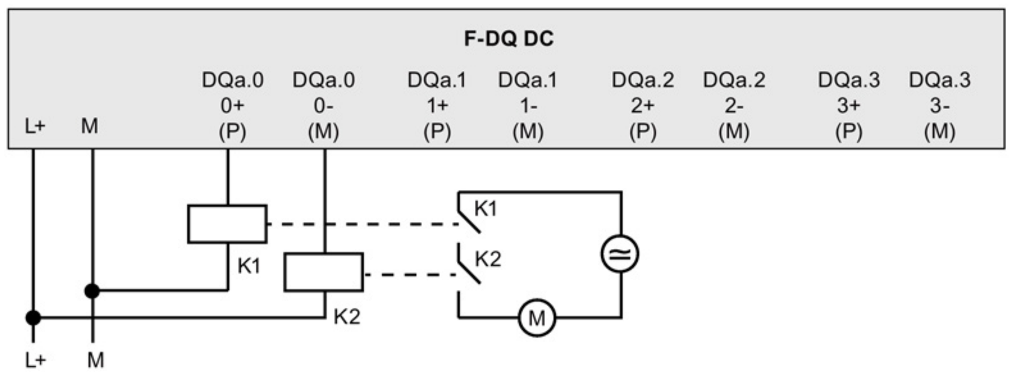
Application	Module	Description
1	DC	Directly-connected SIL-rated actuator
2	DC	External contactors: Separate P and M controlled contactors
3	DC	External contactors: Parallel connected between P and M
4	DC	External contactors: Separate output channels for each contactor
5	Relay	External contactors: Separate circuits of one output channel
6	Relay	Directly-connected SIL-rated actuator
7	Relay	Directly-connected SIL-rated actuator, switching both load conductors

3.2.2 Application 1: Wiring a directly-connected SIL-rated actuator

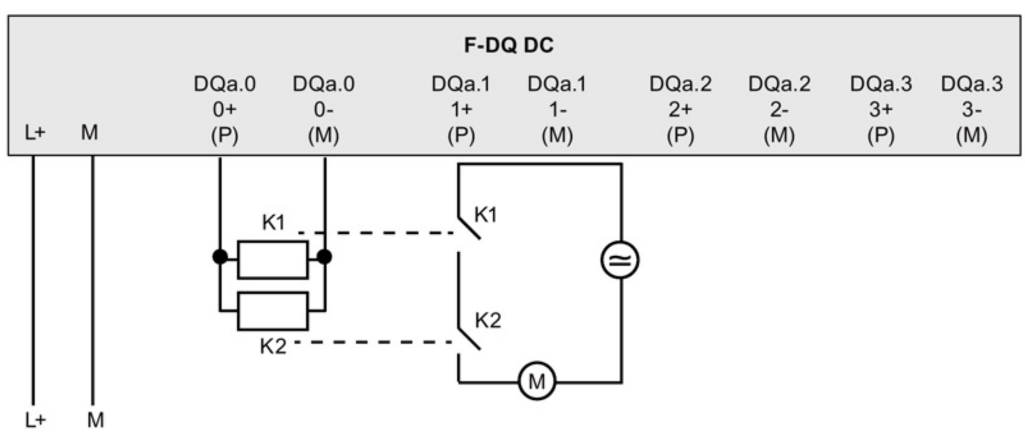


3.2.3 Application 2: Wiring external contactors: Separate P and M controlled contactors

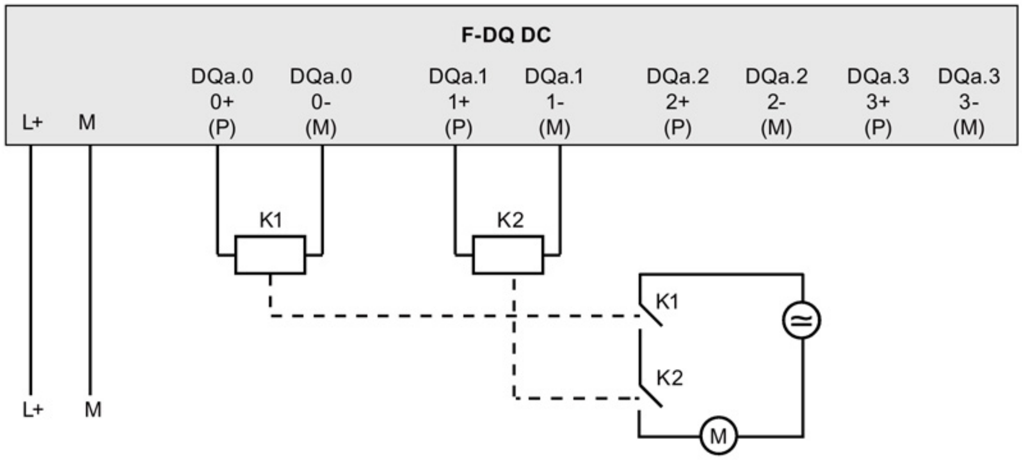
A short-circuit between the P and the M output can immediately lead to dangerous failure. You must prevent this failure mode by proper separation and protection of conductors.



3.2.4 Application 3: Wiring external contactors: Parallel connected between P and M

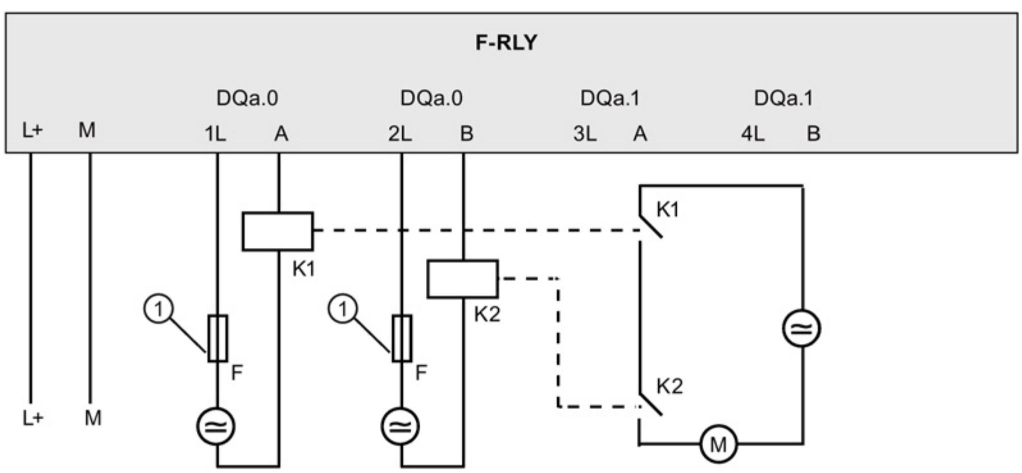


3.2.5 Application 4: Wiring external contactors: Separate P and M output channels for each contactor



3.2.6 Application 5: Separate circuits of a relay channel controlling external contactors

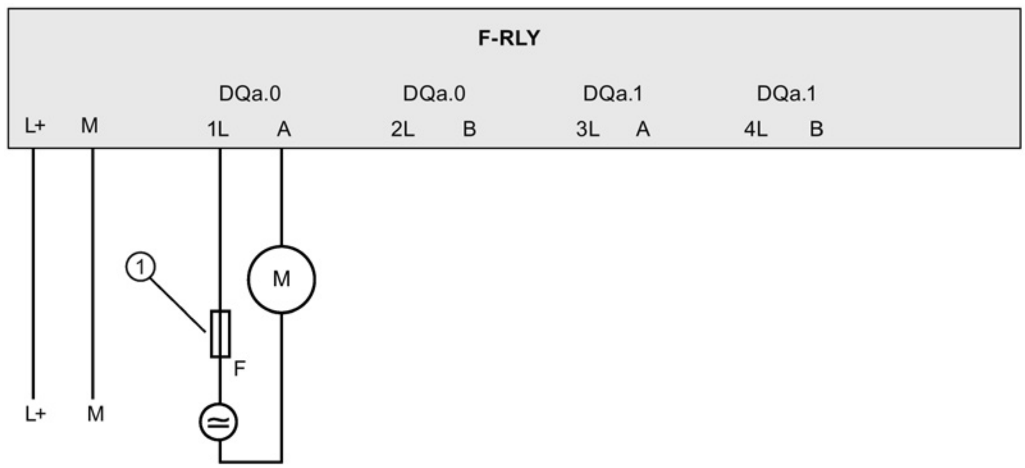
Redundant external relays or contactors are controlled by independent electrical circuits that are switched as a single process variable channel.



① External fuse

3.2.7 Application 6: Wiring a directly-connected SIL-rated actuator

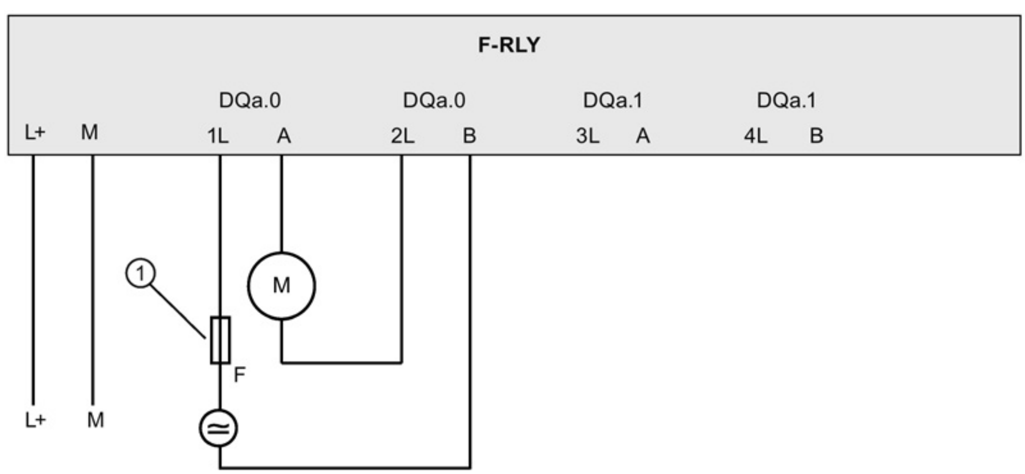
A short-circuit from 1L to A or equivalent fault can lead immediately to a dangerous failure. You must prevent this failure mode by proper separationand protection of conductors.



① External fuse

3.2.8 Application 7: Wiring a directly-connected SIL-rated actuator, switching both load conductors

By switching both conductors to the load, this arrangement provides extra protection for faults to power or ground in the external wiring that might energize the load device.

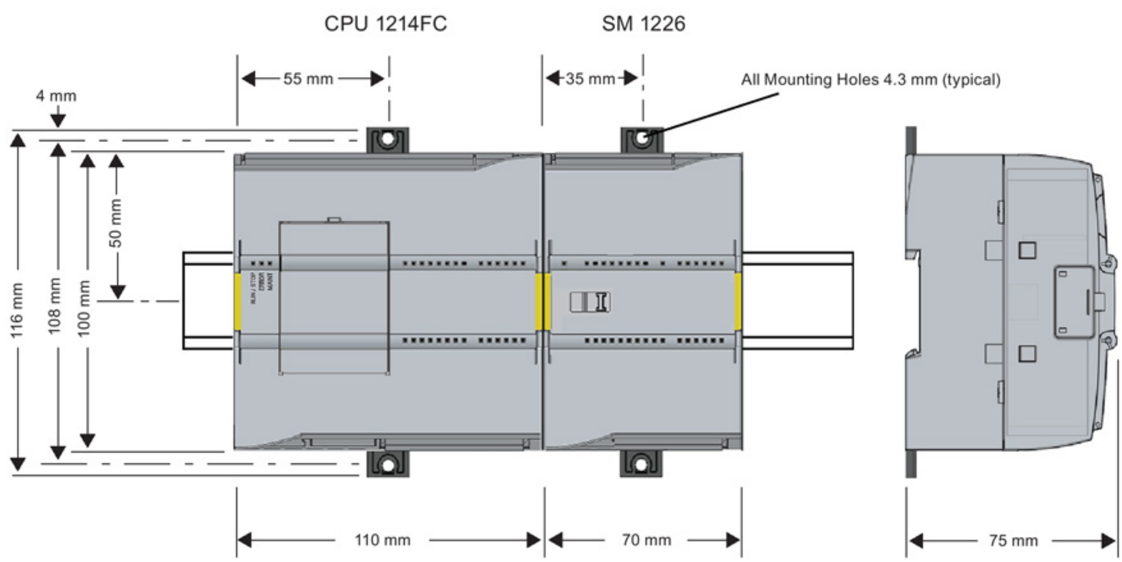


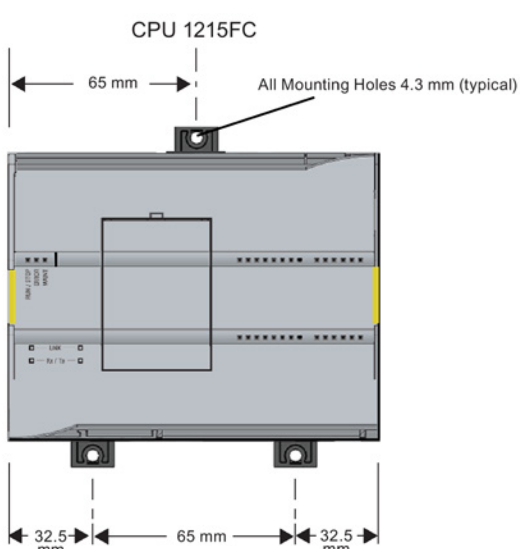
① External fuse

Fail-Safe CPU and signal module (SM) installation 4

4.1 S7-1200 Fail-Safe modules installation and removal

4.1.1 Mounting dimensions for S7-1200 Fail-Safe modules





4.1.2 Guidelines for installing S7-1200 Fail-Safe devices

The S7-1200 equipment is designed to be easy to install. You can install an S7-1200 either on a panel or on a standard rail. The S7-1200 assembly can be oriented either horizontally or vertically. The small size of the S7-1200 allows you to make efficient use of space.

Expansion module installation rules:

- Standard and fail-safe signal modules (SM) are installed on the right side of a CPU. Fail-safe CPUs allow a maximum of 8 signal modules, if the total of all expansion module CPU loads does not exceed the CPU's 5 VDC and 24 VDC power supply load limits. Fail-safe and standard modules may be intermixed on the right side of the CPU.
- Communication modules (CM), are installed on the left side of the CPU. Fail-safe CPU's allow a maximum of 3 communication modules, if the total of all expansion module loads does not exceed the CPU's 5 VDC and 24 VDC power load limits.
- Signal boards (SB), communications boards (CB), and battery boards (BB) are installed on top of the CPU. A maximum of 1 signal board, communication board, or battery board is allowed for any CPU.

The S7-1200 standard signal modules (SM), communication modules (CM), and signal boards (SB) can be used in the same system with fail-safe SMs to complete your application control functions that do not require a rated Safety Integrity Level (SIL). Standard SMs that are supported for use with fail-safe SMs have the MLFB numbers (6ES7 --- ---32 0XB0).

The S7-1200 fail-safe CPUs do not support PROFIBUS or PROFINET distributed fail-safe I/O.

Electrical equipment standards classify the SIMATIC S7-1200 system as Open Equipment. You must install the S7-1200 in a housing, cabinet, or electric control room. You should limit entry to the housing, cabinet, or electric control room to authorized personnel.

The installation should provide a dry environment for the S7-1200. SELV/PELV circuits are considered to provide protection against electric shock in dry locations.

The installation should provide mechanical and environmental protection that is approved for open equipment in your particular location category according to applicable electrical and building codes.

Conductive contamination due to dust, moisture, and airborne pollution can cause operational and electrical faults in the PLC.

If you locate the PLC in an area where conductive contamination may be present, the PLC must be protected by an enclosure with appropriate protection rating. IP54 is one rating that is generally used for electronic equipment enclosures in dirty environments and may be appropriate for your application.

> ⚠ WARNING
>
> **Improper installation of the S7-1200 can result in electrical faults or unexpected operation of machinery.**
>
> Electrical faults or unexpected machine operation can result in death, severe personal injury, and/or property damage.
>
> All instructions for installation and maintenance of a proper operating environment must be followed to ensure the equipment operates safely.

Separate the S7-1200 devices from heat, high voltage, and electrical noise

As a general rule for laying out the devices of your system, always separate the devices that generate high voltage and high electrical noise from the low voltage, logic devices such as the S7-1200.

When designing the layout of an S7-1200 inside your panel, consider the heat generating devices and locate electronic devices in the cooler areas of your cabinet. Reducing the exposure to a high temperature environment extends the operating life of any electronic device.

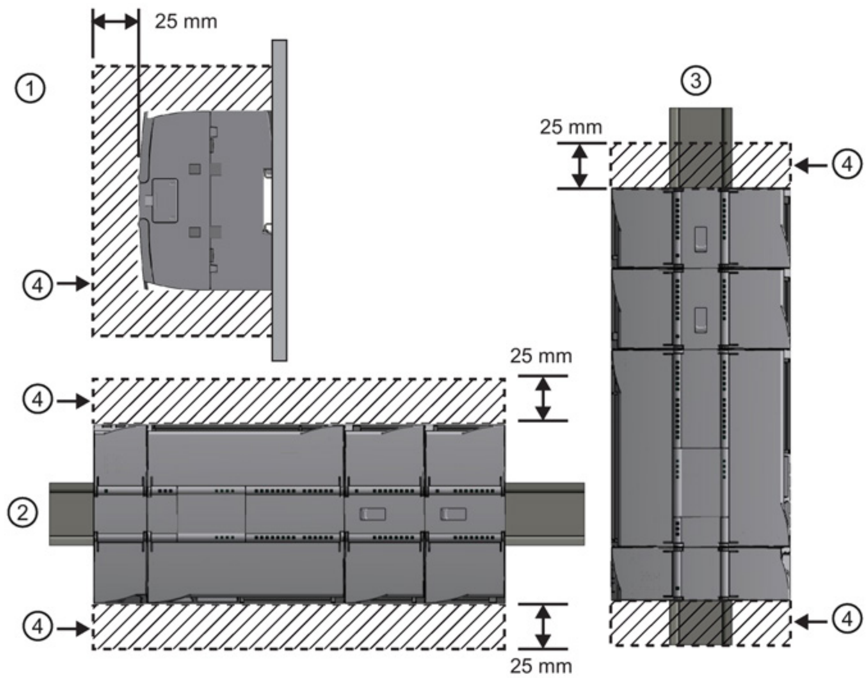
Consider also the routing of the wiring for the devices in the panel. Avoid placing low voltage signal wires and communications cables in the same tray with AC power wiring and high energy, rapidly switched DC wiring.

Provide adequate space for cooling and wiring

S7-1200 devices are designed for natural convection cooling. For proper cooling, you must provide a clearance of at least 25 mm above and below the devices. Also, allow at least 25 mm of space between the front of the modules and the inside of the enclosure.

> ⚠ CAUTION
>
> **For vertical mounting, the maximum allowable ambient temperature is reduced by 10 degrees C.**
>
> Orient a vertically mounted S7-1200 system as shown in the following figure.
>
> Ensure that the S7-1200 system is mounted correctly.

When planning your layout for the S7-1200 system, allow enough clearance for the wiring and communications cable connections.

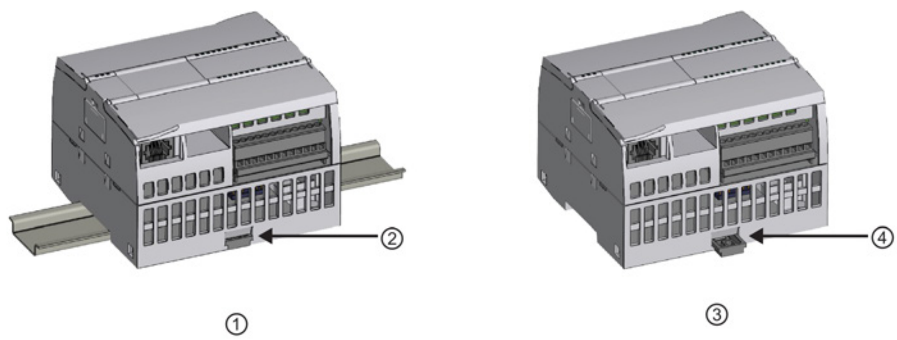


①	Side view	③	Vertical installation
②	Horizontal installation	④	Clearance area

4.1.3 Installation and removal safety rules

Installing and removing the S7-1200 devices

The CPU can be easily installed on a standard DIN rail or on a panel. DIN rail clips are provided to secure the device on the DIN rail. The clips also snap into an extended position to provide a screw mounting position for panel-mounting the unit.



①	DIN rail installation	③	Panel installation
②	DIN rail clip in latched position	④	Clip in extended position for panel mounting

Before you install or remove any electrical device, ensure that the power to that equipment has been turned off. Also, ensure that the power to any related equipment has been turned off.

⚠ WARNING
Installation or removal of S7-1200 or related equipment, with the power applied, could cause electric shock or unexpected operation of equipment. Failure to disable all power to the S7-1200 and related equipment during installation or removal procedures could result in death, severe personal injury and property damage due to electric shock or unexpected equipment operation. Always follow appropriate safety precautions and ensure that power to the S7-1200 is disabled before attempting to install or remove S7-1200 CPUs and related equipment.

Always ensure that whenever you replace or install an S7-1200 device you use the correct module or equivalent device.

WARNING

Incorrect installation of an S7-1200 module may cause the program in the S7-1200 to function unpredictably.

Failure to replace an S7-1200 device with the same model, orientation, or order could result in death, severe personal injury and property damage due to unexpected equipment operation.

Replace an S7-1200 device with the same model, and be sure to orient and position the module correctly.

WARNING

Do not disconnect equipment when a flammable or combustible atmosphere is present.

Disconnection of equipment when a flammable or combustible atmosphere is present may cause a fire or explosion which could result in death, serious injury and property damage.

Always follow appropriate safety precautions when a flammable or combustible atmosphere is present.

Note

Electrostatic discharge can damage the device or the receptacle on the CPU.

Make contact with a grounded conductive pad or wear a grounded wrist strap whenever you handle the device.

4.1.4 Installing and removing an S7-1200 FC CPU

You can install the CPU on a panel or on a DIN rail.

Note

Attach any communication modules to the CPU and install the assembly as a unit. Install signal modules separately after the CPU has been installed.

Set up the CPU rail clips:

- **For DIN rail mounting**, make sure the upper DIN rail clip is in the latched (inner) position and lower DIN rail clip is in the unlatched (extended) position, for both CPU and attached CMs.
  - After installing the devices on the DIN rail, move the lower DIN rail clips to the latched position to lock the devices on the DIN rail.
- **For panel mounting**, make sure the DIN rail clips are pushed to the extended position.

To install the CPU on a panel, follow these steps:

1. Locate, drill, and tap the mounting holes (M4), using the dimensions shown in the mounting dimensions table (Page 79).
2. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power.
3. Extend the mounting clips from the module. Make sure the DIN rail clips on the top and bottom of the CPU are in the extended position.
4. Secure the module to the panel, using a pan head M4 screw with spring and flat washer. Do not use a counter-sink screw with beveled head. Apply only enough torque to flatten the spring washer.

Note

If your system is subject to a high vibration environment or is mounted vertically, then panel mounting the S7-1200 is recommended.

Table 4- 1 Installing the CPU on a DIN rail

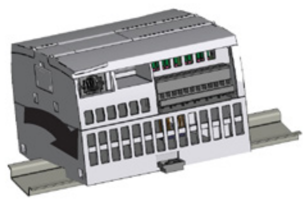
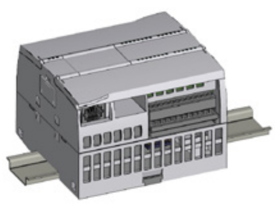
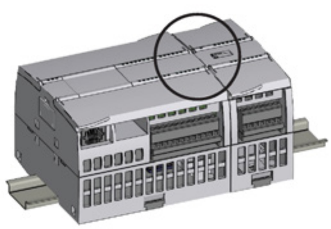
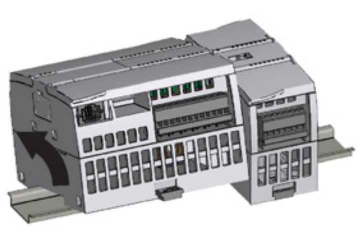
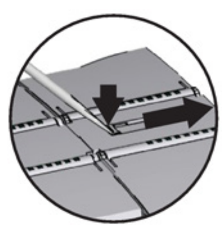
Task	Procedure
 	1. Install the DIN rail. Secure the rail to the mounting panel every 75 mm. 2. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 3. Hook the CPU over the top of the DIN rail. 4. Pull out the DIN rail clip on the bottom of the CPU to allow the CPU to fit over the rail. 5. Rotate the CPU down into position on the rail. 6. Push in the clips to latch the CPU to the rail.

Table 4- 2 Removing the CPU from a DIN rail

Task	Procedure	
 		1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Disconnect the I/O connectors, wiring, and cables from the CPU. Refer to the terminal block removal instructions (Page 89). 3. Remove the CPU and any attached communication modules as a unit. All signal modules should remain installed. 4. If an SM is connected to the CPU, then retract the bus connector: – Place a screwdriver beside the tab on the top of the signal module. – Press down to disengage the connector from the CPU. – Slide the tab fully to the right. 5. Remove the CPU: – Pull out the DIN rail clip to release the CPU from the rail. – Rotate the CPU up and off the rail, and remove the CPU from the system.

4.1.5 Installing and removing a signal module (SM)

Table 4- 3 Installing an SM

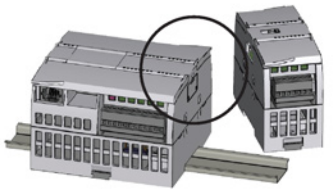
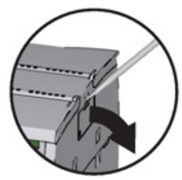
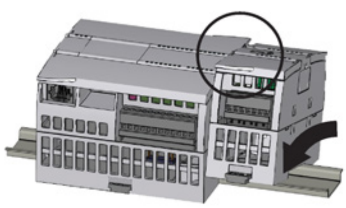
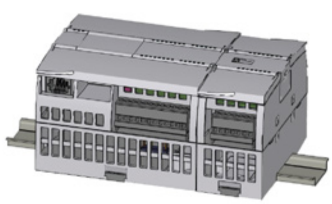
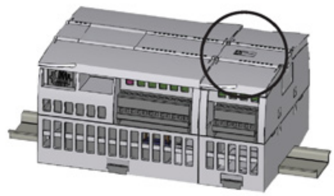
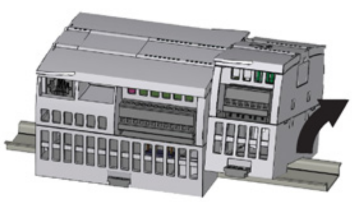
Task	Procedure	
		Install your SM after installing the CPU. 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Remove the cover for the connector from the right side of the CPU. – Insert a screwdriver into the slot above the cover. – Gently pry the cover out at its top and remove the cover. Retain the cover for reuse.
		Connect the SM to the CPU: 1. Position the SM beside the CPU. 2. Hook the SM over the top of the DIN rail. 3. Pull out the bottom DIN rail clip to allow the SM to fit over the rail. 4. Rotate the SM down into position beside the CPU and push the bottom clip in to latch the SM onto the rail.
	Extending the bus connector makes both mechanical and electrical connections for the SM. 1. Place a screwdriver beside the tab on the top of the SM. 2. Slide the tab fully to the left to extend the bus connector into the CPU. Follow the same procedure to install a signal module to a signal module.	

Table 4- 4 Removing an SM

Task	Procedure
 	You can remove any SM without removing the CPU or other SMs in place. 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Remove the I/O connectors and wiring from the SM. Refer to the terminal block removal instructions (Page 89). 3. Retract the bus connector. – Place a screwdriver beside the tab on the top of the SM. – Press down to disengage the connector from the CPU. – Slide the tab fully to the right. When another SM is connected on the right, repeat this procedure for that SM.
	Remove the SM: 1. Pull out the bottom DIN rail clip to release the SM from the rail. 2. Rotate the SM up and off the rail. Remove the SM from the system. 3. If required, cover the bus connector on the CPU to avoid contamination. Follow the same procedure to remove a signal module from a signal module.

4.1.6 Removing and reinstalling the S7-1200 terminal block connector

CPUs, signal boards (SB) and signal modules (SM) have removable connectors to make wiring easy.

Table 4- 5 Removing terminal blocks (CPU example)

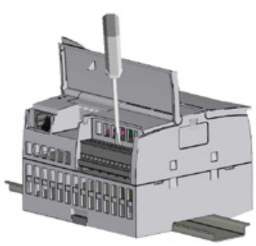
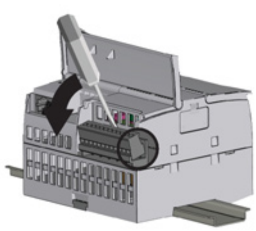
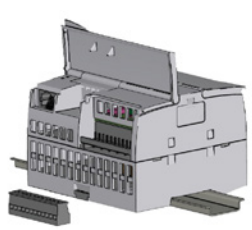
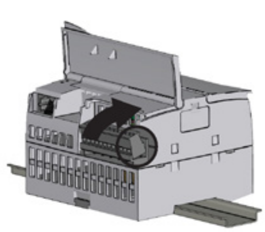
Task	Procedure
	Prepare the system for terminal block connector removal by removing the power from the CPU and opening the cover above the connector. 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Inspect the top of the connector and locate the slot for the tip of the screwdriver. 3. Insert a screwdriver into the slot. 4. Gently pry the top of the connector away from the CPU. The connector releases with a snap. 5. Grasp the connector and pull away from the CPU.
	

Table 4- 6 Installing the connector

Task	Procedure
	Prepare the components for terminal block installation by removing power from the CPU and opening the cover for connector. 1. Ensure that the CPU and all S7-1200 equipment are disconnected from electrical power. 2. Align the connector with the pins on the unit. 3. Align the wiring edge of the connector inside the rim of the connector base. 4. Press firmly down and rotate until the connector snaps into place. Check carefully to ensure that the connector is properly aligned and fully engaged.
	

4.2 Fail-Safe system electrical design rules

4.2.1 Safe functional extra low voltage requirement (power supplies and other system components)

> **WARNING**
>
> **Fail-safe modules must be operated with safe functional extra-low voltage (SELV, PELV) power sources.**
>
> To maintain safe S7-1200 low voltage circuits, external connections to communications ports, analog circuits, 24 VDC nominal power supplies, and I/O circuits must be powered from approved sources that meet the requirements of SELV, PELV, Class 2, Limited Voltage, or Limited Power according to various standards.
>
> The external power supply should limit the maximum voltage to 35 VDC even under fault conditions. Please consult the manufacturer's data for the power supplies that you use.

Maximum applied voltage to S7-1200 Fail-Safe devices

- Operational voltage: The fail-safe CPU and fail-safe signal modules operational voltage is 20.4 VDC - 28.8 VDC, 35 VDC surge for 0.5 second. Operation of the unit to specifications is assured by design and testing. Defined transients from defined source impedances per EN 61000-4-2, 61000-4-4, 61000-4-6, as specified in the data sheet for each product, may be imposed on this voltage without disrupting operation or causing damage. Sustained operation in the range of 28.8 - 35 VDC can result in unacceptable temperature rise and thermal damage, causing the product to become inoperable.
- Absolute maximum rating regarding supply voltage: The absolute maximum rating to prevent module damage and to ensure the functional safety of the modules is 35 VDC. Only use SELV / PELV power supplies, connected directly or through field devices, with the fail-safe CPU and fail-safe signal modules. These power supplies must be specified by the manufacturer to limit the output voltage to 35 VDC or less under fault conditions. Otherwise, external protection must be supplied that will reliably open the circuit or limit the output voltage to less than 35 VDC to the CPU and signal modules.
- Surge immunity: Wiring systems subject to surges from lightning strike coupling must be equipped with external protection. This protection must be sufficient to clamp surge voltages and/or open the supply circuit to assure the PLC system is not exposed to voltages greater than 35 VDC. One specification for evaluation of protection from lightning type surges is found in EN 61000-4-5, with operational limits established by EN 61000-6-2. S7-1200 DC fail-safe CPUs and fail-safe signal modules require external protection to maintain safe operation when subject to surge voltages defined by this standard. Refer to Appendix A.1: "General technical specifications (Page 132)", "Surge immunity" for further information.

> **WARNING**
>
> **All power supply and fail-safe signal module circuits must be connected together to a common voltage reference or must be isolated SELV circuits.**
>
> The power supply M terminals on the fail-safe CPU and the fail-safe SMs must be connected together or isolated as SELV. Failure to do so can result in unexpected machine or process operation, which may cause death or serious injury to personnel, and/or damage to equipment.
>
> Connecting all M terminals together or isolating with approved SELV isolation prevents unwanted current flows in the event of a single fault in the CPU to SM isolation boundary.

4.2.2 Power budget

4.2.2.1 Connecting power to the S7-1200 system

Fail-safe CPUs require an external SELV/PELV 24 VDC power supply for the CPU's 24 VDC power input (the 24 VDC L+ and M terminals, with an **arrow pointing into** the CPU module). The external 24 VDC supply powers the CPU's internal 5 VDC supply that provides power for the CPU, signal modules (SM), signal board (SB), and communication modules (CM). 24 VDC power is available at the CPU's 24 VDC power output (the 24VDC L+ and M terminals, with an **arrow pointing out of** the CPU module).

Note

Sensor supply connections for safety inputs

If you want to use a sensor supply source from the PLC for safety inputs, you should use the sensor supply provided on the fail-safe DI signal modules.

The purpose of a power budget calculation is to ensure that the power requirements of all CPU powered elements (fail-safe CPU, fail-safe SM, standard SM, and CM) do not exceed the available CPU power:

- You may not be able to connect the maximum number of signal modules and communication modules, if you exceed the CPU's 5 VDC power output capability.
- You may need to use external 24 VDC power for some system elements, if you exceed the CPU's 24 VDC power output capability.

Note

Power limits for 5 VDC and 24 VDC supplied from a fail-safe CPU.

Exceeding the power budget of the CPU may result in not being able to connect the allowed maximum number of add-on modules.

Refer to the technical specifications for information about power input requirements (CPUs, SMs, SBs, and CMs) and CPU power output limits (5 VDC and 24 VDC).

Refer to the "Calculating a power budget" (Page 94) to determine CPU power output capability.

Expansion module installation rules:

- Standard and fail-safe signal modules (SM) are installed on the right side of the CPU. Fail-safe CPUs allow a maximum of 8 signal modules, if the total of all add-on module CPU loads does not exceed the CPU's 5 VDC and 24 VDC power supply load limits. Fail-safe and standard modules may be intermixed on the right side of the CPU.
- Communication modules (CM), are installed on the left side of the CPU. A maximum of 3 communication modules is allowed for a Fail-safe CPU, if the total of all add-on module CPU loads does not exceed the CPU's 5 VDC and 24 VDC load limits.
- Signal boards (SB), communications boards (CB), and battery boards (BB) are installed on top of the CPU. A maximum of one signal board, communication board, or battery board is allowed for any CPU.

WARNING

Do not connect separate power supplies directly in parallel.

This can cause a conflict between the power supplies, as each supply tries to establish its preferred output voltage level.

The result of this conflict can be shortened lifetime or the immediate failure of one or both power supplies, with consequent unpredictable operation of the PLC system. Unpredictable operation could result in death, severe personal injury and property damage.

A CPU 24 VDC supply and any external power supply should provide power to different load points.

For improved electrical noise protection, the commons (M) of the different power supplies should be connected.

Some of the 24 VDC power inputs in an S7-1200 system are interconnected, with a common logic circuit connecting multiple M terminals. For example, the following circuits are interconnected when designated as "not isolated" in the technical specifications: the 24 VDC power supply of the CPU, the power input for the relay coil of an SM, or the power supply for a non-isolated analog input. All non-isolated M terminals must connect to the same external reference potential.

WARNING

Connecting non-isolated M terminals to different reference potentials will cause unintended current flows that may cause damage or unpredictable operation in the PLC and any connected equipment.

Failure to comply with this guideline could cause damage or unpredictable operation which could result in death or severe personal injury and property damage.

Always ensure that all non-isolated M terminals in an S7-1200 system are connected to the same reference potential.

4.2.2.2 Calculating a sample power requirement

CPU power budget calculation for example system

The following example shows the power requirements for a system that includes:

Quantity	Module	Module type
1	CPU 1214FC DC/DC/Relay	Fail-safe CPU with 14 standard (not fail-safe) digital inputs and 10 standard (not fail-safe) digital outputs
1	SB 1223 2 x 24 VDC Input/ 2 x 24 VDC Output	Standard I/O signal board with 2 digital inputs
1	CM 1241 RS422/485	Communication module
1	SM 1226 F-DI 16 x 24 VDC	Fail-safe signal module with 16 digital inputs
1	SM 1226 F-DQ 4 x 24 VDC	Fail-safe signal module with 4 digital outputs
1	SM 1226 F-DQ 2 x Relay	Fail-safe signal module with 2 relay outputs
3	SM 1223 8 DC In/8 Relay Out	Standard signal module with 8 digital inputs and 8 relay outputs

This example system uses a total of 56 inputs and 40 outputs with a mix of standard and fail-safe I/O. If a digital input channel is disconnected and not used, then that input is excluded from the power calculation.

The current supply and consumption numbers are obtained from each module's technical specifications.

The example budget shows inadequate 24VDC CPU power

An external 24 VDC power supply is necessary to supply a fail-safe CPU's L+ and M input terminals (with the arrow symbol pointing into the CPU). In the example, fail-safe SM 24 VDC loads are also connected to the external power supply. Other devices in your system may connect to the external 24 VDC supply. You must ensure that the external supply has sufficient power available. A total external power load calculation is not described in the example. The purpose of the example is to verify sufficient power is available for loads that are supplied directly from the CPU.

The fail-safe CPU in this example provides sufficient 5 VDC current for all add-on modules, but insufficient 24 VDC current for all of the standard digital inputs and outputs. The fail-safe SMs connect to a 24 VDC external supply which moves their 24 VDC loads off of the CPU power budget calculation.

The example system requires 424 mA at 24 VDC from the fail-safe CPU, but the CPU can provide only 400 mA. This result requires moving at least 24 mA of the 24 VDC CPU load, to the external 24 VDC power supply. A solution would be to move the 24 VDC power connections for the 24 standard relay outputs, from the CPU to the external power supply. This action would reduce the CPU 24 VDC load by 264 mA.

Note

The power required to drive the fail-safe CPU's internal relay coils is already allocated. Do not include the internal relay power requirements in a power budget calculation.

Table 4- 7 Sample power budget

	5 VDC distributed by internal bus when modules are installed	24 VDC distributed by connection to fail-safe CPU terminals L+ and M, (identified by arrow pointing away from the fail-safe CPU)	24 VDC supplied by connection to external power supply (separate external supply power budget required)
CPU 1214FC DC/DC/Relay maximum output current	1600 mA	400 mA	Obtain maximum current rating from the external power supply manufacturer
		Minus	
System components	**5 VDC CPU loads**	**24 VDC CPU loads**	**24 VDC external power supply loads**
CPU 1214FC, 14 X 24 VDC		14 standard inputs located on the CPU: 14 * 4 mA = 56 mA	
1 SB 1223, 2 X 24 VDC	50 mA	2 standard inputs located on a signal board: 2 * 4 mA = 8 mA	
1 CM 1241 RS422/485	220 mA		
1 SM 1226 F-DI 16 x 24 VDC	155 mA		Module plus 16 fail-safe inputs (8 paired channels): 130 mA + 16 * 6 mA = 226 mA
1 SM 1226 F-DQ 4X 24 VDC	125 mA		4 fail-safe digital outputs: 170 mA + load current for all 4 P-switches + Vs1/Vs2 load current
1 SM 1226 F-DQ 2 X relay	120 mA		2 fail-safe relay outputs: 300 mA
3 SM 1223 DI 8 x 24 VDC, DQ 8 x Relay	3 * 145 mA = 435 mA	24 standard digital inputs: 3 * 8 * 4 mA = 96 mA 24 standard relay outputs: 3 * 8 * 11 mA = 264 mA	
Total requirements	1105 mA	424 mA	
		Equals	
Current balance	**5 VDC CPU power**	**24 VDC CPU power**	**24 VDC external power**
Current balance total	495 mA	(24 mA)	

4.2.2.3 Calculating your power requirement

Form for calculating your power budget

Use the following table to determine how much power (current) is available from the fail-safe CPU and how much is needed by the central rack modules for your system. Refer to the technical specifications in this manual for the power ratings of your fail-safe CPU model (1214FC (Page 149) or 1215FC (Page 160)) and the power requirements of the fail-safe digital input and output signal modules (SM 1226 F-DI 16 x 24 VDC (Page 172), SM 1226 F-DQ 4 x 24 VDC (Page 178), or SM 1226 F-DQ 2 x Relay (Page 185)). Refer to the technical specifications in the S7-1200 Programmable Controller System Manual (http://support.automation.siemens.com/WW/view/en/91696622) for details about standard S7-1200 modules.

Table 4- 8 CPU power budget

	5 VDC distributed by internal bus when modules are installed	24 VDC distributed by connection to fail-safe CPU terminals L+ and M, (identified by arrow pointing away from the fail-safe CPU)	24 VDC supplied by connection to external power supply (separate external supply power budget required)
	Minus		
System components	**5 VDC CPU loads**	**24 VDC CPU loads**	**24 VDC external power supply loads**
Total requirements			
	Equals		
Current balance	**5 VDC CPU power**	**24 VDC CPU power**	**24 VDC external power**
Current balance total			

4.2.3 Fail-Safe module electrical characteristics and terminal assignments

Refer to the respective technical specifications chapter for details about electrical characteristics and terminal assignments.

CPU 1214FC	CPU1215FC
Specifications (Page 149) Wiring diagram (Page 156)	Specifications (Page 160) Wiring diagram (Page 168)

SM 1226 F-DI 16 x 24 VDC	SM 1226 F-DQ 4 x 24 VDC	SM 1226 F-DQ 2 x Relay
Specifications (Page 172) Wiring diagram (Page 175)	Specifications (Page 178) Wiring diagram (Page 183)	Specifications (Page 185) Wiring diagram (Page 190)

4.3 Control system wiring guidelines

4.3.1 Guidelines for grounding and wiring

Proper grounding and wiring of all electrical equipment is important to provide electrical noise protection for your application and the S7-1200. Refer to the technical specifications (Page 132) for the S7-1200 wiring diagrams.

Prerequisites

Before you ground or install wiring to any electrical device, ensure that the power to that equipment has been turned off. Also, ensure that the power to any related equipment has been turned off.

Ensure that you follow all applicable electrical codes when wiring the S7-1200 and related equipment. Install and operate all equipment according to all applicable national and local standards. Contact your local authorities to determine which codes and standards apply to your specific case.

> **WARNING**
>
> **Installing or wiring the S7-1200 or related equipment with power applied could cause electric shock or unexpected operation of equipment.**
>
> Failure to disable all power to the S7-1200 and related equipment during installation or removal procedures could result in death, severe personal injury, and damage due to electric shock or unexpected equipment operation.
>
> Always follow appropriate safety precautions and ensure that power to the S7-1200 is disabled before attempting to install or remove the S7-1200 or related equipment.

Always take safety into consideration as you design the grounding and wiring of your S7-1200 system. Electronic control devices, such as the S7-1200, can fail and cause unexpected operation of the equipment that is being controlled or monitored:

- On-board I/O on the fail-safe CPU and signal modules (SM) other than fail-safe SM: Single point dangerous failures of electronics or software can occur on these devices. You should never depend on these devices as the only protection against personal injury or unacceptable property damage.
- Fail-safe SM: Internal dangerous failures can occur on these devices with a probability as reflected in the SIL rating, PFD, and PFH as stated in this manual.
- Each control's installation: Common cause failure threats can occur such as overvoltage, over-temperature, electrical faults, EMC interference, and fire, water, or mechanical damage to the installation.

You must evaluate every control point for the threat level and consequences of failure. Your installation can require safeguards that are independent of the S7-1200 to achieve an appropriate level of risk for personal injury or equipment damage.

> **WARNING**
>
> **Control devices can fail in an unsafe condition, resulting in unexpected operation of controlled equipment.**
>
> Such unexpected operations could result in death, severe personal injury, and property damage.
>
> When using fail-safe I/O, design safety-related control functions to account for the probability of faults, including redundancy to achieve an appropriate level of risk for the consequences of failure.
>
> When using standard I/O, always include an emergency stop function, electromechanical overrides, or other redundant safeguards when a failure could cause personal injury or significant property damage.

4.3.2 Grounding an S7-1200 system

Guidelines for grounding the S7-1200

The best way to ground your application is to ensure that all the common and ground connections of your S7-1200 and related equipment are grounded to a single point. This single point should be connected directly to the earth ground for your system.

All ground wires should be as short as possible and should use a large wire size, such as 2 mm^2 (14 AWG).

When locating grounds, consider safety-grounding requirements and the proper operation of protective interrupting devices.

4.3.3 Wiring an S7-1200 system

Guidelines for wiring the S7-1200 system

When designing the wiring for your S7-1200, provide a single disconnect switch that simultaneously removes power from the fail-safe CPU power supply, from all input circuits, and from all output circuits. Provide over-current protection, such as a fuse or circuit breaker, to limit fault currents on supply wiring. Consider providing additional protection by placing a fuse or other current limit in each output circuit.

Install appropriate surge suppression devices for any wiring that could be subject to lightning surges.

Avoid placing low voltage signal wires and communications cables in the same wire tray with AC wires and high energy, rapidly switched DC wires. Always route wires in pairs, with the neutral or common wire paired with the hot or signal-carrying wire.

Note

The standard I/O channels integrated in the S7-1200 fail-safe CPUs are not designed to be used for the fail-safe I/O function

In your project, you can use the integrated fail-safe CPU I/O with standard code blocks, but you must use the S7-1200 fail-safe DI and DQ signal modules as the fail-safe digital I/O channels with safety code blocks.

Use the shortest wire possible and ensure that the wire is sized properly to carry the required current. The CPU and SM connectors accept wire sizes from 2 mm^2 to 0.3 mm^2 (14 AWG to 22 AWG). Wire strip length is 6.4 mm.

Wire and cable should have a temperature rating 30 °C higher than the ambient temperature around the S7-1200 (for example, a minimum of 85 °C-rated conductors for 55 °C ambient temperature). You should determine other wiring type and material requirements from the specific electrical circuit ratings and your installation environment.

Use shielded wires for optimum protection against electrical noise. Typically, grounding the shield at the S7-1200 gives the best results. You should ground communication cable shields to S7-1200 communication connector shells using connectors that engage the cable shield, or by bonding the communication cable shields to a separate ground. You should ground other cable shields using clamps or copper tape around the shield to provide a high surface area connection to the grounding point.

When wiring input circuits that are powered by an external power supply, include an overcurrent protection device in that circuit. External protection is not necessary for circuits that are powered by the 24 VDC sensor supply from the S7-1200 because the sensor supply is already current-limited.

All S7-1200 modules have removable connectors for user wiring. To prevent loose connections, ensure that the connector is seated securely and that the wire is installed securely into the connector. To avoid damaging the connector, be careful that you do not over-tighten the screws. The maximum torque for the CPU and SM connector screw is 0.56 N-m (5 inch pounds).

To help prevent unwanted current flows in your installation, the S7-1200 provides isolation boundaries at certain points. When you plan the wiring for your system, you should consider these isolation boundaries. Refer to the technical specifications (Page 132) for the amount of isolation provided and the location of the isolation boundaries. Circuits rated for AC line voltage include safety isolation to other circuits. Isolation boundaries between 24 VDC circuits are functional only, and you should not depend on these boundaries for safety.

4.3.4 Guidelines for lamp loads

Guidelines for lamp loads

Lamp loads are damaging to relay contacts because of the high turn-on surge current. This surge current is 10 to 15 times the steady state current for a tungsten filament lamp. A replaceable interposing relay or surge limiter is recommended for lamp loads that are switched a large number of times during the lifetime of the application.

4.3.5 Guidelines for inductive loads

Guidelines for inductive loads

Use suppressor circuits with inductive loads to limit the voltage rise when a control output turns off. Suppressor circuits protect your outputs from premature failure caused by the high voltage transient that occurs when current flow through an inductive load is interrupted.

In addition, suppressor circuits limit the electrical noise generated when switching inductive loads. High frequency noise from poorly suppressed inductive loads can disrupt the operation of the PLC. Placing an external suppressor circuit so that it is electrically across the load and physically located near the load is the most effective way to reduce electrical noise.

S7-1200 DC outputs include internal suppressor circuits that are adequate for inductive loads in most applications. Since S7-1200 relay output contacts can be used to switch either a DC or an AC load, internal protection is not provided.

A good suppressor solution is to use contactors and other inductive loads for which the manufacturer provides suppressor circuits integrated in the load device, or as an optional accessory. However, some manufacturer provided suppressor circuits may be inadequate for your application. An additional suppressor circuit may be necessary for optimal noise reduction and contact life.

For AC loads, a metal oxide varistor (MOV) or other voltage clamping device may be used with a parallel RC circuit, but is not as effective when used alone. An MOV suppressor with no parallel RC circuit often results in significant high frequency noise up to the clamp voltage.

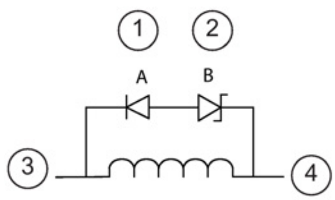
A well-controlled turn-off transient will have a ring frequency of no more than 10KHz, with less than 1KHz preferred. Peak voltage for AC lines should be within +/- 1200V of ground. The data sheets list voltage thresholds for the internal suppression circuits on DC outputs. (Refer to Appendix A: "Technical specifications" for further information.) External suppression should limit the transient to less than this threshold to ensure that the internal suppression circuit does not attempt to suppress an excessive load. Placing an external suppressor circuit so that it is electrically across the load and physically located near the load is the most effective way to reduce electrical noise.

An external suppression circuit connected directly across the load also avoids the hazard of energizing the load if suppression circuit components fail short.

Note

The effectiveness of a suppressor circuit depends on the application and must be verified for your particular usage. Ensure that all components are correctly rated and use an oscilloscope to observe the turn-off transient.

Typical suppressor circuit for DC or relay outputs that switch DC inductive loads



① 1N4001 diode or equivalent

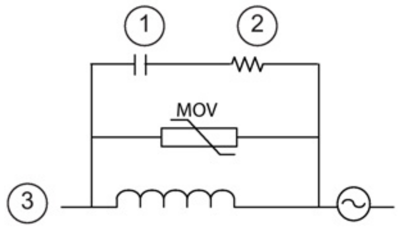
② 8.2 V Zener (DC outputs),
36 V Zener (Relay outputs)

③ Output channel F-DQ (P-switch) or standard DQ output

④ Output channel F-DQ (M-switch) or standard DQ common return

In most applications, the addition of a diode (A) across a DC inductive load is suitable, but if your application requires faster turn-off times, then the addition of a Zener diode (B) is recommended. Be sure to size your Zener diode properly for the amount of current in your output circuit.

Typical suppressor circuit for relay outputs that switch AC inductive loads



① See table for C value
② See table for R value
③ Output channel

Ensure that the working voltage of the MOV is at least 20% greater than the nominal line voltage.

Choose pulse-rated, non-inductive resistors, and capacitors recommended for pulse applications (typically metal film). Verify the components meet average power, peak power, and peak voltage requirements.

If you design your own suppressor circuit, the following table suggests resistor and capacitor values for a range of AC loads. These values are based on calculations with ideal component parameters. "I rms" in the table refers to the steady-state current of the load when fully ON.

Table 4- 9 AC suppressor circuit resistor and capacitor values

Inductive load			Suppressor values		
I rms	**230 VAC**	**120 VAC**	**Resistor**		**Capacitor**
Amps	VA	VA	Ω	W (power rating)	nF
.02	4.6	2.4	15000	.1	15
.05	11.5	6	5600	.25	47
.1	23	12	2700	.5	100
.2	46	24	1500	1	150
.5	115	60	560	2.5	470
1	230	120	270	5	1000
2	460	240	150	10	1500

Conditions satisfied by the table values:

Maximum turn-off transition step < 500V
Resistor peak voltage < 500V
Capacitor peak voltage < 1250V
Suppressor current < 8% of load current (50 Hz)
Suppressor current < 11% of load current (60 Hz)
Capacitor dV/dt < 2 V/μs
Capacitor pulse dissipation : $\int(dv/dt)^2\, dt < 10000\ V^2/\mu s$
Resonant frequency < 300 Hz
Resistor power for 2Hz max switching frequency
Power factor of 0.3 assumed for typical inductive load

4.4 Maintenance guidelines

Each S7-1200 module and CPU is a factory-assembled unit that contains no user replaceable components or repairable components, except for removeable terminal blocks and memory cards. Maintenance of an S7-1200 system consists of the following:

- Observation and response to diagnostic reports from the S7-1200
- Replacement of modules with identified failures
- Replacement of modules at 20 years of operating life
- Inspection and monitoring of the installation environment to ensure continued adherence to all specified operating conditions, to include the following:
  - S7-1200 and field wiring electrically and mechanically secure
  - Ventilation continued as designed for installation
  - Continued protection from moisture, dust, and conductive contamination
  - Voltage of connected circuits in proper range
  - Operating temperature of equipment in proper range

The fail-safe signal modules (SMs) monitor the 24 VDC power supplied at L+/M and passivate the module on voltage out-of-range.

The fail-safe SMs monitor internal temperature and passivate the SM on temperature out-of-range.

You must assess your installation safety and determine if you require additional voltage and temperature monitoring.

Note

Associated equipment including sensors, actuators, circuit breakers, and surge protectors are subject to wear and typically require periodic inspections or proof tests according to manufacturer's instructions or standards to maintain a consistent level of safety integrity.

User cleaning or decontamination of an S7-1200: Use vacuum or a dry cloth applied to the outside of the assembly only. High pressure forced air can damage components or carry entrained contaminants. Liquid cleaners of any kind can deposit conductive contamination onto the circuit boards.

Fail-Safe signal module (SM) I/O configuration 5

All connected fail-safe SM I/O must have their operating properties configured by the STEP 7 Safety configuration software. You have the responsibility to ensure that no unconfigured SMs are connected in a fail-safe automation system.

5.1 Configuring fail-safe SM I/O properties

To configure fail-safe SM I/O properties, follow these steps:

1. Select "Device configuration" in the project tree.
2. Place fail-safe I/O devices into your project's "Device view".

Note

The fail-safe SM's each use both I's and Q's, even though they may physically only have input channels or only have output channels. The extra bytes carry safety status and data integrity information.

Module	Number of channels	Input (I) bytes required	Output (Q) bytes required
SM 1226 F-DI 16 x 24 VDC	8 - 16 (input)	9	5
SM 1226 F-DQ 4 x 24 VDC	4 (output)	6	6
SM 1226 F-DQ 2 x Relay	2 (output)	6	6

3. Select the image of a fail-safe I/O device (on the Device view or Device overview) and view the module's "Properties" tab.
4. On the **"Properties"** view, select the **"General"** tab.
5. Click on the module properties tree and expand the branches for an I/O module. You can select a module (for example, "F-DI16") and see all the properties. You can also select a module branch (for example, "F-parameters", "DI-parameters", or "Channel parameters") and see a subset of the properties.
6. Select a property in the left-side property tree and then set values in the right-side property fields.
7. A successful compile and download of your hardware configuration to an S7-1200 fail-safe CPU automatically puts your new configuration settings in the I/O modules.

5.2 Configuring common F-parameters

Table 5- 1 Common F-parameters

F-parameters	Description	Default	Options
Manual assignment of F-monitoring time	You must select the check box to change F-monitoring time from the central value propagated by the fail-safe CPU.	Check box deselected	Check box: • Selected • Deselected
F-monitoring time [1]	Watchdog timer monitoring safety-related communication between the fail-safe CPU and fail-safe SM (PROFIsafe monitoring time)	150 ms	1 to 65535 ms
F-source address	Unique network-wide address for the fail-safe CPU	1	You can configure the F-source address using the fail-safe CPU parameter "Basis for PROFIsafe addresses".
F-destination address	CPU-wide unique address (usually in descending order, starting with 65534).	-	1 to 65534
Behavior after channel fault	Response by the fail-safe SM to channel faults such as a short-circuit, overload, or discrepancy error.	Passivate channel	Not configurable in the fail-safe SM
Reintegration after channel fault (not available for the SM 1226 F-DQ 2 x Relay)	You have two methods, manual and automatic, to reintegrate your fail-safe SM channels after a channel fault. You can choose to reintegrate in one of three ways: • All channels automatically (no acknowledgement necessary for reintegration) • All channels manually (acknowledgement necessary for reintegration) • Adjustable (channel-by-channel; some channels automatically reintegrated and some channels manually reintegrated)	Adjustable	• Adjustable • All channels automatically • All channels manually

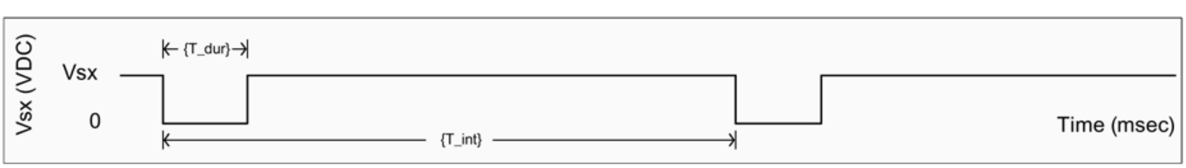
[1] You set the "Default F-monitoring time for central F-IO" in the F-parameters of the fail-safe CPU. STEP 7 uses this number to set the F-monitoring time in each fail-safe SM unless you select the check box for "Manual Assignment of F-monitoring time" in that module configuration and assign a different time.

Refer to the SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual (http://support.automation.siemens.com/WW/view/en/54110126/0/en) for further F-parameter information.

5.3 Configuring SM 1226 F-DI 16 x 24 VDC DI and channel parameters

Table 5- 2 SM 1226 F-DI 16 x 24 VDC DI parameters

DI parameters	Description	Default	Options
Short-circuit test	This test creates short duration OFF pulses on the sensor power supplies. Input circuits powered by Vs1 and Vs2 are expected to be OFF during the sensor OFF time. Failure to detect OFF when a sensor supply is OFF indicates a short-circuit to a power source or another fault that prevents the input from properly detecting a "0". Input channels which fail this test are passivated. During the test, the reported process value will not change, so the configured "Duration of short-circuit test" increases the response time. An actual process "0" occuring near the beginning of a test will not be reported to the user program until after the "Duration of short-circuit test" time has elapsed. The check box must be selected to activate the short-circuit test.	Check box deselected	Check box: • Selected • Deselected
Interval for short-circuit test (see T_int in figure below)	This value is the time between the OFF pulses of the sensor supply. Refer to the figure below for further information. Note: The interval must be a minimum of eight times the duration.	25.6 ms	• 12.8 ms • 25.6 ms • 51.2 ms • 102.4 ms • 204.8 ms • 409.6 ms • 819.2 ms
Duration of short-circuit test (see T_dur in figure below)	This value is the time that the power supply remains off during the test. The short-circuit test OFF pulse must be long enough for the external sensors and wiring to respond and present a "0" to the inputs. Refer to the figure below for further information. Note: The interval must be a minimum of eight times the duration.	1.6 ms	• 1.6 ms • 3.2 ms • 6.4 ms • 12.8 ms



Vsx Vs1 or Vs2 sensor supplies (VDC)

T_int Short-circuit test interval (time period) between the OFF pulses of the sensor supply

T_dur Short-circuit test OFF pulse time duration (msec)

Table 5- 3 SM 1226 F-DI 16 x 24 VDC channel parameters

Channel parameters	Description	Default	Options
Activated	Select the check box to activate the channel. You must activate both required channels before selecting 1oo2. If channels are paired, you must change to 1oo1 and change individually. Deselect the check box and the unused channel is deactivated. If you deactivate a channel, you also deactivate its diagnostic function.	Check box selected	Check box: • Selected • Deselected
Input filters	Digital inputs are filtered to remove contact bounce and short duration noise. This parameter assigns the duration of the filter time.	6.4 ms	• 0.8 ms • 1.6 ms • 3.2 ms • 6.4 ms • 12.8 ms
Channel failure acknowledge	Controls whether the channel is automatically reintegrated after a fault clears, or requires an acknowledgement (manual) in the user program. Refer to "Reactions to faults" (Page 115) for the reintegration procedure.	Manual	• Automatic • Manual
Sensor supply	Assign whether 24 V power is supplied to sensors from a sensor supply output of the module (internal) or from an external power supply (external). Short-circuit tests are not performed for any channel where external power is selected.	External	• Internal • External
Sensor evaluation	Assigns whether channel x input operates individually or is paired with channel x+8 input. **1oo1 evaluation:** One sensor is connected to the module on a single channel. **1oo2 evaluation:** Two input channels are occupied by either: • Two 1-channel sensors • One 2-channel equivalent sensor • One 2-channel non-equivalent sensor If 1oo2 is selected, you must assign the digital input connection type and discrepancy properties.	1oo1 evaluation	• 1oo1 evaluation • 1oo2 evaluation

Channel parameters	Description	Default	Options
Type sensor connection	**1 channel**: One sensor is connected to one channel. For "1oo1 evaluation", the type of sensor connection is set read only to "1 channel". **2 channel equivalent** (with equivalent signals): One two-channel equivalent sensor or two single-channel equivalent sensors are connected to the two channels, in a channel pair. **2 channel - 3 wire non-equivalent**: One two-channel non-equivalent sensor is connected to the two channels, in a channel pair. **2 channel - 4 wire non-equivalent** One two-channel non-equivalent sensor or two single-channel non-equivalent sensors are connected to the two channels, in a channel pair. Note: Refer to "Digital input applications" (Page 68) for illustrations of connection modes.	1 channel	• 1 channel • 2 channel equivalent • 2 channel - 3 wire non-equivalent • 2 channel - 4 wire non-equivalent
Discrepancy behavior	A logical difference between the two signals of a 1oo2 input configuration is allowed, without error, for the configured discrepancy time. You can choose whether the reported process value should be "0" or the last valid value during the configured discrepancy time while the signals do not match. If a logical difference in 1oo2 inputs persists for more than the configured discrepancy time, the channel will be passivated and the process value set to 0.	Supply value 0	• Supply value 0 • Supply last valid value
Discrepancy time	The two signals in a 1oo2 input configuration will not change exactly at the same time, due to differences in sensors, contacts, and wiring. The discrepancy time parameter allows you to configure a normally expected duration for a mis-match between signals during transition.	10 ms	5 to 30000 ms
Reintegration after discrepancy error	Assigns whether a zero state must be detected on both 1oo2 channels before a previously declared discrepancy can be cleared.	Test 0-signal not necessary	• Test 0-signal not necessary • Test 0-signal necessary Note: The test 0-signal must be applied for at least 100 ms.

Note

Safety program access to 1oo2 input data

For 1oo2 evaluation, two paired input channels (for example, F-DI a0.0 and F-DI b0.0) are connected to one or two sensors. The F-DI performs the discrepancy analysis and sends the result to the safety program, **at the input address of the low-numbered channel** (F-DI a0.0, in the example).

Sensor-actuator response time is increased when you add more input discrepancy time

The discrepancy time adds directly to the maximum response time of a 1oo2 evaluation if the two signals do not agree in logical state. If you select the "Supply value 0" option, then the F-DI does not delay a transition from "1" to "0", but can delay the transition from "0" to "1". If you select the "Supply last valid value" option, then the F-DI can delay both transitions from "1" to "0' and "0" to "1". The discrepancy time is influenced by sensor specifications, installation tolerances, and wiring. For best response time, select the smallest discrepancy time that provides reliable normal operation. Refer to "Fail-Safe signal module (SM) response times" (Page 197) for further information.

Discrepancy time variation with short circuit test

If your process input changes near a short-circuit test, a discrepancy is detected in less time than your configured discrepancy time.

With:

Tdisc = configured discrepancy time

Tsct = configured short circuit test duration

Tfilter = configured input filter time

Tda = actual discrepancy time, time between process signal changes that can be detected as a fault

The range of detected discrepancy time is:

If Tfilter < Tsct: {Tdisc - (Tfilter + Tsct)} <= Tda <= Tdisc

If Tfilter >= Tsct: {Tdisc - (2 x Tsct)} <= Tda <= Tdisc

Your configured discrepancy time should account for this variation to avoid unexpected passivations.

5.4 Configuring SM 1226 F-DQ 4 x 24 VDC DQ and channel parameters

Table 5- 4 SM 1226 F-DQ 4 x 24 VDC DQ parameters

DQ parameters	Description	Default	Options
Maximum test period	Assign the time interval between bit pattern tests for F-DQ DC output faults. Functional test bit patterns are applied to the output switches. These tests detect faulted P- or M- output switches and wiring faults that are detectable at the module terminals. Short circuits to other signals or power rails can be detected. Open circuits between the wiring terminals and the load are not detected. If an error is detected on a channel, the test interval is shortened to approx. 1 min. If an error is no longer detected, the configured test interval is used again. A persistent fault is reported to the fail-safe CPU and the affected channels are passivat-ed.	1000 s	• 100 s • 1000 s

Table 5- 5 SM 1226 F-DQ 4 x 24 VDC channel parameters

Channel parameters	Description	Default	Options
Activated	Select the check box to activate the channel. Deselect the check box and the unused channel is deactivated. If you deactivate a channel, you also deactivate its diagnostic function.	Check box selected	Check box: • Selected • Deselected
Channel failure acknowledge	Controls whether the channel is automatically reintegrated after a fault clears, or requires an acknowledgement (manual) in the user program. Refer to "Reactions to faults" (Page 115) for the reintegration procedure.	Manual	• Automatic • Manual
Maximum readback time	The maximum readback time is a user-configured parameter that assigns the maximum time allowed for an output to reach the new state (ON or OFF) due to a process value change without generating an error. Also, this is the maximum width of a diagnostic test pulse applied to verify that an output can be turned OFF while it is ON. The time of the OFF pulse should be as long as possible, but short enough so that the actuator cannot react.	2.0 ms	1 ms to 400 ms, in 0.1 ms increments
Maximum readback time switch on test	The maximum readback time switch on test is a user-configured parameter that assigns the maximum time for which the P-switch or the M-switch of a channel that is currently in OFF state can be switched ON during a bit pattern test step. The F-DQ DC tests the P- and M-switches on a channel such that only one switch is turned on at a time. Unless there is a fault in the system (for example, actuator shorted to ground), the actuator is not energized during either the P- or M-switch on tests. Under single fault conditions (either internal or external to the SM), test pulses applied to either the P- or the M-switch of channels in the OFF state can repeatedly energize the actuator. You must select the parameter so that the duration of such pulses is too short to cause the actuator to react and, therefore, cannot have a hazardous effect on the equipment under control.	1.0 ms	0.5 ms to 5 ms, in 0.1 ms increments

WARNING

In the presence of a single fault, the bit pattern tests can apply energy to the load for a duration up to the configured "Maximum readback time switch on test".

If the load can respond dangerously within the configured readback time, it can respond to bit pattern tests in the presence of a single fault, resulting in death or serious injury to personnel and/or property damage.

Always choose a maximum readback configuration time that is guaranteed not to activate the load.

5.5 Configuring SM 1226 F-DQ 2 x Relay DQ and channel parameters

Table 5- 6 SM 1226 F-DQ 2 x Relay DQ parameters

DQ parameters	Description	Default	Options
Relay continuous on time limit	Maximum number of days that the relay can remain continuously on before automatic passivation. Whenever the relay cycles from the de-energized to energized state, the number-of-days calculation begins again. Note: The 30-day default is the maximum test frequency for SIL 3/Category 4 applications. You can extend the test frequency for SIL 2/Category 3 applications for this product to as much as 366 days.	30	1 to 366 days

Table 5- 7 SM 1226 F-DQ 2 x Relay channel parameters

Channel parameters	Description	Default	Options
Activated	Select the check box to activate the channel. Deselect the check box and the unused channel is deactivated. If you deactivate a channel, you also deactivate its diagnostic function.	Check box selected	Check box: • Selected • Deselected
Channel failure acknowledge	Controls whether the channel is automatically reintegrated after a fault clears, or requires an acknowledgement (manual) in the user program. Refer to "Reactions to faults" (Page 115) for the reintegration procedure.	Manual	Not configurable

Fail-Safe signal module (SM) diagnostics 6

6.1 Reactions to faults

Reactions to startup of the fail-safe system and to faults

The fail-safe concept depends on the identification of a safe state for all process variables. The value "0" (de-energized) represents this safe state for digital fail-safe signal modules (SM). This applies to both sensors and actuators.

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

- When the fail-safe system is started up
- If SM module faults are detected, such as RAM or processor failures
- If errors are detected during safety-related communication between the fail-safe CPU and the fail-safe SM through the PROFIsafe safety protocol (communication error)
- If SM channel faults occur (for example, short-circuit and discrepancy errors)

The fail-safe CPU enters detected system faults into the diagnostic buffer.

Automatic safety measures and the PROFIsafe protocol ensure that the safe state is set if the system detects a fault.

Fail-Safe SMs do not remember errors upon power cycle. When the system is powered down and then restarted, any faults still existing are detected again.

Fail-Safe value for fail-safe signal modules

If channels are passivated in fail-safe DI SMs, the fail-safe system always provides safe state values ("0") for the safety program instead of the process values applied to the fail-safe inputs.

If channels are passivated in the F-DQ DC or F-RLY, the fail-safe system always transfers safe state values "0" to the fail-safe outputs instead of the output values provided by the safety program. The output channels are de-energized.

The passivation safe state value and the output state value in CPU STOP mode are always "0", de-energized. You cannot select or program a default "ON" state for passivation or STOP mode.

Passivation is applied to individual channels when a channel-specific diagnostic failure is detected. Failures that can affect the entire module result in passivation of all channels.

Time-out of the PROFIsafe message (F-monitoring time exceeded) passivates all module channels.

Table 6- 1 Signal module type and passivation result

Signal module type	Passivation result
SM 1226 F-DI 16 x 24 VDC	• Tests are evaluated per channel, in order to allow channel-granular passivation of defective inputs. • If a channel fault occurs for a 1oo1 configuration, only the affected channel is passivated. For a 1oo2, the channel group of two inputs in the 1oo2 configuration are passivated.
SM 1226 F-DQ 4 x 24 VDC	• Tests are evaluated per channel, in order to allow channel-granular passivation of defective outputs. • Diagnostic evaluations are performed separately for each of the two switches of a channel. Failure detection for one switch leads to passivation of the channel.
SM 1226 F-DQ 2 x Relay	• Tests are evaluated per channel, in order to allow channel-granular passivation of defective outputs. • Diagnostic evaluations are performed separately for each of the two relays of a channel. Failure detection for one relay leads to passivation of the channel.

Response to faults in the fail-safe system

You should prepare maintenance procedures for your system to assure that return to operation after a detected fault is controlled and documented.

The following steps must be performed:

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

Reintegration of a fail-safe signal module

A channel or module can be reintegrated after successful diagnostics determine that a fault has cleared.

You can configure reintegration as automatic or manual. You can make this selection on a per channel or module basis in the Device Configuration. Communication errors must always be manually acknowledged.

Channels that you select to be automatically reintegrated are immediately reintegrated when the fault has cleared.

Channels that you select to be manually reintegrated can be acknowledged in your program after the fault has cleared.

The "ACK_REQ" bit for that module goes true to signal that reintegration is possible. After the "ACK_REQ" bit is true, your program can set the "ACK_REI" bit to allow the reintegration of all channels in that module that are ready to be reintegrated.

You can also acknowledge all faults in an F-runtime group using the "ACK_REI_GLOB" input of the "ACK_GL" instruction.

Some fatal diagnostic errors require a power cycle with successful diagnostics to reintegrate.

Reintegration after high stress events

High temperature, high voltage, and excessive current stress can damage electronics, reducing the reliability while components continue to work apparently as expected. Passivation does not remove the potentially damaging effects of high ambient temperature or high applied voltage. Relays and solid state switch outputs can be damaged by high currents prior to protective device activations. The PFD and PFH reliability calculations assume the fail-safe SM is operated within its specified operating parameters. When an SM has passivated due to a high stress event, even though it apparently works correctly and passes all diagnostics, the probability of a future dangerous failure may be increased.

> **WARNING**
>
> **It is possible to reintegrate a channel or module while some fault is still present that is not readily detected by the module diagnostics.**
>
> Reintegration of a faulty system can result in unexpected machine or process operation, which may cause death or serious injury to personnel, and/or damage to equipment.
>
> After any reported fault, the steps outlined in this chapter and in safety standards applicable to your system should be followed to assure that the fault is completely understood and corrected before reintegration.

For an exact list of faults for the SMs, refer to "Fault types, causes, and corrective measures" (Page 125).

At reintegration, the following occurs:

- For a fail-safe DI SM, the process values pending at the fail-safe inputs are provided for the safety program.
- For a fail-safe DQ SM, the output values provided in the safety program are again transferred to the fail-safe outputs.

Safety repair time

The repair time used for PFH and PFD calculations is 100 hours.

Passivation is designed to provide the safe state of the safety function in the event of a single fault. While a channel is passivated and energy is still available to the channel, there is a possibility that additional faults can cause a dangerous failure of the safety function. You should respond to passivations by repairing the fault or taking the passivated channel out of service in less than 100 hours to preserve the safety integrity level of your system.

Deactivated fail-safe I/O is not being diagnosed, and is subject to dangerous failure without warning.

If any channel passivation persists for 100 hours, the entire module is passivated and can only be recovered through power cycle.

If a repair within 100 hours is not possible, passivated fail-safe outputs should be taken out of service by physically disconnecting or opening circuits so that faults in the fail-safe SM cannot apply energy to the load. To remove input channels from service in an operating PLC system, references to any passivated fail-safe inputs must be removed from any operating CPU Safety program logic that can result in activation of a safety function output.

Do not depend on channel or module passivation to maintain safe state for more than 100 hours.

Do not depend on deactivation or unconfiguration to maintain safe state in any circumstances.

Additional information on passivation and reintegration

For further information about fail-safe SM access, refer to the SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual (http://support.automation.siemens.com/WW/view/en/54110126/0/en).

6.2 Fault diagnostics

Diagnostics detect faults that can affect the integrity of safety-related I/O. The faults can be in the fail-safe SM, communication with the CPU, or external circuits. Diagnostic information is assigned either to a single channel or to the entire fail-safe SM.

Most diagnostics operate without user selection. You can configure the following diagnostic options:

- Short-circuit testing using the digital input sensor supply can be enabled. The interval and duration of short-circuit tests is configurable.
- The read-back times for 24 VDC digital outputs is configurable.
- The time-out intervals for failures in the safety communication or failure of a safety program to run is configurable.

  Refer to Chapter 5: "Fail-Safe signal module (SM) I/O configuration" for a complete description of these options.

The safety-critical and validated action of the diagnostics is to passivate I/O when faults are detected. The reporting of status and diagnostic results through the LED displays and diagnostic messages is subject to single point failures in electronics or software. These reports are offered as maintenance and debugging aids, but must be observed and interpreted with caution.

In the presence of single faults, any or all LED indications can be wrong. You should not rely solely on the presence or absence of red or green LED indicators to make safety decisions.

In the presence of single faults, diagnostic messages may fail to be delivered, or the numerical event ID or text message can be wrong. You should not rely solely on the presence, absence, or content of diagnostic reports to make safety decisions.

> **WARNING**
>
> **Diagnostic and status reports through LEDs and text messages are subject to single point failure errors.**
>
> Reliance on such reported information to determine that a system or I/O point is in a safely controlled state can result in death, severe personal injury, or property damage.
>
> If the integrity of your fail-safe system is in doubt, you should use additional measures such as restricted access or power removal to control hazards during maintenance and debug activities.

6.2.1 Diagnostics by LED display

The fail-safe SMs have the following types of LEDs:

- **Module DIAG LED:**
  - Dual color (green / red) LED indicates the operating state and fault status of the module.
  - Only a single DIAG LED on each fail-safe SM
  - The DIAG LED is green ON if no fault is present and the fail-safe SM is configured.
  - The DIAG LED is flashing green if no fault is present and the fail-safe SM is not configured.
  - The DIAG LED is flashing red as soon as a diagnostic function is triggered by the fail-safe SM.
  - The DIAG LED alternates between flashing red and green when a reintegratable module fault has been cleared, but not yet acknowledged.
  - The DIAG LED continues to flash red when a reintegratable channel fault has been cleared, but not yet acknowledged.
  - The DIAG LED is green ON when all faults have been eliminated and acknowledged.
- **Input/Output Status LED**:
  - Green LED for each input shows the input/output state during normal operation.
- **Input/Output Fault LED**:
  - Red LED for each input/output indicates a channel error. If any channel error is present, the DIAG LED is flashing red.
  - The DIAG LED alternates between flashing red and green when a reintegratable channel fault has been cleared, but not yet acknowledged.

SM 1226 F-DI 16 x 24 VDC

Table 6- 2 Module DIAG and 1oo1 input channel LEDs

Description	DIAG LED	Input	
		Fault LED	**Status LED**
LED color	**Green / red**	**Red**	**Green**
I/O bus power off	Off	Off	Off
Module hardware fault [1]	Flashing red	On	Off
PROFIsafe error	Flashing red	Unaffected	Unaffected
Inconsistent firmware versions between Bus-ASIC and F-µCs	Flashing red	Flashing	Off
24 VDC module supply voltage off	Flashing red	Off	Off
24 VDC module supply voltage too high / too low	Flashing red	On	Off
Sensor supply fault: For inputs affected by the fault	Flashing red	On	Off
Sensor supply fault: For inputs not affected by the fault	Flashing red	Unaffected	Input state 0 Input state 1
Module successfully configured; no errors	On green	Off	Input state 0 Input state 1
Not configured	Flashing green	Off	Input state 0 Input state 1
Channel deactivated	On green	Off	Input state 0 Input state 1
Channel fault; passivated	Flashing red	On	Off
Awaiting reintegration, module fault	[2] Flashing red and green	[3] Flashing	
Awaiting reintegration, channel fault	Flashing red	[3] Flashing	

Description	DIAG LED	Input	
		Fault LED	Status LED
LED color	**Green / red**	**Red**	**Green**
Firmware update in progress	✱ Flashing green	○ Off	○ Off

○- Off;●- On;✱- Flashing (Flashing frequency: 2.0 Hz)

1 All channels passivated indicates a module-wide fault occurred. This could be an external condition such as supply voltage low or a detected internal module defect.

2 A single, dual color (green / red) flashing LED

3 Alternating flashing of the separate fault (red) and status (green) LEDs

Table 6- 3 Module DIAG and 1oo2 input channel LEDs

Description	DIAG LED	Primary input		Secondary input	
		Fault LED	Status LED	Fault LED	Status LED
LED color	**Green / red**	**Red**	**Green**	**Red**	**Green**
Input state 0 (equivalent)	● On green	○ Off	○ Off	○ Off	○ Off
Input state 1 (equivalent)			● On		● On
Input state 0 (non-equivalent)			○ Off		● On
Input state 1 (non-equivalent)			● On		○ Off
Discrepancy error	✱ Flashing red	● On	○ Off	● On	○ Off
Discrepancy error resolved; awaiting reintegration	TBD ✱ / ✱[1] Flashing red and green	✱ / ✱[2] Flashing		✱ / ✱[2] Flashing	

○ - Off;● - On;✱- Flashing (Flashing frequency: 2.0 Hz)

1 A single, dual color (green / red) flashing LED

2 Alternating flashing of the separate fault (red) and status (green) LEDs

SM 1226 F-DQ 4 x 24 VDC

Table 6- 4 Module DIAG and output channel LEDs

Description	DIAG LED	Output	
		Fault LED	Status LED
LED color	**Green / red**	**Red**	**Green**
I/O bus power off	○ Off	○ Off	○ Off
Module hardware fault [1]	✱ Flashing red	● On	○ Off
PROFIsafe error	✱ Flashing red	Unaffected	○ Off
Inconsistent firmware versions between Bus-ASIC and F-µCs	✱ Flashing red	✱ Flashing	○ Off
24 VDC module supply voltage off	✱ Flashing red	○ Off	○ Off
24 VDC module supply voltage too high / too low	✱ Flashing red	● On	○ Off
Module successfully configured; no errors	● On green	○ Off	○ Output state 0 ● Output state 1
Not configured	✱ Flashing green	○ Off	○ Off
Channel deactivated	● On green	○ Off	○ Off
Channel fault; passiv-ated	✱ Flashing red	● On	○ Off
Awaiting reintegration	TBD ✱ / ✱ [2] Flashing red and green	✱ / ✱ [3] Flashing	
Firmware update in progress	✱ Flashing green	○ Off	○ Off

○- Off; ●- On; ✱- Flashing (Flashing frequency: 2.0 Hz)

[1] All channels passivated indicates a module-wide fault occurred. This could be an external condition such as supply voltage low or a detected internal module defect.

[2] A single, dual color (green / red) flashing LED

[3] Alternating flashing of the separate fault (red) and status (green) LEDs

SM 1226 F-DQ 2 x Relay

Table 6- 5 Module and output channel LEDs

Description	DIAG LED	Output	
		Fault LED	Status LED
LED color	**Green / red**	**Red**	**Green**
I/O bus power off	Off	Off	Off
Module hardware fault [1]	Flashing red	On	Off
PROFIsafe error	Flashing red	Unaffected	Off
Inconsistent firmware versions between Bus-ASIC and F-µCs	Flashing red	Flashing	Off
24 VDC module supply voltage off	Flashing red	Off	Off
24 VDC module supply voltage too high / too low	Flashing red	On	Off
Module successfully configured; no errors	On green	Off	Output state 0
			Output state 1
Not configured	Flashing green	Off	Off
Channel deactivated	On green	Off	Off
Channel fault; passivated	Flashing red	On	Off
Awaiting reintegration	TBD ✶ / ✶ [2] Flashing red and green	✶ / ✶ [3] Flashing	
Firmware update in progress	Flashing green	Off	Off

○- Off; ●- On; ✶- Flashing (Flashing frequency: 2.0 Hz)

[1] All channels passivated indicates a module-wide fault occurred. This could be an external condition such as supply voltage low or a detected internal module defect.

[2] A single, dual color (green / red) flashing LED

[3] Alternating flashing of the separate fault (red) and status (green) LEDs

6.2.2 Fault types, causes, and corrective measures

The "Fault types, causes, and corrective measures" table below lists the messages of the S7-1200 fail-safe SMs. These messages are displayed in the TIA Portal under "Online & diagnostics" > "Diagnostics" > "Diagnostic buffer". When you highlight an individual text line in the diagnostic buffer, the Event ID for that text item is displayed, along with module identity and location that generated the message. You may need to expand the window to see all information.

Table 6- 6 Fault types, causes, and corrective measures

Event ID	Diagnostic message	Fail-safe signal module	Description	Possible causes	Corrective measures [1]
0x0001	Short-circuit	SM 1226 F-DQ 4 x 24 VDC	A channel problem has been detected where either the P terminal or M terminal is at an unexpected potential.	Short-circuit of the output	Eliminate the short-circuit.
				Short-circuit between channels with different signals	Eliminate the short-circuit.
				Output overload	Eliminate the overload.
				"Maximum readback time switch on test" value is configured too small	Increase "Maximum readback time switch on test" if permissible.
				Short-circuit of output to M	Eliminate the short-circuit.
				Defective output driver	Replace the fail-safe signal module (SM).
0x0005	Overtemperature	All	• Overtemperature at microcomputer • Overtemperature at I/O	Shutdown due to violation of high temperature limit value in the module case	Check the ambient temperature. Once the fault has been eliminated, the power must be switched off and on.
0x004D	PROFIsafe communication error (CRC)	All	Transmission error in data message frame: Data inconsistent (CRC (cyclic redundancy check) error)	Communication interference between the fail-safe CPU and the fail-safe signal module (SM) (for example, due to electromagnetic interference in excess of limits or sign-of-life monitoring error)	• Check the communications connection. • Eliminate the interference.

Event ID	Diagnostic message	Fail-safe signal module	Description	Possible causes	Corrective measures [1]
0x004E	PROFIsafe communication failure (timeout)	All	Monitoring time exceeded for data message frame (timeout)	F-monitoring time exceeded	• Adjust F-monitoring time. • Check Safety program and all other CPU activities for excessive execution or demands: – Interrupts – Ethernet communication – OB scheduling conflicts – Long program paths.
0x0100	Module is defective	All	Internal error	Fail-Safe SM is defective.	Replace the fail-safe SM.
0x0103	Watchdog tripped	All	The watchdog timer in the SM communications processor timed out.	Fail-Safe SM is defective.	Replace the fail-safe SM.
0x0105	Short-circuit to L+	SM 1226 F-DQ 4 x 24 VDC	The fail-safe SM detects a channel problem where the P-terminal is unexpectedly at L+ potential.	Short-circuit to L+	Eliminate the short-circuit.
				Short-circuit between channels with different signals	Eliminate the short-circuit.
				Defective output driver	Replace the fail-safe SM.
				"Maximum readback time" value is configured too small.	Increase readback time.
0x0106	Short-circuit to ground	SM 1226 F-DQ 4 x 24 VDC	The fail-safe SM detects a channel problem where the M-switch output terminal is unexpectedly at M potential.	Short-circuit of output to M, ground, or another channel.	Eliminate the short-circuit.
				Defective output driver	Replace the fail-safe SM.
				"Maximum readback time" value is configured too small.	Increase readback time.
0x0300	Discrepancy failure, channel state 0/0	SM 1226 F-DI 16 x 24 VDC	External discrepancy failure: Channel state 0/0 with 1oo2 non-equivalent configuration	• Process signal faulty, sensor may be defective. • Configured discrepancy time too short	• Check process signal, replace sensor if necessary. • Check the configured discrepancy time. • Check the wiring. • Check that both sen-
0x0301	Discrepancy failure, channel state 0/1	SM 1226 F-DI 16 x 24 VDC	External discrepancy failure: Channel state 0/1 with 1oo2 equivalent configuration		

Event ID	Diagnostic message	Fail-safe signal module	Description	Possible causes	Corrective measures [1]
0x0302	Discrepancy failure, channel state 1/0	SM 1226 F-DI 16 x 24 VDC	External discrepancy failure: Channel state 1/0 with 1oo2 equivalent configuration	• Short-circuit • Sensor mechanical activation or alignment out of tolerance	sors are mounted and aligned to be activated together.
0x0303	Discrepancy failure, channel state 1/1	SM 1226 F-DI 16 x 24 VDC	External discrepancy failure: Channel state 1/1 with 1oo2 non-equivalent configuration		
0x0306	Internal sensor supply short-circuit to P	SM 1226 F-DI 16 x 24 VDC	SM provided sensor supply voltage shorted to P	Sensor supply shorted to P	• Eliminate the short-circuit. • Once the fault is eliminated, the power must be switched off and on.
				Short-circuit test duration configured too short	Increase short-circuit test duration.
				Failed sensor supply	Replace the fail-safe SM.
0x0307	Overload or internal sensor supply shorted to ground	SM 1226 F-DI 16 x 24 VDC	Internal sensor supply voltage shorted to M, ground, or excessive load on sensor supply	Short-circuit	• Eliminate the short-circuit. • Once the fault has been eliminated, the power must be switched off and on.
				Excessive load on sensor supply	Reduce load on sensor supply.
				Failed sensor supply	Replace the fail-safe SM.
0x030B	Channel failure acknowledgement	All	Channel configured for manual acknowledgement is ready to reintegrate	Manual acknowledgement required	Manually acknowledge correction of channel fault so that reintegration can occur.
0x0311	Frequency too high	SM 1226 F-DQ 4 x 24 VDC SM 1226 F-DQ 2 x Relay	Switching frequency exceeded; readback not in time	Process value from safety program changing too rapidly for SM to follow	• Change Safety program logic to guarantee more time between output changes.
0x0312	Undertemperature	All	• Under-temperature at microcomputers • Under-temperature at I/O	Shutdown due to violation of low temperature limit value in the SM case	• Check the ambient temperature. • Once the fault has been eliminated, the power must be switched off and on.

Event ID	Diagnostic message	Fail-safe signal module	Description	Possible causes	Corrective measures [1]
0x0313	Failure in the input circuit	SM 1226 F-DI 16 x 24 VDC	Internal fault at the read circuit/test circuit	The input SM detects a failure during bit pattern testing of inputs. EMI or SM hardware fault.	• If intermittant, probably due to interference. Eliminate interference. • If persistent, or repeats after efforts to eliminate interference, replace the fail-safe SM.
0x0316	Relay cannot be turned on	SM 1226 F-DQ 2 x Relay	Relay activated, but remains deactivated	Relay is faulty. SM supply voltage too low.	• Check for supply voltage warning messages and supply voltage. • Replace the fail-safe SM.
0x0317	Relay cannot be turned off (contacts welded)	SM 1226 F-DQ 2 x Relay	Relay deactivated, but remains activated (Relay contact is welded)	Relay is faulty, due to normal wear, excessive load, or unsuppressed inductive load.	• Replace the fail-safe SM. • Check that load current, including inrush, is within specifications. • Check for adequate inductive load suppression and capacitive load inrush limiting. • Check for circuit faults creating excessive load.
0x031C	Input shorted to P	SM 1226 F-DI 16 x 24 VDC	Input shorted to P failure	External wiring or sensor shorts input signal to L+.	Check/correct external short-circuit.
				Input configured for short-circuit detection but wired to external L+	Make wiring and configuration agree.
				Input defective	Replace the fail-safe SM.
0x031D	Output defective	SM 1226 F-DQ 2 x Relay	Relay coil driver defective	Relay or relay driver faulty	Replace the fail-safe SM.
0x031E	Read back failure	SM 1226 F-DQ 4 x 24 VDC	The SM has detected a channel problem where the expected terminal voltage(s) are not reached.	"Maximum readback time" or "Maximum readback time switch on test" configured value is too small.	Increase readback time.
				Output switch failure	Replace the fail-safe SM if output does not respond.

Event ID	Diagnostic message	Fail-safe signal module	Description	Possible causes	Corrective measures [1]
		SM 1226 F-DQ 2 x Relay	Relay state does not agree with commanded value.	Relay faulty	Replace the fail-safe SM.
0x0320	Overload	SM 1226 F-DQ 4 x 24 VDC	Over load condition at the output driver that leads to passivation of the channel	Over load at output	Eliminate over load.
0x0321	Supply voltage too high	All	Supply voltage maximum exceeded.	Supply voltage is set too high.	Adjust supply voltage.
0x0322	Supply voltage too low	All	Supply voltage minimum exceeded.	Supply voltage is set too low.	Adjust supply voltage.
0x032C	Failsafe error (0x032C)	SM 1226 F-DQ 2 x Relay	Maximum relay switch on time exceeded.	Safety program did not switch the relay within the configured "Relay continuous on time limit".	• Include in the safety program and process operations an opportunity to turn the relay "OFF" briefly, to allow the module to confirm that the relay is still under control. • Increase the "Relay continuous on time limit'. This value cannot exceed 30 days for SIL 3 applications.

[1] Once the fault is eliminated, the fail-safe signal module must be reintegrated (returned to normal state) from passivation into the safety program.

Electromagnetic interference and diagnostic reports

Electromagnetic interference can cause communication errors, disturb external and internal signal measurements, and cause processing errors. When error reports do not apparently relate to an identifiable device failure, wiring problem, programming or configuration error, consider sources of electromagnetic interference and installation and wiring problems that might introduce electromagnetic interference in your installation. Typical problem sources include poor suppression of inductive loads and voltage dips due to excessive load in-rush currents.

Technical specifications A

A.1 General technical specifications

A.1.1 Standards compliance

The S7-1200 Fail-Safe automation system design conforms to the following standards and test specifications. The test criteria for the S7-1200 automation system are based on these standards and test specifications.

Not all S7-1200 models may be certified to these standards, and certification status may change without notification. It is the user's responsibility to determine applicable certifications by referring to the ratings marked on the product. Consult your local Siemens representative if you need additional information related to the latest listing of exact approvals by part number.

Siemens products will generally be in accordance with the latest released standards as of the time of product release. For European Norm (EN) standards, the effective version will be in accordance with listings in the official journal of the European Union. Product certifications including the CE declaration of conformity and certificates from listing agencies cite the exact standards applicable to each certification.

A.1.2 Fail-Safe standards and approvals

All S7-1200 fail-safe CPUs and fail-safe signal modules (SM) are certified by TÜV. The fail-safe CPUs and signal modules are certified to standards and guidelines for functional safety. For further information, refer to the current Annex 1 of the report for the TÜV certificate "SIMATIC Safety" (http://support.automation.siemens.com/WW/view/en/49368678/134200) from the Internet.

A.1.3 PROFIsafe compatibility

- PROFIsafe address type 2
- Supports the RIOforFA-Safety profile

A.1.4 General certifications

CE approval

The S7-1200 Automation System satisfies requirements and safety related objectives according to the EC directives listed below and conforms to the harmonized European standards (EN) for the programmable controllers listed in the Official Journals of the European Community.

- EC Directive 2004/108/EC (EMC Directive) "Electromagnetic Compatibility"
  - Emission standard
    EN 61000-6-4: Industrial Environment
  - Immunity standard
    EN 61000-6-2:2005: Industrial Environment
- EC Directive 2006/42/EC (Machine Directive) "Machinery and Amending Directive 95/16/EC"
  - Safety of Machinery

    EN ISO 13849-1:2008/AC:2009 and EN ISO 13849-2:2012: Safety Related Parts of Control Systems

    EN 62061:2005/A1:2013: Functional Safety of Safety Related Electrical, Electronic, and Programmable Electronic Control Systems
- EC Directive 2006/95/EC (Low Voltage Directive) "Electrical Equipment Designed for Use within Certain Voltage Limits"
  - EN 61131-2: Programmable Controllers - Equipment requirements and Tests
- EC Directive 94/9/EC (ATEX) "Equipment and Protective Systems Intended for Use in Potentially Explosive Atmosphere"
  - EN 60079-15: Type of Protection 'n'

Note

Not all S7-1200 products are suitable for potentially explosive atmosphere locations. Only S7-1200 products that are marked with the ATEX symbol are suitable for ATEX classified hazardous locations as marked.

The CE Declaration of Conformity is held on file available to competent authorities at:

Siemens AG
Sector Industry
DF FA AS DH AMB
Postfach 1963
D-92209 Amberg
Germany

cULus approval

Underwriters Laboratories Inc. complying with:

- Underwriters Laboratories, Inc.: UL 508 Listed (Industrial Control Equipment)
- Canadian Standards Association: CSA C22.2 Number 142 (Process Control Equipment)

Note

The SIMATIC S7-1200 series meets the CSA standard.

The cULus logo indicates that the S7-1200 has been examined and certified by Underwriters Laboratories (UL) to standards UL 508 and CSA 22.2 No. 142.

FM approval

Factory Mutual Research (FM)
Approval Standard Class Number 3600 and 3611
Approved for use in:
Class I, Division 2, Gas Group A, B, C, D, Temperature Class T3C Ta = 55 °C
Class I, Zone 2, IIC, Temperature Class T3 Ta = 55 °C
Canadian Class I, Zone 2 Installation per CEC 18-150

WARNING

Substitution of components may impair the suitability for Class I, Division 2 and Zone 2.

Failure to comply with these guidelines could cause damage or unpredictable operation which could result in death or severe personal injury and/or property damage.

Repair of units should only be performed by an authorized Siemens Service Center.

IECEx approval

EN 60079-0: Explosive Atmospheres – General Requirements

EN60079-15: Electrical Apparatus for Potentially Explosive Atmospheres;
Type of protection ‘nA’
IECEX FMG14.0012X
Ex nA IIC Tx Gc

IECEx rating information may appear on the product with the FM Hazardous Location information.

Only products marked with an IECEx rating are approved. Consult your local Siemens representative if you need additional information related to the latest listing of exact approvals by part number.

Relay models are not included in IECEx approvals.

Refer to specific product marking for temperature rating.

Install modules in a suitable enclosure providing a minimum degree of protection of IP54 according to IEC 60079-15.

ATEX approval

ATEX approval applies to DC models only. ATEX approval does not apply to Relay models.

EN 60079-0: Explosive Atmospheres - General Requirements

EN 60079-15: Electrical Apparatus for Potentially Explosive Atmospheres;
Type of protection 'nA'
II 3 G Ex nA IIC T4 or T3 Gc

Install modules in a suitable enclosure providing a minimum degree of protection of IP54 according to EN 60529 or a location providing an equivalent degree of protection.

Attached cables and conductors shall be rated for the actual temperature measured under rated conditions.

Modules shall be protected from overvoltage according to the "Safe functional extra low voltage requirement (power supplies and other system components)" (Page 90), "Surge immunity" section.

C-Tick approval

The S7-1200 automation system satisfies requirements of standards to AS/NZS CISPR16 (Class A).

Korea Certification

The S7-1200 automation system satisfies the requirements of the Korean Certification (KC Mark). It has been defined as Class A Equipment and is intended for industrial applications and has not been considered for home use.

Eurasian Customs Union approval (Belarus, Kazakhstan, Russian Federation)

EAC (Eurasion Conformity): Declaration of Conformity according to Technical Regulation of Customs Union (TR CU)

Maritime approval

The S7-1200 products are periodically submitted for special agency approvals related to specific markets and applications. Consult your local Siemens representative if you need additional information related to the latest listing of exact approvals by part number.

Classification societies:

- ABS (American Bureau of Shipping)
- BV (Bureau Veritas)
- DNV (Det Norske Veritas)
- GL (Germanischer Lloyd)
- LRS (Lloyds Register of Shipping)
- Class NK (Nippon Kaiji Kyokai)
- Korean Register of Shipping

A.1.5 Industrial environments

The S7-1200 automation system is designed for use in industrial environments.

Table A- 1 Industrial environments

Application field	Emission requirements	Immunity requirements
Industrial	EN 61000-6-4	EN 61000-6-2

A.1.6 Electromagnetic compatibility

Electromagnetic Compatibility (EMC) is the ability of an electrical device to operate as intended in an electromagnetic environment and to operate without emitting levels of electromagnetic interference (EMI) that may disturb other electrical devices in the vicinity.

For safety related functions, additional EMC requirements are applied according to IEC 61326-3-1 and IEC 61326-3-2.

Table A- 2 Immunity per EN 61000-6-2

Electromagnetic compatibility - Immunity per EN 61000-6-2	
EN 61000-4-2 Electrostatic discharge	8 kV air discharge to all surfaces 6 kV contact discharge to exposed conductive surfaces
EN 61000-4-3 Radiated, radio-frequency, electromagnetic field immunity test	80 to 1000 MHz, 10 V/m, 80% AM at 1 kHz 1.4 to 2.0 GHz, 3 V/m, 80% AM at 1 kHz 2.0 to 2.7 GHz, 1 V/m, 80% AM at 1 kHz
EN 61000-4-4 Fast transient bursts	2 kV, 5 kHz with coupling network to AC and DC system power 2 kV, 5 kHz with coupling clamp to I/O
EN 61000-4-5 Surge immunity	AC systems - 2 kV common mode, 1kV differential mode DC systems - 2 kV common mode, 1kV differential mode For DC systems (I/O signals, DC power systems) external protection is required. Refer to "Safe functional extra low voltage requirement (power supplies and other system components)" (Page 90), "Surge immunity" for the recommended protection devices.
EN 61000-4-6 Conducted disturbances	150 kHz to 80 MHz, 10 V RMS, 80% AM at 1kHz
EN 61000-4-11 Voltage dips	AC systems 0% for 1 cycle, 40% for 12 cycles and 70% for 30 cycles at 60 Hz

A.1.7 Surge immunity

Wiring systems subject to surges from lightning strike coupling must be equipped with external protection. One specification for evaluation of protection from lightning type surges is found in EN 61000-4-5, with operational limits established by EN 61000-6-2. S7-1200 DC CPUs and signal modules require external protection to maintain safe operation when subject to surge voltages defined by this standard.

Listed below are some devices that support the needed surge immunity protection. These devices only provide the protection if they are properly installed according to the manufacturer's recommendations. Devices manufactured by other vendors with the same or better specifications can also be used:

Table A- 3 Devices that support surge immunity protection

Sub-system	Protection device
+24 VDC power	BLITZDUCTOR VT, BVT AVD 24, Part Number 918 422
Industrial Ethernet	DEHNpatch DPA M CLE RJ45B 48, Part Number 929 121
+24 VDC digital inputs	DEHN, Inc., Type DCO SD2 E 24, Part Number 917 988
+24 VDC digital outputs and sensor supply	DEHN, Inc., Type DCO SD2 E 24, Part Number 917 988
Analog IO	DEHN, Inc., Type DCO SD2 E 12, Part Number 917 987
Relay outputs	None required

Table A- 4 Conducted and radiated emissions per EN 61000-6-4

Electromagnetic compatibility - Conducted and radiated emissions per EN 61000-6-4		
Conducted Emissions EN 55011, Class A, Group 1	0.15 MHz to 0.5 MHz	< 79dB (µV) quasi-peak; <66 dB (µV) average
	0.5 MHz to 5 MHz	< 73dB (µV) quasi-peak; <60 dB (µV) average
	5 MHz to 30 MHz	< 73dB (µV) quasi-peak; <60 dB (µV) average
Radiated Emissions EN 55011, Class A, Group 1	30 MHz to 230 MHz	< 40dB (µV/m) quasi-peak; measured at 10 m
	230 MHz to 1 GHz	< 47dB (µV/m) quasi-peak; measured at 10 m
	1 GHz to 3 GHz	< 76dB (uV/m) quasi peak, measured at 10 m

A.1.8 Environmental conditions

Table A- 5 Transport and storage

Environmental conditions - Transport and storage	
EN 60068-2-2, Test Bb, Dry heat and EN 60068-2-1, Test Ab, Cold	-40 °C to +70 °C
EN 60068-2-30, Test Db, Damp heat	25 °C to 55 °C, 95% humidity
EN 60068-2-14, Test Na, temperature shock	-40 °C to +70 °C, dwell time 3 hours, 5 cycles
EN 60068-2-32, Free fall	0.3 m, 5 times, product packaging
Atmospheric pressure	1080 to 660h Pa (corresponding to an altitude of -1000 to 3500m)

Table A- 6 Operating conditions

Environmental conditions - Operating	
Ambient temperature range (Inlet Air 25 mm below unit)	0 °C to 55 °C horizontal mounting 0 °C to 45 °C vertical mounting 95% non-condensing humidity
Atmospheric pressure	1080 to 795 hPa (corresponding to an altitude of -1000 to 2000m)
Concentration of contaminants	$S0_2$: < 0.5 ppm; H_2S: < 0.1 ppm; RH < 60% non-condensing
EN 60068-2-14, Test Nb, temperature change	5 °C to 55 °C, 3 °C/minute
EN 60068-2-27 Mechanical shock	15 G, 11 ms pulse, 6 shocks in each of 3 axis
EN 60068-2-6 Sinusoidal vibration	DIN rail mount: 3.5 mm from 5-9 Hz, 1G from 9 - 150 Hz Panel Mount: 7.0 mm from 5-9 Hz, 2G from 9 to 150 Hz 10 sweeps each axis, 1 octave per minute

Table A- 7 High potential isolation test

High potential isolation test [2]	
24 V/5 V nominal circuits	520 VDC (type test of optical isolation boundaries)
115/230 V circuits to ground	1500 VAC
115/230 V circuits to 115/230 V circuits	1500 VAC
115 V/230V circuits to 24 V/5 V circuits	1500 VAC (3000 VAC / 4242 VDC type test)
Ethernet port to 24 V/5 V circuits and ground[1]	1500 VAC (type test only)

1 Ethernet port isolation is designed to limit hazard during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

2 SM 1226 F-DQ 2 x Relay has higher test voltages. See data sheet for that product.

A.1.9 Protection class

Protection Class II according to EN 61131-2:

- S7-1200 is open equipment and must be enclosed in additional protection as described in Section 4.1.2: "Guidelines for installing S7-1200 Fail-Safe devices" (Page 80).
- S7-1200 systems including AC power supply or relays which can be connected to AC voltage achieve Class II when installed in a suitable enclosure.
- S7-1200 systems including only connections to SELV / PELV achieve Class III when installed in a suitable enclosure.
- You do not require a protective conductor. The S7-1200 has no protective ground connection.

A.1.10 Degree of protection

- IP20 Mechanical Protection, EN 60529
- Protects against finger contact with high voltage as tested by standard probe. External protection required for dust, dirt, water and foreign objects of < 12.5mm in diameter.

A.1.11 Rated voltages

Rated voltage	Tolerance
24 VDC	20.4 VDC to 28.8 VDC

When you suddenly apply 24 VDC power to the S7-1200 CPU or digital I/O signal modules (SM), including fail-safe SM, short-term current flows can occur which briefly mimic the effect of "1" signals at process outputs and inputs. Digital outputs can trigger to ON state for approximately 50 microseconds at power application. The SMs deliberately test functional safety P- and M-switch outputs ON at different times for up to the user-configurable "Maximum readback time switch on test" (500 microseconds to 5 ms) during the power up sequence and as a cyclic bit-pattern test. This test pulse can energize the load in the presence of a switch or wiring fault on the opposite side of the load circuit. Such short pulses are typically not a hazard for electromechanical loads, but you must consider the effect. High-speed electronic receiver circuits can detect short pulses and improperly interpret the short pulses as deliberate "1" signals.

WARNING

Short term current and voltage pulses can occur on 24 VDC I/O circuits near the time that power is applied.

Such short term pulses can cause unexpected activation or position changes in machinery, resulting in death or serious injury to personnel and/or property damage.

If your installation includes receivers which can be responsive to short pulses as described above, you should apply measures such as power sequencing or progressive removal of safety lockouts to assure that unexpected machine operations do not occur.

A.1.12 Reverse voltage protection

Reverse voltage protection circuitry is provided on each terminal pair of +24 VDC power or user input power for CPUs, signal modules (SM), and signal boards (SB). It is still possible to damage the system by wiring different terminal pairs in opposite polarities.

Some of the 24 VDC power input ports in the S7-1200 system are interconnected, with a common logic circuit connecting multiple M terminals. For example, the following circuits are interconnected when designated as "not isolated" in the data sheets: the 24 VDC power supply of the CPU, the power input for the relay coil of an SM, or the power supply for a non-isolated analog input. All non-isolated M terminals must connect to the same external reference potential.

> **WARNING**
>
> **Connecting non-isolated M terminals to different reference potentials will cause unintended current flows that may cause damage or unpredictable operation in the PLC and any connected equipment.**
>
> Failure to comply with these guidelines could cause damage or unpredictable operation which could result in death or severe personal injury and/or property damage.
>
> Always ensure that all non-isolated M terminals in an S7-1200 system are connected to the same reference potential.

A.1.13 DC outputs

Short-circuit protection circuitry is not provided for DC outputs on CPUs, signal modules (SM) and signal boards (SB).

A.1.14 Relay electrical service life

The typical performance data estimated from sample tests is shown below. Actual performance may vary depending upon your specific application. An external protection circuit that is adapted to the load will enhance the service life of the contacts. N.C. contacts have a typical service life of about one-third that of the N.O. contact under inductive and lamp load conditions.

An external protective circuit will increase the service life of the contacts.

Table A- 8 Typical performance data

Data for selecting an actuator				
Continuous thermal current		2 A max.		
Switching capacity and life of the contacts				
	For ohmic load	Voltage	Current	Number of operating cycles (typical)
		24 VDC	2.0 A	0.1 million
		24 VDC	1.0 A	0.2 million
		24 VDC	0.5 A	1.0 million
		48 VAC	1.5 A	1.5 million
		60 VAC	1.5 A	1.5 million
		120 VAC	2.0 A	1.0 million
		120 VAC	1.0 A	1.5 million
		120 VAC	0.5 A	2.0 million
		230 VAC	2.0 A	1.0 million
		230 VAC	1.0 A	1.5 million
		230 VAC	0.5 A	2.0 million
	For inductive load (according to IEC 947-5-1 DC13/AC15)	Voltage	Current	Number of operating cycles (typical)
		24 VDC	2.0 A	0.05 million
		24 VDC	1.0 A	0.1 million
		24 VDC	0.5 A	0.5 million
		24 VAC	1.5 A	1.0 million
		48 VAC	1.5 A	1.0 million
		60 VAC	1.5 A	1.0 million
		120 VAC	2.0 A	0.7 million
		120 VAC	1.0 A	1.0 million
		120 VAC	0.5 A	1.5 million
		230 VAC	2.0 A	0.7 million
		230 VAC	1.0 A	1.0 million
		230 VAC	0.5 A	1.5 million
Activating a digital input		Possible		
Switching frequency				
	Mechanical	Max. 10 Hz		
	At ohmic load	Max. 1 Hz		
	At inductive load (according to IEC 947-5-1 DC13/AC15)	Max. 0.5 Hz		

Data for selecting an actuator		
	At lamp load	Max. 1Hz

A.1.15 Internal CPU memory retention

- Lifetime of retentive data and data log data: 10 years
- Power down retentive data, Write cycle endurance: 2 million cycles
- Data log data, up to 2 KB per data log entry, Write cycle endurance: 500 million data log entries

---

Note

Effect of data logs on internal CPU memory

Each data log write consumes at a minimum 2 KB of memory. If your program writes small amounts of data frequently, it is consuming at least 2 KB of memory on each write. A better implementation would be to accumulate the small data items in a data block (DB), and to write the data block to the data log at less frequent intervals.

If your program writes many data log entries at a high frequency, consider using a replaceable SD memory card.

A.1.16 Overvoltage Category III

Relay contacts of the SM 1226 F-DQ 2 x Relay (6ES7 226 6RA32 0XB0) are designed to Overvoltage Category III and may be used in AC mains circuits without further overvoltage protection.

Relay contact outputs on the following products do not meet requirements for Overvoltage Category III, the requirement for EN 50156-1 conforming equipment:

- CPU 1214FC DC/DC/RLY CPU (6ES7 214-1HF40-0XB0)
- CPU 1215FC DC/DC/RLY CPU (6ES7 215-1HF40-0XB0)
- SM 1222 DQ 8 x Relay (6ES7 222-1HF32-0XB0)
- SM 1222 DQ 16 x Relay (6ES7 222-1HH32-0XB0)
- SM 1223 DI 8 x 120/230 VAC In / DQ 8 x Relay (6ES7 223 1QH32 0XB0)

When using the SM 1226 F-DQ 2 x Relay in safety critical circuits of burner applications, the relays on any of the products listed above can be used, but only if used in one of the following:

- SELV/PELV circuits
- Circuits connected to the electrical mains with permanent, recognized protection that reduces transients to Overvoltage Category II

Otherwise, the CPU and I/O system, including the SM 1226 F-DQ 2 x Relay, will not meet the Overvoltage Category III requirement for burner applications.

> **WARNING**
>
> **Adjacent relay contacts in the same channel of the SM 1226 F DQ 2 x Relay are not rated to separate AC line from SELV / PELV.**
>
> Death or serious personal injury and damage to machines and equipment can result if SELV/PELV circuits are wired adjacent to high voltage circuits on this module.
>
> The A and B circuits of each output must either be both AC line or both SELV.

A.2 Fail-Safe CPU technical specifications

A.2.1 Fail-Safe additions/exceptions

The following sections discuss exceptions and additions for the CPU 1214FC and CPU1215FC that differentiates them from the standard CPU 1214C and CPU 1215C.

A.2.1.1 Areas of application

The S7-1200 fail-safe CPUs are intended for applications including Functional Safety requirements. In addition to the safety program, you can also program standard applications.

A.2.1.2 Restrictions with "READ_DBL" and "WRIT_DBL"

If an F-DB is specified as the target address, a READ_DBL instruction execution fails when reading data from load memory into work memory.

If an F-DB is specified as the target address, a WRIT_DBL instruction execution fails when writing data from work memory to load memory.

A.2.1.3 Restrictions to configuring the retentive behavior of data blocks

The configuration of retentive data blocks is not supported for F-DBs.

This means that the current values of the F-DBs will not be retentive in the event of Power OFF/ON and Restart (STOP-RUN) of the fail-safe CPU. The F-DBs are always set to the initial values from the load memory.

In the F-DBs, for all tags the "Retain" check box is grayed out.

A.2.1.4 Probabilities of failure

Probability of failure values are estimated using standard data tables and calculation methods according to international standards, specifically for the purpose of calculating PFD and PFH values according to IEC 61508:2010 and related functional safety standards. The calculations assume products operated within specifications and repair of diagnosed faults within 100 hours:

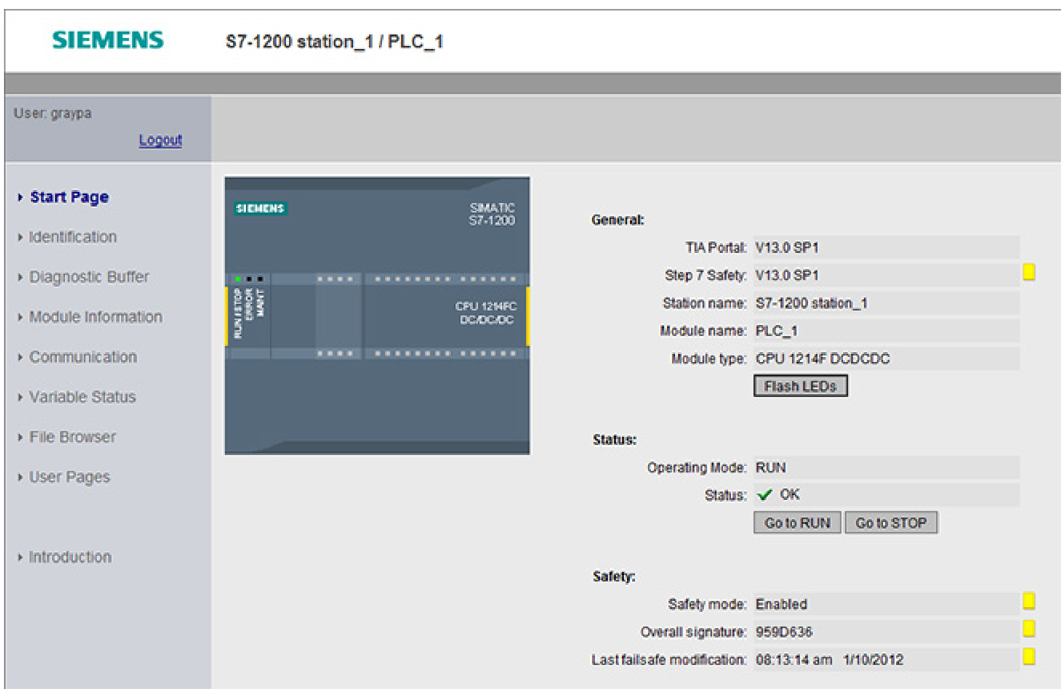
	Operation in Low Demand Mode, Average probability of a dangerous failure on demand (PFD_avg)	Operation in High Demand or Continuous Mode, Average frequency of a dangerous failure per hour (PFH)	Proof test interval (Mission time or Useful lifetime)
S7-1200 fail-safe CPUs	< 2.00E-05	< 1.00E-09 1/h	20 years

A.2.1.5 Web server

The S7-1200 fail-safe CPUs show you the following information on the "Start Page" of the web server:

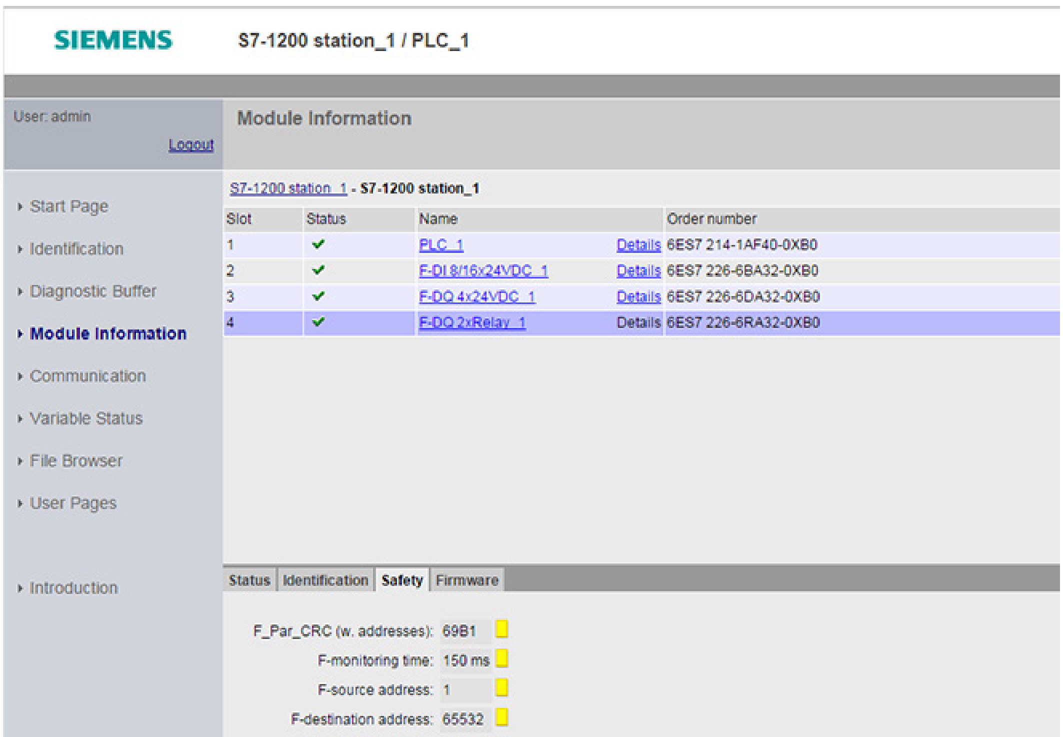
- TIA Portal and STEP 7 Safety versions
- Safety mode enabled/disabled
- Overall signature
- Last fail-safe modification

Note: The time displayed for "Last fail-safe modification" depends on the time being correctly set in the PLC when you load the program. Note the time is not correct in the PLC if you remove power from the PLC for an extended time before the program was loaded. The BB 1297 Battery Board allows a longer power down without loss of correct time.



Each F-I/O shows you the following information on the "Module information" page in the "Safety" tab:

- F_Par_CRC (w addresses) (F-parameter signature)
- Safety mode
- F-monitoring time
- F-source address
- F-destination address



You do not have write access to F-blocks.

A.2.1.6 Using a memory card with the S7-1200 Fail-Safe CPU

The S7-1200 memory card used as a transfer card is a way to copy a program into the PLC Internal Load Memory (ILM) without a connected TIA Portal. You remove the transfer card after program installation, and subsequent power cycles use the program stored in the ILM.

A memory card used as a program card keeps the PLC program on the card. If you remove the memory card, the ILM is empty, and there is no program in the PLC.

Refer to the S7-1200 Programmable Controller System Manual (http://support.automation.siemens.com/WW/view/en/91696622) for general instructions for creating and using transfer cards and memory cards. The S7-1200 fail-safe CPU behavior when using a memory card has some differences from the standard CPU:

- When the S7-1200 fail-safe CPU starts with no memory card and the ILM is empty, the fail-safe CPU's STOP and MAINT LEDs flash for three seconds. This provides a temporary visual indication that the ILM is empty. The TIA Portal or a memory card must be used to load a user program.
- When the fail-safe CPU starts with a program memory card installed and the ILM is not empty, the fail-safe CPU erases the ILM and then stops, flashing the STOP and MAINT LEDs. This is a visual indication that the ILM is erased and that the fail-safe CPU is waiting for a power cycle or a memory reset command in order to continue. Continuation and subsequent power cycles load the program from the memory card.
- When the fail-safe CPU starts with an empty memory card installed and the ILM is not empty, the fail-safe CPU copies the program from the ILM to the memory card. The fail-safe CPU then erases the ILM and stops, flashing the STOP and MAINT LEDs. This is an indication that the ILM is erased and that the fail-safe CPU is waiting for a power cycle or a memory reset command in order to continue. Continuation and subsequent power cycles load the program from the memory card.
- When the fail-safe CPU starts with a transfer memory card installed and the ILM is not empty, the fail-safe CPU erases the ILM and then stops, flashing the STOP and MAINT LEDs. This is a visual indication that the ILM is erased and that the fail-safe CPU is waiting for a power cycle or a memory reset command in order to continue. Continuation copies the user program from the memory card to the ILM, and then the fail-safe CPU stops, with the STOP LED on and the MAINT LED flashing. At this point, you must remove the transfer memory card and then power cycle or command a memory reset in order to continue. Continuation and subsequent power cycles load the program from the ILM.

Refer to the SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual (http://support.automation.siemens.com/WW/view/en/54110126/0/en), Section 10.4: "Function test of safety program and protection through program identification" for instructions on transferring programs.

> **WARNING**
>
> **Loading an incorrect user program into a fail-safe CPU results in incorrect execution and total or partial loss of the safety function.**
>
> Loss of the safety function can result in unexpected machine or process operation, which can cause death, severe personal injury, and/or property damage.
>
> Follow the instructions as provided in the *SIMATIC, IndustrialSoftware, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual* for properly identifying safety programs and controlling how you load programs into a fail-safe CPU.

A.2.2 CPU 1214FC

A.2.2.1 General specifications and features

Table A- 9 General

Technical data	CPU 1214FC DC/DC/Relay	CPU 1214FC DC/DC/DC
Article number	6ES7 214-1HF40-0XB0	6ES7 214-1AF40-0XB0
Dimensions W x H x D (mm)	110 x 100 x 75	
Shipping weight	435 grams	415 grams
Power dissipation	12 W	
Current available (SM and CM bus)	1600 mA max. (5 VDC)	
Current available (24 VDC)	400 mA max. (sensor power)	
Digital input current consumption (24 VDC)	4 mA/input used	

Table A- 10 CPU features

Technical data		Description
User memory (Refer to "General technical specifications (Page 132), "Internal CPU memory retention".)	Work	125 Kbytes
	Load	4 Mbytes internal, expandable up to SD card size
	Retentive	10 Kbytes
On-board digital I/O		14 inputs/10 outputs
On-board analog I/O		2 inputs
Process image size		1024 bytes of inputs (I)/1024 bytes of outputs (Q)
Bit memory (M)		8192 bytes
Temporary (local) memory		• 16 Kbytes for startup and program cycle (including associated FBs and FCs) • 6 Kbytes for each of the other interrupt priority levels (including FBs and FCs)
Signal modules expansion		8 SMs max.
SB, CB, BB expansion		1 max.
Communication module expansion		3 CMs max.
High-speed counters		Up to 6 configured to use any built-in or SB inputs. (Refer to the *S7-1200 System Manual*. for more information.) • 100/[1]80 kHz (Ia.0 to Ia.5) • 30/[1]20 kHz (Ia.6 to Ib.5)
Pulse outputs[2]		Up to 4 configured to use any built-in or SB outputs • 100 kHz (Qa.0 to Qa.3) • 30 kHz (Qa.4 to Qb.1)
Pulse catch inputs		14

Technical data	Description
Time delay interrupts	4 total with 1 ms resolution
Cyclic interrupts	4 total with 1 ms resolution
Edge interrupts	12 rising and 12 falling (16 and 16 with optional signal board)
Memory card	SIMATIC Memory Card (optional)
Real time clock accuracy	+/- 60 seconds/month
Real time clock retention time	20 days typ./12 days min. at 40 °C (maintenance-free Super Capacitor)

[1] The slower speed is applicable when the HSC is configured for quadrature mode of operation.

[2] For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

A.2.2.2 Performance

Table A- 11 Performance

Type of instruction	Execution speed
Boolean	0.08 μs/instruction
Move Word	1.7 μs/instruction
Real math	2.3 μs/instruction

A.2.2.3 Timers, counters and code blocks supported

Table A- 12 Blocks, timers and counters supported by CPU 1214FC

Element		Description
Blocks	Type	OB, FB, FC, DB
	Size	64 Kbytes
	Quantity	Up to 1024 blocks total (OBs + FBs + FCs + DBs)
	Address range for FBs, FCs, and DBs	FB and FC: 1 to 65535 (such as FB 1 to FB 65535) DB: 1 to 59999
	Nesting depth	16 from the program cycle or startup OB 6 from any interrupt event OB
	Monitoring	Status of 2 code blocks can be monitored simultaneously
OBs	Program cycle	Multiple
	Startup	Multiple
	Time-delay interrupts	4 (1 per event)
	Cyclic interrupts	4 (1 per event)
	Hardware interrupts	50 (1 per event)
	Time error interrupts	1
	Diagnostic error interrupts	1
	Pull or plug of modules	1
	Rack or station failure	1
	Time of day	Multiple
	Status	1
	Update	1
	Profile	1
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, 16 bytes per timer
Counters	Type	IEC
	Quantity	Limited only by memory size

Element		Description
	Storage	Structure in DB, size dependent upon count type • SInt, USInt: 3 bytes • Int, UInt: 6 bytes • DInt, UDInt: 12 bytes

Table A- 13 Communication

Technical data	Description
Number of ports	1
Type	Ethernet
HMI device	4
Programming device (PG)	1
Connections	• 8 for Open User Communication (active or passive): TSEND_C, TRCV_C, TCON, TDISCON, TSEND, and TRCV • 3 for server GET/PUT (CPU-to-CPU) S7 communication • 8 for client GET/PUT (CPU-to-CPU) S7 communication
Data rates	10/100 Mb/s
Isolation (external signal to PLC logic)	Transformer isolated, 1500 VAC, for short term event safety only
Cable type	CAT5e shielded

Table A- 14 Power supply

Technical data		CPU 1214FC DC/DC/Relay	CPU 1214FC DC/DC/DC
Voltage range		20.4 VDC to 28.8 VDC	
Line frequency		--	
Input current (max. load)	CPU only	500 mA at 24 VDC	
	CPU with all expansion accessories	1500 mA at 24 VDC	
Inrush current (max.)		12 A at 28.8 VDC	
Isolation (input power to logic)		Not isolated	
Ground leakage, AC line to functional earth		-	
Hold up time (loss of power)		10 ms at 24 VDC	
Internal fuse, not user replaceable		3 A, 250 V, slow blow	

Table A- 15 Sensor power

Technical data	CPU 1214FC DC/DC/Relay	CPU 1214FC DC/DC/DC
Voltage range	L+ minus 4 VDC min.	
Output current rating (max.)	400 mA (short-circuit protected)	
Maximum ripple noise (<10 MHz)	Same as input line	
Isolation (CPU logic to sensor power)	Not isolated	

A.2.2.4 Digital inputs and outputs

Table A- 16 Digital inputs

Technical data	CPU 1214FC DC/DC/Relay	CPU 1214FC DC/DC/DC
Number of inputs	14	
Type	Sink/Source (IEC Type 1 sink)	
Rated voltage	24 VDC at 4 mA, nominal	
Continuous permissible voltage	30 VDC, max.	
Surge voltage	35 VDC for 0.5 sec.	
Logic 1 signal (min.)	15 VDC at 2.5 mA	
Logic 0 signal (max.)	5 VDC at 1 mA	
Isolation (field side to logic)	500 VAC for 1 minute	
Isolation groups	1	
Filter times	us settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
HSC clock input rates (max.) (Logic 1 Level = 15 to 26 VDC)	100/80 kHz (Ia.0 to Ia.5) 30/20 kHz (Ia.6 to Ib.5)	
Number of inputs on simultaneously	14 inputs at 55 °C horizontal or 45 °C vertical	
Cable length (meters)	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs	

Table A- 17 Digital outputs

Technical data	CPU 1214FC DC/DC/Relay	CPU 1214FC DC/DC/DC
Number of outputs	10	
Type	Relay, mechanical	Solid state - MOSFET (sourcing)
Voltage range	5 to 30 VDC or 5 to 250 VAC	20.4 to 28.8 VDC
Logic 1 signal at max. current	--	20 VDC min.
Logic 0 signal with 10 KΩ load	--	0.1 VDC max.
Current (max.)	2.0 A	0.5 A
Lamp load	30 W DC / 200 W AC	5 W
ON state resistance	0.2 Ω max. when new	0.6 Ω max.
Leakage current per point	--	10 μA max.
Surge current	7 A with contacts closed	8 A for 100 ms max.
Overload protection	No	
Required external overload protection [4]	10 A maximum must be limited to any common	5 A maximum must be limited to any common
Isolation (field side to logic)	1500 VAC for 1 minute (coil to contact) None (coil to logic)	500 VAC for 1 minute
Isolation resistance	100 MΩ min. when new	--
Isolation between open contacts	750 VAC for 1 minute	--

Technical data	CPU 1214FC DC/DC/Relay	CPU 1214FC DC/DC/DC
Isolation groups	2	1
Isolation (group-to-group)	1500 VAC [1]	--
Inductive clamp voltage	--	L+ minus 48 VDC, 1 W dissipation
Switching delay (Qa.0 to Qa.3)	10 ms max.	1.0 μs max., off to on 3.0 μs max., on to off
Switching delay (Qa.4 to Qb.1)	10 ms max.	50 μs max., off to on 200 μs max., on to off
Maximum relay switching frequency	1 Hz	--
Pulse Train Output rate	Not recommended [2]	100 kHz (Qa.0 to Qa.3) [3], 2 Hz min. 20 kHz (Qa.4 to Qb.1) [3]
Lifetime mechanical (no load)	10,000,000 open/close cycles	--
Lifetime contacts at rated load	100,000 open/close cycles	--
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Number of outputs on simultaneously	10 outputs at 55 °C horizontal or 45 °C vertical	
Cable length (meters)	500 m shielded, 150 m unshielded	

[1] Relay group-to-group isolation separates line voltage from SELV/PELV and separates different phases up to 250 VAC line to ground.

[2] For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

[3] Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

[4] External overload protection is to limit fire hazard. Overload can damage relay or transistor output.

A.2.2.5 Analog inputs

Table A- 18 Analog inputs

Technical data	Description
Number of inputs	2
Type	Voltage (single-ended)
Full-scale range	0 to 10 V
Full-scale range (data word)	0 to 27648
Overshoot range	10.001 to 11.759 V
Overshoot range (data word)	27649 to 32511
Overflow range	11.760 to 11.852 V
Overflow range (data word)	32512 to 32767
Resolution	10 bits
Maximum withstand voltage	35 VDC
Smoothing	None, Weak, Medium, or Strong See the table for step response (ms) for the analog inputs of the CPU (Page 155).
Noise rejection	10, 50, or 60 Hz
Impedance	≥100 KΩ
Isolation (field side to logic)	None
Accuracy (25 °C / 0 to 55 °C)	3.0% / 3.5% of full-scale
Cable length (meters)	100 m, shielded twisted pair

Step response of built-in analog inputs of the CPU

Table A- 19 Step Response (ms), 0 V to 10 V measured at 95%

Smoothing selection (sample averaging)	Rejection frequency (Integration time)		
	60 Hz	50 Hz	10 Hz
None (1 cycle): No averaging	50 ms	50 ms	100 ms
Weak (4 cycles): 4 samples	60 ms	70 ms	200 ms
Medium (16 cycles): 16 samples	200 ms	240 ms	1150 ms
Strong (32 cycles): 32 samples	400 ms	480 ms	2300 ms
Sample time	**4.17 ms**	**5 ms**	**25 ms**

Sample time for the built-in analog ports of the CPU

Table A- 20 Sample time for built-in analog inputs of the CPU

Rejection frequency (Integration time selection)	Sample time
60 Hz (16.6 ms)	4.17 ms
50 Hz (20 ms)	5 ms
10 Hz (100 ms)	25 ms

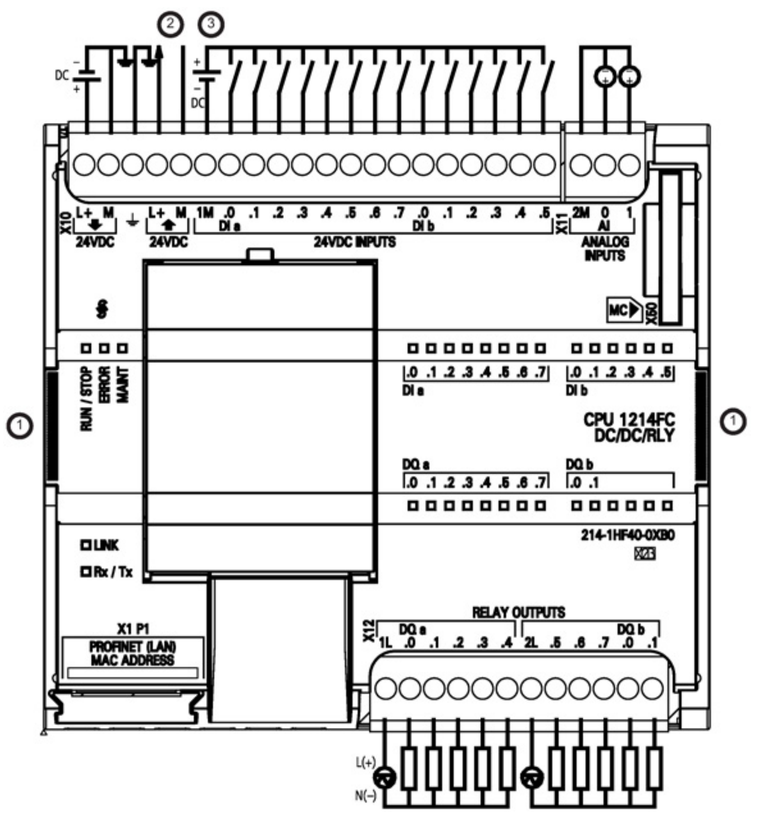
Measurement ranges of the analog inputs for voltage of the CPU

Table A- 21 Analog input representation for voltage of the CPU

System		Voltage Measuring Range	
Decimal	**Hexadecimal**	**0 to 10 V**	
32767	7FFF	11.851 V	Overflow
32512	7F00		
32511	7EFF	11.759 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range
20736	5100	7.5 V	
34	22	12 mV	
0	0	0 V	
Negative values		Negative values are not supported	

A.2.2.6 CPU 1214FC wiring diagrams

Table A- 22 CPU 1214FC DC/DC/Relay (6ES7 214-1HF40-0XB0)

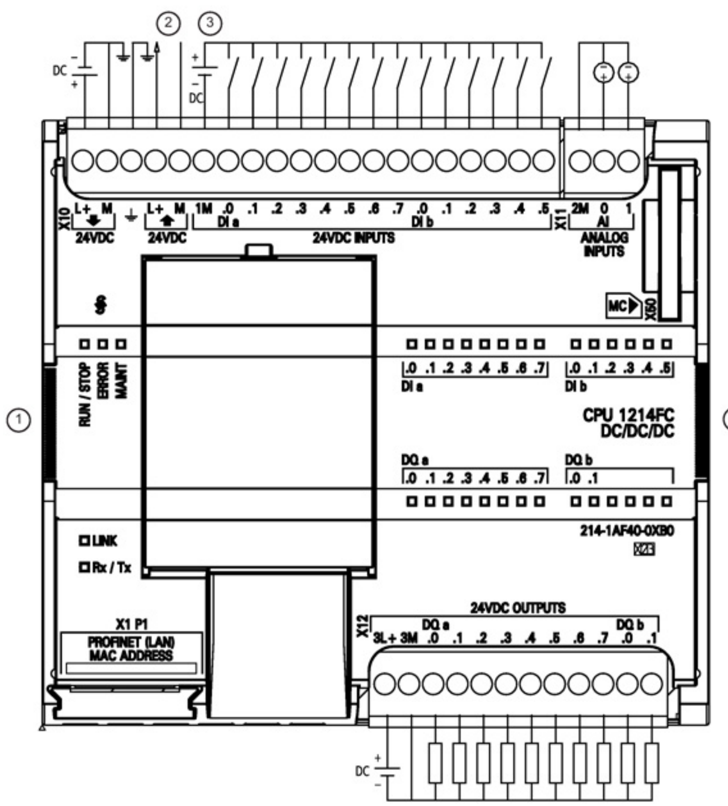


①	The two rectangular areas are yellow. These are only on the fail-safe CPUs.
②	24 VDC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
③	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note: X11 connectors must be gold. See Appendix B, Spare Parts for article number.	

Table A- 23 Connector pin locations for CPU 1214FC DC/DC/Relay (6ES7 214-1HF40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24VDC	2 M	1L
2	M / 24VDC	AI 0	DQ a.0
3	Functional Earth	AI 1	DQ a.1
4	L+ / 24VDC Sensor Out	--	DQ a.2
5	M / 24VDC Sensor Out	--	DQ a.3
6	1M	--	DQ a.4
7	DI a.0	--	2L
8	DI a.1	--	DQ a.5
9	DI a.2	--	DQ a.6
10	DI a.3	--	DQ a.7
11	DI a.4	--	DQ b.0
12	DI a.5	--	DQ b.1
13	DI a.6	--	--
14	DI a.7	--	--
15	DI b.0	--	--
16	DI b.1	--	--
17	DI b.2	--	--
18	DI b.3	--	--
19	DI b.4	--	--
20	DI b.5	--	--

Table A- 24 CPU 1214FC DC/DC/DC (6ES7 214-1AF40-0XB0)



①	The two rectangular areas are yellow. These are only on the fail-safe CPUs.
②	24 VDC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
③	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

Note: X11 connectors must be gold. See Appendix B, Spare Parts for article number.

Table A- 25 Connector pin locations for CPU 1214FC DC/DC/DC (6ES7 214-1AF40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24VDC	2 M	3L+
2	M / 24VDC	AI 0	3M
3	Functional Earth	AI 1	DQ a.0
4	L+ / 24VDC Sensor Out	--	DQ a.1
5	M / 24VDC Sensor Out	--	DQ a.2
6	1M	--	DQ a.3
7	DI a.0	--	DQ a.4
8	DI a.1	--	DQ a.5
9	DI a.2	--	DQ a.6
10	DI a.3	--	DQ a.7
11	DI a.4	--	DQ b.0
12	DI a.5	--	DQ b.1
13	DI a.6	--	--
14	DI a.7	--	-
15	DI b.0	--	--
16	DI b.1	--	--

Pin	X10	X11 (gold)	X12
17	DI b.2	--	--
18	DI b.3	--	--
19	DI b.4	--	--
20	DI b.5	--	--

Note

Unused analog inputs should be shorted.

A.2.3 CPU 1215FC

A.2.3.1 General specifications and features

Table A- 26 General

Technical data	CPU 1215FC DC/DC/Relay	CPU 1215FC DC/DC/DC
Article number	6ES7 215-1HF40-0XB0	6ES7 215-1AF40-0XB0
Dimensions W x H x D (mm)	130 x 100 x 75	
Shipping weight	550 grams	520 grams
Power dissipation	12 W	
Current available (SM and CM bus)	1600 mA max. (5 VDC)	
Current available (24 VDC)	400 mA max. (sensor power)	
Digital input current consumption (24 VDC)	4 mA/input used	

Table A- 27 CPU features

Technical data		Description
User memory (Refer to "General technical specifications (Page 132), "Internal CPU memory retention".)	Work	150 Kbytes
	Load	4 Mbytes, internal, expandable up to SD card size
	Retentive	10 Kbytes
On-board digital I/O		14 inputs/10 outputs
On-board analog I/O		2 inputs/2 outputs
Process image size		1024 bytes of inputs (I)/1024 bytes of outputs (Q)
Bit memory (M)		8192 bytes
Temporary (local) memory		• 16 Kbytes for startup and program cycle (including associated FBs and FCs) • 6 Kbytes for each of the other interrupt priority levels (including FBs and FCs)
Signal modules expansion		8 SMs max.
SB, CB, BB expansion		1 max.
Communication module expansion		3 CMs max.
High-speed counters		Up to 6 configured to use any built-in or SB inputs. (Refer to the *S7-1200 System Manual* for more information.) • 100/[1]80 kHz (Ia.0 to Ia.5) • 30/[1]20 kHz (Ia.6 to Ib.5)
Pulse outputs[2]		Up to 4 configured to use any built-in or SB outputs • 100 kHz (Qa.0 to Qa.3) • 30 kHz (Qa.4 to Qb.1)
Pulse catch inputs		14

Technical data	Description
Time delay interrupts	4 total with 1 ms resolution
Cyclic interrupts	4 total with 1 ms resolution
Edge interrupts	12 rising and 12 falling (16 and 16 with optional signal board)
Memory card	SIMATIC Memory Card (optional)
Real time clock accuracy	+/- 60 seconds/month
Real time clock retention time	20 days typ./12 days min. at 40 °C (maintenance-free Super Capacitor)

[1] The slower speed is applicable when the HSC is configured for quadrature mode of operation.

[2] For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

Table A- 28 Performance

Type of instruction	Execution speed
Boolean	0.08 μs/instruction
Move Word	1.7 μs/instruction
Real math	2.3 μs/instruction

A.2.3.2 Timers, counters and code blocks supported

Table A- 29 Blocks, timers and counters supported by CPU 1215FC

Element		Description
Blocks	Type	OB, FB, FC, DB
	Size	64 Kbytes
	Quantity	Up to 1024 blocks total (OBs + FBs + FCs + DBs)
	Address range for FBs, FCs, and DBs	FB and FC: 1 to 65535 (such as FB 1 to FB 65535) DB: 1 to 59999
	Nesting depth	16 from the program cycle or startup OB 6 from any interrupt event OB
	Monitoring	Status of 2 code blocks can be monitored simultaneously
OBs	Program cycle	Multiple
	Startup	Multiple
	Time-delay interrupts	4 (1 per event)
	Cyclic interrupts	4 (1 per event)
	Hardware interrupts	50 (1 per event)
	Time error interrupts	1
	Diagnostic error interrupts	1
	Pull or plug of modules	1
	Rack or station failure	1
	Time of day	Multiple
	Status	1
	Update	1
	Profile	1

Element		Description
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, 16 bytes per timer
Counters	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size dependent upon count type • SInt, USInt: 3 bytes • Int, UInt: 6 bytes • DInt, UDInt: 12 bytes

Table A- 30 Communication

Technical data	Description
Number of ports	2
Type	Ethernet
HMI device	4
Programming device (PG)	1
Connections	• 8 for Open User Communication (active or passive): TSEND_C, TRCV_C, TCON, TDISCON, TSEND, and TRCV • 3 for server GET/PUT (CPU-to-CPU) S7 communication • 8 for client GET/PUT (CPU-to-CPU) S7 communication
Data rates	10/100 Mb/s
Isolation (external signal to PLC logic)	Transformer isolated, 1500 VAC, for short term event safety only
Cable type	CAT5e shielded

Table A- 31 Power supply

Technical data		CPU 1215FC DC/DC/Relay	CPU 1215FC DC/DC/DC
Voltage range		20.4 VDC to 28.8 VDC	
Line frequency		--	
Input current (max. load)	CPU only	500 mA at 24 VDC	
	CPU with all expansion accessories	1500 mA at 24 VDC	
Inrush current (max.)		12 A at 28.8 VDC	
Isolation (input power to logic)		Not isolated	
Ground leakage, AC line to functional earth		-	
Hold up time (loss of power)		10 ms at 24 VDC	
Internal fuse, not user replaceable		3 A, 250 V, slow blow	

Table A- 32 Sensor power

Technical data	CPU 1215FC DC/DC/Relay	CPU 1215FC DC/DC/DC
Voltage range	L+ minus 4 VDC min.	
Output current rating (max.)	400 mA (short-circuit protected)	
Maximum ripple noise (<10 MHz)	Same as input line	
Isolation (CPU logic to sensor power)	Not isolated	

A.2.3.3 Digital inputs and outputs

Table A- 33 Digital inputs

Technical data	CPU 1215FC DC/DC/Relay	CPU 1215FC DC/DC/DC
Number of inputs	14	
Type	Sink/Source (IEC Type 1 sink)	
Rated voltage	24 VDC at 4 mA, nominal	
Continuous permissible voltage	30 VDC, max.	
Surge voltage	35 VDC for 0.5 sec.	
Logic 1 signal (min.)	15 VDC at 2.5 mA	
Logic 0 signal (max.)	5 VDC at 1 mA	
Isolation (field side to logic)	500 VAC for 1 minute	
Isolation groups	1	
Filter times	us settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
HSC clock input rates (max.) (Logic 1 Level = 15 to 26 VDC)	100/80 kHz (Ia.0 to Ia.5) 30/20 kHz (Ia.6 to Ib.5)	
Number of inputs on simultaneously	14 inputs at 55 °C horizontal or 45 °C vertical	
Cable length (meters)	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs	

Table A- 34 Digital outputs

Technical data	CPU 1215FC DC/DC/Relay	CPU 1215FC DC/DC/DC
Number of outputs	10	10
Type	Relay, mechanical	Solid state - MOSFET (sourcing)
Voltage range	5 to 30 VDC or 5 to 250 VAC	20.4 to 28.8 VDC
Logic 1 signal at max. current	--	20 VDC min.
Logic 0 signal with 10 KΩ load	--	0.1 VDC max.
Current (max.)	2.0 A	0.5 A
Lamp load	30 W DC / 200 W AC	5 W
ON state resistance	0.2 Ω max. when new	0.6 Ω max.
Leakage current per point	--	10 μA max.
Surge current	7 A with contacts closed	8 A for 100 ms max.
Overload protection	No	No
Required external overload protection [4]	10 A maximum must be limited to any common	5 A maximum must be limited to any common
Isolation (field side to logic)	1500 VAC for 1 minute (coil to contact) None (coil to logic)	500 VAC for 1 minute
Isolation resistance	100 MΩ min. when new	--
Isolation between open contacts	750 VAC for 1 minute	--
Isolation groups	2	1
Isolation (group-to-group)	1500 VAC [1]	--
Inductive clamp voltage	--	L+ minus 48 VDC, 1 W dissipation
Switching delay (Qa.0 to Qa.3)	10 ms max.	1.0 μs max., off to on 3.0 μs max., on to off
Switching delay (Qa.4 to Qb.1)	10 ms max.	50 μs max., off to on 200 μs max., on to off
Maximum relay switching frequency	1 Hz	--
Pulse Train Output rate	Not recommended [2]	100 kHz (Qa.0 to Qa.3) [3], 2 Hz min. 20 kHz (Qa.4 to Qb.1) [3]
Lifetime mechanical (no load)	10,000,000 open/close cycles	--
Lifetime contacts at rated load	100,000 open/close cycles	--
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Number of outputs on simultaneously	10 outputs at 55 °C horizontal or 45 °C vertical	
Cable length (meters)	500 m shielded, 150 m unshielded	

1 Relay group-to-group isolation separates line voltage from SELV/PELV and separates different phases up to 250 VAC line to ground.

2 For CPU models with relay outputs, you must install a digital signal board (SB) to use the pulse outputs.

3 Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) may improve pulse signal quality and noise immunity.

4 External overload protection is to limit fire hazard. Overload can damage relay or transistor output.

A.2.3.4 Analog inputs and outputs

Table A- 35 Analog inputs

Technical data	Description
Number of inputs	2
Type	Voltage (single-ended)
Full-scale range	0 to 10 V
Full-scale range (data word)	0 to 27648
Overshoot range	10.001 to 11.759 V
Overshoot range (data word)	27649 to 32511
Overflow range	11.760 to 11.852 V
Overflow range (data word)	32512 to 32767
Resolution	10 bits
Maximum withstand voltage	35 VDC
Smoothing	None, Weak, Medium, or Strong See the table for step response (ms) for the analog inputs of the CPU.
Noise rejection	10, 50, or 60 Hz
Impedance	≥100 KΩ
Isolation (field side to logic)	None
Accuracy (25 °C / 0 to 55 °C)	3.0% / 3.5% of full-scale
Cable length (meters)	100 m, shielded twisted pair

Step response of built-in analog inputs of the CPU

Table A- 36 Step Response (ms), 0 V to 10 V measured at 95%

Smoothing selection (sample averaging)	Rejection frequency (Integration time)		
	60 Hz	**50 Hz**	**10 Hz**
None (1 cycle): No averaging	50 ms	50 ms	100 ms
Weak (4 cycles): 4 samples	60 ms	70 ms	200 ms
Medium (16 cycles): 16 samples	200 ms	240 ms	1150 ms
Strong (32 cycles): 32 samples	400 ms	480 ms	2300 ms
Sample time	**4.17 ms**	**5 ms**	**25 ms**

Sample time for the built-in analog ports of the CPU

Table A- 37 Sample time for built-in analog inputs of the CPU

Rejection frequency (Integration time selection)	Sample time
60 Hz (16.6 ms)	4.17 ms
50 Hz (20 ms)	5 ms
10 Hz (100 ms)	25 ms

Measurement ranges of the analog inputs for voltage of the CPU

Table A- 38 Analog input representation for voltage of the CPU

System		Voltage Measuring Range	
Decimal	**Hexadecimal**	**0 to 10 V**	
32767	7FFF	11.851 V	Overflow
32512	7F00		
32511	7EFF	11.759 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range
20736	5100	7.5 V	
34	22	12 mV	
0	0	0 V	
Negative values		Negative values are not supported	

Analog output specifications

Table A- 39 Analog outputs

Technical data	Description
Number of outputs	2
Type	Current
Full-scale range	0 to 20 mA
Full-scale range (data word)	0 to 27648
Overshoot range	20.01 to 23.52 mA
Overshoot range (data word)	27649 to 32511
Overflow range	see footnote [1]
Overflow range data word	32512 to 32767
Resolution	10 bits
Output drive impedance	≤500 Ω max.
Isolation (field side to logic)	None
Accuracy (25 °C / 0 to 55 °C)	3.0% / 3.5% of full-scale
Settling time	2 ms
Cable length (meters)	100 m, shielded twisted pair

[1] In an overflow condition, analog outputs will behave according to the device configuration properties settings. In the "Reaction to CPU STOP" parameter, select either: "Use substitute value" or "Keep last value".

Measurement ranges of the analog outputs for current of the CPU

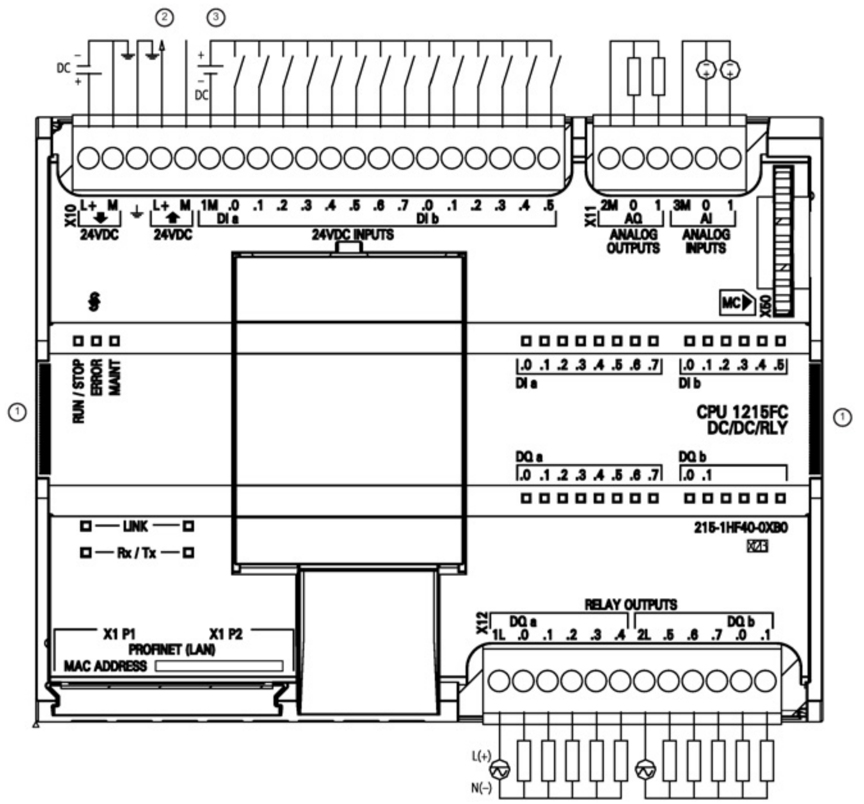
Table A- 40 Analog output representation for current of the CPU

System		Current output range	
Decimal	**Hexadecimal**	**0 mA to 20 mA**	
32767	7FFF	See note 1	Overflow
32512	7F00	See note 1	
32511	7EFF	23.52 mA	Overshoot range
27649	6C01		
27648	6C00	20 mA	Rated range
20736	5100	15 mA	
34	22	0.0247 mA	
0	0	0 mA	
Negative values		Negative values are not supported	

[1] In an overflow condition, analog outputs will behave according to the device configuration properties settings. In the "Reaction to CPU STOP" parameter, select either: "Use substitute value" or "Keep last value".

A.2.3.5 CPU 1215FC wiring diagrams

Table A- 41 CPU 1215FC DC/DC/Relay (6ES7 215-1HF40-0XB0)



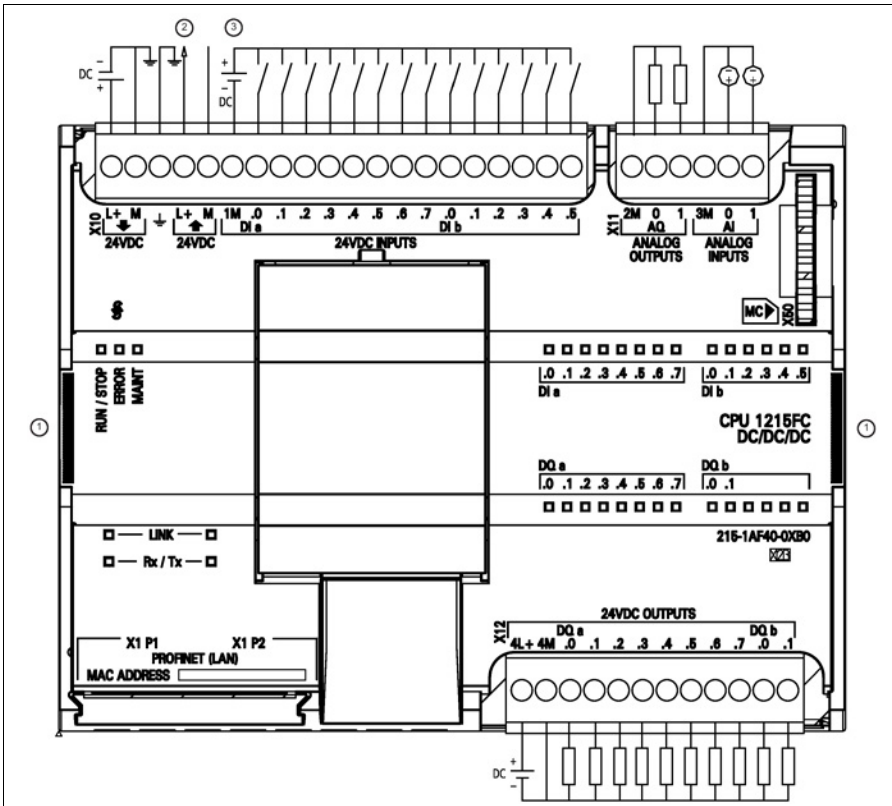
①	The two rectangular areas are yellow. These are only on the fail-safe CPUs.
②	24 VDC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
③	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".
Note: X11 connectors must be gold. See Appendix B, Spare Parts for article number.	

Table A- 42 Connector pin locations for CPU 1215FC DC/DC/Relay (6ES7 215-1HF40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24VDC	2M	1L
2	M / 24VDC	AQ 0	DQ a.0
3	Functional Earth	AQ 1	DQ a.1
4	L+ / 24VDC Sensor Out	3M	DQ a.2
5	M / 24VDC Sensor Out	AI 0	DQ a.3
6	1M	AI 1	DQ a.4
7	DI a.0	--	2L
8	DI a.1	--	DQ a.5
9	DI a.2	--	DQ a.6
10	DI a.3	--	DQ a.7
11	DI a.4	--	DQ b.0
12	DI a.5	--	DQ b.1
13	DI a.6	--	--
14	DI a.7	--	--

Pin	X10	X11 (gold)	X12
15	DI b.0	--	--
16	DI b.1	--	--
17	DI b.2	--	--
18	DI b.3	--	--
19	DI b.4	--	--
20	DI b.5	--	--

Table A- 43 CPU 1215FC DC/DC/DC (6ES7 215-1AF40-0XB0)



①	The two rectangular areas are yellow. These are only on the fail-safe CPUs.
②	24 VDC Sensor Power Out For additional noise immunity, connect "M" to chassis ground even if not using sensor supply.
③	For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

Note: X11 connectors must be gold. See Appendix B, Spare Parts for article number.

Table A- 44 Connector pin locations for CPU 1215FC DC/DC/DC (6ES7 215-1AF40-0XB0)

Pin	X10	X11 (gold)	X12
1	L+ / 24VDC	2 M	4L+
2	M / 24VDC	AQ 0	4M
3	Functional Earth	AQ 1	DQ a.0
4	L+ / 24VDC Sensor Out	3M	DQ a.1
5	M / 24VDC Sensor Out	AI 0	DQ a.2
6	1M	AI 1	DQ a.3
7	DI a.0	--	DQ a.4
8	DI a.1	--	DQ a.5
9	DI a.2	--	DQ a.6
10	DI a.3	--	DQ a.7
11	DI a.4	--	DQ b.0
12	DI a.5	--	DQ b.1
13	DI a.6	--	--
14	DI a.7	--	--
15	DI b.0	--	--
16	DI b.1	--	--
17	DI b.2	--	--
18	DI b.3	--	--
19	DI b.4	--	--
20	DI b.5	--	--

Note

Unused analog inputs should be shorted.

A.3 Fail-Safe signal module (SM) technical specifications

A.3.1 Fail-Safe signal modules (SM)

Table A- 45 Fail-Safe signal modules

Signal module model	Digital inputs	Digital outputs	Removable connector
SM 1226 F-DI 16 x 24 VDC	8 x 24 VDC (1oo2), 16 x 24 VDC (1oo1), or a mix	-	Y
SM 1226 F-DQ 4 x 24 VDC	-	4 x 24 VDC	Y
SM 1226 F-DQ 2 x Relay	-	2 x Relay	Y

A.3.2 SM 1226 F-DI 16 x 24 VDC

A.3.2.1 Properties

Article number

6ES7 226-6BA32-0XB0

Properties

The SM 1226 F-DI 16 x 24 VDC has the following features:

- 16 inputs (SIL 2/Category 3/PL d), 8 inputs (SIL 3/Category 3 or Category 4/PL e), or a mix
- 24 VDC-rated input voltage
- Suitable for switches and 3/4-wire proximity switches (BEROs)
- Two short circuit-proof sensor supplies, each one for eight inputs
- External sensor supply possible
- Module fault display (DIAG; green and red LED)
- Status display for each input (green LED)
- Fault display for each input (red LED)
- Assignable diagnostics
- Refer to "Fault diagnostics" (Page 119) for a description of LED and diagnostic message functions.

A.3.2.2 User data space

The SM 1226 F-DI 16 x 24 VDC user data space is 2 bytes (16 bits) of process value input followed by 2 bytes of quality bits.

This is the bit structure for an F-DI configured with input start address 8:

Input terminal	Process value	Quality bit
DI a.0	I8.0	I10.0
DI a.7	I8.7	I10.7
DI b.0	I9.0	I11.0
DI b.7	I9.7	I11.7

A.3.2.3 Specifications

Table A- 46 General specifications

Model	SM 1226 F-DI 16 x 24 VDC	
Article number	6ES7 226-6BA32-0XB0	
Dimensions W x H x D (mm)	70 x 100 x 75	
Weight	250 grams	
Power dissipation	7 W	
Current consumption (SM Bus, 5 VDC)	155 mA	
Current consumption (24 VDC)	130 mA + 6 mA / input used + any Vs1/Vs2 current used	
Isolation	• Signal terminals on this module are referenced to this module's M terminal and NOT ISOLATED from each other. • Signal terminals on this module are isolated to 500VAC for 1 min from S7-1200 system internal logic and Ground.	
Assigned address area: • I/O area for inputs • I/O area for outputs	 9 bytes 5 bytes	
Maximum achievable safety class: • In accordance with IEC 61508:2010 • In accordance with EN ISO 13849-1:2008	1-channel SIL 2 Category 3, PL d	2-channel SIL 3 Category 4, PL e
Fail-safe performance characteristics: • Operation in Low Demand Mode (Average probability of a dangerous failure on demand), PFD_avg • Operation in High Demand or Continuous Mode (Average frequency of a dangerous failure per hour), PFH • Proof test interval (Mission time or Useful lifetime) • Safety repair time	SIL 2 5e-4 1e-8 20 years 100 hours	SIL 3 1e-5 1e-10 20 years 100 hours
Inputs status display	Green LED / channel	
Inputs fault display	Red LED / channel	

Model	SM 1226 F-DI 16 x 24 VDC
Module fault display	Red / Green LED (DIAG)
Diagnostic information can be displayed	Possible (TIA Portal, HMI, or Web page)

Table A- 47 Performance

Model	SM 1226 F-DI 16 x 24 VDC
Tmax_i: Internal cycle time	TBD Note: Refer to "Fail-Safe signal module (SM) response times" (Page 197) for further information.

Table A- 48 Power supply (L+, M)

Model	SM 1226 F-DI 16 x 24 VDC
Voltage range	20.4 VDC to 28.8 VDC
Surge voltage	35 VDC for 0.5 s
Input current	• 130 mA with no current out of Vs1 and Vs2 • 730 mA with maximum current out of Vs1 and Vs2
Hold up time (loss of power)	1.0 ms at 20.4 VDC
Internal fuse, not user replaceable	2.5 A
Reverse polarity protection	Yes

Table A- 49 Sensor power (Vs1 / Vs2)

Model	SM 1226 F-DI 16 x 24 VDC
Number of outputs	2
Voltage range	L+ minus 2.0 VDC minimum
Output current rating (maximum)	300 mA
Permissible total current of outputs	600 mA
Short-circuit protection: • Operating value	Yes 0.7 A to 2.1 A

Table A- 50 Digital inputs

Model	SM 1226 F-DI 16 x 24 VDC
Number of inputs: • 1oo1 evaluation • 1oo2 evaluation	 16 maximum 8 maximum Note: You can individually assign each pair of inputs "a.x" and "b.x" as a single 1oo2 channel or as 2 separate 1oo1 channels.
Type	Sink (IEC 61131-2 Type 1)
Rated voltage	24 VDC at 5 mA, nominal
Surge voltage	35 VDC for 0.5 s
Logic 1 signal	15 VDC at 3 mA to 30 VDC at 6 mA
Logic 0 signal	-30 VDC to 5 VDC
Connection of 2-wire proximity switch (BERO): • Permissible quiescent current	Not possible 0.5 mA maximum
Filter times	• 0.8 ms • 1.6 ms • 3.2 ms • 6.4 ms • 12.8 ms Note: Refer to "Fail-Safe signal module (SM) response times" (Page 197) for further information.
Number of inputs on simultaneously	16 inputs at 55 °C horizontal or 45 °C vertical
Cable length (meters)[1]	• 200 m unshielded with input filter time of 1.6 ms to 12.6 ms • 200 m shielded with input filter time of 0.8 ms to 12.6 s[1]

[1] With an input delay of 0.8 ms, shielded cables must be used for the digital inputs and the sensor supply.

A.3.2.4 Wiring diagrams

Table A- 51 SM 1226 F-DI 16 x 24 VDC (6ES7 226-6BA32-0XB0)

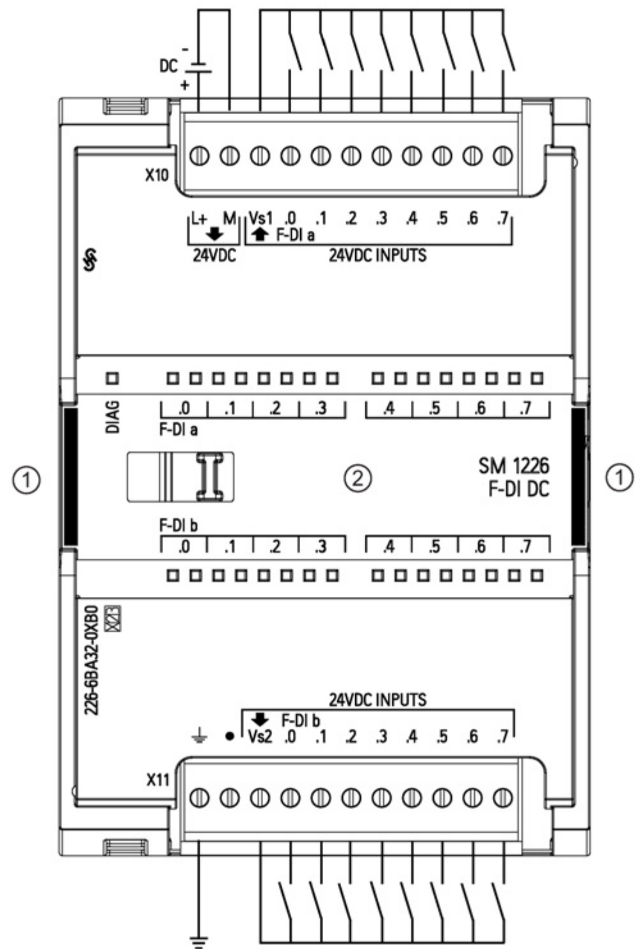
	① The two rectangular areas are yellow. These are only on the fail-safe signal modules. ② Two LEDs per input: • One for channel status: Green (on = input on, off = input off) • One for channel faults: Red (on = problem/passivated, off = ok, blink = ready to reintegrate (activate)) Note: Refer to "Digital input applications" (Page 68) for alternate applications wiring.

Table A- 52 Connector pin locations for SM 1226 F-DI 16 x 24 VDC (6ES7 226-6BA32-0XB0)

Pin	X10	X11
1	L+ / 24 VDC	Functional Earth
2	M / 24 VDC	No connection
3	Vs1 / 24VDC Sensor Supply Output 1	Vs2 / 24VDC Sensor Supply Output 2
4	DI a.0	DI b.0
5	DI a.1	DI b.1
6	DI a.2	DI b.2
7	DI a.3	DI b.3
8	DI a.4	DI b.4
9	DI a.5	DI b.5
10	DI a.6	DI b.6
11	DI a.7	DI b.7

A.3.3 SM 1226 F-DQ 4 x 24 VDC

A.3.3.1 Properties

Article number

6ES7 226-6DA32-0XB0

Properties

The SM 1226 F-DQ 4 x 24 VDC has the following features:

- Four outputs, P- and M-switching
- 2 A output current
- Rated load voltage 24 VDC
- Suitable for solenoid valves, DC contactors, and indicator LEDs
- Module fault display (DIAG; green and red LED)
- Status display for each output (green LED)
- Fault display for each output (red LED)
- Safety class SIL 3 attainable
- Assignable diagnostics
- Refer to "Fault diagnostics" (Page 119) for a description of LED and diagnostic message functions.

A.3.3.2 User data space

The SM 1226 F-DQ 4 x 24 VDC user data space is 4 process value output bits followed by 4 quality bits.

This is the bit structure for an F-DQ DC module configured with input start address 8:

Terminal	Process value	Quality bit
F-DQ a.0	Q8.0	I8.0
F-DQ a.1	Q8.1	I8.1
F-DQ a.2	Q8.2	I8.2
F-DQ a.3	Q8.3	I8.3

A.3.3.3 Specifications

Table A- 53 General specifications

Model	SM 1226 F-DQ 4 x 24 VDC
Article number	6ES7 226-6DA32-0XB0
Dimensions W x H x D (mm)	70 x 100 x 75
Weight	270 grams
Power dissipation	8 W
Current consumption (SM Bus, 5 VDC)	125 mA
Current consumption (24 VDC)	170 mA + load current for all P-switch outputs
Isolation	• Signal terminals on this module are referenced to this module's M terminal and NOT ISOLATED from each other. • Signal terminals on this module are isolated to 500VAC, for 1 min from S7-1200 system internal logic and Ground.
Assigned address area: • I/O area for inputs • I/O area for outputs	 6 bytes 6 bytes
Maximum achievable safety class: • In accordance with IEC 61508:2010 • In accordance with EN ISO 13849-1:2008	 SIL 3 Category 4, PL e
Fail-safe performance characteristics: • Operation in Low Demand Mode (Average probability of a dangerous failure on demand), PFD_avg • Operation in High Demand or Continuous Mode (Average frequency of a dangerous failure per hour), PFH • Proof test interval (Mission time or Useful lifetime) • Safety repair time	SIL 3 1e-5 4e-9 20 years 100 hours
Outputs status display	Green LED / channel
Outputs fault display	Red LED / channel
Module fault display	Red / Green LED (DIAG)
Diagnostic information can be displayed	Possible (TIA Portal, HMI, or Web page)

Table A- 54 Performance

Model	SM 1226 F-DQ 4 x 24 VDC
Tmax_i: Internal cycle time	TBD Note: Refer to "Fail-Safe signal module (SM) response times" (Page 197) for further information.

Table A- 55 Power supply (L+, M)

Model	SM 1226 F-DQ 4 x 24 VDC
Voltage range	20.4 VDC to 28.8 VDC
Surge voltage	35 VDC for 0.5 s
Input current	170 mA (does not include current in all P-switch loads)
Hold up time (loss of power)	• None for outputs • 1.0 ms at 20.4 VDC for internal power
Internal fuse, not replaceable	• 1 A for logic power • 7 A common for P-switch outputs F-DQ a.0 and F-DQ a.1 • 7 A common for P-switch outputs F-DQ a.2 and F-DQ a.3
Reverse polarity protection	Yes Note: Refer to "Reverse polarity protection" in the SM 1226 F-DQ 4 x 24 VDC "Digital outputs" table for more information.

Table A- 56 Digital outputs

Model	SM 1226 F-DQ 4 x 24 VDC
Number of outputs	4
Type	P- and M-switching
Logic 1 signal at maximum current	L+ minus 2.0 VDC (minimum): • P-switch: L+ minus 1.5 VDC (maximum) • M-switch: 0.5 VDC (maximum)
Logic 1 current	• 2 A nominal • 10 mA to 2.4 A
Lamp load	10 W (maximum)
Logic 0 current (residual)	• P-switch: 0.5 mA, maximum • M-switch: 0.5 mA, maximum
Wire break monitoring	None
Output overload protection: • M-switch • P-switch	Yes, electronic in addition to internal non-replaceable fuse. Threshold of 25 A to 45 A turns M-switch OFF. Threshold of 2.4 A to 3.8 A, 400 ms time constant filter, measured at P-switch, turns both switches OFF. 7 A fuse can open for large faults. Note: Refer to "Fuse and electronic overload protection" (Page 180) for more information.
Current per common (maximum)	8 A
Inductive clamp voltage	• M-switch: + 48 VDC referenced to M • P-switch: - 26 VDC referenced to M
Behavior on RUN to STOP	Only 0 (OFF) is allowed
Number of outputs on simultaneously	4 at 55 °C horizontal or 45 °C vertical
Parallel connection of 2 outputs	Not possible
Control of a digital input	Not possible

Model	SM 1226 F-DQ 4 x 24 VDC
Switching frequency: • With resistive load • With inductive load in accordance with IEC 60947-5-1, DC13 • With lamp load	 30 Hz symmetrical, maximum 0.1 Hz symmetrical, maximum 10 Hz symmetrical, maximum
Cable length (meters)	• 200 m unshielded • 200 m shielded
Reverse polarity protection	Yes, except loads connected between M-switch and L+ will conduct if M and L+ are reversed. Note: Refer to Digital Output Application Mode 2 (Page 76) for more information.

A.3.3.4 Fuse and electronic overload protection

Overload protection attempts to protect the module from damage from moderate faults in the range of 2.4 A to 15 A at the P switch. Above 15 A on each P-switch fuse, the internal non-replaceable fuse can open. Supply your SM 1226 F-DQ 4 x 24 VDC from a source limited to less than 15 A, or use an external fuse or non-shorting load element to prevent opening of the internal fuse.

The internal electronic limiting causes the channel to passivate and reports as an overload. If no damage results, you can reintegrate the channel after removal of the external fault.

A.3.3.5 Switching of loads

Connecting capacitive loads

Load capacitance can delay the voltage response as seen at the P- and M- switches of the SM 1226 F-DQ 4 x 24 VDC. For a capacitive load with capacitance C across P and M, and a parallel load resistance R, the "Maximum readback time" needs to be longer than 1 time constant (R * C) of the load. This allows enough time for an appreciable voltage change to be seen when you briefly de-energize an energized load during bit pattern testing. If the resulting "Maximum readback time" is too long for your application, you can reduce this time constant by adding parallel resistance across the load to reduce the realized R * C time constant.

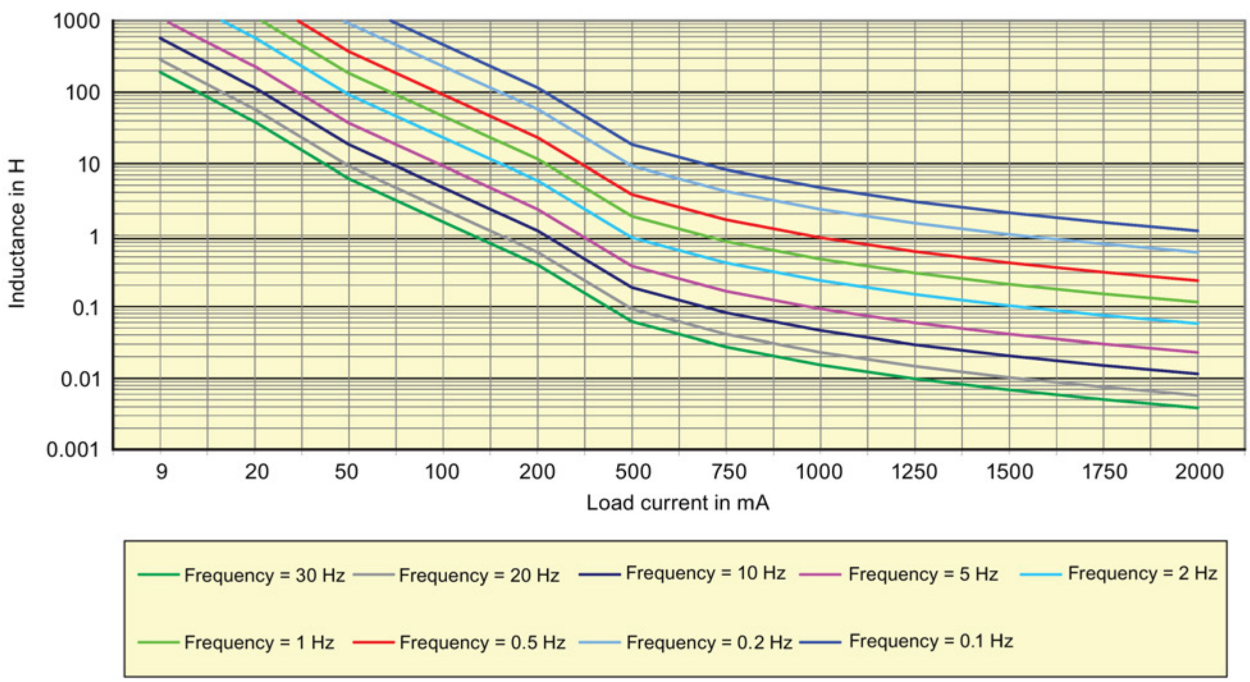
Stray capacitance between the load circuit and ground, M, and P increases the time required for the "Maximum readback time switch on test". When module diagnostics switch "ON" a P or M switch to a de-energized load during bit pattern testing, both sides of the load are driven towards L+ or M, limited by stray capacitance. This effect is typically small.

Your "Maximum readback time switch on test" should be long enough for the load circuit voltage to react, but short enough that if one side of the load faults to P or M, testing of the opposite switch should not cause the load to mechanically react.

Capacitive loads (including power supplies with input capacitors) with low series resistance can have a large inrush current. If you have a large capacitive load, you should add series resistance to reduce the inrush current to reduce the risk of opened fuses or overcurrent fault detection on normal load switch ON events.

Switching of inductive loads

The graph below shows the maximum permitted inductive load and switching frequency allowed using only the internal suppression circuits of the F-DQ DC outputs. You should equip larger or more frequently switched inductive loads with external suppression circuits to avoid early failure of the F-DQ DC output switch. The external suppression must conduct the load current at a voltage less than the internal suppression threshold to avoid overloading the internal suppression. Refer to "Guidelines for inductive loads" (Page 101) for more information:



WARNING

Unsuppressed inductive loads can lead to failures.

The following failures can result:

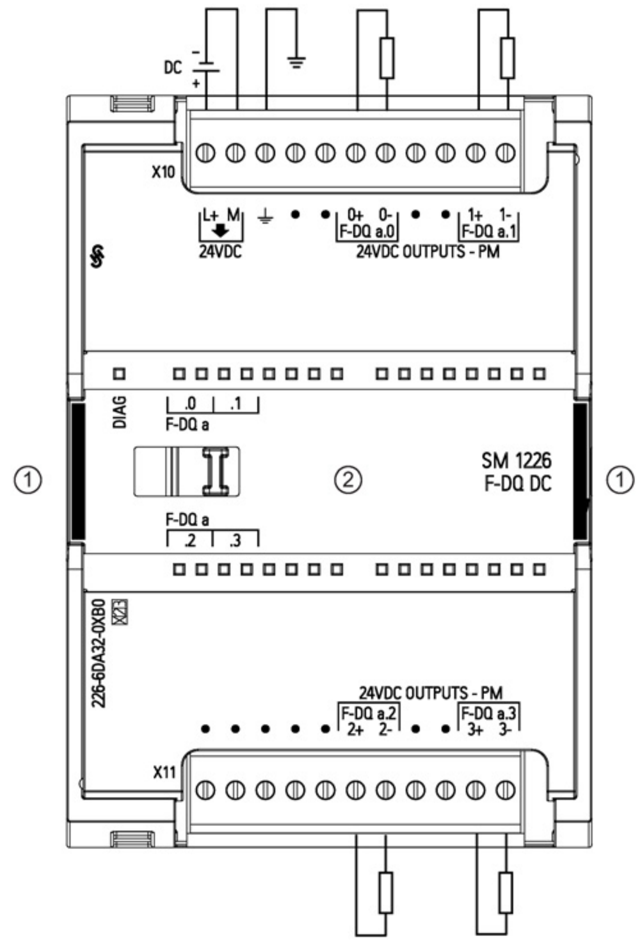
- Unsuppressed inductive loads can lead to early "stuck-on"' failures of F-DQ DC and F-RLY outputs.
- Unsuppressed inductive load switching generates an EMI hazard to the PLC system and correct processing of the safety function.

Death or serious personal injury and damage to machines and equipment may result if proper precautions are not taken.

You should use suppressor circuits with inductive loads to limit the voltage rise when a control output turns off and to limit the electrical noise generated when switching inductive loads.

A.3.3.6 Wiring diagrams

Table A- 57 SM 1226 F-DQ 4 x 24 VDC (6ES7 226-6DA32-0XB0)



① The two rectangular areas are yellow. These are only on the fail-safe signal modules.

② Two LEDs per output:

- One for channel status: Green (on = output on, off = output off)
- One for channel faults: Red (on = problem/passivated, off = ok, blink = ready to reintegrate (activate))

Note: Refer to "Digital output applications" (Page 75) for alternate applications wiring.

Table A- 58 Connector pin locations for SM 1226 F-DQ 4 x 24 VDC (6ES7 226-6DA32-0XB0)

Pin	X10	X11
1	L+ / 24VDC	No connection
2	M / 24VDC	No connection
3	Functional Earth	No connection
4	No connection	No connection
5	No connection	No connection
6	F-DQ a.0+ / P-switch	F-DQ a.2+ / P-switch
7	F-DQ a.0- / M-switch	F-DQ a.2- / M-switch
8	No connection	No connection
9	No connection	No connection
10	F-DQ a.1+ (P-switch)	F-DQ a.3+ (P-switch)
11	F-DQ a.1- (M-switch)	F-DQ a.3- (M-switch)

A.3.4 SM 1226 F-DQ 2 x Relay

A.3.4.1 Properties

Article number

6ES7 226-6RA32-0XB0

Properties

The SM 1226 F-DQ 2 x Relay has the following features:

- Two relay outputs (each output switches two circuits)
- 5 A output current
- Rated load voltage 24 VDC or 24 VAC to 230 VAC
- Module fault display (DIAG; green and red LED)
- Status display for each output (green LED)
- Fault display for each output (red LED)
- Safety class SIL3 attainable
- Assignable diagnostics
- Refer to "Fault diagnostics" (Page 119) for a description of LED and diagnostic message functions.

A.3.4.2 User data space

The SM 1226 F-DQ 2 x Relay user data space is 2 process value output bits followed by 2 quality bits.

This is the bit structure for an F-RLY module configured with input start address 8:

Terminal	Process value	Quality bit
F-DQ a.0	Q8.0	I8.0
F-DQ a.1	Q8.1	I8.1

A.3.4.3 Specifications

Table A- 59 General specifications

Model	SM 1226 F-DQ 2 x Relay
Article number	6ES7 226-6RA32-0XB0
Dimensions W x H x D (mm)	70 x 100 x 75
Weight	340 grams
Power dissipation	10 W
Current consumption (SM Bus, 5 VDC)	120 mA
Current consumption (24 VDC)	300 mA
Assigned address area: • I/O area for inputs • I/O area for outputs	 6 bytes 6 bytes
Maximum achievable safety class: • In accordance with IEC 61508:2010 • In accordance with EN ISO 13849-1:2008	 SIL 3 Category 4, PL e
Fail-safe performance characteristics: • Operation in Low Demand Mode (Average probability of a dangerous failure on demand), PFD_avg • Operation in High Demand or Continuous Mode (Average frequency of a dangerous failure per hour), PFH • Proof test interval (Mission time or Useful lifetime) • Safety repair time	SIL 3 1e-5 4e-9 20 years 100 hours
Outputs status display	Green LED / channel
Outputs fault display	Red LED / channel
Module fault display	Red / Green LED (DIAG)
Diagnostic information can be displayed	Possible (TIA Portal, HMI, or Web page)

Table A- 60 Performance

Model	SM 1226 F-DQ 2 x Relay
Tmax_i: Internal cycle time	TBD Note: Refer to "Fail-Safe signal module (SM) response times" (Page 197) for further information.

Table A- 61 Power supply (L+, M)

Model	SM 1226 F-DQ 2 x Relay
Voltage range	20.4 VDC to 28.8 VDC
Surge voltage	35 VDC for 0.5 s
Input current	300 mA
Isolation (L+, M to S7-1200 internal logic and Ground)	500 VAC for 1 min
Hold up time (loss of power)	• None for outputs • 1.0 ms at 20.4 VDC for internal power with outputs off • 0.5 ms at 20.4 VDC with either output or both outputs on
Internal fuse, not user replaceable	1 A for internal power
Reverse polarity protection	Yes

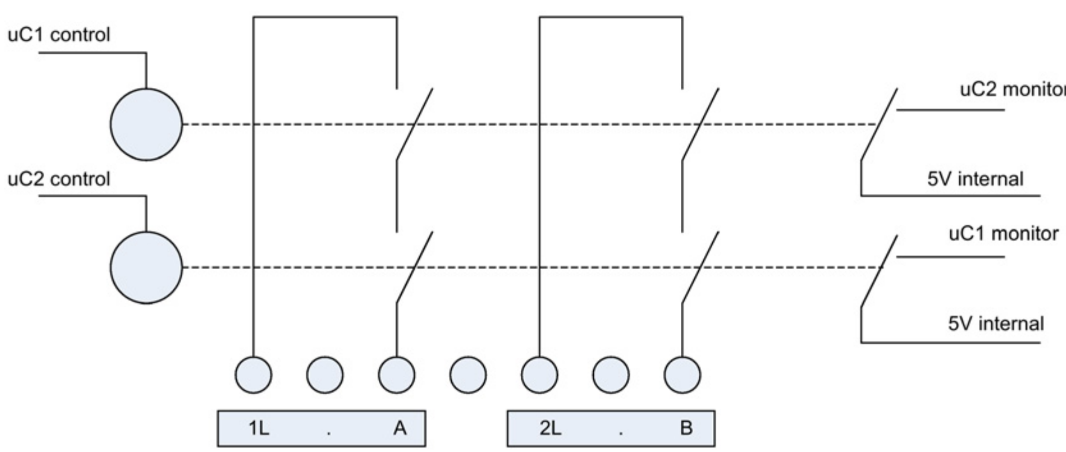
Table A- 62 Digital outputs

Model	SM 1226 F-DQ 2 x Relay
Number of outputs	2 (2 circuits per output)
Type	Relay, mechanically linked sense contact monitored internal to module
Voltage range	5 to 30 VDC or 5 to 250 VAC
Output current: • Continuous thermal current • Minimum load current	 5 A maximum per circuit 5 mA
Current per common	5 A
Current per module (maximum) – all output circuits	10A at 55 °C horizontal or 45 °C vertical
ON state contact resistance	0.2 Ω maximum when new
Wire break monitoring	None
Short-circuit protection of output	None; external fuse or circuit breaker required. General purpose fuse type gG per IEC 60269, 5A maximum on each circuit. Some application standards require derating.
Overload protection of output	None
Isolation (output circuits to logic)	2200 VAC for 1 min, rated for Overvoltage Category III
Isolation (output circuits to power supply)	2200 VAC for 1 min, rated for Overvoltage Category III
Isolation (circuit to circuit on same output)	2200 VAC for 1 min Note : Circuit-to-circuit isolation (A circuit to B circuit) on the same output is not rated to separate line voltage from SELV / PELV.
Isolation (output to output)	2200 VAC for 1 min; rated for Overvoltage Category III, including Overvoltage Category III to SELV separation or different phase separation.
Isolation groups	4
Inductive clamp voltage	None; external protection required.
On delay time	Typically 20 ms to both series contacts closed, including 8 ms separation between commands to series contacts

Model	SM 1226 F-DQ 2 x Relay
Off delay time	Typically 16 ms to first series contact open, second contact opens approximately 40 ms later.
Behavior on RUN to STOP	Only 0 (OFF) is allowed.
Number of outputs on simultaneously	2
Parallel connection of 2 outputs	Allowed for redundant availability. Do not exceed single relay load rating.
Control of a digital input	With 24 VDC SELV supply
Switching frequency:	
• With resistive load	2 Hz, maximum
• With inductive load in accordance with IEC 60947-5-1, DC13	0.1 Hz, maximum
• With inductive load in accordance with IEC 60947-5-1, AC15	2 Hz, maximum
• Inductive load in accordance with UL 508	Pilot Duty B300, R300
Cable length (meters)	• 200 m shielded • 200 m unshielded
Reverse polarity protection	No

A.3.4.4 Relay output circuits

The SM 1226 F DQ 2 x Relay has two output channels (F-DQ a.0 and F-DQ a.1). Each channel includes two circuits that switch mechanically-linked contacts at the same time. Each circuit has two contacts in series controlled by independent relay coils. Opening and closing of the series contacts in each circuit is sequenced to avoid common wear-out failures.



Output channel a.0: Two circuits controlled as one process output channel

Refer to the isolation description in the SM 1226 F-DQ 2 x Relay (Page 185) specifications, Digital outputs table.

⚠ WARNING

Adjacent relay contacts in the same channel of the SM 1226 F DQ 2 x Relay are not rated to separate AC line from SELV / PELV.

Death or serious personal injury and damage to machines and equipment may result if SELV/PELV circuits are wired adjacent to high voltage circuits on this module.

The A and B circuits of each output must either be both AC line or both SELV.

A.3.4.5 Switching performance and service life of contacts

Note the "Switching performance and service life of contacts" table below. You should equip Inductive loads with suppression circuits to avoid shortened relay contact life and to avoid excessive switching noise. Refer to "Guidelines for inductive loads" (Page 101) for more information:

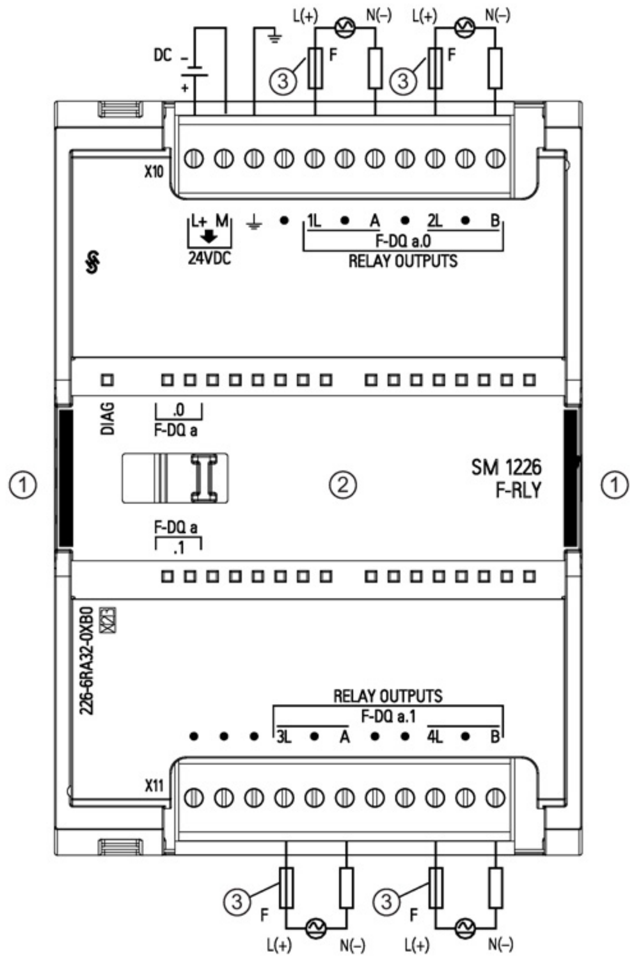
Table A- 63 Switching performance and service life of contacts

Resistive load	Voltage	Current	Duty cycle (typical) Normally-Open (NO) contact
For resistive load	24 VDC	5.0 A	0.35 million
		3.0 A	0.5 million
		2.0 A	0.75 million
		1.0 A	1.8 million
		0.5 A	4 million
	230 VAC	5.0 A	0.1 million
		3.0 A	0.15 million
		2.0 A	0.2 million
		1.0 A	0.4 million
		0.5 A	0.8 million
For inductive load to IEC 60947-5-1 DC13/AC15	24 VDC	1.0 A	0.1 million
		0.5 A	0.2 million
	230 VAC	1.0 A	0.2 million
		0.5 A	0.35 million

> **⚠ WARNING**
>
> **Unsuppressed inductive loads can lead to failures.**
>
> The following failures can result from unsuppressed inductive loads:
>
> - Unsuppressed inductive loads can lead to early "stuck-on"' failures of F-DQ and F-relay outputs.
> - Unsuppressed inductive load switching generates an EMI hazard to the PLC system and correct processing of the safety function.
>
> Death or serious personal injury and damage to machines and equipment may result if proper precautions are not taken.
>
> You should use suppressor circuits with inductive loads to limit the voltage rise when a control output turns off and to limit the electrical noise generated when switching inductive loads.

A.3.4.6 Wiring diagrams

Table A- 64 SM 1226 F-DQ 2 x Relay (6ES7 226-6RA32-0XB0)

	① The two rectangular areas are yellow. These are only on the fail-safe signal modules. ② Two LEDs per output: • One for channel status: Green (on = output on, off = output off) • One for channel faults: Red (on = problem/passivated, off = ok, blink = ready to reintegrate (activate)) ③ External fuse Note: Refer to "Digital output applications" (Page 75) for alternate applications wiring.

> **⚠ WARNING**
>
> **External fuse or circuit breaker required**
>
> Use a general purpose fuse type gG per IEC 60269, 5A maximum on each circuit. Some application standards require derating to exclude contact welding as a fault.
>
> Failure to follow these installation requirements could result in death, severe personal injury, and property damage.
>
> Always follow these requirements when installing S7-1200 modules.

Table A- 65 Connector pin locations for SM 1226 F-DQ 2 x Relay (6ES7 226-6RA32-0XB0)

Pin	X10	X11
1	L+ / 24VDC	No connection
2	M / 24VDC	No connection
3	Functional Earth	No connection
4	No connection	3L
5	1L	No connection
6	No connection	A / DQ a.1
7	A / DQ a.0	No connection
8	No connection	No connection
9	2L	4L
10	No connection	No connection
11	B / DQ a.0	B / DQ a.1

A.4 Companion products

A.4.1 PM1207 power module

The PM1207 is a power supply module for the SIMATIC S7-1200. It provides the following features:

- Input: 120/230 VAC, output: 24 VDC/2.5A
- Article number: 6ESP 332-1SH71-4AA0

For more information about this product and for the product documentation, refer to the product catalog web site for the PM1207 (https://eb.automation.siemens.com/mall/en/de/Catalog/Product/6AG1332-1SH71-4AA0)

Ordering information

B

B.1 Fail-Safe CPUs

Table B- 1 Fail-Safe CPUs

Item		Article number
CPU 1214FC	CPU 1214FC DC/DC/DC	6ES7 214-1AF40-0XB0
	CPU 1214FC DC/DC/Rly	6ES7 214-1HF40-0XB0
CPU 1215FC	CPU 1215FC DC/DC/DC	6ES7 215-1AF40-0XB0
	CPU 1215FC DC/DC/Rly	6ES7 215-1HF40-0XB0

B.2 Fail-Safe signal modules (SM)

Table B- 2 Fail-Safe signal modules (SM)

Item		Article number
Digital input	SM 1226 F-DI 16 x 24 VDC	6ES7 226-6BA32-0XB0
Digital output	SM 1226 F-DQ 4 x 24 VDC	6ES7 226-6DA32-0XB0
	SM 1226 F-DQ 2 x Relay	6ES7 226-6RA32-0XB0

B.3 Other modules

Table B- 3 Companion products

Item		Article number
Power supply	PM 1207 power supply	6EP1 332-1SH71-4AA0

B.4 Spare parts and other hardware

Table B- 4 Expansion cables, simulators, connector blocks and terminal blocks

Item			Article number
I/O expansion cable	I/O Expansion cable, 2 m		6ES7 290-6AA30-0XA0
Input simulator	Simulator (1214FC/1215FC - 14 position)		6ES7 274-1XH30-0XA0
Potentiometer module	S7-1200 Potentiometer module		6ES7 274-1XA30-0XA0
Spare door kit	CPU 1214FC		6ES7 291-1AB30-0XA0
	CPU 1215FC		6ES7 291-1AC30-0XA0
	Signal module, 45 mm		6ES7 291-1BA30-0XA0
	Signal module, 70 mm		6ES7 291-1BB30-0XA0
	Communication module		6ES7 291-1CC30-0XA0
Connector block	Tin	7 terminal, 4/pk	6ES7 292-1AG30-0XA0
		8 terminal, 4/pk	6ES7 292-1AH30-0XA0
		10 terminal, 4 pk	6ES7 292-1AK30-0XA0
		11 terminal, 4/pk	6ES7 292-1AL30-0XA0
		12 terminal, 4/pk	6ES7 292-1AM30-0XA0
		14 terminal, 4/pk	6ES7 292-1AP30-0XA0
		16 terminal, 4/pk	6ES7 292-1AR30-0XA0
		18 terminal, 4/pk	6ES7 292-1AT30-0XA0
		20 terminal, 4/pk	6ES7 292-1AV30-0XA0
	Gold	3 terminal, 4/pk (for analog CPU)	6ES7 292-1BC30-0XA0
		6 terminal, 4 pk (for analog CPU	6ES7 292-1BF30-0XB0
		6 terminal, 4/pk (for signal board)	6ES7 292-1BF30-0XA0
		6 terminal, 4/pk (for analog CPU)	6ES7 292-1BF30-0XB0
		7 terminal, 4/pk (for analog signal module)	6ES7 292-1BG30-0XA0
		11 terminal, 4/pk (for analog signal module)	6ES7 292-1BL30-0XA0
Terminal block	Keyed left, 7 contact		6ES7 292-1AG40-0XA1
	Keyed right, 7 contact		6ES7 292-1AG40-0XA0
	Keyed right, 8 contact		6ES7 292-1AH40-0XA0
	Keyed right, 11 contact		6ES7 292-1AL40-0XA0
	Keyed right, 12 contact		6ES7 292-1AM40-0XA0
	Keyed right, 14 contact		6ES7 292-1AP40-0XA0
	Keyed right, 20 contact		6ES7 292-1AV40-0XA0

B.5 Programming software

Table B- 5 Programming software

SIMATIC software		Article number
Programming software	STEP 7 Basic V13 SP1	6ES7 822-0AA01-0YA0
	STEP 7 Professional V13 SP1	6ES7 822-1AA01-0YA5
	STEP 7 Safety Advanced V13 SP1	6ES7 833-1FA12-0YA5
	STEP 7 Safety Basic V13 SP1	6ES7 833-1FB13-0YA5
Visualization software	WinCC Basic V12 SP1	6AV2100-0AA01-0AA0
	WinCC Comfort V12 SP1	6AV2101-0AA01-0AA5
	WinCC Advanced V12 SP1	6AV2102-0AA01-0AA5
	WinCC Professional 512 PowerTags V12 SP1	6AV2103-0DA01-0AA5
	WinCC Professional 4096 PowerTags V12 SP1	6AV2103-0HA01-0AA5
	WinCC Professional max. PowerTags V12 SP1	6AV2103-0XA01-0AA5

Fail-Safe response times

C

C.1 Manual update note

Appendix C: "Fail-Safe response times" is not available at the time of manual publication.

Refer to the S7-1200 Functional Safety Manual Update (http://support.automation.siemens.com/WW/view/en/105898775)for the fail-safe response time information.

Glossary

1oo1

A functional safety architecture with no redundancy. The safety function requires 1 out of 1 provided signal/logic channels for implementation. A single dangerous fault results in dangerous loss of the safety function.

1oo2

A functional safety architecture with two channels. The safety function requires 1 out of 2 provided signal/logic channels for implementation. The safety function is still fulfilled in the presence of a dangerous fault in one channel.

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 fail-safe CPU and the safety program).

Actuator

Field device that converts the electrical signal from the PLC into an action of controlled machinery. In this manual, the term can include interposing contactors and relays that control machinery, as well as directly connected motors or solenoids.

Category

Category according to EN ISO 13849 defines architectural requirements for functional safety. The products in this manual can fulfill Category 2 to Category 4. Category 4 requires that no single fault can be dangerous and no undetected accumulation of faults can be dangerous.

See also Overvoltage category.

Channel

In IEC 61508 terminology, a channel is a single signal/logic path that supports a safety function. The definition of 1oo1 and 1oo2 above uses channel in this sense. In most uses in this manual, a channel refers to one process value, whether implemented as 1oo1 or 1oo2.

Channel fault

A fault that causes one process value to be passivated, such as a detected wiring fault on one input. Other channels in the module can continue to support a safety function.

See also Module fault:

- SM 1226 DI 16 x 24 VDC:
  - When configured as 1oo1, a detected fault related to one digital input terminal results in the process value being set to "0". The 1oo1 configuration is exposed to the risk of a single undetected fault (for example, a sensor stuck ON).
  - When configured as 1oo2, both associated digital input terminals are represented by a single process value. A detected fault related to either digital input in the 1oo2 pair, or a failure of the two inputs to compare, results in the process value being set to "0".
- SM 1226 DQ 4 x 24 VDC and SM 1226 DQ 2 x Relay: These modules always operate as 1oo2, with two DC switches or two relays required to be ON to supply energy to the load. A detected fault associated with either switch or either relay results in an attempt to turn off both switches or relays, and a report to the user program that the channel is passivated.

CRC signature

The CRC (Cyclic Redundancy Check) signature is a cyclic redundancy checksum that confirms the integrity of the PROFIsafe message contents and sequence.

Cyclic interrupt / cycle time

The start-to-start user configured time delay between executions of the safety program.

Dark test / dark time

The test or time in which a "0" signal is deliberately created to confirm that "0" can be controlled or detected when needed. On inputs, the F-DI performs a dark test by briefly turning off the sensor supply. On DC outputs, the F-DQ DC performs a dark test by briefly turning off one of the P or M output switches.

Discrepancy time (of inputs)

The configured discrepancy time during which you expect 1oo2 inputs to disagree due to mechanical and electrical differences in input signals. The F-DI interprets differences between inputs lasting longer than the discrepancy time as a channel fault.

Equivalent (input)

A 1oo2 input channel where both signal inputs interpret high voltage as a process value "1" and low voltage as a process value "0".

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.

Fail-safe

A system or component designed to reliably provide a defined, safe result in the event of a fault.

F-DI, F-DQ DC, and F-RLY

The manual uses the following short names for the S7-1200 fail-safe SMs:

- F-DI: SM 1226 DI 16 x 24 VDC
- F-DQ DC: SM 1226 DQ 4 x 24 VDC
- F-RLY: SM 1226 DQ 2 x Relay

F-FBs /F-FCs

Fail-safe function blocks (FB) and function calls (FC) are program units in which you program the safety program in F-FBD or F-LAD. FBs include an instance DB (Data Block) that retains information about that particular usage of the function in your program. For example, each specific instance of a timer has a DB to retain the results of each timer update. FCs do not include an instance DB, and no information is carried over between calls to FCs.

F-I/O

A general term for fail-safe input and output signal modules (SM).

F-monitoring time

The F-monitoring time is the amount of time an SM or CPU waits for an error-free communication including the expected new Virtual Monitoring Number before passivating channels.

F-runtime group

An F-runtime group consists of an F-OB (cycle OB or cyclic interrupt OB) that calls a main safety block (FB or FC). Additional user-specific safety functions must then be called from this main safety block.

F-system

A fail-safe system.

Light test / light time

The test or time in which a "1" signal is deliberately created to confirm that "1" can be controlled or detected when needed. The signal modules described in this manual do not deliberately conduct light tests that can affect your program or the output load. The SM 1226 F-DQ 4 x 24 VDC produces ON test pulses up to the Maximum readback time switch on test on each of the P and M switches individually, but do not intentionally turn on both P and M switches at once for a test when commanded process value is "0". In the unlikely event of an undetected fault on the opposite switch, the test pulses can result in energy applied to the load.

M

Refers to the 24 VDC power circuit 0 VDC reference. In the context of the F-DQ DC module outputs, M can refer to the switch output connecting the load to M.

Module fault

A fault that affects all channels of a fail-safe signal module (SM). The fail-safe SM attempts to passivate all channels in the module.

See also Channel fault.

Non-equivalent (input)

A 1oo2 input channel where one signal input interprets high voltage as a process value "1" and the redundant signal input interprets high voltage as a process value "0". A common configuration is complementary normally-open and normally-closed switches connected to the same process event.

Overvoltage category

A definition of transient voltage threat due to lightning strikes and other sources, generally associated with how closely the circuit is coupled to outdoor electrical wiring. Category III represents a higher voltage level threat than Category II.

P

Refers to the 24 VDC positive supply. In the context of the F-DQ DC module outputs, P can refer to the switch output connecting the load to P.

Passivate / passivated / passivation

The fail-safe CPU or fail-safe SM has identified a channel or module as faulty. The fail-safe CPU or fail-safe SM supplies the fail-safe process value "0" instead of any detection or logic evaluation that can result in process value "1".

PFD_avg

Average probability of a dangerous failure on demand (PFD_avg). An estimate of how likely a safety function will fail to perform as expected when required to function only rarely (on demand). PFD is typically used for safety function applications that are required to operate in response to unusual accidental or emergency events occurring less frequently than once per year.

PFH

Average frequency of a dangerous failure per hour (PFH). The average frequency of dangerous failures for systems that are required more frequently than once per year to initiate or maintain a safe state. Most safety functions associated with routine machine operation use PFH as a defining safety metric.

PL

Performance Level (PL) : Levels "a" through "e" are defined in EN ISO 13849, with level "e" being the high level of safety performance. A higher PL is associated with a lower probability of dangerous failure.

PM

In the context of the F-DQ DC output module, refers to the DC output point including a switch to P and a switch to M. The typical application is for the load to be connected between the P and M switches, sometimes called "PM mode".

Process value bit

The data bit accessible to the user program representing the process value. If an input channel is passivated, the process value bit is set to "0". If an output channel is passivated, the user program can set the process value bit to "1", but this is not effective at the SM outputs.

PROFIsafe

A communication protocol providing for secure transport of safety information, including provisions for sequence and time monitoring of messages.

PROFIsafe address

A unique identifier for every F-IO in a network including central F-IOs. The PROFIsafe address consists of the F-source address and the F-destination address.

Proof-test / Proof-test interval

A proof test is a verification that a safety component or system operates as expected. Immediately after each successful proof test, the safety component or system is considered to have a minimum probability of dangerous failure. The probability of dangerous failure increases with time until the next proof test. The maximum probability of dangerous failure is calculated assuming the component or system is tested or replaced within the proof test interval.

Quality bit

The data bit accessible to the user program indicating whether or not a safety I/O channel is passivated. If the quality bit is "0", the channel is passivated or deactivated. For a 1oo2 input, the low numbered quality bit is effective, and the high numbered quality bit is always 0.

Reintegration

The procedure that allows a passivated channel or module to become active again after diagnostics indicate that faults are removed or corrected.

Safe state

The basic principle behind the safety concept is the identification of a safe state for all process variables. The value "0" (de-energized) represents this safe state for digital fail-safe signal modules (SM). This applies to both sensors and actuators.

Safety Administration Editor (SAE)

A view in the TIA Portal, for each PLC, allowing the user to configure safety program scheduling and time out parameters, identify the safety blocks and data types, and set protection for the safety program.

Safety function (context: PLC internals)

The term "safety function" can refer to PLC system internal features, including program block elements, that contribute to the development of your safety program and the assurance that your user or application safety function is executed as designed.

Safety function (context: user or application level)

One specific action of a safety system. While the term can be used for general goals (for example, "Protect the operator from the saw blade"), safety system analysis typically includes decomposing the general goal into elemental specific actions designed to minimize risk (for example, "When the hand control is released, turn off the motor" or "Keep the access guard locked until the motor has been deenergized for at least 60 seconds"). Each of these items can be considered a safety function.

Safety mode

1. Safety mode is the operating mode of the fail-safe signal modules (SM) that allows safety-related communication using safety message frames. S7-1200 fail-safe SMs are designed for safety mode only.
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.

Sensor

Field device that converts a physical quantity (for example, location, temperature, or speed) into an electrical signal that can be read by the PLC. The only fail-safe sensor inputs presently available for the S7-1200 are digital (binary) ON/OFF inputs operating at 24 VDC nominal.

SIL

Safety Integrity Level (SIL) values 1 through 4 are defined in IEC 61508. A higher safety integrity level is associated with a lower probability of dangerous failure.

Standard user program

The standard user program is a non-safety-related user program.

Index

G

H

I

L

M

O

P

R

S

T

U

V

W