

Monitoring of the Feedback Circuit in the Safety Program

Safety Integrated

https://support.industry.siemens.com/cs/ww/en/view/21331098

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG (“Siemens”). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.
By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer’s exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/cert.

© Siemens AG 2023 All rights reserved

Table of Contents

Legal information **2**

1 Task **4**

2 Solution **4**

2.1 Overview 4
2.2 Hardware and software components 6
2.2.1 Validity 6
2.2.2 Components used 6

3 Basics **8**

3.1 Basic terms 8
3.2 Functional safety 9
3.3 Feedback circuit 10

4 Mode of Operation **11**

4.1 General overview 11
4.2 Monitoring the emergency-stop control devices 12
4.3 Monitoring the feedback circuit 15
4.4 Data exchange between standard user program and safety program 16

5 Configuration and Settings **17**

5.1 Settings of the DI 17
5.2 Settings of the F-DI 18
5.3 Settings of the F-DQ 20

6 Installation and Commissioning **21**

7 Operating the Application **24**

8 Evaluation of the Safety Function **26**

8.1 Standards 26
8.2 Safety functions 26
8.3 Evaluation according to IEC 62061 27
8.4 Evaluation according to ISO 13849-1 28

9 Alternative solution using coupling relays **30**

10 Appendix **31**

10.1 Service and support 31
10.2 Links & Literature 32
10.3 History 33

© Siemens AG 2023 All rights reserved

1 Task

A machine executing dangerous movements is controlled via a fail-safe controller and switched by means of contactors. In order to protect the operating personnel, technical safety functions (e. g. an emergency-stop control device and a safety door) are implemented on the machine. The correct functioning of the contactors shall be monitored in order to ensure a high diagnostic coverage and, thus, a high SIL (safety integrity level according to IEC 62061) or PL (performance level according to ISO 13849-1).

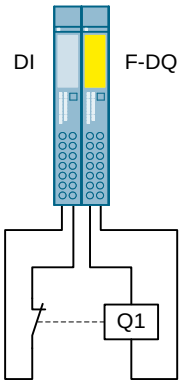
2 Solution

2.1 Overview

Schematic layout

Monitoring the actuators represents a diagnostic function and significantly contributes to the SILCL (SIL claim limit) or PL of the corresponding subsystem. For electromechanical components (e. g. relays or contactors), a positively driven auxiliary contact often is fed back to the controller and then evaluated. This process is referred to as monitoring of the feedback circuit or readback of the contactors.

Figure 2-1 Typical wiring of an actuator and its feedback circuit



This is particularly required for a redundant setup. If one of the two contactors welds (without this being noticed), the two-channel system would become a single-channel system.

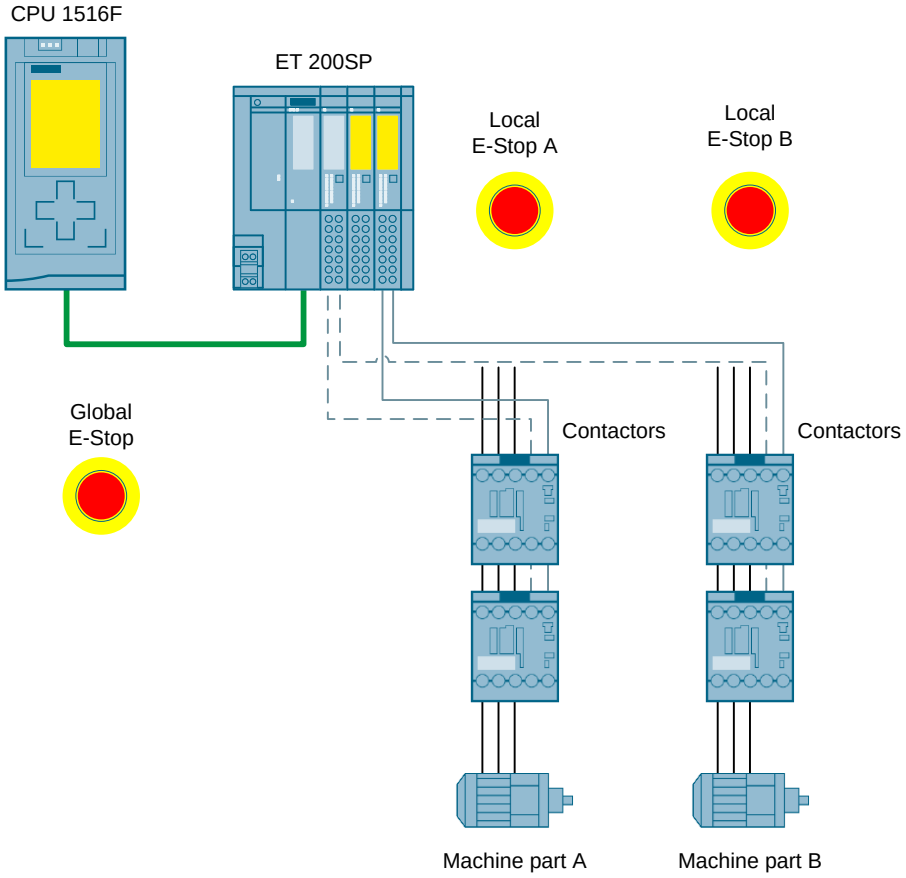
Instead, the welding will be detected and it will be prevented that the system is switched on again until the error is eliminated.

© Siemens AG 2023 All rights reserved

Setup

In this application example, two machine parts are switched separately in order to illustrate the monitoring of the feedback circuit. Only the affected machine part shall be switched off via the local emergency-stop control devices. By means of the global emergency-stop control device, both machine parts are switched off safely.

Figure 2-2 Overview of the main components



Both contactors of a machine part are controlled in parallel via a failsafe output of the ET 200SP.

The auxiliary contacts of both contactors of a machine part are connected in series and fed back to a DI of the ET 200SP. In the safety program, the signal of the feedback circuit is compared to the control signal of the contactors.

Topics not covered by this application

This application does not include a description of:

- Analysis of the sensors
- Monitoring of electronic components such as converters

Assumed knowledge

The following knowledge is required:

© Siemens AG 2023 All rights reserved

- Basics of functional safety
- Basics of STEP 7 programming

2.2 Hardware and software components

2.2.1 Validity

This application is valid for

- All fail-safe SIMATIC controllers
- STEP 7 Professional as of V18 with STEP 7 Safety Advanced

Note When using a SIMATIC S7-1200 controller with centralized configuration, STEP 7 Basic as of V18 with STEP 7 Safety Basic is sufficient.

2.2.2 Components used

The application was created using the following components:

© Siemens AG 2023 All rights reserved

Hardware components

Table 2-1 Hardware components

Component	Qty.	Article number	Note
Power supply	1	6EP1332-4BA00	PM 190 W
Fail-safe S7-CPU	1	6ES7516-3FN02-0AB0	CPU 1516F-3 PN/DP
SIMATIC memory card	1	6ES7954-8LF02-0AA0	SMC 24MB
Interface module for ET 200SP	1	6ES7155-6AU00-0BN0	IM155-6PN ST
Digital input module	1	6ES7131-6BF00-0BA0	8 DI ST, DC 24V
Fail-safe digital input module	1	6ES7136-6BA00-0CA0	8 F-DI, DC 24V
Fail-safe digital output module	1	6ES7136-6DB00-0CA0	4 F-DQ, DC 24V/2A
Base Unit	1	6ES7193-6BP00-0DA0	Supply terminal separated
Base Unit	2	6ES7193-6BP00-0BA0	Supply terminal bridged
Bus adapter	1	6ES7193-6AR00-0AA0	BA 2xRJ45
DIN rail S7-1500	1	6ES7590-1AE80-0AA0	Length: 482 mm
DIN rail 35mm	1	6ES5710-8MA11	Length: 483 mm
Emergency-stop control device	3	3SU1801-0NA00-2AA2	Mushroom push button with housing
Contact module 1 NC contact	3	3SU1400-2AA10-1CA0	Additional contact for emergency stop
Contactor	4	3RT2015-1BB42	NO00, DC24V, 1NC

Software components

Table 2-2 Software components

Component	Qty.	Article number	Note
STEP 7 Professional	1	6ES7822-1AA08-0YA7	V18
STEP 7 Safety Advanced	1	6ES7833-1FA18-0YA5	V18

Example files and projects

The following list includes all files and projects that are used in this example.

Table 2-3 Example files

Component	Note
21331098_Feedback_DOC_V6_en.pdf	This document
21331098_Feedback_PROJ_V6.zip	TIA Portal project
21331098_Feedback_TST_V6.zip	Evaluation of the safety function as TST project

© Siemens AG 2023 All rights reserved

3 Basics

3.1 Basic terms

Diagnostic coverage

The diagnostic coverage (DC) describes the effectiveness of the diagnostic function(s) of a safety function by considering the rate of detected dangerous failures (λ_{DD}) in relation to the rate of all dangerous failures (λ_{Dtotal}).

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

The diagnostic coverage is required to calculate the PFH_D of a safety function and, thus, to determine the SIL achieved according to IEC 62061 or the PL according to ISO 13849-1 of a safety function.

Appendix E of ISO 13849-1 describes examples for estimating the DC.

Feedback circuit

A feedback circuit is used for the monitoring of controlled actuators (e. g. relay or load contactors) with positively driven contacts or mirror contacts. The outputs can only be enabled when the feedback circuit is closed. When using a redundant switch-off path, the feedback circuit of both actuators has to be evaluated. For this purpose, they may also be connected in series.

© Siemens AG 2023 All rights reserved

PFH_D

The PFH_D (Probability of dangerous Failure per Hour) describes the average probability of a dangerous failure per hour of a safety-related system with regard to performing a certain safety function.

This value is required to determine the SIL achieved according to IEC 62061 or the PL according to ISO 13849-1 of a safety function.

The calculation of the PFH_D depends on the architecture/structure of the system considered.

Note PFH_D must not be confused with the probability of a dangerous failure on demand (PFD).

Positively driven contacts

For a component with positively driven contacts (mirror contacts), it is guaranteed that the NC and NO contacts are never closed at the same time (EN 60947-5-1).

3.2 Functional safety

From the view of the goods to be protected, safety is indivisible. However, since the causes of the hazards and therefore also the technical measures for avoiding them may be very different, the types of safety are also distinguished, for example, by specifying the respective cause of possible hazards. For this reason it is referred to “electrical safety” when hazards from electricity are expressed or “functional safety” when the safety depends on the correct function.

In order to achieve functional safety of a machine or plant, it is necessary for the safety-relevant parts of the protective equipment and control devices to function correctly and that they behave in a way that the plant stays in a safe state or is brought to a safe state in the event of an error.

A very high-quality technology is necessary to achieve this, where the requirements described in the appropriate standards are met. The requirements to achieve functional safety are based on the following basic targets:

- Avoiding systematic faults
- Control of systematic faults
- Managing accidental faults or failures

The measure for the functional safety achieved, is the probability of dangerous failures, the error tolerance and the quality through which the freedom from systematic errors is to be guaranteed. In the respective standards, this is expressed by means of different terms:

- In IEC 62061: “Safety Integrity Level” (SIL)
- In ISO 13849-1: “Performance Level” (PL)

For further information on functional safety, please refer to \5\.

© Siemens AG 2023 All rights reserved

3.3 Feedback circuit

The feedback circuit is used to monitor electromechanical components and represents a diagnostic function of a safety-related system.

Recommendations

The feedback circuit is to be implemented based on the risk assessment and the general requirements regarding the diagnostic function of a safety-related system as described in chapter 6.8 of IEC 62061. In addition, Appendix E of ISO 13849-1 can be referred to for selecting an appropriate diagnostic function.

Generally, the following points should be considered in the implementation.

- The auxiliary contact is positively driven.
- The auxiliary contact is a NC contact.
- When using a redundant switch-off path, both actuators have to be evaluated. For this purpose, the auxiliary contacts of the actuators may also be connected in series.
- Monitoring and controlling of the actor is done for example with the STEP 7 block “FDBACK”.

© Siemens AG 2023 All rights reserved

Connecting the feedback circuit

Considering the points listed above, connecting the feedback circuit to a DI is in many cases sufficient. This variant is implemented in this application example.

In the following cases, it might be reasonable or necessary to connect the feedback circuit to an F-DI:

- Single-channel setup of actuators, but a high diagnostic coverage is nevertheless required.
- Certain diagnostic functions (e. g. STEP 7 block “FDBACK”) are not possible.
- Use of a fail-safe module in a distributed I/O in order to use the safety mechanisms of PROFIsafe.

4 Mode of Operation

4.1 General overview

Program overview

The figure below shows the standard user program and the safety program as well as the data exchange between the two programs via global data blocks.

Figure 4-1 Data exchange between standard user program and safety program

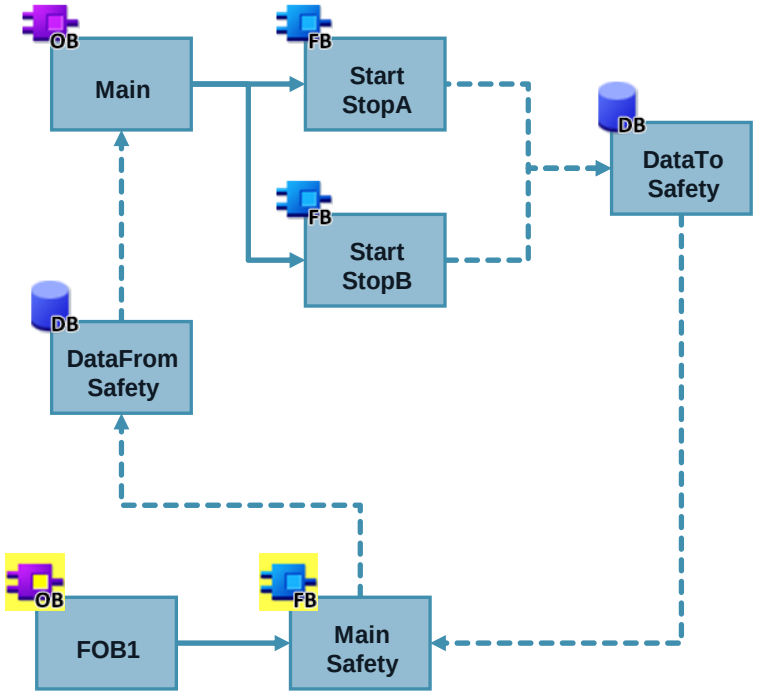


Table 4-1 Program blocks

Block	Function
StartStopA	This block represents the standard user program for machine part A.
StartStopB	This block represents the standard user program for machine part B.
MainSafety	This block contains the safety program and calls all the other safety-relevant instructions.
DataToSafety	In this global data block, the blocks “StartStopA” and “StartStopB” provide the safety program with their control signals.
DataFromSafety	In this global data block, the safety program provides the standard user program with diagnostic information.

© Siemens AG 2023 All rights reserved

Figure 4-2 Setup of the safety program

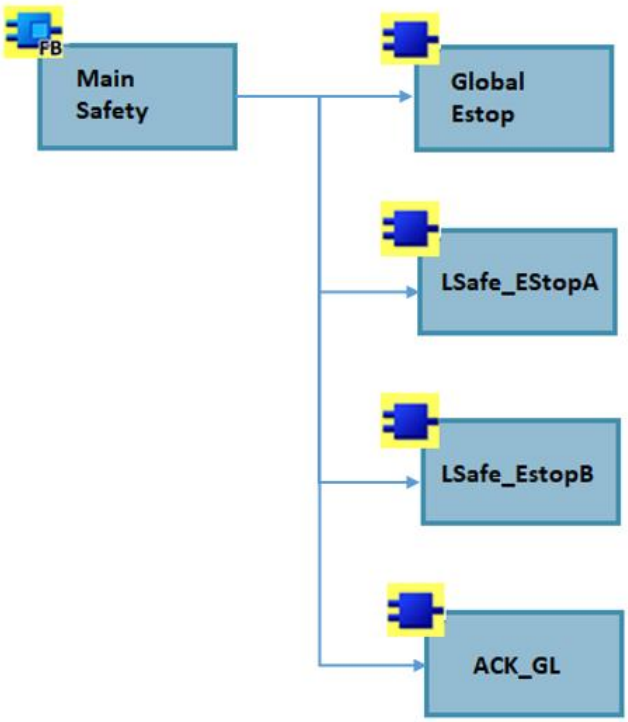


Table 4-2 Explanation of the safety program blocks

Block	Function
GlobalEstop	This block monitors the global emergency-stop control device switching off both machine parts and is an instance of the STEP 7 instruction ESTOP1.
LSafe_EstopA	This function block monitors the local emergency stop command device that switches off machine part A. In addition, the function block monitors the feedback circuit of the actuators of machine part A.
LSafe_EStopB	This function block monitors the local emergency stop command device that switches off machine part B. In addition, the function block monitors the feedback circuit of the actuators of machine section B.
ACK_GL	This instruction is intended for reintegration of passivated channels.

4.2 Monitoring the emergency-stop control devices

Introduction

In the application example, three emergency-stop control devices are monitored:

- Global emergency stop switching off both machine parts
- Local emergency stop switching off only machine part A
- Local emergency stop switching off only machine part B

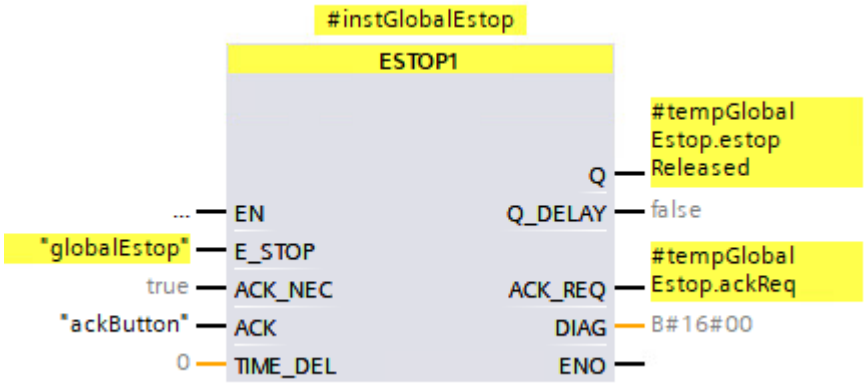
© Siemens AG 2023 All rights reserved

Any of the three emergency-stop control devices is monitored via the ESTOP1 instruction. For subsystems A and B, the ESTOP1 instruction is called internally in LSafe_EStop.

Program description

The ESTOP1 instruction from STEP 7 Safety Advanced is used directly for the Global Emergency Stop.
If the emergency stop is not actuated, the instruction outputs TRUE at output Q. After actuating the emergency stop, it has to be unlocked and acknowledged via the ACK input. It is output via the ACK_REQ output that an acknowledgement is required. The Q output is intermediately saved in a temporary tag in order to simplify access to it in the following networks.

Figure 4-3 Monitoring the global emergency-stop control device in the safety program

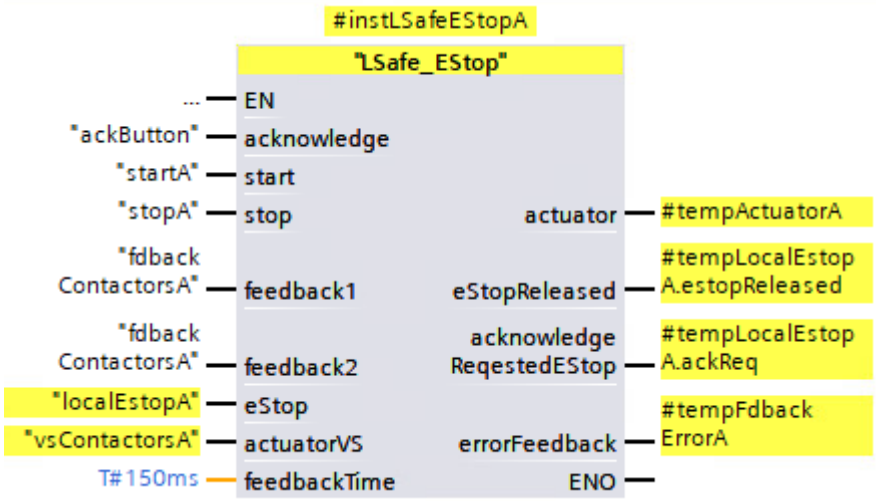


For the two subsystems A and B, the LSafe_EStop module from the TÜV-tested LSafe library is used. This offers the advantage that the feedback loop monitoring (see chapter 4.3) of the actuators is realized at one block. The function for monitoring the emergency stop is also implemented internally via the ESTOP1 instruction.

If the emergency stop is not actuated, the instruction outputs TRUE at the "estopReleased" output. After the emergency stop has been actuated, it must be unlocked and acknowledged via the "acknowledge" input. The fact that acknowledgement is required is output via the "acknowledgeRequestedEstop" output.

© Siemens AG 2023 All rights reserved

Figure 4-4 Configuration LSafe_EStop subsystem A for monitoring the emergency stop command device



Note

Both channels of the emergency-stop control device are monitored for discrepancy and cross-circuit by the F-DI module. In the user program, a processed signal will be available then for both channels. The individual channels cannot be accessed.

For an application example giving further information on monitoring an emergency-stop control device, please refer to \4\.

© Siemens AG 2023 All rights reserved

4.3 Monitoring the feedback circuit

Introduction

For switching and monitoring the actuators (in this example: the two contactors of each of the two machine parts), the FDBACK instruction included in STEP 7 is used. This is also used internally in the LSafe_EStop module.

This instruction continuously compares the signal of the feedback circuit to the control signal of the actuators. Thus, the following errors can be detected:

Table 4-3 FDBACK error detection

Error	Instant
Wire break of control line	In switched-off state: when switching on the actuators
	In switched-on state: immediately
Welding of a contact	When switching off the actuators

As both machine parts are controlled and monitored independently of each other, a separate instance of Lsafe_EStop is used for each machine part. The following description applies to both machine parts.

© Siemens AG 2023 All rights reserved

Program description

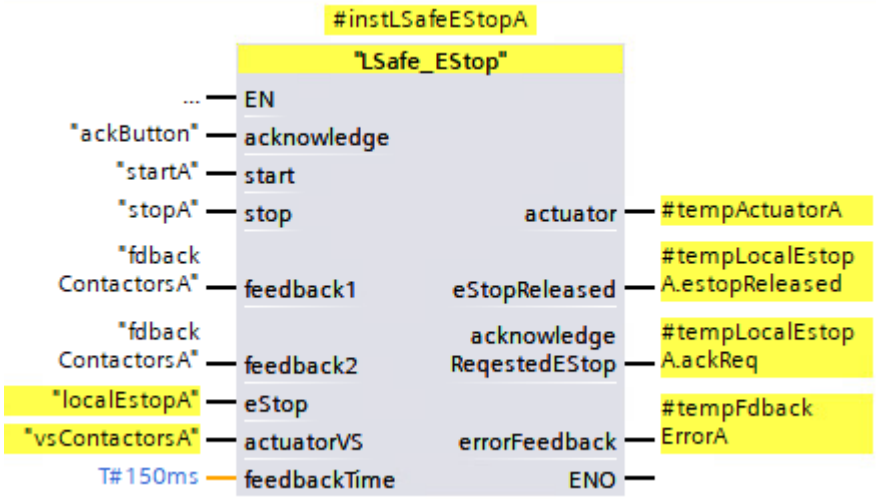
The contactors are switched via output “actuator” of the Lsafe_Estop block under the following conditions:

- Release signal of local emergency stop is applied
- Start signal of the standard user program is applied

The signal on the “feeback1” resp. “feedback2” input has to be switched to be inverse to the Q output signal within the configured “feedbackTime” time. If this is not the case, there may be an error in the feedback circuit and the contactors are switched off. Afterwards it has to be acknowledged via the “acknowledge” input.

For each program cycle, it is checked whether the signal of the feedback circuit is inverse to the output signal “actuator”. Thus, an error in the control line, the contactors or the feedback circuit will be detected immediately.

Figure 4-5 Monitoring the feedback circuit of machine part A in the safety program



The value status of the channel to which the contactors are connected is monitored at the “actuatorVS” input.

Since, in addition to the enable signal from the local emergency stop, the enable signal from the global emergency stop must also be present so that the condition for switching the contactors is fulfilled, this is realized by interconnecting the "actuator" output and the enable signal of the global ESTOP.

Figure 4-6 Condition for switching contactors



Note

In the newer controllers S7-1200 and S7-1500, the channel-granular QBAD bit is replaced by the value status. The following rules apply for the value status:

FALSE: Substitute values are output.

TRUE: Process values are output.

The value status behaves inversely to the QBAD bit and is entered into the process image of the inputs (PII).

For more information on the value status, please refer to \3\.

4.4 Data exchange between standard user program and safety program

In order to exchange data between the standard user program and the safety program, two global data blocks are used:

- DataToSafety

© Siemens AG 2023 All rights reserved

- DataFromSafety

The DataToSafety data block is written by the standard user program and read by the safety program. The DataFromSafety data block is written by the safety program and read by the standard user program.

Note For further information on data exchange between the standard user program and the safety program, please refer to \3\.

5 Configuration and Settings

The enclosed project does not require any further configuration. If you want to replicate the application example with other components, then the most important settings are shown in this chapter.

ATTENTION	**The settings displayed below help to meet PL e / SIL 3. Changes on the settings may cause loss of the safety function.**

ATTENTION	**The default values used in the example projects may also differ from your individual requirements.**

© Siemens AG 2023 All rights reserved

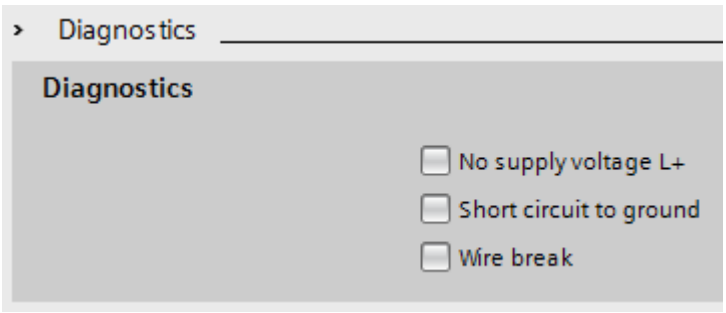
5.1 Settings of the DI

Diagnostics

The SIMATIC input modules of ET 200SP provide the option of enabling diagnostic functions. In this application example, these functions are demonstratively disabled, as they are not part of the safety function.

Possible errors in the feedback circuit are detected by means of the safety program and the FDBACK instruction.

Figure 5-1 Diagnostics settings of the DI

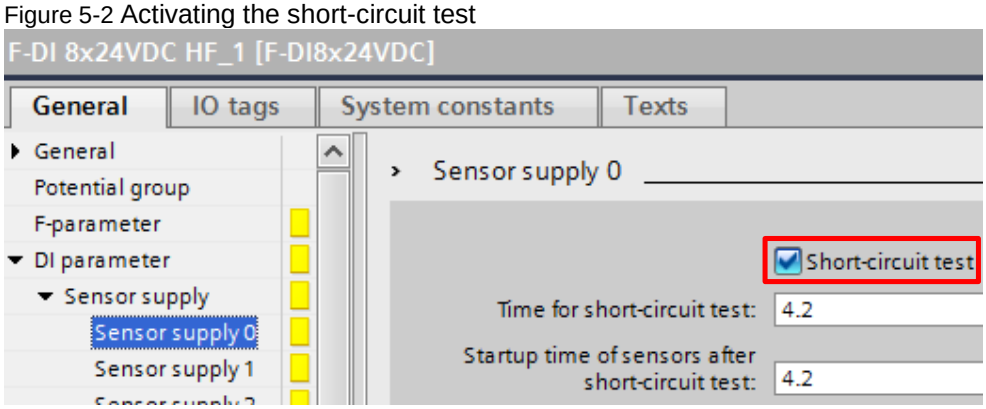


5.2 Settings of the F-DI

Short-circuit test

The short-circuit test for the channels 0, 1, 2, 4, 5 and 6 used is activated.

Figure 5-2 Activating the short-circuit test

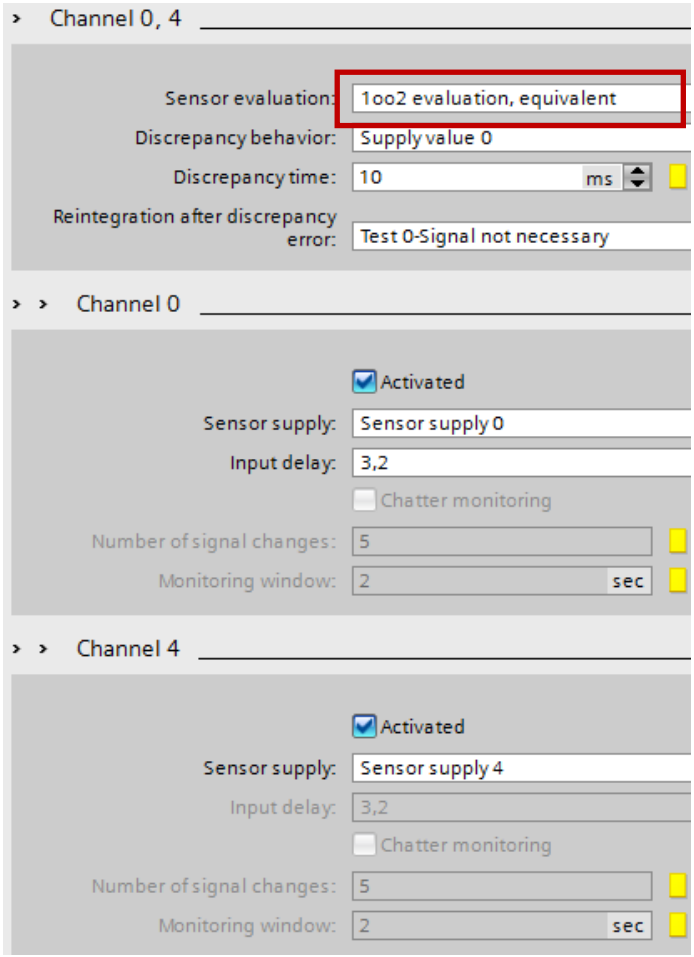


© Siemens AG 2023 All rights reserved

Channel parameters

The monitoring of the global emergency-stop control device is done via channel pair 0, 4. The evaluation of the encoder has to be set to “1oo2 evaluation, equivalent” in order to detect discrepancies between the two channels and thus to achieve the demanded safety level.

Figure 5-3 Setting “1oo2 evaluation, equivalent”



For the two local emergency-stop control devices (channel pairs 1, 5 and 2, 6), the same settings are made.

Note Channels which are not used must be deactivated.

© Siemens AG 2023 All rights reserved

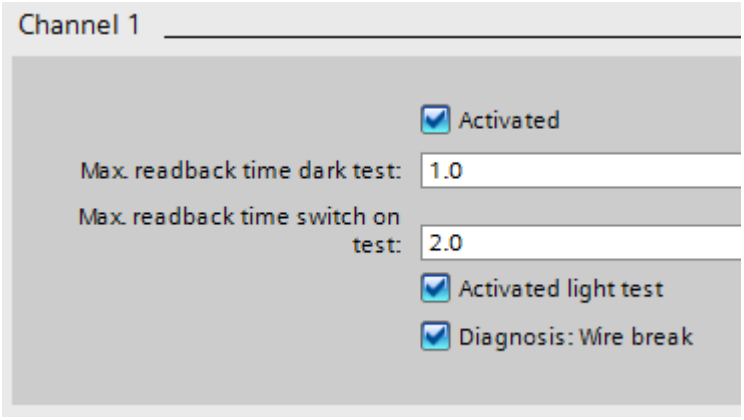
5.3 Settings of the F-DQ

Channel settings

For channels 0 and 1, which control the contactors, maximum readback times of 1 ms for the dark test and 2 ms for the switch on test have been specified.

Depending on the actuators used, you might have to adjust these times. For further information, please refer to the manual of the respective module in chapter \6\.

Figure 5-4 Channel settings F-DQ



ATTENTION	As the error response time will be prolonged by the readback time of the dark test, we recommend to carefully set a readback time for the dark test which is as short as possible, but long enough in order not to passivate the output channel.

Note	Channels which are not used must be deactivated.

© Siemens AG 2023 All rights reserved

6 Installation and Commissioning

In order to recreate this application example, wire the hardware components as illustrated below.

DI wiring

In the enclosed project, the start, stop and acknowledgement buttons are simulated via a watch table.

Figure 6-1 DI wiring diagram

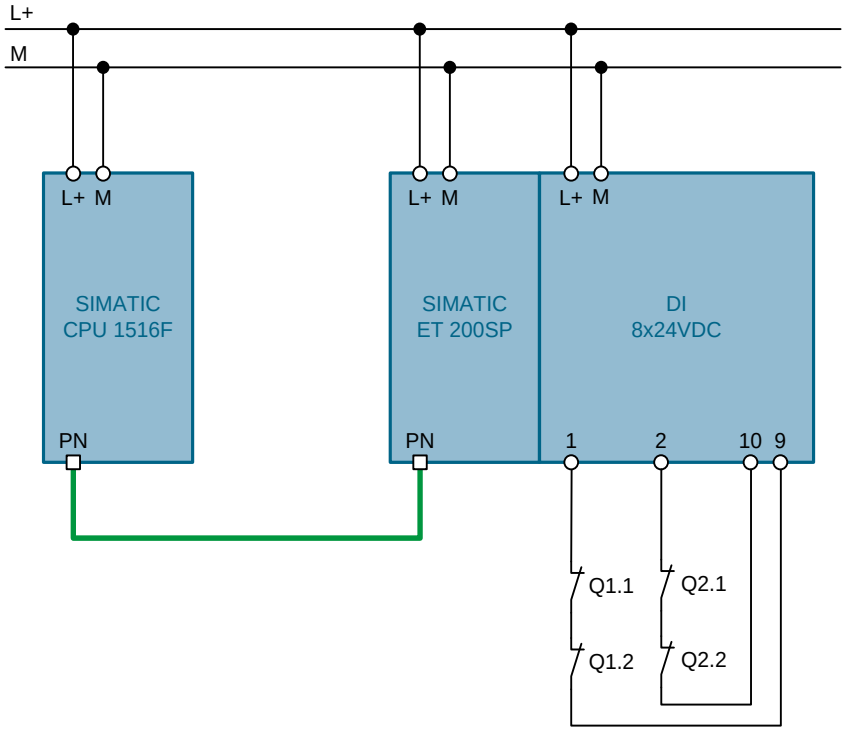


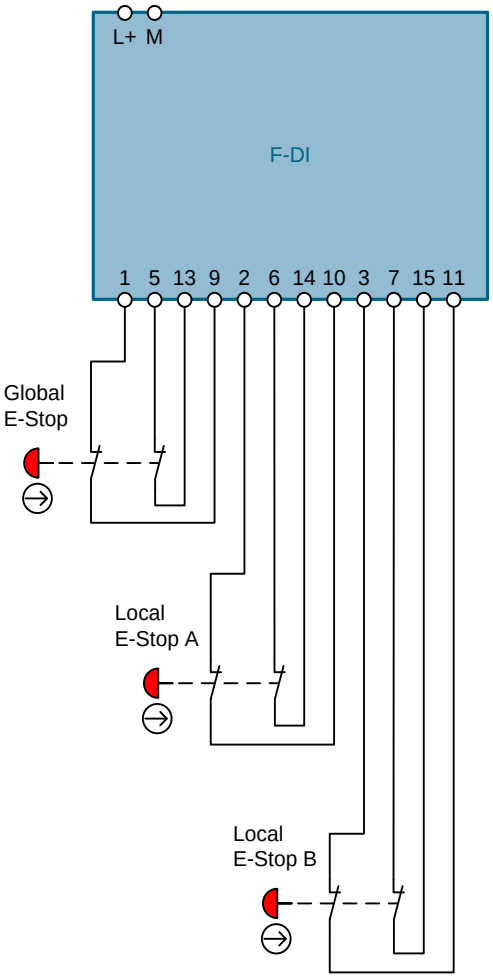
Table 6-1 Instruction for DI connection

No.	Action
1.	Connect the controller to the power supply.
2.	Connect the interface module of the ET 200SP to the power supply.
3.	Connect the BaseUnit of the DI to the power supply.
4.	Connect “21 NC” of Q1.1 to terminal 1 of the DI BaseUnit.
5.	Connect “22 NC” of Q1.1 to “21 NC” of Q1.2.
6.	Connect “22 NC” of Q1.2 to terminal 9 of the DI BaseUnit.
7.	Connect “21 NC” of Q2.1 to terminal 2 of the DI BaseUnit.
8.	Connect “22 NC” of Q2.1 to “21 NC” of Q2.2.
9.	Connect “22 NC” of Q2.2 to terminal 10 of the DI BaseUnit.
10.	Connect the controller to the interface module of the ET 200SP by means of an Ethernet cable.

© Siemens AG 2023 All rights reserved

F-DI wiring

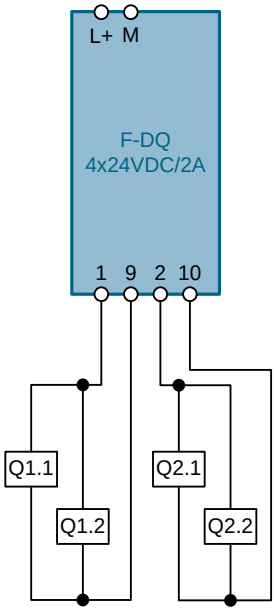
Figure 6-2 F-DI wiring diagram



© Siemens AG 2023 All rights reserved

F-DQ wiring

Figure 6-3 F-DQ wiring diagram



Commissioning

For detailed instructions for loading and commissioning a TIA Portal project with a safety program, please refer to \4\.

© Siemens AG 2023 All rights reserved

7 Operating the Application

In the enclosed project, the inputs for start, stop and acknowledge buttons can be simulated via an watch table or controlled via real buttons.
Open the project and the watch table, and connect to the controller to monitor or to modify the application.

Testing the emergency-stop control devices

The table below demonstrates the function principle:

Table 7-1 Testing the emergency-stop control devices

No.	Action	Result / Note
1.	Modify the “ackButton” tag to TRUE and then reset it to FALSE or press the acknowledge button.	Acknowledgement after restart
2.	Modify the “startA” tag to TRUE and then reset it to FALSE or press the start button A	Contactors of machine part A are switched on
3.	Modify the “startB” tag to TRUE and then reset it to FALSE or press the start button B.	Contactors of machine part B are switched on
4.	Actuate the local emergency-stop control device for machine part A.	Contactors of machine part A are switched off
5.	Unlock the local emergency-stop control device.	
6.	Modify the “ackButton” tag to TRUE and then reset it to FALSE or press the acknowledge button.	Acknowledgement after triggering the safety function
7.	Modify the “startA” tag to TRUE and then reset it to FALSE or press the start button A	Contactors of machine part A are switched on
8.	Actuate the global emergency-stop control device.	Contactors of both machine parts are switched off
9.	Unlock the global emergency-stop control device.	
10.	Modify the “ackButton” tag to TRUE and then reset it to FALSE or press the acknowledge button.	Acknowledgement after triggering the safety function

© Siemens AG 2023 All rights reserved

Simulating a welded contact

The table below demonstrates how you can test the diagnostic function of the feedback circuit:

Table 7-2 Simulating a welded contact

No.	Action	Result / Note
11.	Modify the “ackButton” tag to TRUE and then reset it to FALSE or press the acknowledge button.	Acknowledgement after restart
12.	Modify the “startA” tag to TRUE and then reset it to FALSE or press the start button A	Contactors of machine part A are switched on
13.	Hold the bolt of a contactor in the retracted position by means of a screwdriver.	
14.	Modify the “stoptA” tag to TRUE and then reset it to FALSE or press the stop button A	The intact contactor is switched off. Restart is prevented.
15.	Release the bolt of the contactor.	

No.	Action	Result / Note
16.	Modify the “ackButton” tag to TRUE and then reset it to FALSE or press the acknowledge button.	Acknowledgement of the error in the feedback circuit
17.	Modify the “startA” tag to TRUE and then reset it to FALSE or press the start button A	Contactors of machine part A are switched on

Simulating a wire break

The table below demonstrates how you can test the diagnostic function of the feedback circuit:

Table 7-3 Simulating a wire break

No.	Action	Result / Note
18.	Modify the “ackButton” tag to TRUE and then reset it to FALSE or press the acknowledge button.	Acknowledgement after restart
19.	Modify the “startA” tag to TRUE and then reset it to FALSE or press the start button A	Contactors of machine part A are switched on
20.	Interrupt the power supply of one of the two contactors.	Contactors of machine part A are switched off. Restart is prevented.
21.	Reconnect the contactor to the power supply.	
22.	Modify the “ackButton” tag to TRUE and then reset it to FALSE or press the acknowledge button.	Acknowledgement of the error in the feedback circuit
23.	Modify the “startA” tag to TRUE and then reset it to FALSE or press the start button A	Contactors of machine part A are switched on

© Siemens AG 2023 All rights reserved

8 Evaluation of the Safety Function

8.1 Standards

For an evaluation of the safety function, the following versions of the standards were used:

Table 8-1 Versions of standards

Version	Abbreviated notation in this document
EN ISO 13849-1:2015	ISO 13849-1
EN ISO 13849-2:2012	ISO 13849-2
EN 62061:2015	IEC 62061

8.2 Safety functions

Preliminary remarks

- Emergency stop is not a means of risk reduction.
- Emergency stop is a “supplementary safety function”.

© Siemens AG 2023 All rights reserved

Safety functions

The following safety functions are realized in this application example:

Table 8-2

Safety function	Description
SF1	If the global emergency stop is actuated, the contactors of machine parts A and B must switch off safely.
SF2	If the local emergency stop in machine part A is actuated, the contactors of machine part A must switch off safely.
SF2	If the local emergency stop in machine part B is actuated, the contactors of machine part B must switch off safely.

In the following, the “Reaction” subsystem of the SF2 safety function is evaluated according to the standards IEC 62061 and ISO 13849-1, ISO 13849-2.

For a detailed evaluation of the overall safety function, please refer to the enclosed TST project or to \4\.

8.3 Evaluation according to IEC 62061

In the following, the evaluation according to IEC 62061 is carried out by means of the Safety Evaluation in the TIA Selection Tool. Please find the link to the Safety Evaluation in the TIA Selection Tool on the Internet at \7\.

Evaluation of "Reaction"

The contactor parameters relevant for the evaluation are provided by the manufacturer and specified by the user.

Table 8-3

Parameter	Value	Explanation	Definition
B10 B10 value Contactor	1,000,000	Manufacturer information	SIEMENS AG
Percentage of dangerous failures Contactor	0.73 (73%)	Manufacturer information	
T1 Lifetime	175,000 h (20 years)	Manufacturer information	
Subsystem architecture	D	2 channels, 2 components: Single fault tolerance with diagnostic function	User
Actuations/ test interval	1/h	Assumption	
β **(CCF factor)** Susceptibility to common cause failures	0.1 (10%)	For installations according to IEC 62061, a CCF factor of 0.1 (10%) is achieved.	
DC Diagnostic coverage	≥ 0.99 (99%)	Redundant switch-off path and dynamic monitoring of the contactors	

Result "Reaction"

Table 8-4

PFH_D	SILCL achieved
$7.30 \cdot 10^{-9}$	SILCL 3

© Siemens AG 2023 All rights reserved

Result of the evaluation according to IEC 62061

Table 8-5

Subsystem	PFH_D	SIL achieved
Detection	$1.19 \cdot 10^{-10}$	SILCL 3
Evaluation	$4.00 \cdot 10^{-9}$	SILCL 3
Reaction	$7.30 \cdot 10^{-9}$	SILCL 3
Total	**$1.14 \cdot 10^{-8}$**	**SILCL 3**
	SIL 3	

For the values of the “Detection” and “Evaluation” subsystems, please refer to the enclosed TST project or to \4\.

8.4 Evaluation according to ISO 13849-1

In the following, an evaluation according to ISO 13849-1 is carried out by means of the Safety Evaluation in the TIA Selection Tool Please find the link to the Safety Evaluation in the TIA Selection Tool on the Internet at \7\.

For reasons of better comparability, the results of calculations according to ISO 13849-1 are shown as PFH_D values (conversion according to Annex K, Table K.1).

© Siemens AG 2023 All rights reserved

Evaluation of “Reaction”

The contactor parameters relevant for the evaluation are provided by the manufacturer and specified by the user.

Table 8-6

Parameter	Value	Explanation	Definition
B10 B10 value Contactor	1,000,000	Manufacturer information	SIEMENS AG
Percentage of dangerous failures Contactor	0.73 (73%)	Manufacturer information	
T1 Lifetime	175,000 h (20 years)	Manufacturer information	
Architecture	Category 4	2 channels, 2 components	User
Actuations/ test interval	1/h	Assumption	
CCF measures (points) Susceptibility to common cause failures	≥ 65	Sufficient measures against CCF according to ISO 13849-1 table F.1 have to be provided	
DC Diagnostic coverage	≥ 0.99 (99%)	Redundant switch-off path and dynamic monitoring of the contactors	

Result “Reaction”

Table 8-7

PFH_D	PL achieved
$1.45 \cdot 10^{-9}$	PL e

Result of the evaluation according to ISO 13849-1, ISO 13849-2

Table 8-8

Subsystem	PFH_D	PL achieved
Detection	$9.06 \cdot 10^{-10}$	PL e
Evaluation	$4.00 \cdot 10^{-9}$	PL e
Reaction	$1.45 \cdot 10^{-9}$	PL e
Total	**$6.36 \cdot 10^{-9}$**	**PL e**
	PL e	

For the values of the “Detection” and “Evaluation” subsystems, please refer to the enclosed TST project or to \4\.

© Siemens AG 2023 All rights reserved

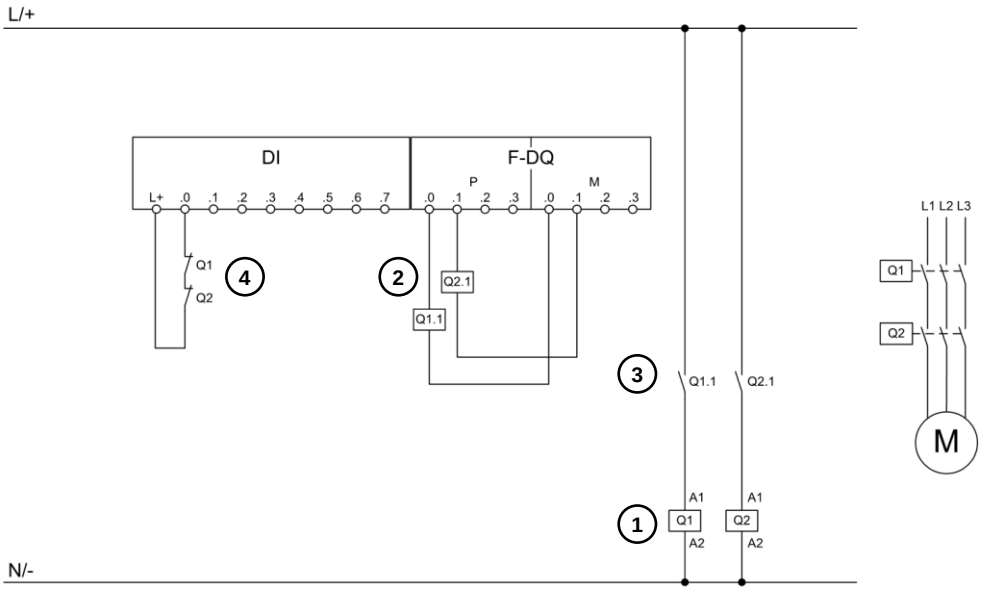
9 Alternative solution using coupling relays

If the power contactors cannot be switched via an F-DQ, coupling relays or contactor relays can be used. This enables the power contactors to be shut down safely. One option for this is shown below.

Interconnection

Per power contactor (1), one coupling relay (2) is used. One F-DQ output switches one coupling relay. The actuator is switched when the contacts (NO) of the coupling relay (3) are closed.

Figure 9-1 Interconnection of the coupling relays



The mirror contacts (4) of the power contactors are read back via the DI.

Evaluation

The coupling relays are part of the safety function and are included in the calculation of the PFHD value. The coupling relays do not need to be monitored since the mirror contacts of the power contactors ensure any errors are detected, at the latest when the device is switched on again. The same level of diagnostics coverage (DC) therefore applies for the coupling relays as for the power contactors.

Dynamic feedback circuit monitoring (by the F-CPU) can be implemented by using the fail-safe FDBACK FB from STEP 7 Safety. This allows PL e/SIL 3 to be achieved in this case, too.

More information

For more information on this topic, see the following FAQ:

https://support.industry.siemens.com/cs/ww/en/view/91689359

© Siemens AG 2023 All rights reserved

10 Appendix

10.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts.

Please send queries to Technical Support via Web form:

support.industry.siemens.com/cs/my/src

© Siemens AG 2023 All rights reserved

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that’s tailored to the customer’s specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

support.industry.siemens.com/cs/ww/en/sc/2067

10.2 Links & Literature

Table 10-1

	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Download page of the entry https://support.industry.siemens.com/cs/ww/en/view/21331098
\3\	SIMATIC Safety – Configuring and Programming https://support.industry.siemens.com/cs/ww/en/view/54110126
\4\	Application example “Emergency stop up to SIL 3 / PL e on a fail-safe S7-1500 controller” https://support.industry.siemens.com/cs/ww/en/view/21064024
\5\	Functional Safety at Siemens http://www.siemens.com/safety-integrated
\6\	SIMATIC ET 200SP Digital output module F-DQ 4x24VDC/2A PM HF – Manual – Readback time dark test https://support.industry.siemens.com/cs/ww/en/view/78645789/55822410379
\7\	Safety Evaluation with TIA Selection Tool http://siemens.com/safety-evaluation/
\8\	LSafe Library for TIA Portal STEP 7 https://support.industry.siemens.com/cs/ww/en/view/109793462

© Siemens AG 2023 All rights reserved

10.3 History

Table 10-2

Version	Date	Modifications
V1.0	02/2005	First version
V2.0	09/2007	Updating the contents regarding: • Hardware and software • Performance data • Screenshots Chapter “Evaluation of the safety function example according to the new standards EN 62061 and EN ISO 13849-1:2006” added
V3.0	06/2016	New version of the application example for TIA Portal V13 SP1
V3.1	01/2017	Update of the results Table 8-7 and Table 8-8 in according to ISO 13849-1:2015
V3.2	11/2018	• Solution with coupling relays (chapter 9) • Upgrade of the project to TIA Portal V15
V4.0	07/2019	Update TIA Portal V15.1
V5.0	03/2021	Migration of Safety Evaluation Tool to Safety Evaluation with TIA Selection Tool
V6.0	01/2023	Update TIA Portal V18 Update LSafe Library

© Siemens AG 2023 All rights reserved