

The Siemens logo is displayed in a white rectangular box with a thin black border. The word "SIEMENS" is written in a bold, teal, sans-serif font. The background of the entire advertisement is a blurred industrial setting with a man in a light blue shirt looking at a tablet. Overlaid on the image are various digital graphics: a clock face, a "24/7" icon with a circular arrow, a "NEWS" header with a user icon, a "Home" button, and a network diagram with three nodes and binary code (0s and 1s) floating around.

SIEMENS

Monitoring a Protective Door up to PL e / SIL 3 with a Fail-Safe S7-1500 Controller

SIMATIC Safety Integrated

<https://support.industry.siemens.com/cs/ww/en/view/21331363>

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>.

Table of Contents

Legal information	2
1 Introduction	4
1.1 Overview.....	4
1.2 Mode of operation	5
1.2.1 Monitoring the position of the protective door	6
1.2.2 Controlling and monitoring the actuators	8
1.3 Components used	9
2 Engineering	10
2.1 Hardware setup	10
2.2 Configuration	11
2.2.1 Configuring F-DI	11
2.2.2 Configuring F-DQ	13
2.3 Commissioning	14
2.3.1 Preparation	14
2.3.2 Loading the project into the CPU	14
2.3.3 Assigning PROFIsafe addresses	16
2.4 Operation	17
3 Valuable Information	19
3.1 Basics	19
3.1.1 Basic terms.....	19
3.1.2 Functional safety	19
3.1.3 Guards.....	20
3.2 Details of the mode of operation	22
3.2.1 Reintegrating passivated channels	22
3.2.2 Data exchange between standard user program and safety program	22
3.3 Evaluating the safety function	23
3.3.1 Standards	23
3.3.2 Safety function.....	23
3.3.3 Evaluation according to ISO 13849-1	24
Evaluation of "Detection"	24
Evaluation of "Evaluation"	25
Evaluation of "Reaction"	25
Result of the evaluation according to ISO 13849-1	26
3.3.4 Evaluation according to IEC 62061	27
Evaluation of "Detection"	27
Evaluation of "Evaluation"	28
Evaluation of "Reaction"	28
Result of the evaluation according to IEC 62061	29
4 Appendix	30
4.1 Service and support	30
4.2 Links and literature	31
4.3 Change documentation	31

1 Introduction

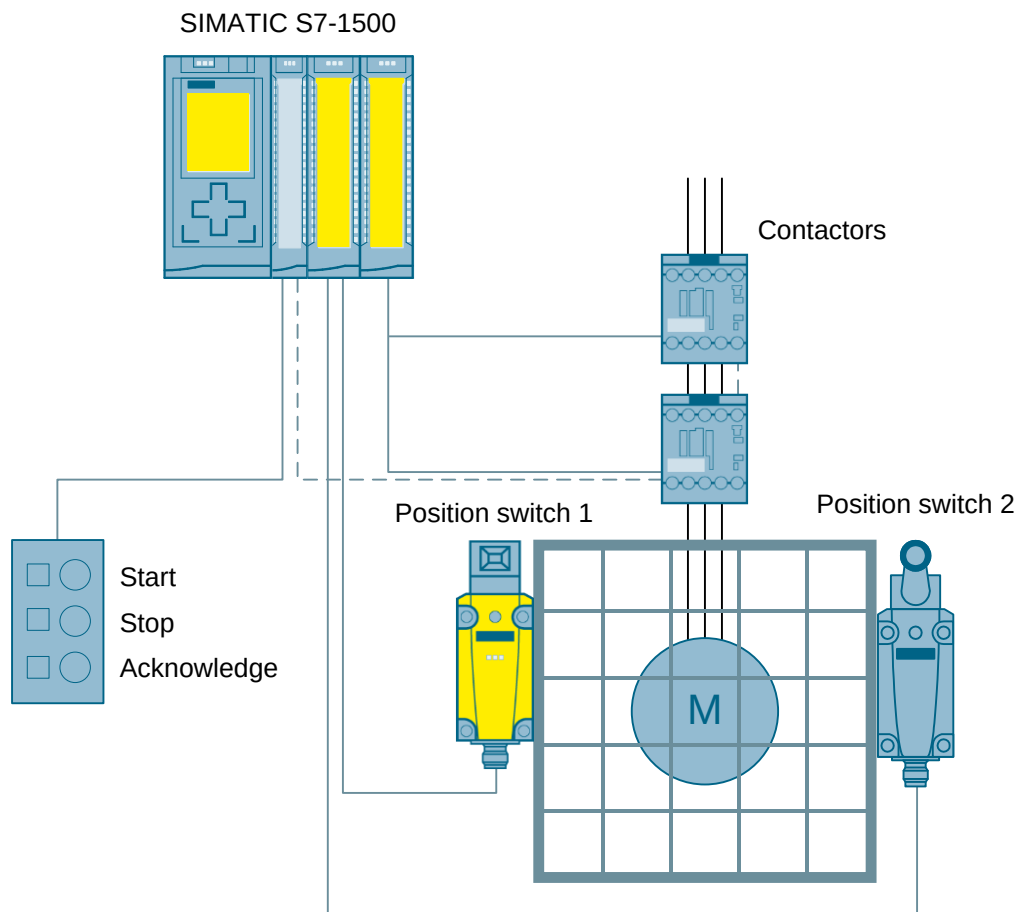
1.1 Overview

To prevent access to the danger range of a machine, a protective door is installed. The machine can only be started, if the protective door is closed. If the protective door is opened during operation or if an error is detected, the machine will be shut down safely.

Monitoring of the protective door position is designed according to EN ISO 13849-1:2015 for requirements up to PL e and according to EN 62061:2005/A2:2015 for requirements up to SIL 3.

The figure below shows a schematic overview of the most important components of the solution:

Figure 1-1: Setup



Advantages

- Minimal wiring by using fail-safe SIMATIC CPU. The significance of this advantage increases with the number of safety functions increasing.
- Programming the safety program with engineering tools integrated in TIA Portal
- Only one fail-safe S7-CPU is required, since standard user program and safety program run on a coexistent basis in the S7-CPU.

Assumed knowledge

Basic knowledge of the following topics is required:

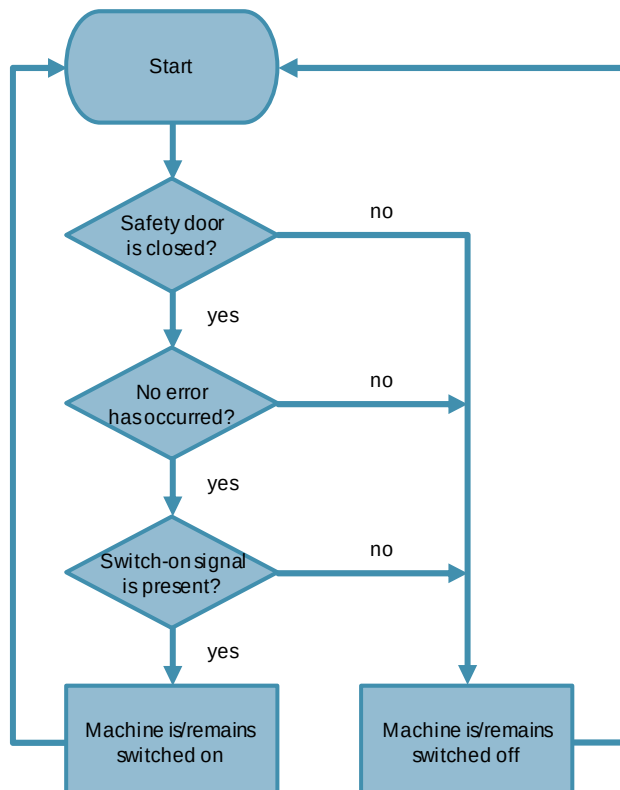
- Functional safety
- STEP 7 programming
- Fail-safe automation systems

1.2 Mode of operation

Process flow

The figure below shows the program flow:

Figure 1-2: Process flow



1.2.1 Monitoring the position of the protective door

To ensure the required safety, the position of the protective door is monitored by two SIRIUS 3SE5 position switches (see [Figure 1-1](#)). If one position switch fails, the second position switch still recognizes that the protective door is opened. The discrepancy monitoring in the controller detects a failure of one position switches and prevents that the system is switched on again until the error is eliminated.

In order to prevent failures of a common cause, position switches with different operating principles are used. In case of the position switch of position 1 the protective door position is detected via a separate actuator which is moved into the position switch when the protective door is being closed. The position switch of position 2 is provided with a swiveling lever which is actuated when the protective door is open.

In both position switches, a NC contact is evaluated each and assigned to the fail-safe digital input module (see [Figure 2-1](#)). The controller detects cross-circuits between the two signals of the position switches.

In the safety program, the "MainSafety" function block calls the "LSafe_FDoor" instruction. This is from the TÜV certified LSafe library.

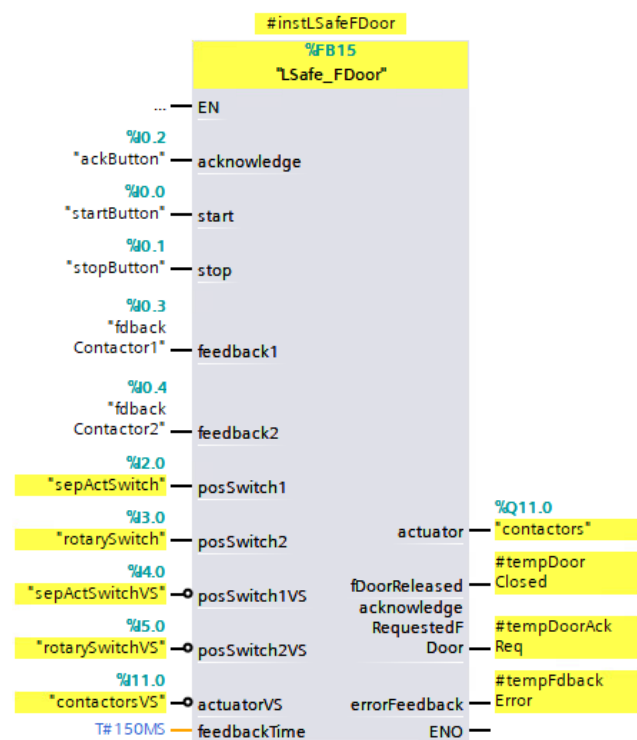
Note

More information about „LSafe_FDoor“ or general information about the “LSafe”-Library can be found on following link:

<https://support.industry.siemens.com/cs/ww/en/view/109793462>

The two inputs "posSwitch1" and "posSwitch2" are monitored with regard to discrepancy to that a wire break is detected immediately and a failure of one of the two position switches (e. g. drop-out of the position switch) is detected when the protective door is opened the next time at the latest.

Figure 1-3: Calling the "LSafe_FDoor" instruction



Note

In this application example it is assumed that the protective door is accessible from behind. For this reason, an manual acknowledgment is required after having opened the protective door before switching the machine on again.

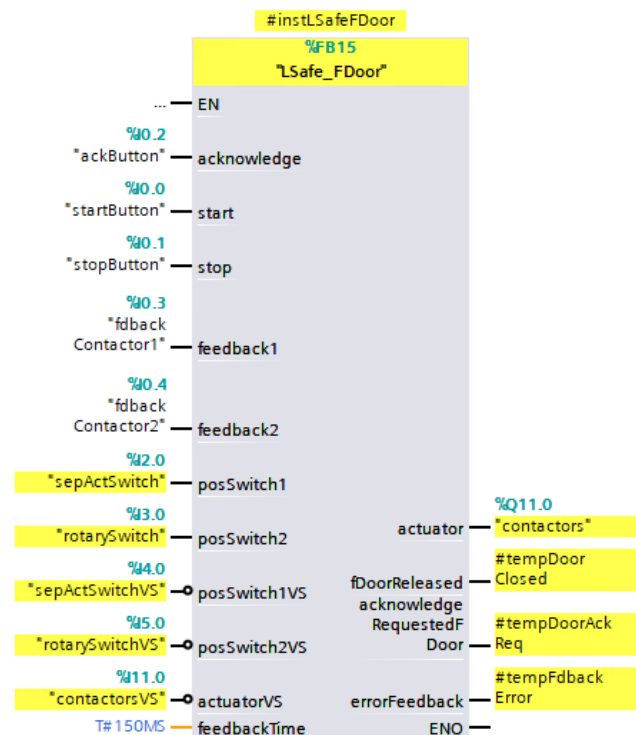
1.2.2 Controlling and monitoring the actuators

To comply with PL e according to ISO 13849-1 or with SIL 3 according to IEC 62061, shutdown is carried out redundantly. For this, two SIRIUS 3RT contactors are used. The fail-safe controller monitors the correct functioning of the contactors via their auxiliary contacts.

If one of the two contactors is welded, the second contactor still ensures safe shutdown. Welding of a contactor will be detected when the next signal change occurs and it will be prevented that the machine is switched on again until the error is eliminated.

The feedback circuit monitoring is also realized via the "LSafe_FDoor" block. If a "1" signal is applied to input "start", output "actuator" will be switched on. The signal on the "feedback1" resp. "feedback2" input has to be switched inversely to output signal "actuator" within the configured "feedbackTime" time. Otherwise, "actuator" will be switched off and an error will be displayed on the "errorFeedback" output. The error has to be acknowledged via the "acknowledge" input.

Figure 1-4: Calling the "LSafe_FDoor" instruction



To switch the machine on, the following conditions must be fulfilled:

- The protective door must first be opened and then closed.
- The operative signal for switching on the machine is set.

1.3 Components used

This application example has been created using the following hardware and software components:

Table 1-1: Components used

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	6ES7954-8LF01-0AA0	SMC 24MB
Digital input/output module	1	6ES7523-1BL00-0AA0	DI 16/DQ 16x24VDC
Fail-safe digital input module	1	6ES7526-1BH00-0AB0	-
Fail-safe digital output module	1	6ES7526-2BF00-0AB0	-
DIN rail S7-1500	1	6ES7590-1AE80-0AA0	Length: 482 mm
Safety position switch with separate actuator	1	3SE5132-0QV20	-
Separate actuator	1	3SE5000-0AV01	Standard actuator
Position switch with swiveling lever	1	3SE5112-0KH01	-
Push button	3	3SU1	2NO, 1NC
Contactor	2	3RT2015-1BB42	NO00, DC24V, 1NC
STEP 7 Professional	1	6ES7822-1AA08-0YA7	V18
STEP 7 Safety Advanced	1	6ES7833-1FA18-0YA5	V18

This application example consists of the following components:

Table 1-2: Example documents and projects

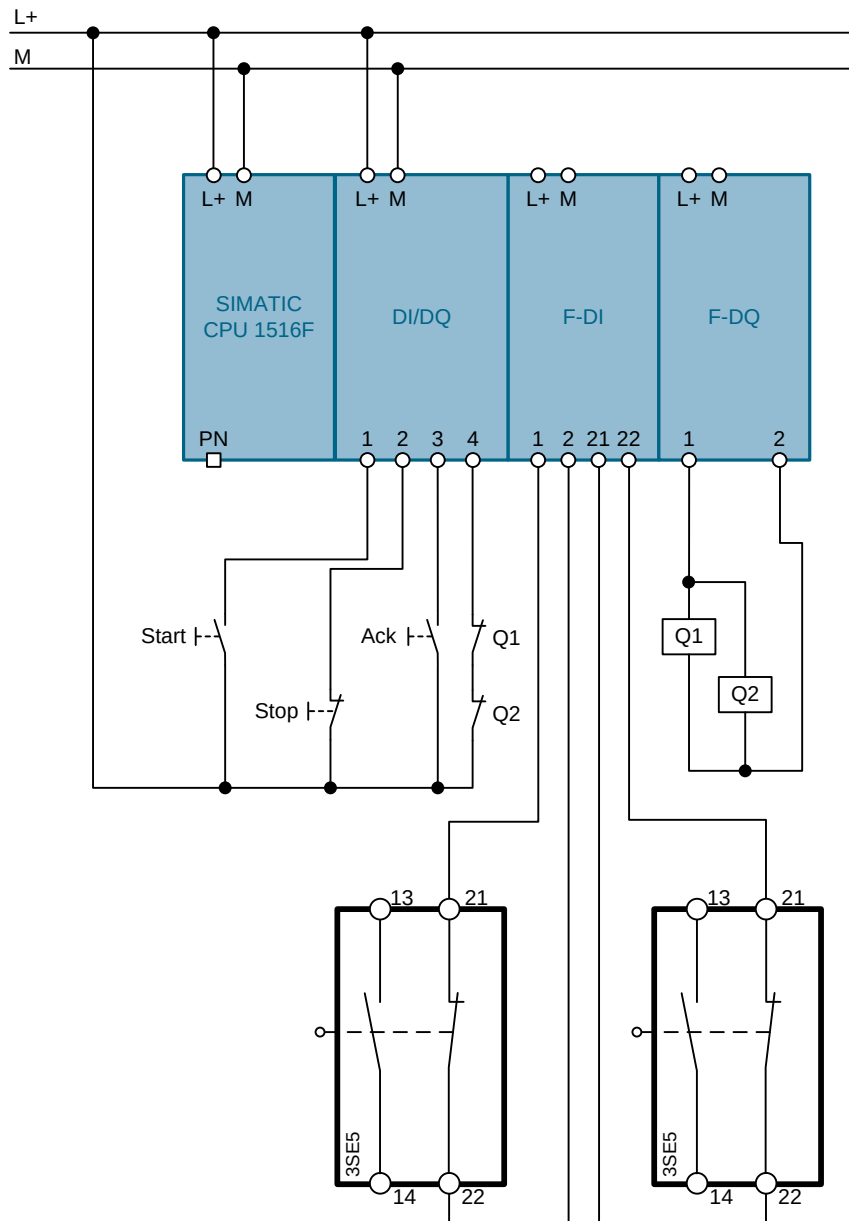
Component	Note
21331363_Protective-Door-SIL3_DOC_V6_en.pdf	This document.
21331363_Protective-Door-SIL3_PROJ_V6.zip	This zip file includes the TIA Portal project.
21331363_Protective-Door-SIL3_SE_TST_V6.tia	Evaluation of the safety functions with the Safety Evaluation in TIA Selection Tool.

2 Engineering

2.1 Hardware setup

The figure below shows the hardware setup of the application.

Figure 2-1: Wiring diagram



2.2 Configuration

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

NOTICE

The settings shown below help to ensure the required safety. If you use different settings, the safety function may be lost.

2.2.1 Configuring F-DI

Short-circuit test

Activate the short circuit tests for the channels 0 and 8.

Figure 2-2: Activating short-circuit tests for sensor supply 0

> > Sensor supply 0

Supplied channels: Channels [0...3]

☒ Short-circuit test activated

Time for short-circuit test: 4.2 ms

Startup time of sensor after short-circuit test: 4.2 ms

Figure 2-3: Activating short-circuit tests for sensor supply 2

> > Sensor supply 2

Supplied channels: Channels [8...11]

☒ Short-circuit test activated

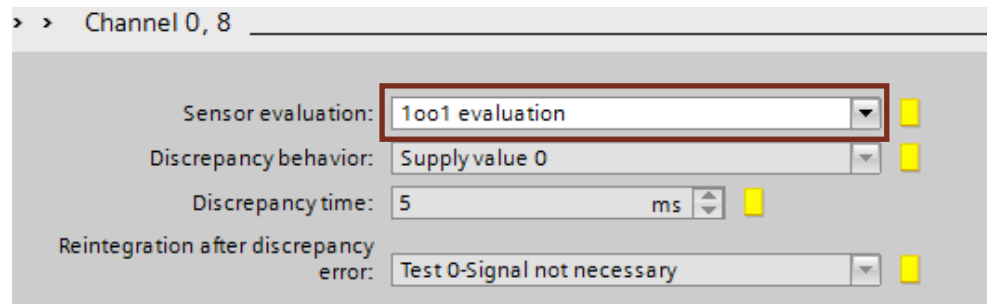
Time for short-circuit test: 4.2 ms

Startup time of sensor after short-circuit test: 4.2 ms

Channel parameters

The monitoring of the protective door position is carried out via channel pair 0, 8. Set the sensor evaluation to "1oo1 evaluation", because the discrepancy evaluation is done in the LSafe_FDoor via SFDOOR function block.

Figure 2-4: Sensor evaluation



Since the two position switches are often placed at different points of the protective door (e. g. hinge switch), they might not trigger at the same time. For this reason, a high discrepancy time is required.

Thus, the discrepancy evaluation via the hardware (1oo2 evaluation) is not suitable, because the hardware allows discrepancies as long as they do not take longer than the set discrepancy time.

In case of discrepancy monitoring via the SFDOOR instruction, which is used internally in LSafe_FDoor, the discrepancy time is infinite, but every discrepancy is detected as an error.

The table below describes differences for discrepancy evaluation:

Table 2-1: Differences for discrepancy evaluation

	Situation	Evaluation via hardware	Evaluation via SFDOOR
1.	Both channels open within the set discrepancy time.	Machine switches off, no error.	Machine switches off, no error.
2.	Channel 1 opens, channel 2 follows after the set discrepancy time has elapsed.	Machine switches off, error is detected and has to be acknowledged.	Machine switches off, no error.
3.	Channel 1 opens, channel 2 remains closed, channel 1 closes within the set discrepancy time.	Machine switches off, no error.	Machine switches off, error is detected. The instruction remains in the error state until the operator opens and closes the protective door during which a valid switching sequence is detected.

Note

It is not possible to evaluate discrepancies both via the hardware and via the function block, because with the "1oo2 evaluation" being activated, it is not allowed to access the individual channels in the program.

2.2.2 Configuring F-DQ

Channel parameters

Activate the wire break detection and the light test.

Figure 2-5: Channel parameters of contactors

The screenshot displays the configuration interface for Channel 0, organized into three main sections: Diagnostics, Output parameters, and Monitoring parameters. Each section contains various settings, many of which are accompanied by a yellow status indicator (a small yellow square with a red exclamation mark) and a blue circular icon with a red arrow pointing to the right.

- Diagnostics:** Contains a checkbox labeled "Wire break" which is checked. A yellow status indicator and a blue circular icon are present to the right of this checkbox.
- Output parameters:** Contains a checkbox labeled "Channel activated" which is checked. Below it, a dropdown menu for "Channel failure acknowledge" is set to "Manual". A yellow status indicator is present to the right of the dropdown.
- Monitoring parameters:** Contains two time settings: "Max. readback time dark test" set to "1.0 ms" and "Max. readback time switch on test" set to "0.8 ms". Both have yellow status indicators. Between these two settings is a checkbox labeled "Disable dark test for 48 hours" which is unchecked. At the bottom of this section is a checkbox labeled "Activated light test" which is checked. A yellow status indicator and a blue circular icon are present to the right of this checkbox.

2.3 Commissioning

2.3.1 Preparation

1. Download the project file "21331363_Protective-Door-SIL3_PROJ_V6.zip":
<https://support.industry.siemens.com/cs/ww/en/view/21331363>
2. Save the ZIP file in any directory on your computer and extract it.
3. Set the IP address of the PG/PC in a way so that the PC is located in the same subnet as the CPU.
4. Use an Ethernet cable to connect the PC with the Ethernet interface of CPU S7-1516F.

For this application example, the following IP address has been used:

CPU S7-1516F

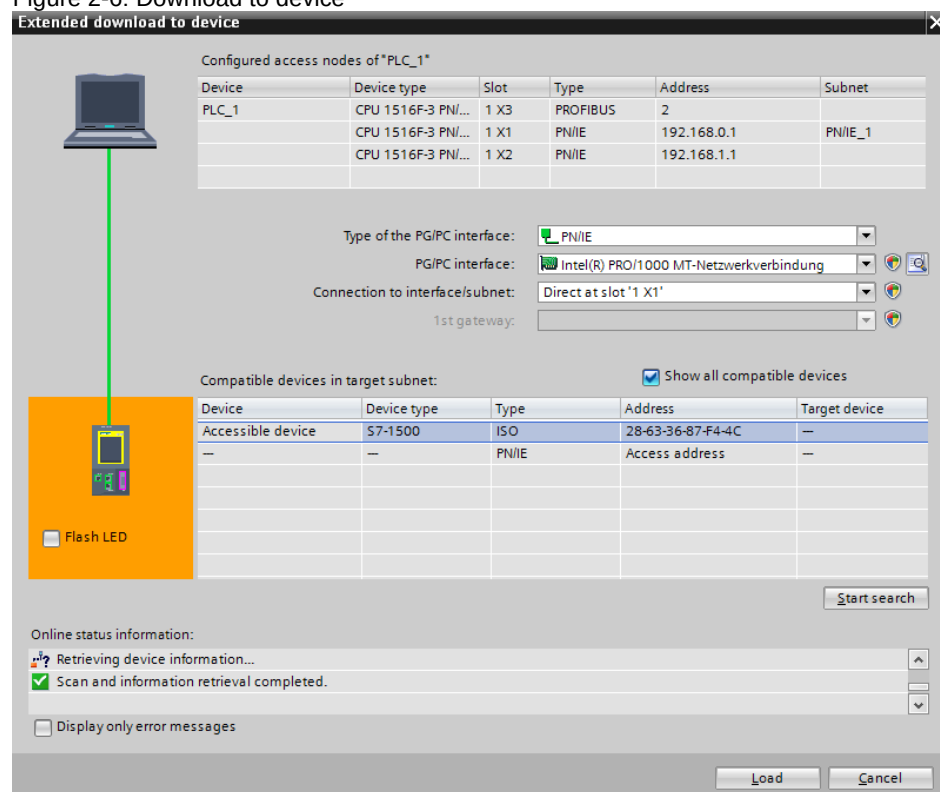
IP address: 192.168.0.30

Subnet mask: 255.255.255.0

2.3.2 Loading the project into the CPU

1. Open TIA Portal.
2. Go to the project view.
3. In the menu bar in TIA Portal, click "Project > Open".
4. Click on "Browse" and open the extracted project.
5. Set the CPU S7-1516F to STOP.
6. In the Project tree, right-click "PLC_1 [CPU1516F-3 PN/DP]" and then select "Download to device > Hardware and software (only changes)".
7. Select the corresponding interface and click "Start search".

Figure 2-6: Download to device



8. Select the CPU based on the MAC address and then click "Load".

Note

The IP address and the device name are automatically assigned when downloading the project to the CPU.

9. Confirm the dialog by clicking "Load".
10. Click "Finish" when loading is complete.

2.3.3 Assigning PROFIsafe addresses

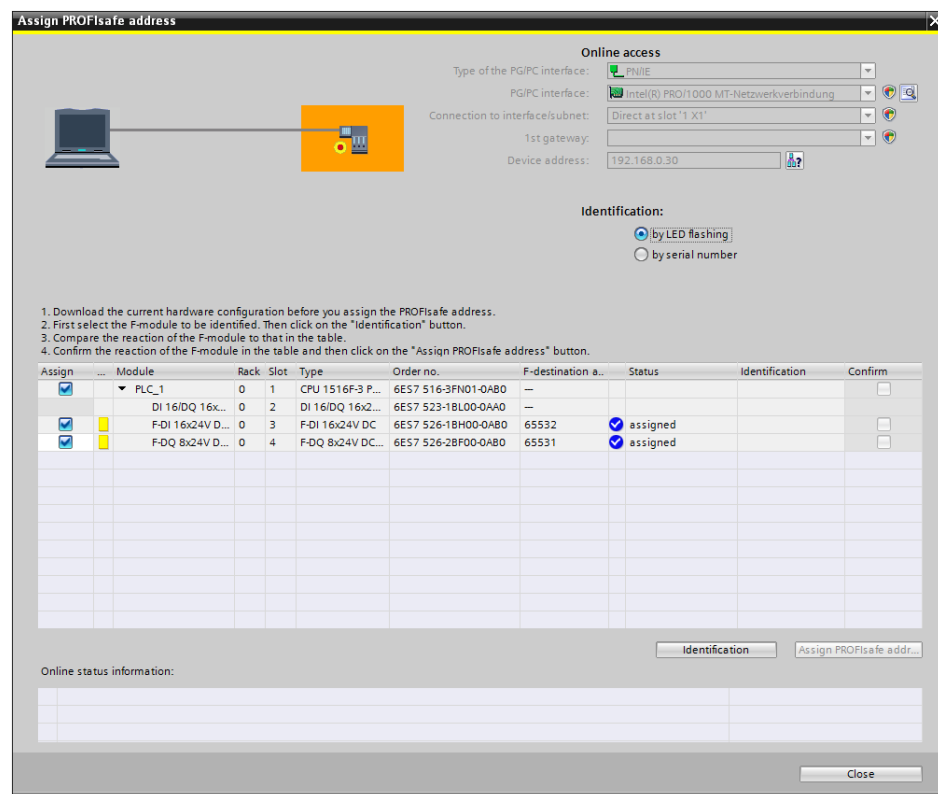
In order to establish a secure communication between the controller and the fail-safe modules, you must assign PROFIsafe addresses to the modules.

Note

As the PROFIsafe address is saved in the electronic coding element, the following steps are only required if the coding element has not already been assigned a different PROFIsafe address.

1. In the Project tree, open "Devices & networks".
2. Right-click the F-CPU and select "Assign PROFIsafe address".
3. Check the check box of the first fail-safe module and click the "Identification" button.
4. When the LEDs of the F-DI flash green simultaneously every second, check the "Confirm" check box.
5. Then click the "Assign PROFIsafe address" button and confirm the dialog by clicking "Yes".

Figure 2-7: Assigning PROFIsafe addresses



6. Repeat the steps 1 to 5 for the other failsafe modules.
7. Close the window.

Note

All red LEDs of the fail-safe modules go off after assigning the PROFIsafe addresses. If this is not the case, check the wiring.

8. Now, set the CPU S7-1516F to "RUN".

2.4 Operation

Starting the machine

Table 2-2: Starting the machine

No.	Action	Remark
1.	Open and Close the protective door.	-
2.	Press the acknowledgement button.	-
3.	Press the start button.	The machine is starting.

Acknowledging discrepancy faults

If the function block used for monitoring the protective door position detects a discrepancy fault between the two position switches (e. g. due to bouncing of a contact or in case of a wire break in a channel), the machine will be switched off immediately and a restart will be prevented. Proceed as follows to acknowledge a discrepancy fault after it has been eliminated.

Table 2-3: Acknowledging discrepancy fault

No.	Action	Remark
1.	Open the protective door so that both position switches are actuated.	Both channels give a "0" signal.
2.	Open and Close the protective door.	Both channels give a "1" signal.
3.	Press the acknowledgement button.	
4.	Press the start button.	The machine is starting.

Acknowledging other faults of the safety function

If another fault occurs in the safety function, the machine will be switched off immediately and a restart will be prevented. Proceed as follows to acknowledge the fault.

Possible fault that have to be acknowledged this way:

- Cross-circuit between the two channels of the position switches
- External voltage applied to the fail-safe outputs
- Removing a fail-safe module
- Welding of a contactor

Table 2-4: Acknowledging other faults of the safety function

No.	Action	Remark
1.	Check the LEDs of the fail-safe modules. If a red LED lights, a fault has been detected in the hardware. Search for the fault in the online diagnostic in TIA Portal. If all LEDs light up in green, a fault has been detected by the safety program. Watch the tag table to find the fault.	-
2.	Eliminate the fault.	-
3.	Open and Close the protective door.	-
4.	Press the acknowledgement button.	Passivated channels of the fail-safe modules are reintegrated. Detected faults of the safety program are acknowledged.
5.	Press the start button.	The machine is starting.

3 Valuable Information

3.1 Basics

3.1.1 Basic terms

Cross-circuit

The cross-circuit detection is a diagnostic function of an evaluation device, as a result of which short-circuits or cross-circuits are detected between the two input channels (sensor circuits).

A cross-circuit can occur, for example, if a light plastic-sheathed cable is crushed. Without cross-circuit detection this would lead to, for example, a 2-channel emergency stop circuit not to trigger a shut-down even if only one NC contact is faulty (second error).

Feedback circuit

A feedback circuit monitors controlled actuators (e. g. relay or 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.

Positive opening operation

Positive opening switches are designed in a way that the operation of the switch inevitably leads to an opening of the contacts. Welded contacts are forced open through the operation (EN 60947-5-1).

Positively driven contacts

For a component with positively driven contacts it is guaranteed that the make and break contacts are never closed at the same time (EN 60947-5-1).

3.1.2 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, safety-relevant parts of the protective equipment and control devices must function correctly and 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 ISO 13849-1: "Performance Level" (PL)
- In IEC 62061: "Safety integrity level" (SIL)

You can find further information on functional safety here:

www.siemens.com/safety-integrated

3.1.3 Guards

The solution mostly used with regard to plants and machines is the safeguarding of danger areas by means of mechanical guards or access panels. The goal is to monitor unauthorized access to plant areas and to prevent dangerous machine functions, if the guard is not closed. You can find principles for the design and selection of interlocking devices associated with guards in EN ISO 14119.

Guard monitoring can be performed both with mechanical position or safety switches and with non-contact safety switches based on a magnetic principle or RFID.

Major requirements for position switches

The following list of requirements for position switches is not exhaustive.

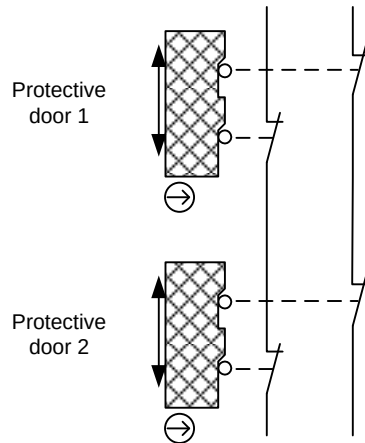
- Position switches have to be arranged in such a way that they cannot be damaged when they are approached or passed. This is why position switches must not be used as a mechanical stop.
- Only sensors with positive opening contacts may be used as sensors.
- Sensor cables must be laid with appropriate protection.
- Evaluation shall always be made via the NC contacts or via a combination of the NC and NO contacts of the position switches.
- Automatic restart of the machine after closing the protective door is only allowed if it can be excluded that a person is in the danger area (e. g. near access panels or safety hoods) when the protective door is closed.
- In order to prevent common cause failures (CCF), it is recommended to use position switches with different operating principles (e. g. with separate actuator and swiveling lever).

Series connection of position switches

Position switches up to PL e (according to ISO 13849-1) or SIL 2 (according to IEC 62061) may only be connected in series if regular simultaneous opening of several protective doors can be excluded (as otherwise errors cannot be detected).

Series connection complying with PL e (according to ISO 13849-1) or with SIL 3 (according to IEC 62061) is not possible.

Figure 3-1: Series connection of position switches



Guard locking of protective doors

In combination with protective door monitoring, very often a guard locking of the protective door is implemented as well. Interlocking devices with guard locking secure danger areas against unauthorized access. In most cases, this is due to two reasons:

1. Protection of people against run-down dangerous machine movements, high temperatures etc. by making sure that the danger area can be accessed only after the dangerous machine movement has been stopped.
2. Guard locking may be reasonable for reasons of process safety. This is the case if no danger exists after opening the guard, but results in damaging of the machine or workpiece. In this case, the machine first will be moved to a proper stop position before access is granted.

Note

You can find an application example regarding the safety function "Guard locking for protective doors" here:

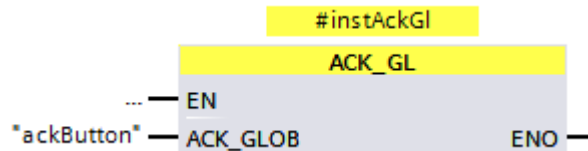
<https://support.industry.siemens.com/cs/ww/en/view/21063946>

3.2 Details of the mode of operation

3.2.1 Reintegrating passivated channels

The "ACK_GL" instruction contained in STEP 7 Safety generates an acknowledgment for the simultaneous reintegration of all F IOs/channels of the F periphery of an F runtime group after communication errors or F IO/channel errors.

Figure 3-2: Calling the ACK_GL instruction



Examples of events that cause passivation:

- Wire break on the F-DQ
- Missing power supply on the F-DI

Note

If an error occurs on the hardware, e. g. detected wire break, it may take – depending on the type of error – up to a couple of minutes until the module detects that the error has been eliminated. Only then an acknowledgment will have an effect.

3.2.2 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"
- "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 the manual "SIMATIC Safety – Configuring and Programming":

<https://support.industry.siemens.com/cs/ww/en/view/54110126>

3.3 Evaluating the safety function

3.3.1 Standards

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

Table 3-1: Standards

Version	Mentioned in this document
EN ISO 13849-1:2015	ISO 13849-1
EN ISO 13849-2:2012	ISO 13849-2
EN 62061:2005/A2:2015	IEC 62061
EN ISO 14119:2013	ISO 14119

3.3.2 Safety function

In this application example, the following safety function is implemented:

Table 3-2: Safety function

Safety function	Description
SF1	If the protective door is opened, the machine must be switched off safely.

Below, the SF1 safety function is evaluated according to the standards ISO 13849-1 and IEC 62061.

The supplied TST project contains the evaluation of the safety function in the Safety Evaluation in TIA Selection Tool.

3.3.3 Evaluation according to ISO 13849-1

Below, the evaluation according to EN ISO 13849-1 is carried out with the Safety Evaluation in TIA Selection Tool:

<http://siemens.com/safety-evaluation>

Evaluation of "Detection"

The position of the protective door is monitored by means of two position switches which might result in a single fault not leading to the loss of the safety function and being detected immediately. For this reason, the subsystem meets the requirements of Category 4.

The safety-relevant parameters of the component are provided by the manufacturer. The resulting probability of a dangerous failure PFH_D and the PL depend on the actual operating cycles and the type of installation of the component which have to be completed by the user.

Table 3-3: Parameters of subsystem "Detection"

Parameter	Value	Explanation	Definition
B10 Switching cycles		Manufacturer information	SIEMENS AG
Safety position switch with separate actuator	1,000,000		
Standard position switch	10,000,000		
Percentage of dangerous failures	0.20 (20 %)	Manufacturer information	
T1 Lifetime	175,000 h (20 years)	Manufacturer information	
Architecture	Category 4	2 channels, 2 components	User
Actuations/ test interval	3/day	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 taken	
DC Diagnostic coverage	≥ 0.99 (99 %)	Cross-comparison of input signals, detection of static failures and short-circuits	

Table 3-4: Results for subsystem "Detection"

PFH_D	PL achieved
$9.06 \cdot 10^{-10}$	PL e

Evaluation of "Evaluation"

The subsystem "Evaluation" comprises the fail-safe controller, the F-DI module for monitoring the position switches and the F-DQ module for controlling the contactors.

Table 3-5: Calculation for subsystem "Evaluation"

Component	PFH _D	PL	Definition
CPU 1516F-3PN/DP incl. PROFI-safe	$2.00 \cdot 10^{-9}$	PL e	SIEMENS AG
ET 200MP F-DI	$1.00 \cdot 10^{-9}$	PL e	
ET 200MP F-DQ	$2.00 \cdot 10^{-9}$	PL e	
Total	$5.00 \cdot 10^{-9}$	PL e	

Evaluation of "Reaction"

The subsystem "Reaction" consists of two actuators which might result in a single fault not leading to the loss of the safety function and being detected before the safety function is requested for the next time. For this reason, the subsystem meets the requirements of Category 4.

The safety-relevant parameters of the component are provided by the manufacturer. The resulting probability of a dangerous failure PFH_D and the SILCL depend on the actual operating cycles and the type of installation of the component which have to be completed by the user.

Table 3-6: Parameters of subsystem "Reaction"

Parameter	Value	Explanation	Definition
B10 Switching cycles	1,000,000	Manufacturer information	SIEMENS AG
Percentage of dangerous failures	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	3/day	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 taken	
DC Diagnostic coverage	≥ 0.99 (99 %)	Redundant switch-off path with direct monitoring of the driving elements	

3 Valuable Information

Table 3-7: Results for subsystem "Reaction"

PFH _D	PL achieved
$9.06 \cdot 10^{-10}$	PL e

Result of the evaluation according to ISO 13849-1

Table 3-8: Result of the evaluation according to ISO 13849-1

Subsystem	PFH _D	PL achieved
Detection	$9.06 \cdot 10^{-10}$	PL e
Evaluation	$5.00 \cdot 10^{-9}$	PL e
Reaction	$9.06 \cdot 10^{-10}$	PL e
Total	$6.81 \cdot 10^{-9}$	PL e
	PL e	

3.3.4 Evaluation according to IEC 62061

In the following, the evaluation according to IEC 62061 is carried out by means of the Safety Evaluation in TIA Selection Tool:

<http://siemens.com/safety-evaluation>

Evaluation of "Detection"

The position of the protective door is monitored by means of two position switches which are monitored with regard to discrepancies and cross-circuits. This is a basic subsystem architecture D according to IEC 62061: Single fault tolerance with diagnostic function.

The safety-relevant parameters of the component are provided by the manufacturer. The resulting probability of a dangerous failure PFH_D and the SILCL depend on the actual operating cycles and the type of installation of the components.

Table 3-9: Parameters of subsystem "Detection"

Parameter	Value	Explanation	Definition
B10 Switching cycles		Manufacturer information	SIEMENS AG
Safety position switch with separate actuator	1,000,000		
Standard position switch	10,000,000		
Percentage of dangerous failures	0.20 (20 %)	Manufacturer information	User
T1 Lifetime	175,000 h (20 years)	Manufacturer information	
Subsystem architecture	D	2 channels, 2 components: Single fault tolerance with diagnostic function	
Actuations/ test interval	3/day	Assumption	
CCF factor	10 %	The installation must achieve a CCF factor of 0.1 (10 %)	
DC Diagnostic coverage	≥ 0.99 (99 %)	Cross-comparison of input signals, detection of static failures and short-circuits	

Table 3-10: Results for subsystem "Detection"

PFH_D	SILCL achieved
$1.37 \cdot 10^{-10}$	SILCL 3

Evaluation of "Evaluation"

The subsystem "Evaluation" comprises the fail-safe controller, the F-DI module for monitoring the position switches and the F-DQ module for controlling the contactors.

Table 3-11: Calculation for subsystem "Evaluation"

Component	PFH _D	SILCL	Definition
CPU 1516F-3PN/DP incl. PROFIsafe	$2.00 \cdot 10^{-9}$	SILCL 3	SIEMENS AG
ET 200MP F-DI	$1.00 \cdot 10^{-9}$	SILCL 3	
ET 200MP F-DQ	$2.00 \cdot 10^{-9}$	SILCL 3	
Total	$5.00 \cdot 10^{-9}$	SILCL 3	

Evaluation of "Reaction"

The machine is switched-off by two SIRIUS 3RT contactors. The controller monitors the correct functioning of the contactors by means of positively driven auxiliary contacts in the contactors (NC contacts). This is a basic subsystem architecture D according to IEC 62061: Single fault tolerance with diagnostic function.

The safety-relevant parameters of the component are provided by the manufacturer. The resulting probability of a dangerous failure PFH_D and the SILCL depend on the actual operating cycles and the type of installation of the components.

Table 3-12: Parameters of subsystem "Reaction"

Parameter	Value	Explanation	Definition
B10 Switching cycles	1,000,000	Manufacturer information	SIEMENS AG
Percentage of dangerous failures	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	3/day	Assumption	
CCF factor	10 %	The installation must achieve a CCF factor of 0.1 (10 %)	
DC Diagnostic coverage	≥ 0.99 (99 %)	Redundant switch-off path with direct monitoring of the driving elements	

Table 3-13: Results for subsystem "Reaction"

PFH _D	SILCL achieved
$9.12 \cdot 10^{-10}$	SILCL 3

Result of the evaluation according to IEC 62061

Table 3-14: Result of the evaluation according to IEC 62061

Subsystem	PFH _D	SIL achieved
Detection	$1.37 \cdot 10^{-10}$	SILCL 3
Evaluation	$5.00 \cdot 10^{-9}$	SILCL 3
Reaction	$9.12 \cdot 10^{-10}$	SILCL 3
Total	$6.05 \cdot 10^{-9}$	SILCL 3
	SIL 3	

4 Appendix

4.1 Service and support

Industry Online Support

Do you have any questions or need support?

Siemens Industry Online Support offers access to our entire service and support know-how as well as to our services.

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

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

<https://support.industry.siemens.com>

Technical Support

Siemens Industry's Technical Support offers quick and competent support regarding all technical queries with numerous tailor-made offers – from basic support to individual support contracts.

Please address your requests to the Technical Support via the web form:

siemens.com/SupportRequest

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 service offer comprises, among other things, the following services:

- Product Training
- Plant Data Services
- Spare Parts Services
- Repair Services
- Field & Maintenance Services
- Retrofit & Modernization Services
- Service Programs and Agreements

Detailed information on our service offer is available in the Service Catalog:

<https://support.industry.siemens.com/cs/sc>

Industry Online Support app

Thanks to the "Siemens Industry Online Support" app, you will get optimum support even when you are on the move. The app is available for iOS and Android.

<https://support.industry.siemens.com/cs/ww/en/sc/2067>

4.2 Links and literature

Table 4-1: Links and literature

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to this entry https://support.industry.siemens.com/cs/ww/en/view/21331363
\3\	Functional Safety at Siemens http://www.siemens.com/safety-integrated
\4\	Safety Evaluation with TIA Selection Tool http://siemens.com/safety-evaluation
\5\	SIMATIC Safety – Configuring and Programming https://support.industry.siemens.com/cs/ww/en/view/54110126
\6\	SIRIUS position switch product website http://www.siemens.com/sirius-detecting
\7\	Application example "Protective door with spring-loaded engagement" https://support.industry.siemens.com/cs/ww/en/view/21063946
\8\	LSafe Library for TIA Portal STEP 7 https://support.industry.siemens.com/cs/ww/en/view/109793462

4.3 Change documentation

Table 4-2: Change documentation

Version	Date	Modifications
V1.0	02/2005	First version
V2.0	11/2007	Updating the contents regarding: • Hardware and software • Performance data • Screenshots Evaluation of the application according to the new standards ISO 13849-1 and IEC 62061
V3.0	02/2017	• Migration to TIA Portal V14 • Replacing components by SIMATIC S7-1500 with central modules
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 blocks