Protective Door with Spring-loaded Interlocking with an S7-1500

SIMATIC Safety Integrated

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

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/industrialsecurity.

Table of Contents

1 Introduction

1.1 Overview

To prevent access to the hazard zone of a machine during operation, a protective door is installed and the position of the protective door is monitored. Since overrunning machine components may cause hazards, the protective door is interlocked and can only be opened after the machine is in standstill. It shall only be possible to start the machine after the protective door has been closed and locked. In the case of a fault, the machine shall be shut down safely.

The monitoring of the position of the protective door is designed up to PL e in accordance with EN ISO 13849-1:2015 and SIL 3 in accordance with EN 62061:2005/A2:2015.

The interlocking function of the protective door is designed up to PL d in accordance with EN ISO 13849-1:2015 and SIL 2 in accordance with EN 62061:2005/A2:2015.

Table 1-1: Safety functions

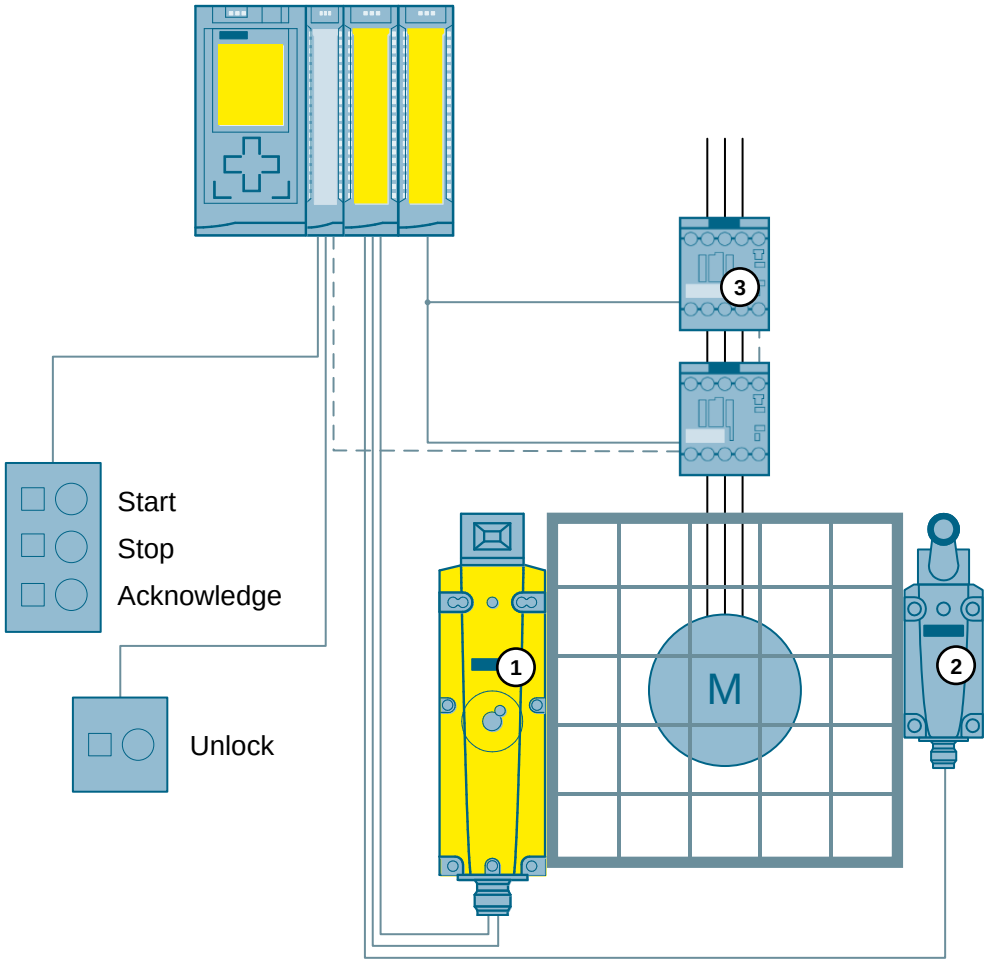
Safety function	Description	Requirement
SF1	If the protective door is opened, the machine is switched off safely.	PL e or SIL 3
SF2	The protective door remains interlocked until the machine has stopped.	PL d or SIL 2

Note

According to the standard EN ISO 14119 "Safety of machinery – Interlocking devices associated with guards – Principles for design and selection" the PL_r or required SIL of the interlocking function is usually lower than that of the position monitoring of the protective door. Based on the risk assessment, the interlocking function in this example is designed up to PL d or SIL 2. The evaluation of the safety function is performed in chapter 3.

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

Figure 1-1: Overview of the hardware configuration



Advantages

- Minimal wiring expenses by using fail-safe S7-CPU. The significance of this advantage increases with the increase in realized safety functions.
- 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

The following knowledge is assumed:

- Basics of functional safety
- Basic knowledge of STEP 7 programming
- Basic knowledge of fail-safe automation systems

1.2 Mode of operation

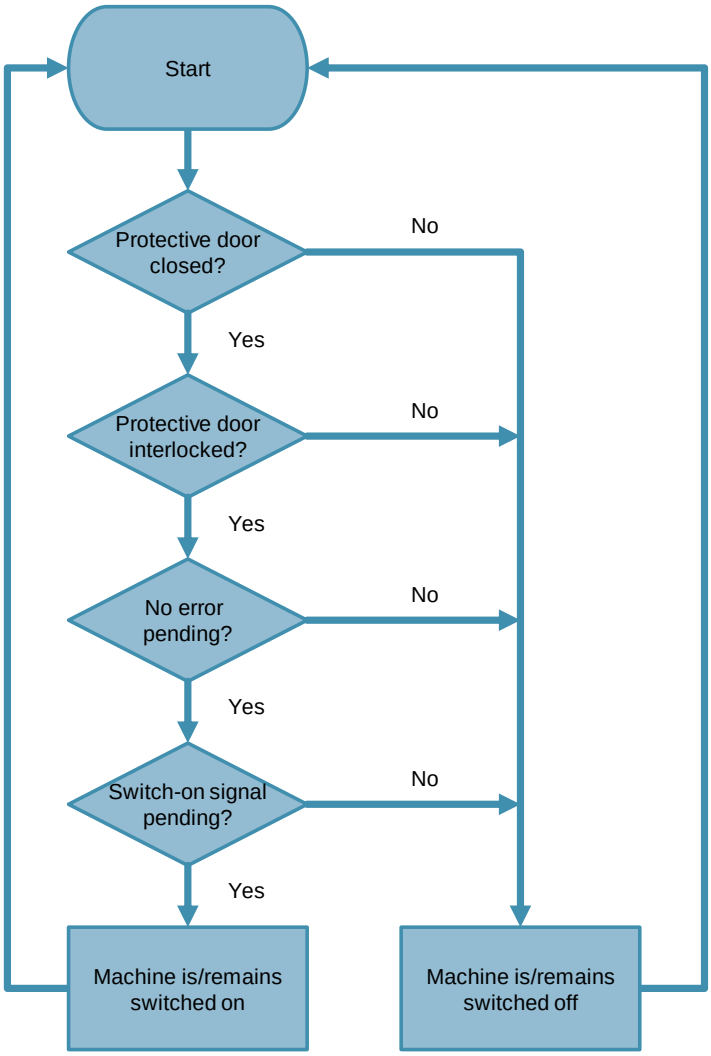
In this application example two safety functions are discussed:

- Monitoring the position of the protective door
- Interlocking function of the protective door

Both safety functions are realized in the function block ProtDoorWithInterlocking of the safety program.

Flowchart

Figure 1-2: Flowchart

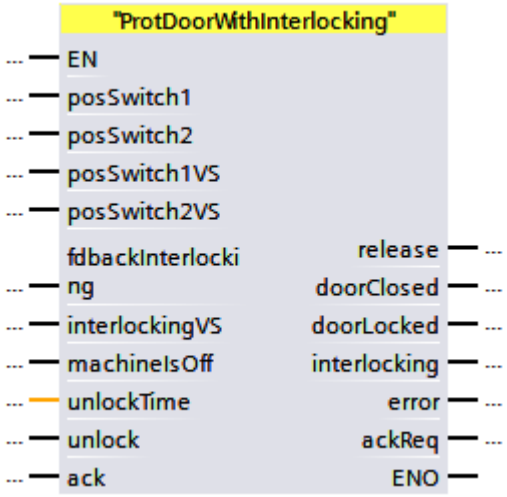


1.2.1 Parameters of the function block ProtDoorWithInterlocking

Overview

Function block ProtDoorWithInterlocking realizes monitoring of the position of the protective door and unlocking and monitoring of the interlocking.

Figure 1-3: Call of the function block ProtDoorWithInterlocking



Input parameters

Table 1-2: Input parameters of the function block ProtDoorWithInterlocking

Formal parameter	Data type	Meaning
posSwitch1	BOOL	Signal of position switch 1. "1" = door is closed.
posSwitch2	BOOL	Signal of position switch 2. "1" = door is closed.
posSwitch1VS	BOOL	Value status of the channel at which position switch 1 is connected.
posSwitch2VS	BOOL	Value status of the channel at which position switch 2 is connected.
fdbackInterlocking	BOOL	Status signal of the interlocking. "1" = protective door is locked.
interlockingVS	BOOL	Value status of the channel at which the solenoid for unlocking the protective door is connected.
machineIsOff	BOOL	Status signal of the actuators. "1" = machine is switched off. With a rising edge the unlock time starts.
unlockTime	TIME	Time the machine requires between switching-off and safe standstill before the protective door can be unlocked.
unlock	BOOL	Command for unlocking the door. Only possible if the machine has been switched off. Does not cause the machine to switch off.
ack	BOOL	Command for acknowledging detected errors and reintegration of passivated channels.

Output parameters

Table 1-3: Output parameters of the function block ProtDoorWithInterlocking

Formal parameter	Data type	Meaning
release	BOOL	Release signal of the safety function (door is closed and locked).
doorClosed	BOOL	Protective door is closed.
doorLocked	BOOL	Protective door is locked.
interlocking	BOOL	Output signal for unlocking the protective door.
error	BOOL	An error occurred.
ackReq	BOOL	User acknowledgment is required.

1.2.2 Monitoring the position of the protective door

Hardware

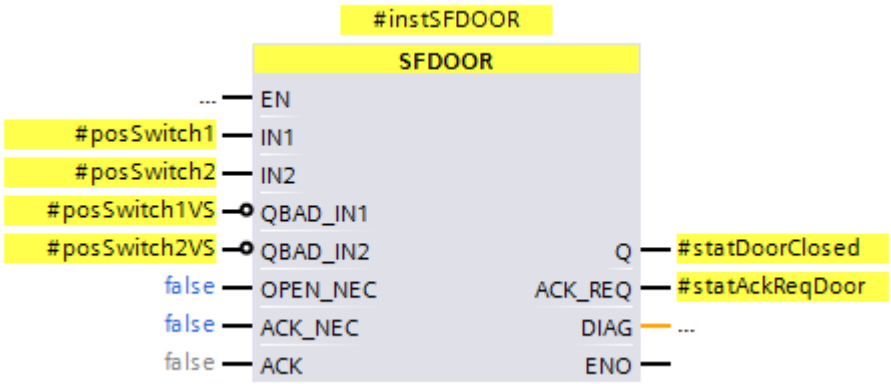
Monitoring the position of the protective door (SF1) is performed via two position switches SIRIUS 3SE5 (Figure 1-1, positions 1 & 2) to implement the demanded safety. If one position switch fails, an opened protective door is still detected by the second position switch. A failed position switch is detected by the discrepancy monitoring in the controller, and switching it back on is prevented until the failure has been removed.

Position switches with different functions are used to counter common cause failures. For position switch 1, the position of the protective door is detected by means of a separate actuator that engages the position switch when closing the position switch. Position switch 2 has a swiveling lever that is actuated when the protective door is open. In both position switches, one NC contact each is evaluated and connected to the fail-safe inputs of the ET 200SP (see Figure 2-1: Wiring diagram). Cross-circuits between the two signals of the position switches are detected by the failsafe input module.

Software

The function block ProtDoorWithInterlocking uses the SFDOOR instruction that is included in STEP 7 Safety. Both inputs IN1 and IN2 are monitored for discrepancy so wire break is detected immediately, and a failure of both position switches (e.g. a dropped off position switch) is detected at the latest during the next opening of the protective door.

Figure 1-4: Call of SFDOOR instruction



In this application example, acknowledgement after opening the protective door is not necessary, since the protective door can only be opened after the machine has been switched off.

1.2.3 Interlocking function of the protective door

Mode of operation of the SIRIUS 3SE5 position switch with interlocking

The position switch with position 1 (see Figure 1-1) is a position switch with interlocking. Apart from monitoring the position of the protective door, the door can be kept closed during operation and hence entry into the hazard zone be prevented (SF2).

An actuator installed at the protective door engages a form-fit mounted safety position switch with interlocking. The SIRIUS 3SE5 position switch with interlocking used here uses a spring-loaded interlocking device and works according to the closed-current principle. That is, in the zero potential state, the door is interlocked and only disengaged after voltage is applied.

If the door is closed and no voltage is applied, a locking mechanism engages the separate actuator and hence prevents the door from being opened. When applying voltage, the locking mechanism disengages the separate actuator by means of a magnet, and the interlocking is unlocked.

Figure 1-5: SIRIUS 3SE5 Position switch with interlocking

The SIRIUS 3SE5 position switches are equipped with a mechanical fail-locking system that prevents the door from interlocking unless it is closed.

Controlling/Monitoring of the interlocking

Engaging and disengaging the interlocking is controlled via the fail-safe output module. An NC contact in the position switch is used by the controller for monitoring the position of the locking mechanism and comparing it with the control command. The normally closed contact is closed if the protective door is interlocked.

Software

To be able to switch on the machine, the protective door must be closed and locked. Unlocking the protective door is only possible at the end of a configured period of time, after the machine has been switched off, so the operator is protected against hazardous machine overrun motion.

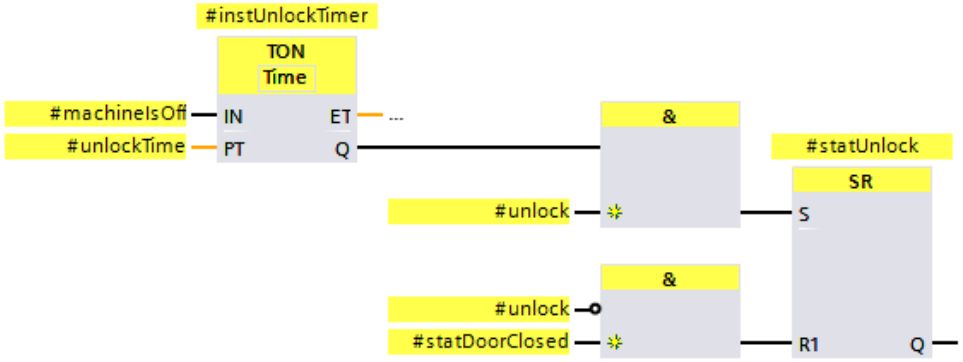
The door is unlocked under the following conditions:

- The actuators switched off ("1” signal at #machineIsOff).
- The configured time after switching off the actuators has elapsed.
- The command for unlocking is pending ("1” signal at #unlock).

The door is locked again under the following conditions:

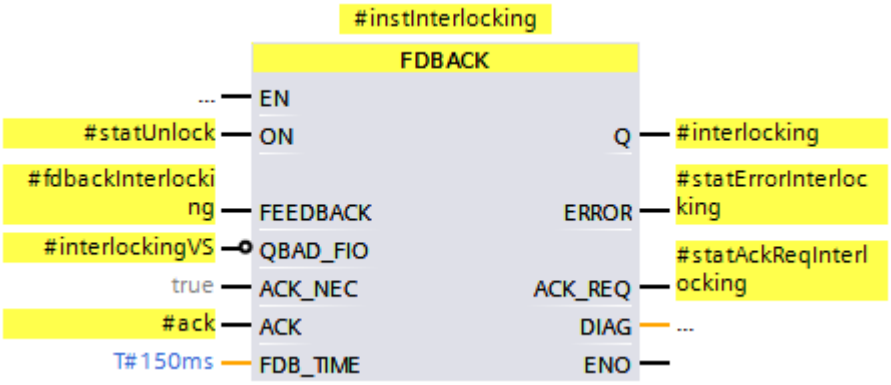
- The protective door is closed ("1” signal at #statDoorClosed).
- The command for unlocking is not pending ("0” signal at #unlock).

Figure 1-6: Evaluation of the unlock signal



To disengage and monitor the interlocking the function block ProtDoorWithInterlocking uses the FDBACK instruction that is included in STEP 7 Safety. If "1" is pending at input ON, output Q switched on. Within the configured FDB_TIME time, the signal at the FEEDBACK input must be switched inverse to output signal Q. Otherwise, Q is switched off and an error displayed at output ERROR. Afterwards, the error must be acknowledged via input ACK. It is output via the ACK_REQ output that an acknowledgement is required.

Figure 1-7: Call of the instruction FDBACK



A contact in the position switch (#fdbackInterlocking) is used for monitoring whether the interlocking switches correctly. In the event of an error, the protective door is locked and the machine is switched off safely.

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 \5\.

1.2.4 Controlling and monitoring of the actors

Hardware

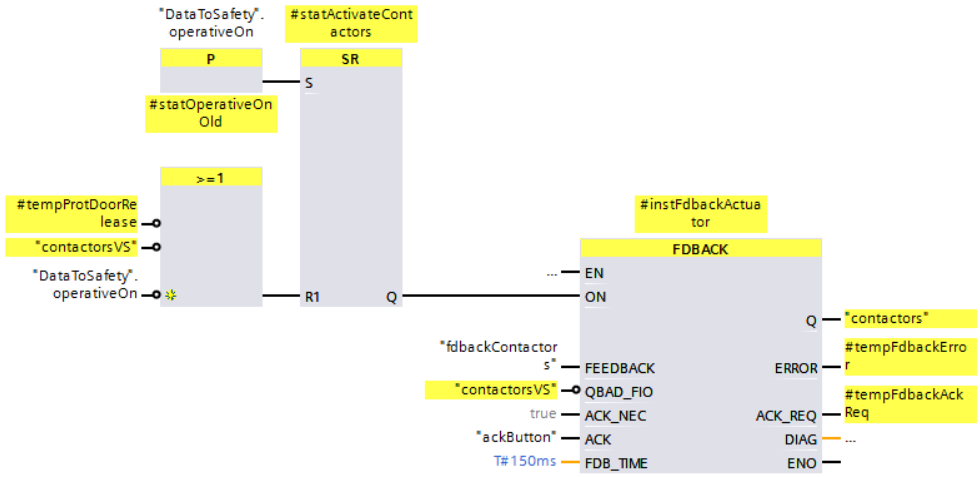
To achieve SIL 3 in accordance with IEC 62061, or PL e in accordance with ISO 13849-1, double channel switch off is performed. Two SIRIUS 3RT2 contactors (Figure 1-1, position 3) are used, and their correct function is monitored via the auxiliary contacts of the contactors through the fail-safe controller.

If one of both contactors welds, the second contactor continues to ensure a safe shut-down. Welding of a contactor is detected at the next signal change, and renewed switching on is prevented until the failure has been removed.

Software

The function block MainSafety uses the FDBACK instruction that is included in STEP 7 Safety. If "1" is pending at input ON, output Q switched on. Within the configured FDB_TIME time, the signal at the FEEDBACK input must be switched inverse to output signal Q. Otherwise, Q is switched off and an error displayed at output ERROR. Afterwards, the error must be acknowledged via input ACK. It is output via the ACK_REQ output that an acknowledgement is required.

Figure 1-8: Controlling and monitoring of the actors



The following requirements must be met for switching the machine on:

- The protective door must be closed and interlocked (Release signal from ProtDoorWithInterlocking).
- No error must be pending in the feedback circuit monitoring of the interlocking.
- The operative switch-on signal must provide a rising edge.

1.3 Hardware and software components

This application example was created with the following hardware and software components:

Table 1-4: Hardware and software components

Component	Qty	Article number	Note
Power supply	1	6EP1332-4BA00	PM 190 W
Fail-safe S7-CPU	1	6ES7516-3FN01-0AB0	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	6ES7526-2BF00-0AB0	
Fail-safe digital output module	1	6ES7526-2BF00-0AB0	
S7-1500 mounting rail	1	6ES7590-1AE80-0AA0	Length: 482 mm
Position switch with interlocking	1	3SE5322-0SD21	Spring-loaded interlocking with auxiliary release
Separate actuator	1	3SE5000-0AV01	Standard actuator
Position switches	1	3SE5112-0KH01	with swiveling lever
Push button	3	3SU1	2NO, 1NC
Selector switch	1		1S
Contactor	2	3RT2015-1BB42	S00, DC24V, 1NC
SIMATIC STEP 7 Professional	1	6ES7822-1AA05-0YA5	V15.1
STEP 7 Safety Advanced	1	6ES7833-1FA15-0YA5	V15.1

This application example consists of the following components:

Table 1-5: Components of the application example

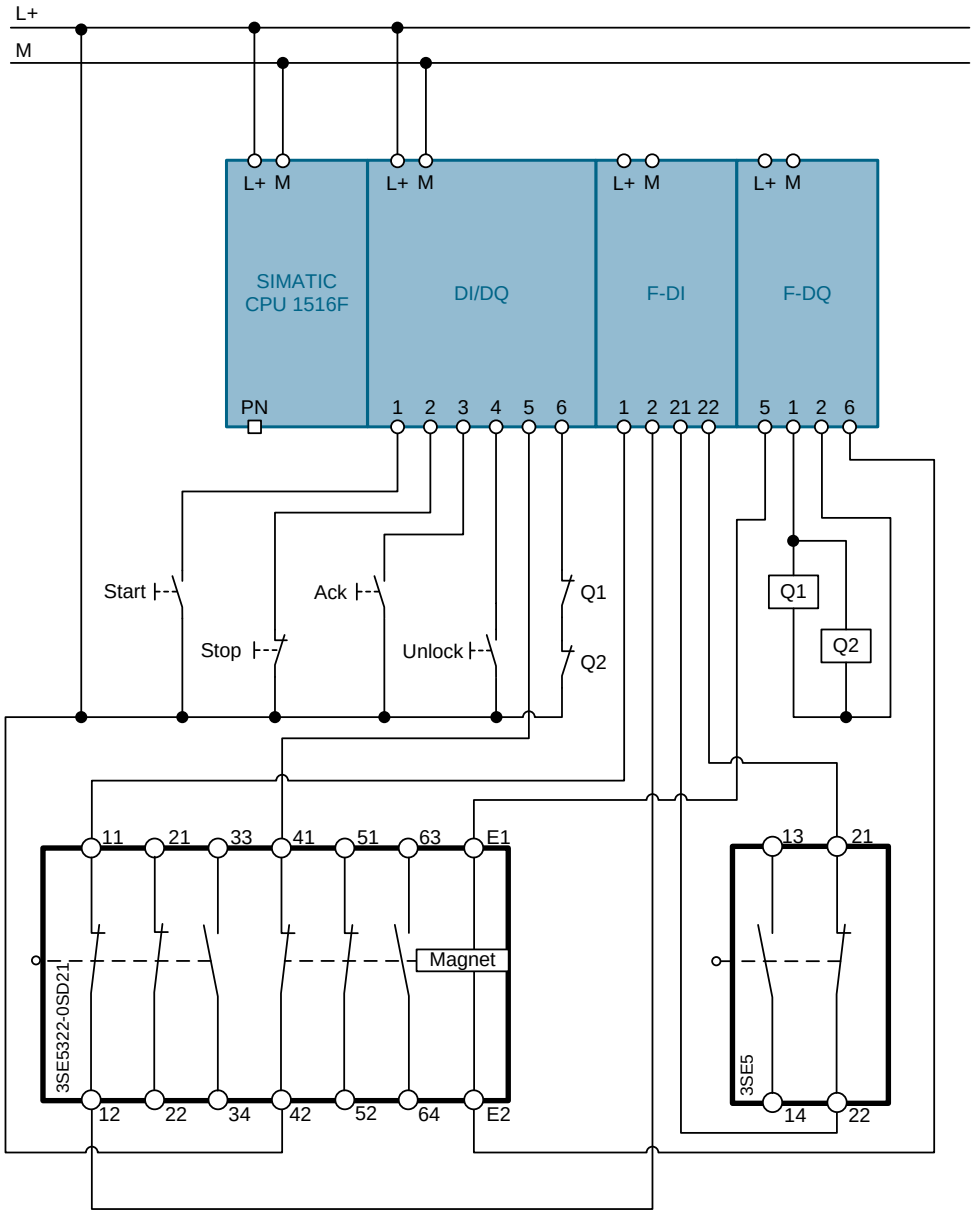
Component	Note
21063946_ProtDoor-Interlocking_DOC_V50_en.pdf	This document
21063946_ProtDoor-Interlocking_PROJ_V50.zip	This zip file contains the TIA Portal project.
21063946_ProtDoor-Interlocking_SE_TST_V50.set	TIA Selection Tool project with Safety Evaluation of the safety functions

2 Engineering

2.1 Hardware setup

The figure below shows the hardware configuration of the application.

Figure 2-1: Wiring diagram



2.2 Configuration

The enclosed TIA Portal 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.

NOTICE	**The settings shown below contribute to implementing the required safety. Changes on the settings may cause loss of the safety function.**

2.2.1 Settings of the F-DI

Short circuit test

The short-circuit tests of the channels 0 and 8 are activated.

Figure 2-2: Short-circuit test for sensor supply 0

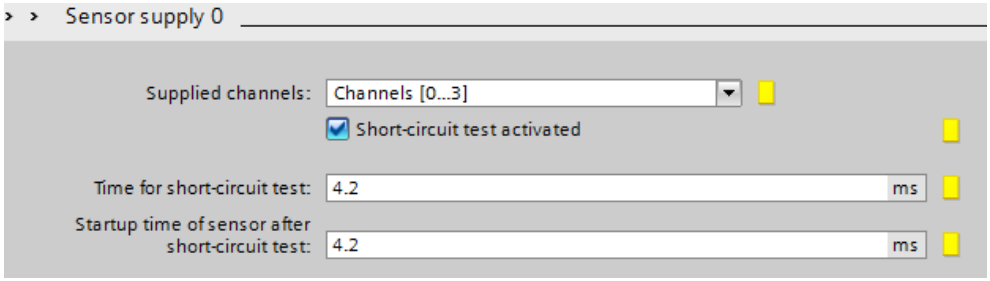
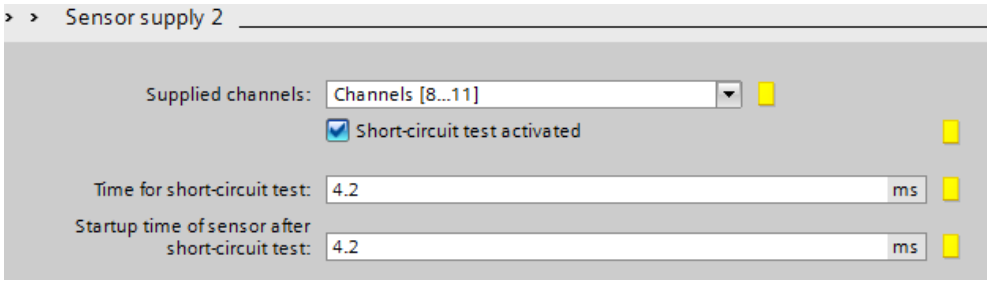


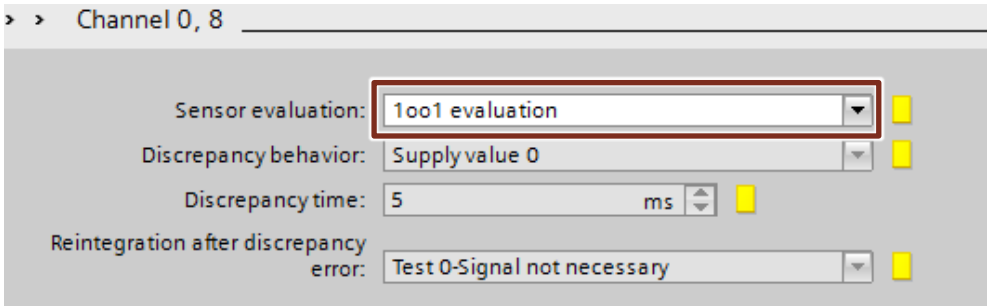
Figure 2-3: Short-circuit test for sensor supply 2



Channel parameters

Monitoring the position of the protective door is performed via channel pair 0, 4. The evaluation of the encoders must be set to "1oo1 evaluation" since the discrepancy evaluation is performed in function block SFDOOR.

Figure 2-4: Evaluation of the sensors



Since both position switches are often attached at different locations of the protective door (e.g. hinge switch) they might not trip simultaneously. Therefore, a high discrepancy time is required.

Evaluating discrepancies through the hardware (1oo2 evaluation) is therefore not suitable since discrepancies are permitted as long as they do not exceed the set discrepancy time.

For discrepancy monitoring through function block SFDOOR the discrepancy time is infinite; however, any discrepancy is detected as a fault.

The table below discusses the differences when evaluating discrepancies:

Table 2-1: Differences in the discrepancy evaluation

	Situation	Evaluation through hardware	Evaluation through SFDOOR
1.	Both channels open within the set discrepancy time.	Machine switches off, no fault.	Machine switches off, no fault.
2.	Channel 1 opens, channel 2 follows after the set discrepancy time has elapsed.	Machine switches off fault; is detected and must be acknowledged.	Machine switches off, no fault.
3.	Channel 1 opens, channel 2 remains closed, channel 1 closes within the set discrepancy time.	Machine switches off, no fault.	Machine switches off fault; is detected and must be acknowledged.

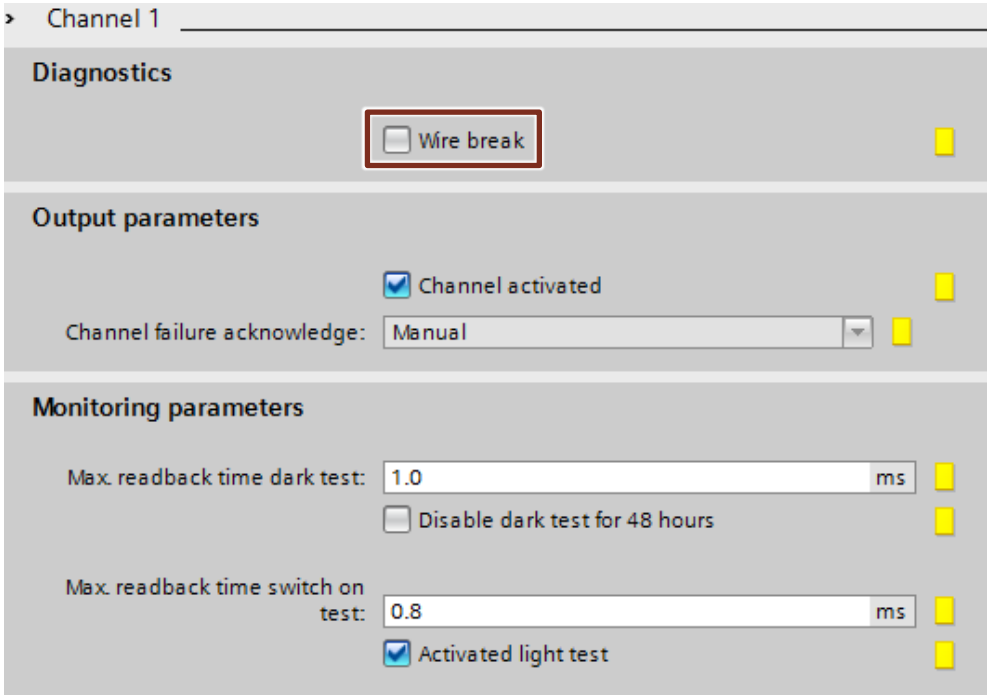
Note Evaluating discrepancies through the hardware as well as through the function block is not possible since for an activated 1oo2 evaluation, the access to the individual channels is not permitted in the program code.

2.2.2 Settings of the F-DQ

Channel parameters

Wire-break detection for controlling the contactors can be activated; for controlling the interlocking it must be deactivated.

Figure 2-5: Channel parameters interlocking



2.3 Commissioning

2.3.1 Preparation

1. Download the "21063946_ProtDoor-Interlocking_PROJ_V41.zip” project file. The download can be found in \2\.
2. Save the zip file in any directory on your computer and unzip it.
3. Set the IP address of the PG/PC in a way so that the PG/PC is located in the same subnet as the CPU.
4. Use an Ethernet cable to connect the PG/PC with the Ethernet interface of CPU S7-1516F.

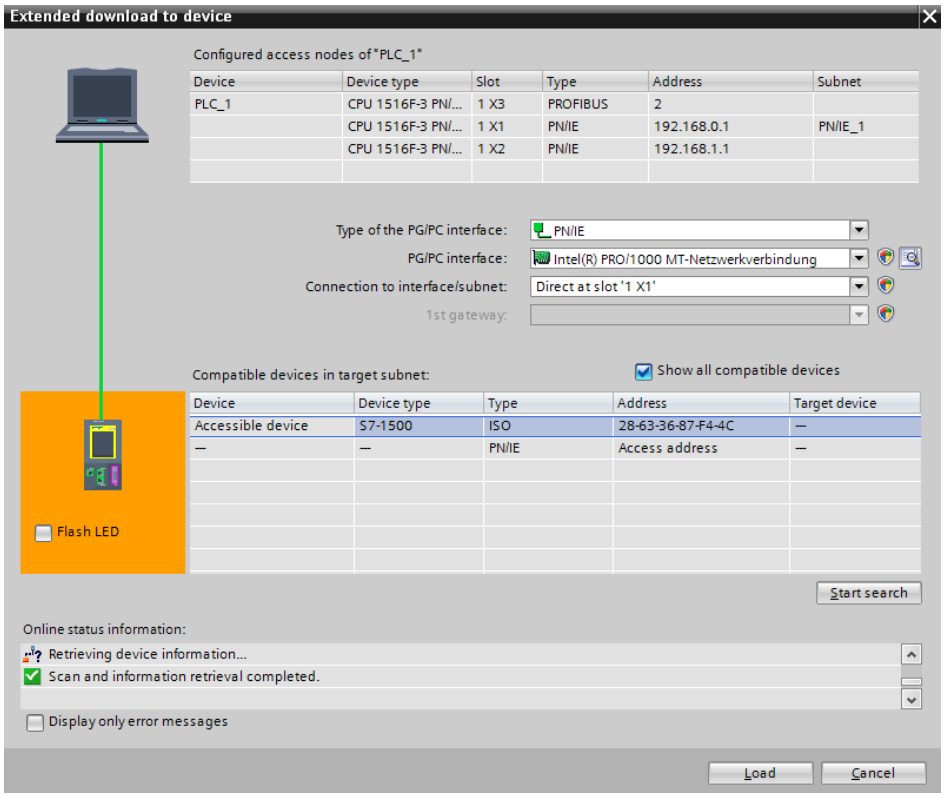
For this application example, the following IP addresses were used:

CPU S7-1516F
IP address: 192.168.0.30
Subnet mask: 255.255.255.0

2.3.2 Loading the S7 project into CPU S7-1516F

1. Open "TIA Portal”.
2. Go to the project view.
3. Click "Project > Open” in the menu bar in the TIA Portal.
4. Click "Browse” and open the unzipped project.
5. Set the CPU S7-1516F to STOP.
6. Right click "PLC_1 [CPU1516F-3 PN/DP]” and then "Download to device > Hardware and Software (only changes)”).
7. Select the respective 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 into the CPU.

9. Confirm the dialog by clicking "Load”.
10. Click "Finish” when the loading process is completed.

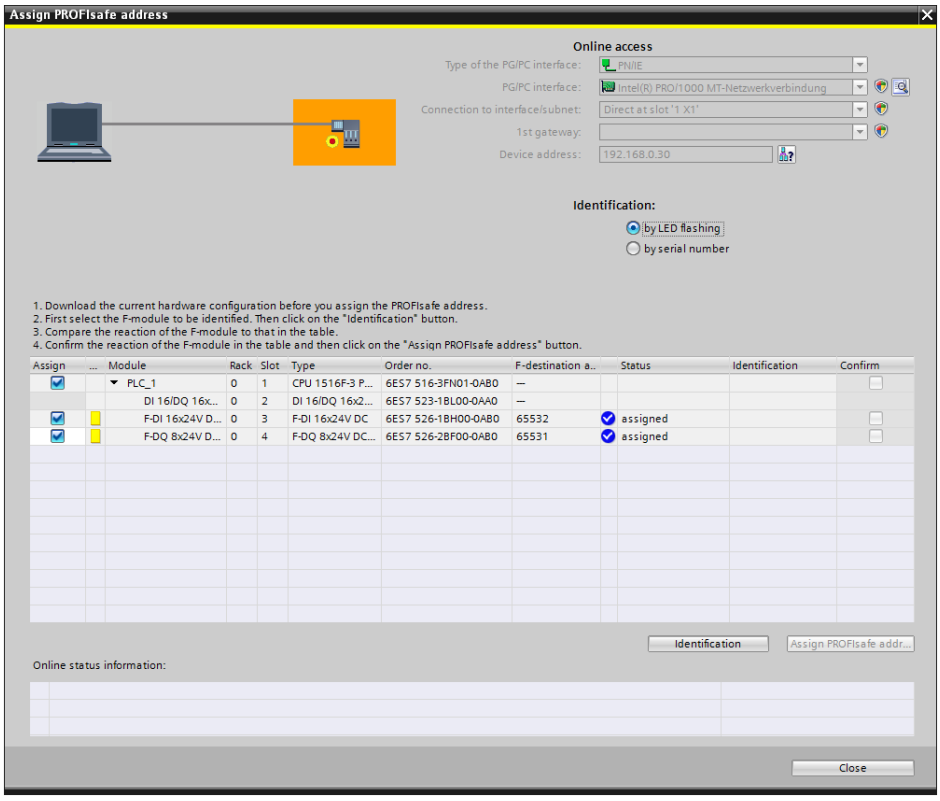
2.3.3 Assigning PROFIsafe address

In order to establish a secure communication between the F-CPU and the fail-safe modules of the ET 200SP, the modules have to be assigned PROFIsafe addresses.

Note Since the F address is saved in the electronic coding element, the following steps are only required if the coding element has not previously been assigned an F address or another F address.

1. Open "Devices & networks" from the project tree.
2. Right click the F-CPU and select the "Assign PROFIsafe address" action.
3. Enable the checkbox of the first fail-safe module and click the "Identification" button.
4. When the LEDs of the F-DI are simultaneously flashing green every second, enable the "Confirm" checkbox.
5. Then click the "Assign F-destination address" button and confirm the dialog with "Yes".

Figure 2-7: Assigning PROFIsafe addresses



6. Repeat the steps for the other fail-safe modules.
7. Close the window.

Note All red LEDs of the fail-safe modules should go out after assigning the F-target address. If this is not the case, there may be a fault in the wiring.

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

2.4 Operating the Application

Starting the machine

Table 2-2: Starting the machine

No.	Action	Notes
1.	Shut the protective door.	
2.	Press the knob switch, to interlock the protective door.	The power supply at the magnet is interrupted and the locking mechanism engages the actuator.
3.	Press the acknowledgement button.	An acknowledgement is necessary after restarting the machine.
4.	Press the start button.	The machine starts.

Unlocking and opening the protective door

Table 2-3: Unlocking and opening the protective door

No.	Action	Notes
1.	Press the stop button	The machine switches off and coasts down.
2.	Wait until the configured delay time has elapsed and unlock the protective door.	
3.	Press the knob switch, to unlock the protective door.	The magnet is supplied with voltage and the locking mechanism disengages the actuator.
4.	Open the protective door.	

Acknowledging a discrepancy fault

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

Table 2-4: Acknowledging a discrepancy fault

No.	Action	Notes
1.	Press the knob switch, to unlock the protective door.	The magnet is supplied with voltage and the locking mechanism disengages the actuator.
2.	Open the protective door so both position switches can be actuated.	Both channels report "0".
3.	Shut the protective door.	Both channels report "1", the fault is acknowledged.
4.	Press the knob switch, to interlock the protective door.	The power supply at the magnet is interrupted and the locking mechanism engages the actuator.
5.	Press the acknowledgement button.	This is only necessary if the fault occurred while the protective door was locked.
6.	Press the start button	The machine starts.

Acknowledging other faults of the safety function

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

Possible faults that are acknowledged in this way are, amongst others:

- Cross-circuit between both channels of the position switches
- External voltage at the fail-safe outputs
- Pulling a fail-safe module
- Welding of a contactor

Table 2-5: Acknowledging other faults of the safety function

No.	Action	Notes
1.	Check the LEDs of the fail-safe modules. If a red LED lights, a fault in the hardware was detected. Use the online diagnostics in TIA Portal to search for faults.	
2.	If all LEDs light green, a fault was detected by the safety program. Monitoring the tag table to find the fault.	The tags #fault and #ackReq of the instructions of the ProtDoorWithInterlocking block can help during the search.
3.	Clear the fault.	
4.	Shut the protective door.	
5.	Press the knob switch, to interlock the protective door.	The power supply at the magnet is interrupted and the locking mechanism engages the actuator.
6.	Press the acknowledgement button.	Passivated channels of the fail-safe modules are reintegrated. Detected faults by the safety program are acknowledged.
7.	Press the start button.	The machine starts.

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.

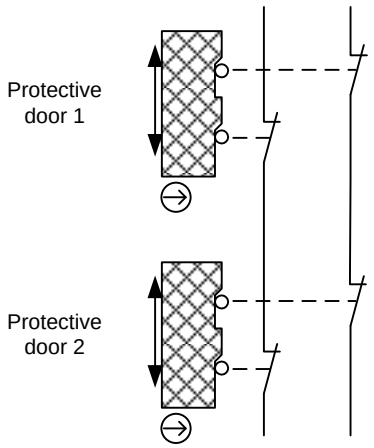
- Position switches have to be arranged in such a way that they cannot be damaged when they are approached or passed. This is why position switches must not be used as a mechanical stop.
- Only sensors with positive opening contacts may be used as sensors.
- Sensor cables must be laid with appropriate 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



Interlocking of protective doors

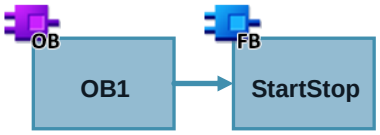
In combination with protective door monitoring, very often an interlocking of the protective door is implemented as well. Guards with interlocking secure danger areas against unauthorized access. In most cases, this is due to two reasons:

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. Interlocking 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.

3.2 Details of the mode of operation

3.2.1 Standard user program

Figure 3-2: Standard user program



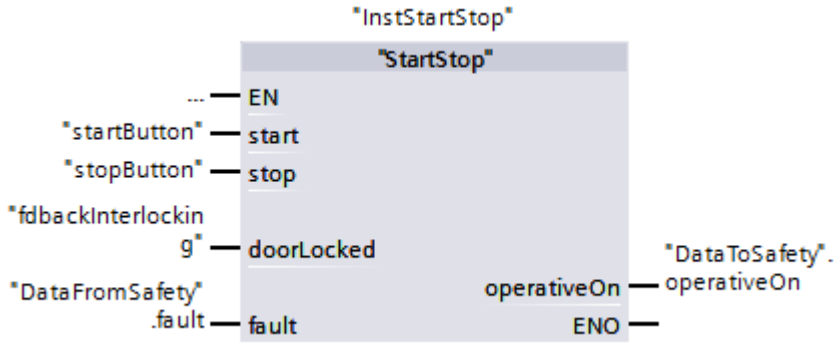
Operative switching on and off of the machine

The StartStop function block represents the operative (non-failsafe) switching of the machine. Here, the switch-on signal that is used in the safety program is generated. Since the machine must be switched off safely, the actual setting and resetting of the fail-safe outputs is performed in the safety program.

The function block evaluates:

- Start button
- Stop button
- State of the interlocking
- Possible detected faults

Figure 3-3: Call of function block StartStop



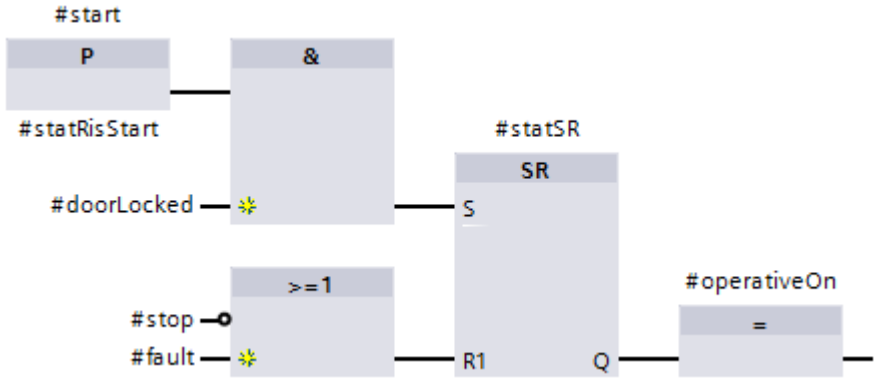
To create a switch-on signal, the protective door must be interlocked and the start button be pressed. If the stop button is pushed or a fault is detected, the switch-on signal is reset.

Evaluating the state of the interlocking prevents creating a switch-on signal even though the door is not locked. The machine is hence protected from starting immediately when locking the door without first pressing the start button again.

The fail-locking system of the position switch prevents the door from interlocking unless it is closed. For this reason, the position of the protective door is not explicitly evaluated here.

Monitoring of the interlocking is performed in the safety program.

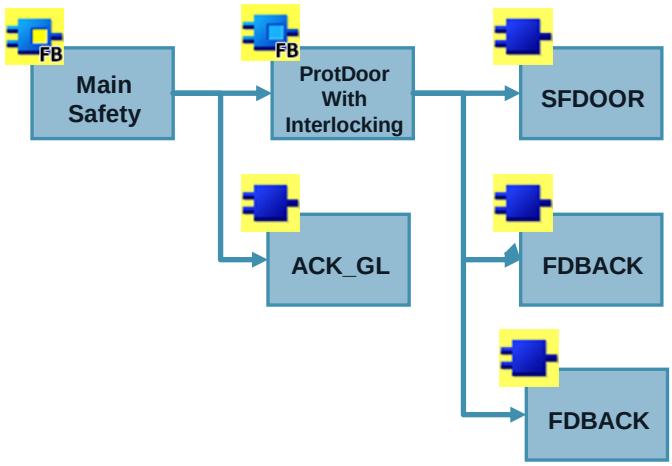
Figure 3-4: Function block StartStop



3.2.2 Safety program

Overview

Figure 3-5: Safety program

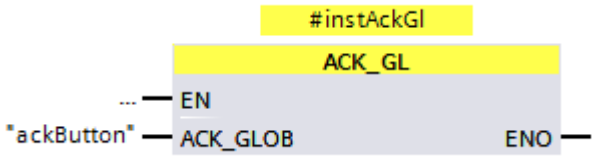


Function block MainSafety is called cyclically by means of an F-runtime group. This contains all further fail-safe program components.

Reintegration of passivated channels

The ACK_GL instruction included in STEP 7 Safety is used here. It generates an acknowledgement for the simultaneous reintegration of all F-I/Os/channels of the F periphery of an F-runtime group after communication faults or F-I/O/channel faults.

Figure 3-6: Call of ACK_GL



Examples of events that cause passivation:

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

Note If a fault occurs in the hardware (e.g. due to wire break), it may take several seconds, depending on the fault type, until the module detects that the fault has been removed. Only then will acknowledgement take effect.

3.2.3 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. Data block DataFromSafety is read by the standard user program and written by the safety 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 Evaluation of the Safety Function

3.3.1 Standards

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

Table 3-1: Standards

Version	Mentioned below
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 functions

In this application example, the following safety functions are realized.

Table 3-2: Description of the safety functions

Safety function	Description	Requirement
SF1	If the protective door is opened, the machine must be switched off safely.	SIL 3 or PL e
SF2	The protective door is kept closed until the machine has stopped.	SIL 2 or PL d

Monitoring the position of the protective door (SF1) is designed according to SIL 3 or PL e. According to the standard EN ISO 14119 "Safety of machinery – Interlocking devices associated with guards – Principles for design and selection" the required PL_r or SIL of the interlocking function (SF2) is usually lower than that of the position monitoring of the protective door. For this reason, the interlocking function is in this example designed up to SIL 2, or PL d respectively.

Below, the safety function SF2 is evaluated in accordance with the standards ISO 13849-1 and IEC 62061.

Since the safety function SF1 is explained in detail in a different application example, it is not further discussed here. That application example is available in \7\.

The supplied TIA Selection Tool project contains the Safety Evaluation of both safety functions.

3.3.3 Evaluation in accordance with 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 "Detecting”

In this application example, the safe state for enabling the protective door is not detected via sensors, but can be estimated regarding the time if the overrun of the dangerous motion is always the same. The protective door is therefore enabled via a time delay after switching off the actuators that are evaluated in the safety program. After enabling the protective door, it can be unlocked by the operator.

Subsystem "Detecting” is therefore not relevant for this application example.

Evaluation of "Evaluating”

Subsystem "Evaluating” involves the fail-safe controller and the F-DQ module for controlling the interlocking. The position of the interlocking magnet is read back to the controller via a standard DI. However, as a mere diagnostic function, the standard DI needs not be considered in the evaluation.

Table 3-3: Evaluation of subsystem "Evaluation"

Component	PFH_D	PL	Definition
CPU 1516F-3PN/DP incl. PROFIsafe	$2.00 \cdot 10^{-9}$	PL e	SIEMENS AG
ET 200MP F-DQ	$2.00 \cdot 10^{-9}$	PL e	
Total	$\mathbf{4.00 \cdot 10^{-9}}$	**PL e**	

Evaluation of "Reacting”

For SF2, the SIRIUS 3SE5 position switch with interlocking represents the subsystem "Reacting”. Correct functioning of the interlocking is monitored by the controller via an NC contact in the position switch. A fault in the interlocking control is detected immediately by the dynamic feedback circuit monitoring and causes the machine to switch off.

The probability that the fault occurs at the very moment the operator tries to access the hazard zone is neglectable (see also chapter 8.4 ISO 14119).

The $MTTF_D$ of the position switch is 45,662.10 years which is limited to 100 years by ISO 13849-1.
The MTBF of the digital input module that the NC contact of the position switch is connected to is 90.98 years. Treating every fault as a dangerous fault, a $MTTF_D$ of 90.98 years can be assumed. The $MTTF_D$ of the testing channel is therefore greater than one half of the $MTTF_D$ of the functional channel.

The architecture therefore corresponds to category 2 in accordance with ISO 13849-1.

A breaking of the interlocking mechanism is also excluded (see also chapter 8.5 ISO 14119).

The safety-relevant parameters of the component are provided by the manufacturer. The resulting probability of a dangerous failure, as well as the SILCL depends on the actual actuation cycles and the installation type of the component to be completed by the user.

Table 3-4: Parameters of subsystem "Reaction"

Parameter	Value	Explanation	Definition
B10 Switching cycles	1.000.000	Manufacturer information	SIEMENS AG
Dangerous failure fraction	0.20 (20%)	Manufacturer information	
T1 Lifetime	175,000 h (20 years)	Manufacturer information	
Architecture	Category 2	Single channel system with test facility	User
Actuations/ test interval	3/day	Assumption	
CCF measures (points) Susceptibility to common cause failures	≥ 65	Suitable measures against CCF have to be taken in accordance with ISO 13849-1 table F.1	
DC Diagnostic coverage	≥ 0.90 (90%)	Dynamic monitoring of the interlocking taking into consideration the fault exclusion	

Table 3-5: Result of subsystem "Reacting"

PFH_D	PL achieved
$2.29 \cdot 10^{-7}$	PL d

Result of the evaluation in accordance with ISO 13849-1

Table 3-6: Result of the evaluation in accordance with ISO 13849-1

Subsystem	PFH_D	PL achieved
Evaluating	$4.00 \cdot 10^{-9}$	PL d
Reaction	$2.29 \cdot 10^{-7}$	PL e
Total	$2.33 \cdot 10^{-7}$	**PL d**
	PL d	

3.3.4 Evaluation in accordance with 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 "Detecting”

In this application example, the safe state for enabling the protective door is not detected via sensors, but can be estimated regarding the time if the overrun of the dangerous motion is always the same. The protective door is therefore enabled via a time delay after switching off the actuators that are evaluated in the safety program. After enabling the protective door, it can be unlocked by the operator.

Subsystem "Detecting” is therefore not relevant for this safety function.

Evaluation of "Evaluation"

The parameters relevant for the evaluation are provided by the manufacturer and are available in the SET:

Table 3-7: Evaluation of 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-DQ	$2.00 \cdot 10^{-9}$	SILCL 3	
Total	$\mathbf{4.00 \cdot 10^{-9}}$	**SILCL 3**	

Evaluation of "Reacting”

For SF2, the SIRIUS 3SE5 position switch with interlocking represents the subsystem "Reacting”. Correct functioning of the interlocking is monitored by the controller via an NC contact in the position switch. This is a basic subsystem architecture C in accordance with IEC 62061: Zero fault tolerance with diagnostic function.

For a single channel setup (hardware fault tolerance = 0) and DC ≥ 90%, SILCL 2 or 3 can only be achieved with additional measures. That is, after fault detection, a defined safe state of the machine must be initiated with a respective fault reaction. A fault in the interlocking control is detected immediately by the dynamic feedback circuit monitoring and causes the machine to switch off.

The probability that the fault occurs at the very moment the operator tries to access the hazard zone is neglectable (see also chapter 8.4 ISO 14119).

A breaking of the interlocking mechanism is also excluded (see also chapter 8.5 ISO 14119).

The safety-relevant parameters of the component are provided by the manufacturer. The resulting probability of a dangerous failure, as well as the SILCL depends on the actual actuation cycles and the installation type of the component to be completed by the user.

Table 3-8: Parameters of the subsystem "Reacting"

Parameter	Value	Explanation	Definition
B10 Switching cycles	1.000.000	Manufacturer information	SIEMENS AG
Dangerous failure fraction	0.20 (20%)	Manufacturer information	
T1 Lifetime	175,000 h (20 years)	Manufacturer information	
Subsystem architecture	C	Zero fault tolerance with diagnostic function	User
Actuations/ test interval	3/day	Assumption	
Structural restriction	Yes	Due to the fault exclusion, structural restrictions apply	
DC Diagnostic coverage	≥ 0.90 (90%)	Dynamic monitoring of the interlocking taking into consideration the fault exclusion	

Table 3-9: Result of the subsystem "Reacting"

PFH_D	SILCL achieved
$2.50 \cdot 10^{-10}$	SILCL 2

Result of the evaluation in accordance with IEC 62061

Table 3-10: Result of the evaluation in accordance with IEC 62061

Subsystem	PFH_D	SIL achieved
Evaluating	$4.00 \cdot 10^{-9}$	SILCL 3
Reaction	$2.50 \cdot 10^{-10}$	SILCL 2
Total	$\mathbf{4.25 \cdot 10^{-9}}$	**SILCL 2**
	SIL 2	

4 Appendix

4.1 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

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

4.2 Links and Literature

Table 4-1: Links and literature

	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/21063946
\3\	Functional Safety at Siemens www.siemens.com/safety-integrated
\4\	Safety Evaluation in 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 https://www.siemens.com/sirius-detecting
\7\	Monitoring the position of a protective door up to SIL 3 / PL e https://support.industry.siemens.com/cs/ww/en/view/21331363

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 in accordance with new standards IEC 62061 and ISO 13849-1
V3.0	11/2015	• Migration of the application example to TIA V13 SP1 • Replacement of the components with S7-1500 and ET 200SP • Evaluation of the interlocking function in accordance with IEC 62061 and ISO 13849-1
V4.0	04/2017	• Upgrade to TIA Portal V14 • Replacement of decentral periphery with central modules
V4.1	07/2019	Update TIA Portal V15.1
V5.0	05/2021	Migration of Safety Evaluation Tool to Safety Evaluation with TIA Selection Tool