Emergency Stop 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/21064024

Siemens Industry Online Support

Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice.
If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications − e.g. Catalogs − the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.
Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.
Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

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 only form one element of such a concept.
Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.
Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Table of Contents

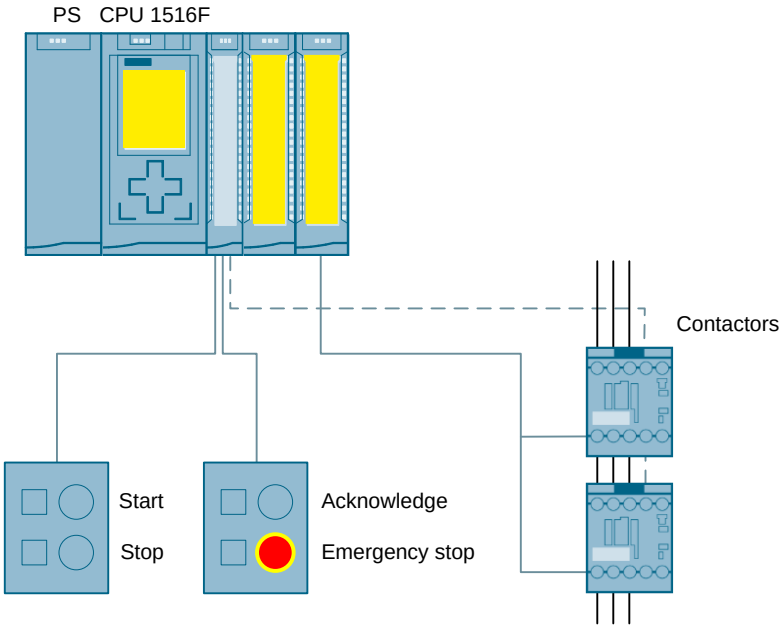
1 Introduction

1.1 Overview

In order to be able to safely switch of a machine even in an emergency situation, an emergency stop command device is attached and the actuators are controlled via two contactors. The safety function is designed up to PL e in accordance with EN ISO 13849-1 and SIL 3 in accordance with IEC 62061.

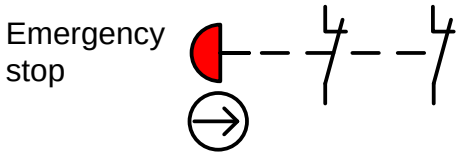
For a seamless integration into the automation process, the failsafe S7-1516F controller is used, in which standard user program and safety program run next to each other.

Figure 1-1: Overview of the hardware configuration



In order to achieve the demanded safety level, the emergency stop is designed with two channels and monitored for discrepancy and cross-circuit by the controller

Figure 1-2: Emergency stop with two channels



The actuators are also set up redundantly, so in case one contactor fails (e.g. welding of the contacts) the machine is still safely switched off by the second contactor.

NOTICE	**SIL 3 / PL e can only be achieved, if the function of the contactors is monitored in the feedback circuit.** For more information regarding the "Feedback circuit" topic, please refer to \3\.

Customer benefits

- Integration of safety function in the complete application:
  - Status of the emergency stop is also available in the standard user program and can be processed there.
  - No complicated synchronization (extra wiring or data mapping) between standard and safety automation.
- The diagnostic is performed channel granular even for several emergency stop command devices:
  - Error localization is accelerated.
- Diagnostic messages can be displayed without the additional effort of a message configuration on
  - an HMI panel,
  - by means of web server or
  - on the display on the CPU.

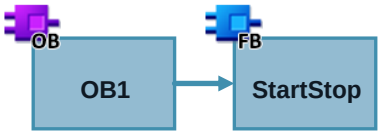
1.2 Mode of Operation

In this application example the following functions are realized:

- Resetting a failsafe digital output (stopping the application), after actuating the emergency stop button
- Interlocking against a restart of the machine after triggering the safety function until the following conditions are fulfilled:
  - Emergency stop is unlocked
  - Acknowledgement has been given (does not automatically start the application)
  - Start button is pressed
- Monitoring the correct function of the contactors
- Interlocking against a restart of the machine when a faulty contactor has been detected

1.2.1 Standard user program

Figure 1-3: Overview standard user program



StartStop function block

This block is used to evaluate start and stop button. With a positive edge at the input of the start button, a start signal is written into the global data block "DataToSafety". The start signal is then evaluated in the safety program where the machine is switched on and off.

The block evaluates:

- Start button
- Stop button
- Error signal "fault" from the safety program via the "DataFromSafety" data block, see chapter 1.2.3.

If the stop button is pushed or an error is detected by the "DataFromSafety" global data block via the "fault" signal, the start signal is reset.

Figure 1-4: Call of function block "StartStop"

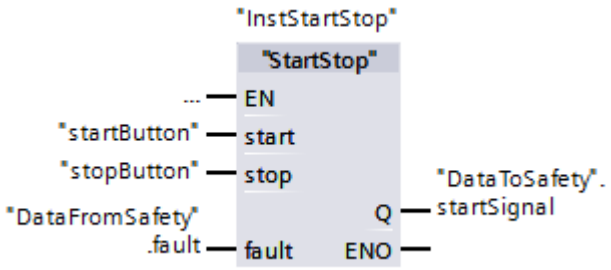
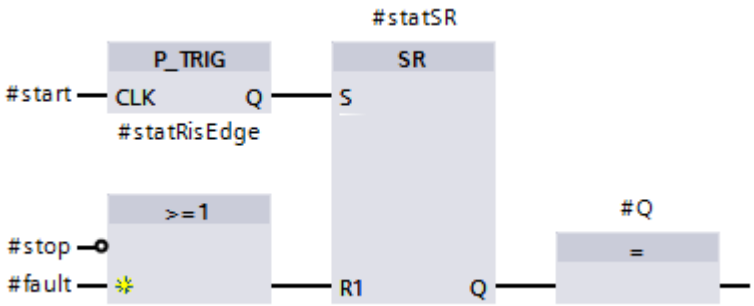
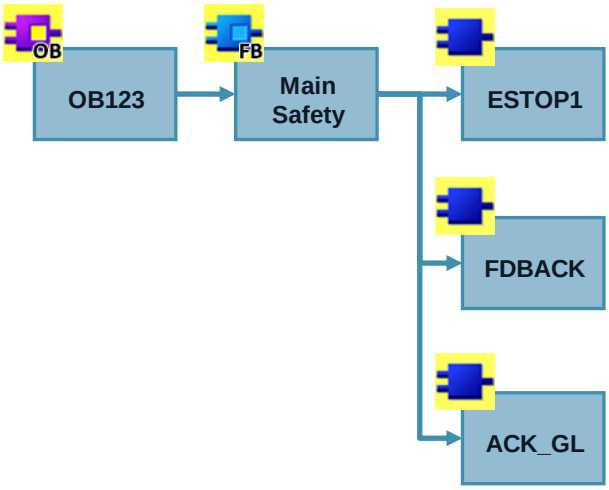


Figure 1-5: Function block "StartStop"



1.2.2 Safety program

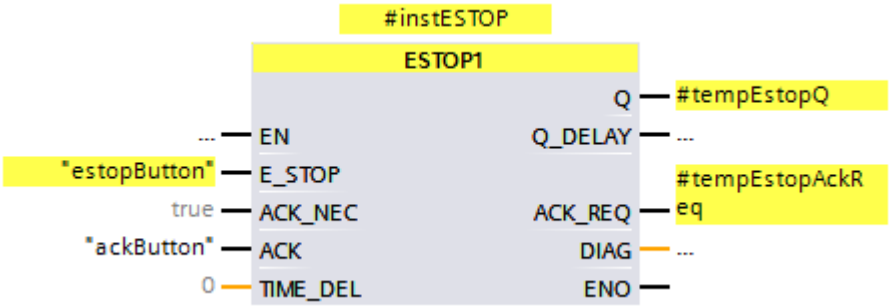
Figure 1-6: Overview safety program



ESTOP1 instruction

The ESTOP1 instruction is included in STEP 7 Safety Advanced. If the emergency stop is not actuated, the instruction sets the output Q to TRUE. After pushing the emergency stop, it has to be unlocked and acknowledged via the ACK input. It is output via ACK_REQ that an acknowledgement is required. The Q output is intermediately saved in the temporary #tempEstopQ tag, in order to simplify access in the next instruction.

Figure 1-7: Call of instruction ESTOP1



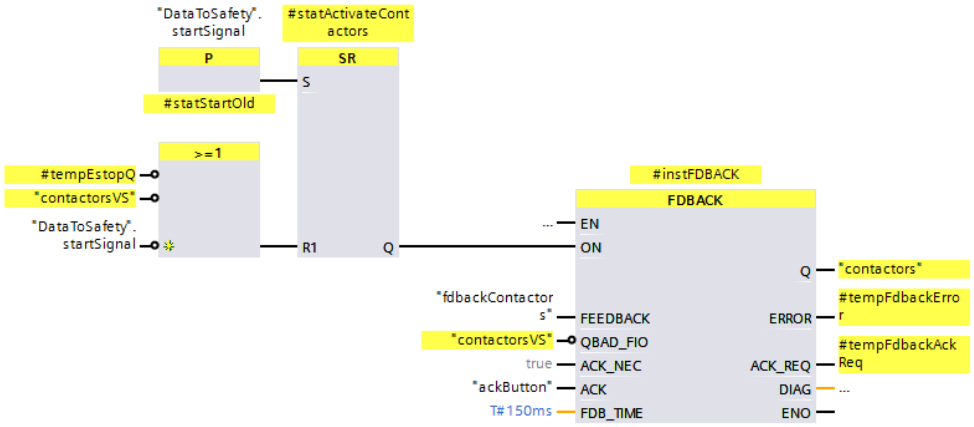
Note Both channels of the emergency stop are monitored for discrepancy and cross-circuit by the F-DI module. There will then be one processed signal available in the user program for both channels. The individual channels cannot be accessed.

FDBACK instruction

The FDBACK instruction is included in STEP 7 Safety Advanced. It switches the actuators (in this example the two contactors) and monitors their correct function via the feedback circuit.

When a start signal from the standard user program is received (see chapter 1.2.3), the release signal of the ESTOP1 instruction is present and no error in the safety program is present, the contactors are switched on. The signal on the FEEDBACK input has to switch inverse to the Q output signal within the configured FDB_TIME time. If this is not the case, the contactors are switched off again. Afterwards it has to be acknowledged via the ACK input. It is output via ACK_REQ that an acknowledgement is required.

Figure 1-8: Call of instruction FDBACK



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.

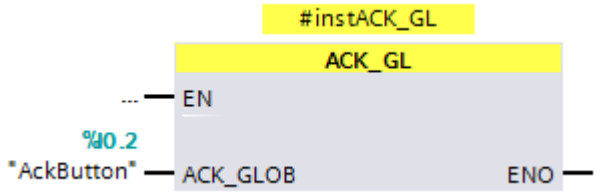
The value status behaves inversely to the QBAD bit and is entered into the process image of the inputs (PII).

For more information on the value status, please refer to \5\.

ACK_GL instruction

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

Figure 1-9



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, it may take a couple of seconds until the module detects that the error has been removed (e.g. fixed wire break). Only then is there an effect from pressing the acknowledgement button.

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

The processed "StartSignal" is transferred from the standard user program to the safety program. The safety program reports a fail-safe shutdown or errors in the safety program via the "fault" tag to the standard user program.

Note For more information about the data exchange between the standard user program and the safety program, please refer to \5\.

1.3 Components used

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

Table 1-1: Hardware and software components

Component	No.	Article number	Note
Power supply	1	6EP1332-4BA00	PM 190 W
Fail-safe S7-CPU	1	6ES7516-3FN01-0AB0	CPU 1516F-3 PN/DP FW 2.0
SIMATIC memory card	1	6ES7954-8LF01-0AA0	SMC 24 MB
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
Emergency stop	1	3SU1851-0NB00-2AA2	Mushroom push 2NC
Push button	3	3SU1	2NO, 1NC
Contactor	2	3RT2015-1BB42	S00, DC 24 V, 1NC
STEP 7 Professional	1	6ES7822-1AA04-0YA5	V14 Update 1
STEP 7 Safety Advanced	1	6ES7833-1FA14-0YA5	V14 Update 1

Note The functionality was tested with the hardware components specified. Similar products that are not included in the list above can also be used. In this case, please note that changes to the example code (e.g. different addresses) may become necessary.

This application example consists of the following components:

Table 1-2: Components of the application example

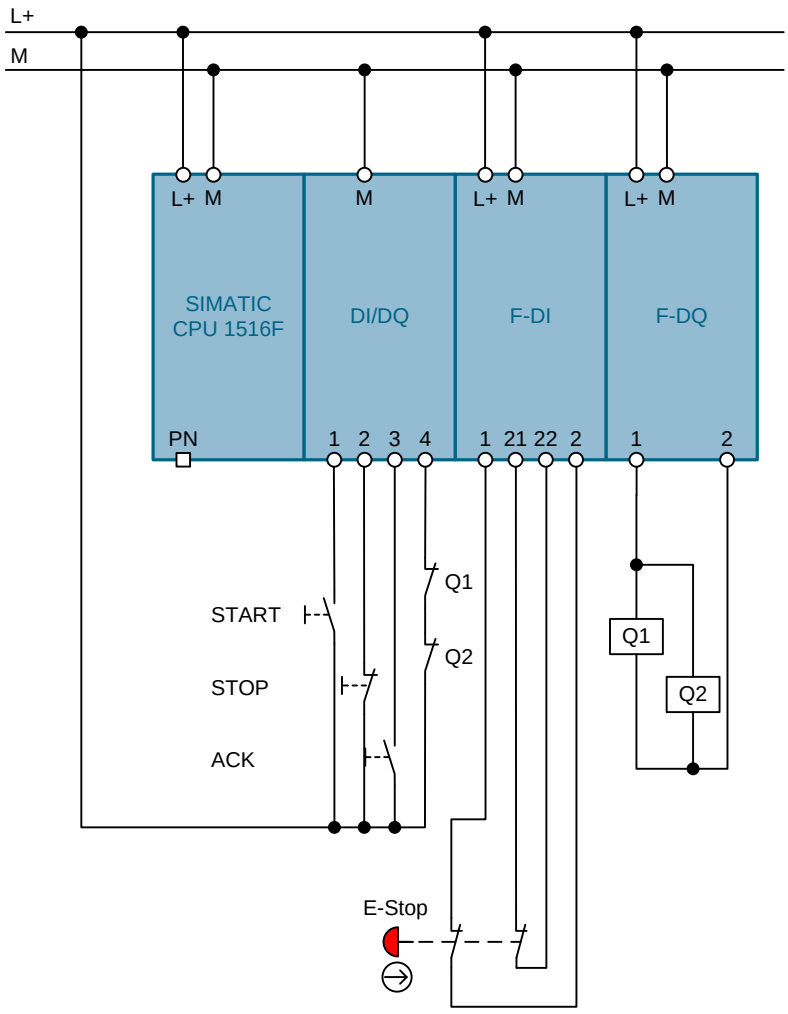
Component	Note
21064024_ESTOP_SIL3_1500F_DOC_V50_en.pdf	This document
21064024_ESTOP_SIL3_1500F_PROJ_V50.zip	This zip file contains the TIA Portal project.
21064024_ESTOP_SIL3_1500F_SET_V50.zip	Evaluation of the safety functions as SET project

2 Engineering

2.1 Hardware setup

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

Figure 2-1: Wiring the hardware components



2.2 Configuration

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

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

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

2.2.1 Settings of the F-DI

Short circuit test

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

Figure 2-2: Activating the short-circuit test for sensor supply 0

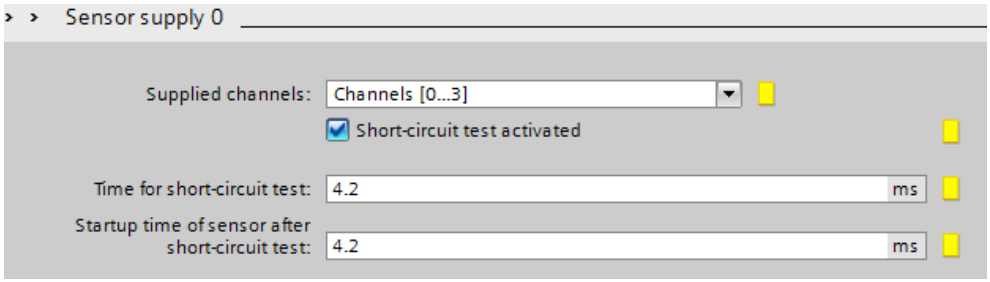
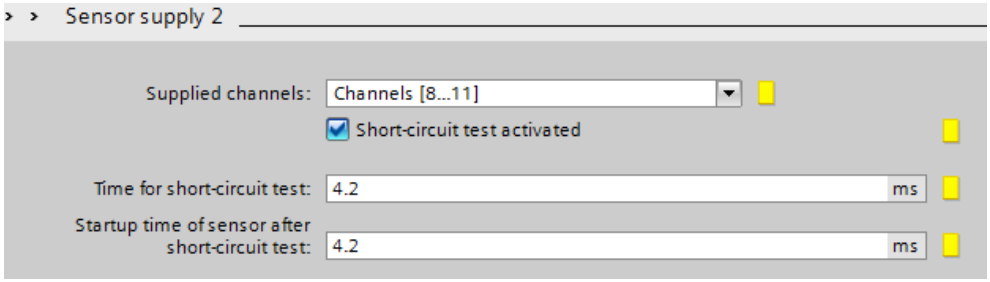


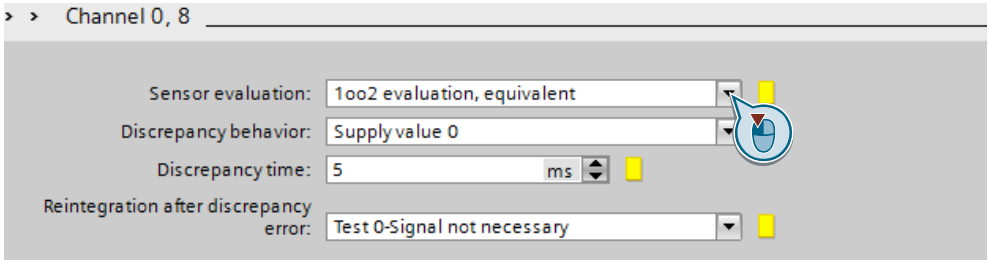
Figure 2-3: Activating the short-circuit test for sensor supply 2



Channel parameters

The monitoring of the emergency stop is via the channel pair 0, 8. In order to detect discrepancies between the two channels and to therefore achieve the demanded safety level set the evaluation of the sensor to "1oo2 evaluation, equivalent”.

Figure 2-4: Channel parameters emergency stop



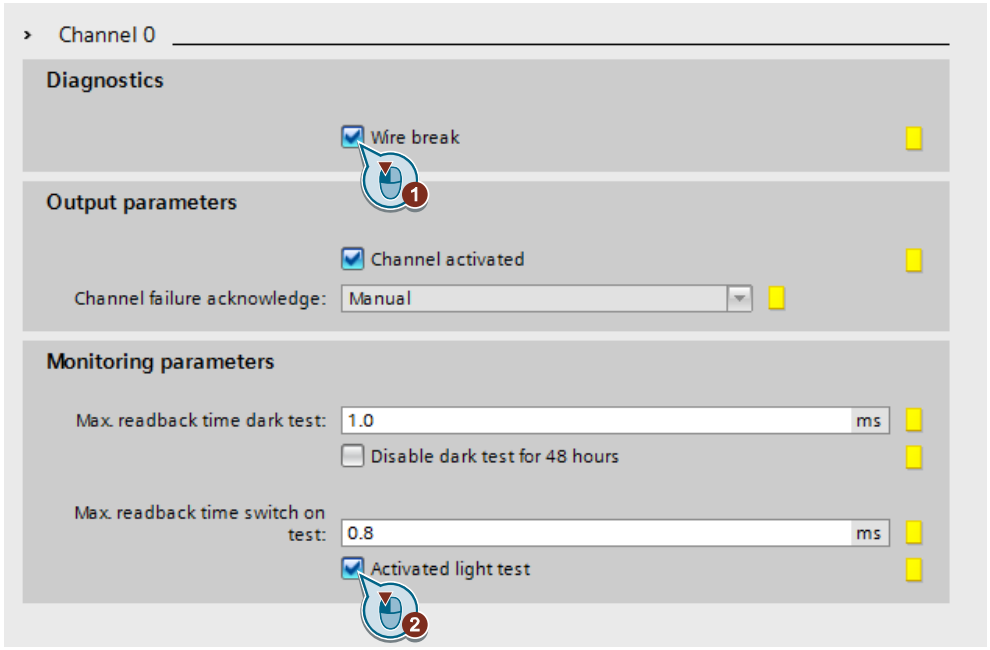
NOTE Set the discrepancy time as short as possible, so that no discrepancy fault is detected during error-free operation of the emergency stop command device.

2.2.2 Settings of the F-DQ

Channel parameters

Activate the wire break diagnostics and the light test.

Figure 2-5: Channel parameters contactors



2.3 Commissioning

2.3.1 Preparation

1. Download the "21064024_ESTOP_SIL3_1500F_PROJ_V50.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.

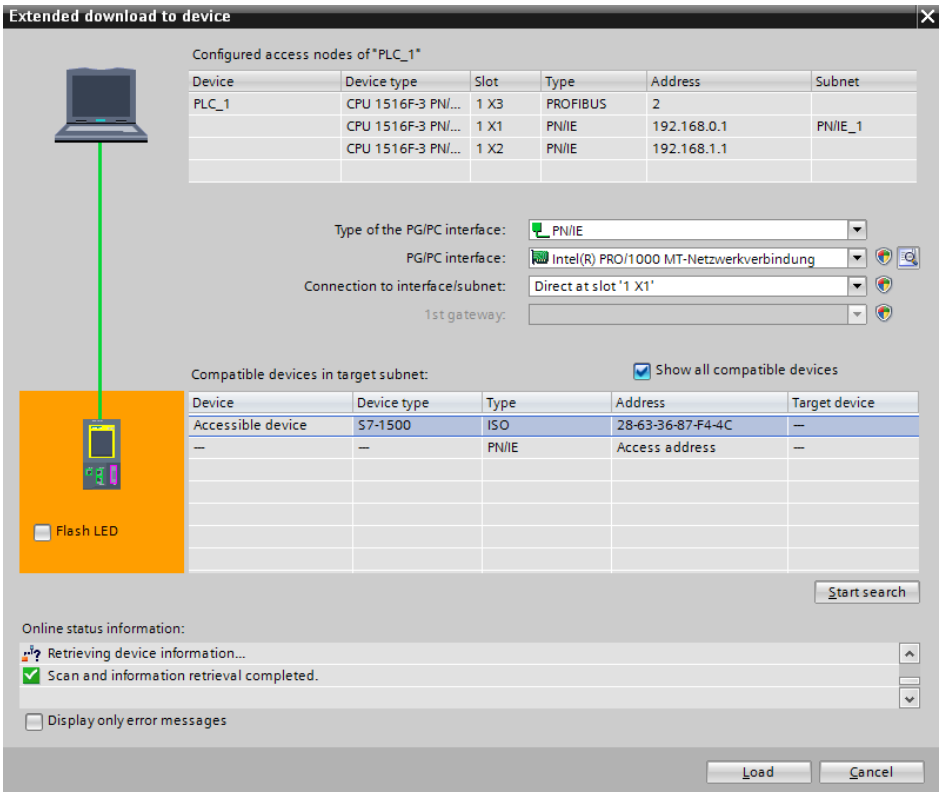
For this application example, the following IP address is used:

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 V14”
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 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 next dialog by clicking "Load”.
10. Click "Finish” when the loading process is completed.

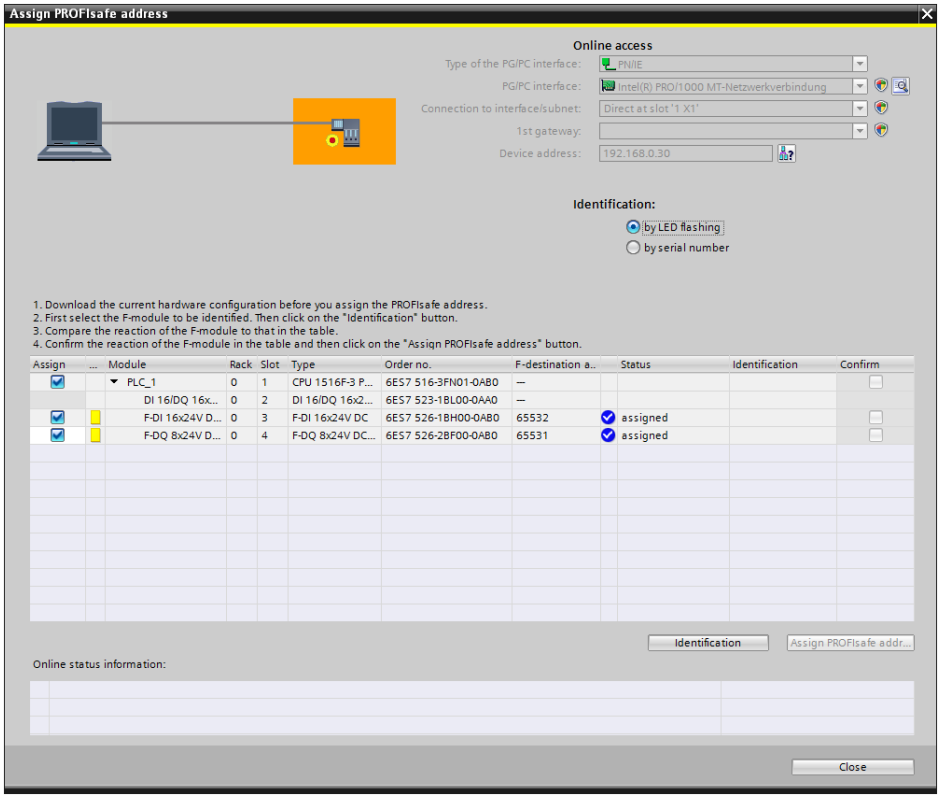
2.3.3 Assigning the PROFIsafe addresses

In order to establish safe communication between the F-CPU and the fail-safe modules, the modules have to be assigned PROFIsafe addresses.

Note Since the PROFIsafe address is saved in the electronic coding element, the following steps are only required if the coding element has not previously been assigned or has been assigned another PROFIsafe 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, enable the "Confirm” checkbox.
5. Then click the "Assign PROFIsafe 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. You can then close the window.

Note All red LEDs of the F modules should go out after assigning the PROFIsafe address. If this is not the case, there may be an error in the wiring.

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

2.4 Operating the Application

The table below demonstrates the function principle:

Table 2-1: Operating instruction

No.	Action	Result / Note
1	Press the acknowledge button	Acknowledgement
2	Press the start button	Contactors are switched on
3	Press the stop button	Contactors are switched off
4	Press the start button	Contactors are switched on
5	Press the emergency stop	Contactors are switched off
6	Unlock the emergency stop	
7	Repeat actions 1 and 2	Contactors are switched on

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 normally-closed contact is faulty (second error).

Feedback circuit

A feedback circuit is used for the monitoring of controlled actuators (e.g. relay or power 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 normally-closed and normally-open 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, it is necessary for the safety-relevant parts of the protective equipment and command devices to function correctly and that they behave in a way that the plant stays in a safe state or is brought to a safe state in the event of an error.

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

- avoidance of systematic faults
- control of systematic faults
- managing accidental errors 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. This expressed in the standards through different terms:

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

More information on function safety can be found in \8\.

3.1.3 Emergency stop

The emergency stop command device is a widely used component to protect personnel, plants and the environment from hazards and to initiate a standstill in the event of an emergency. This chapter describes applications with safety functions from exactly this range of application.

Facilities, functional aspects and general principles for design of the emergency stop are documented in EN ISO 13850. Additionally, the standard EN 60204-1 must also be observed.

Typical applications

The emergency stop command device with its positive opening contacts is monitored by an evaluation unit. If the emergency stop is pressed, the evaluation unit safely switches off the actuators according to stop category 0 in accordance with EN 60204-1. Before switching back on or acknowledging the emergency stop, it is checked whether the contacts of emergency stop command device are closed and the actuators are switched off.

Note Emergency stop is not a means of risk reduction. Emergency stop is an "additional safety function” (if the "emergency stop” has to be pressed, the motor must be switched off).

Unintentional actuation

It is often required that an emergency stop command device has to be protected from unintentional actuation and therefore to increase plant availability. The first step is the correct placement of the emergency stop command device on the machine. The emergency stop command device has to be easily accessible, easily reachable and safe to press.

In addition, there is the option to use a protective collar to protect from unintentional actuation. It also has to be made sure that easy accessibility is guaranteed.

Note

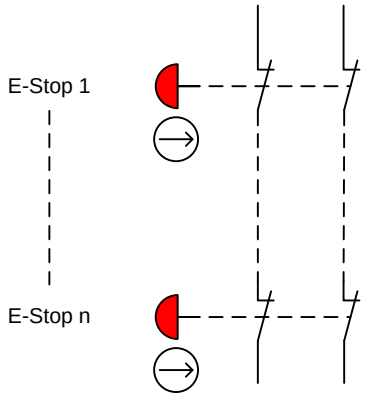
SIEMENS SIRIUS emergency stop command devices with protective collar correspond to the requirements of EN ISO 13850 "Safety of machinery - Emergency stop - Principles for design".

So far, no particular requirements exist for the protective collar, since they are not mentioned explicitly in any standard on functional safety. It is often at the discretion of the third-party expert to accept them for a certain machine.

Conditions for series connection

Up to PL e (according to ISO 13849-1) or SIL 3 (according to IEC 62061) emergency stop command devices may only be connected in series if the failure and the simultaneous pressing of the emergency stop command devices can be excluded. For further information please refer to \9\.

Figure 3-1: Series connection of emergency stops



If several emergency stop command devices are electrically connected in series, each fail-safe switch off via an emergency stop command device represents an individual supplementary safety function. If identical emergency stop command devices are used, it is sufficient to look at one additional safety function, as an example and representative for all additional safety functions. For further information please refer to \6\.

3.2 Evaluation of the Safety Function

3.2.1 Standards

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

Table 3-1: Versions

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

3.2.2 Safety function

Preliminary remarks

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

Supplementary safety function

For the following considerations are based on the supplementary safety function below:

Table 3-2: Definition of the safety function

Safety function	Description
SF1	If the emergency stop is pressed, the machine has to safely switch off.

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

3.2.3 Evaluation according to ISO 13849-1

Below, an evaluation according to ISO 13849-1 is carried out with the Safety Evaluation Tool (SET). For the link to the SET, refer to the Internet in \4\.

Evaluation of "Detection"

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

Table 3-3: Parameters of subsystem "Detection"

Parameter	Value	Explanation	Definition
B10 B10 value Emergency stop command device	100.000	Manufacturer information	SIEMENS AG
Percentage of dangerous failures Emergency stop command device	0.2 (20%)	Manufacturer information	
T1 Lifetime	175,200 h (20 years)	Manufacturer information	
Architecture	Category 4	2 channels, 1 component	User
Actuations/ test interval	1/week	Assumption	
CCF measures (points) Susceptibility to common cause failures	≥ 65	Sufficient measures against CCF according to ISO 13849-1 table F.1 have to be provided	
DC Diagnostic coverage	≥ 0.99 (99%)	Cross-comparison in F-DI	

Table 3-4: Result of subsystem "Detection"

PFH_D	PL achieved
$2.47 \cdot 10^{-8}$	PL e

Evaluation of "Evaluation"

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

Table 3-5: 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-DI	$1.00 \cdot 10^{-9}$	PL e	
ET 200MP F-DQ	$2.00 \cdot 10^{-9}$	PL e	
Total	$\mathbf{5.00 \cdot 10^{-9}}$	**PL e**	

Evaluation of "Reaction"

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

Table 3-6: Parameters of subsystem "Reaction"

Parameter	Value	Explanation	Definition
B10 B10 value Contactor	1.000.000	Manufacturer information	SIEMENS AG
Percentage of dangerous failures Contactor	0.73 (73%)	Manufacturer information	
T1 Lifetime	175,000 h (20 years)	Manufacturer information	
Architecture	Category 4	2 channels, 2 components	User
Actuations/ test interval	1/h	Assumption	
CCF measures (points) Susceptibility to common cause failures	≥ 65	Sufficient measures against CCF according to ISO 13849-1 table F.1 have to be provided	
DC Diagnostic coverage	≥ 0.99 (99%)	Redundant switch-off path and dynamic monitoring of the contactors	

Table 3-7: Result of subsystem "Reaction"

PFH_D	PL achieved
$2.47 \cdot 10^{-8}$	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	$2.47 \cdot 10^{-8}$	PL e
Evaluation	$5.00 \cdot 10^{-9}$	PL e
Reaction	$2.47 \cdot 10^{-8}$	PL e
Total	$\mathbf{5.44 \cdot 10^{-8}}$	**PL e**
	PL e	

3.2.4 Evaluation according to IEC 62061

Below, the evaluation according to IEC 62061 is carried out with the Safety Evaluation Tool (SET). For the link to the SET, refer to the Internet in \4\.

Evaluation of "Detection"

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

Table 3-9: Parameters of subsystem "Detection"

Parameter	Value	Explanation	Definition
B10 B10 value Emergency stop command device	100.000	Manufacturer information	SIEMENS AG
Percentage of dangerous failures Emergency stop command device	0.2 (20%)	Manufacturer information	
T1 Lifetime	175,200 h (20 years)	Manufacturer information	
Subsystem architecture	D	2 channels, 1 component: Single fault tolerance with diagnostic function	User
Actuations/ test interval	1/week	Assumption	
β **(CCF factor)** Susceptibility to common cause failures	0.1 (10%)	For installations according to IEC 62061, a CCF factor of 0.1 (10%) is achieved.	
DC Diagnostic coverage	≥ 0.99 (99%)	Cross-comparison in F-DI	

Table 3-10: Result of subsystem "Detection"

PFH_D	SILCL achieved
$1.19 \cdot 10^{-10}$	SILCL 3

Evaluation of "Evaluation"

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

Table 3-11: Evaluation of subsystem "Evaluation"

Component	PFH_D	SILCL	Definition
CPU 1516F-3PN/DP incl. PROFIsafe	$2.00 \cdot 10^{-9}$	SILCL 3	SIEMENS AG
F-DI of the ET 200SP	$1.00 \cdot 10^{-9}$	SILCL 3	
F-DQ of the ET 200SP	$2.00 \cdot 10^{-9}$	SILCL 3	
Total	$\mathbf{5.00 \cdot 10^{-9}}$	**SILCL 3**	

Evaluation of "Reaction"

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

Table 3-12: Parameters of subsystem "Reaction"

Parameter	Value	Explanation	Definition
B10 B10 value Contactor	1.000.000	Manufacturer information	SIEMENS AG
Percentage of dangerous failures Contactor	0.73 (73%)	Manufacturer information	
T1 Lifetime	175,000 h (20 years)	Manufacturer information	
Subsystem architecture	D	2 channels, 2 components: Single fault tolerance with diagnostic function	User
Actuations/ test interval	1/h	Assumption	
β **(CCF factor)** Susceptibility to common cause failures	0.1 (10%)	For installations according to IEC 62061, a CCF factor of 0.1 (10%) is achieved.	
DC Diagnostic coverage	≥ 0.99 (99%)	Redundant switch-off path and dynamic monitoring of the contactors	

Table 3-13: Result of subsystem "Reaction"

PFH_D	SILCL achieved
$7.30 \cdot 10^{-9}$	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	$1.19 \cdot 10^{-10}$	SILCL 3
Evaluation	$5.00 \cdot 10^{-9}$	SILCL 3
Reaction	$7.30 \cdot 10^{-9}$	SILCL 3
Total	$\mathbf{1.24 \cdot 10^{-8}}$	**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:
www.siemens.com/industry/supportrequest

Service offer

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

- Product Training
- Plant Data Services
- Spare Parts Services
- Repair Services
- On Site and 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 Apple iOS, Android and Windows Phone.
https://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/21064024
\3\	Application example "feedback circuit” https://support.industry.siemens.com/cs/ww/en/view/21331098
\4\	Safety Evaluation Tool (SET) http://siemens.com/safety-evaluation-tool
\5\	SIMATIC Safety - Configuring and Programming https://support.industry.siemens.com/cs/ww/en/view/54110126
\6\	Series connection of several emergency stop command devices https://support.industry.siemens.com/cs/ww/en/view/35444028
\7\	Migrating a safety program to TIA Portal https://support.industry.siemens.com/cs/ww/en/view/109475826
\8\	Functional Safety at Siemens www.siemens.de/safety-integrated
\9\	Define of Diagnostic Coverage for subsystem with electromechanical components https://support.industry.siemens.com/cs/ww/en/view/35444114

4.3 Change documentation

Table 4-2: Change documentation

Version	Date	Modifications
V1.0	02/2005	First version
V2.0	09/2007	Updating the contents regarding: • Hardware and software • Performance data • Screenshots
		New chapter: • Evaluating the function example according to the new standards EN 62061 and EN ISO 13849-1:2006.
V3.0	01/2015	Migration of STEP 7 V5.4 with Distributed Safety to TIA Portal (STEP 7 Professional V13 with STEP 7 Safety V13)
V4.0	07/2015	• Publication of migration instruction as independent application example • Replacement of the light indicator to simulate the actuators against two contactors • Supplement of the evaluation of the safety function by the "Reaction” subsystem
V5.0	01/2017	• Upgrade to TIA Portal V14 • Replacement of decentral periphery with central modules