SIEMENS

Industrial Controls

SIRIUS Safety Integrated

Application Manual

Edition 10/2014

Answers for industry.

SIEMENS

Industrial Controls

SIRIUS
Safety Integrated Application Manual

Application manual

10/2014

A5E03752040020A/RS-AC/003

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

3ZX1012-0SK11-1AC1
℗ 10/2014 Subject to change

Table of contents

Introduction 1

Purpose of the documentation

This documentation provides an insight into the fundamental safety requirements in the manufacturing industry. Using the SIRIUS Safety Integrated products, the documentation shows you simple example circuits for safety functions from the application areas:

- Stopping in an emergency
- Protective door monitoring
- Speed/standstill monitoring
- Monitoring of open danger zones
- Safe operator input
- Typical combinations of safety functions

Following the simple example circuits, you will find detailed background information on regulations and standards, as well as the specification and design of safety-related controller parts.

Target group

This documentation contains information for the following target groups:

- Decision makers
- Technologists
- Configuration engineers

Required knowledge

A general knowledge of the following areas is needed in order to understand this documentation:

- Low-voltage controls and distribution
- Digital circuit logic
- Automation technology

Warranty and liability

Note

The application examples are non-binding and do not claim to be complete in terms of configuration and equipment or to take account of any other contingencies. The application examples do not represent specific customer solutions; they are intended only as support for typical tasks. The user has sole responsibility for ensuring correct operation of the products described. These application examples do not exempt the user from their due diligence obligation with regard to application, installation, operation and maintenance. We reserve the right to make changes to these application examples at any time and without prior notice. In the case of deviations between the recommendations in this information and other Siemens publications, such as catalogs, the contents of the other documentation have priority.

We give no guarantee that the information contained in this document is complete, accurate, or up-to-date.

We assume no liability, irrespective of the legal basis, for any damage arising from the use of the examples, instructions, programs, configuring and performance data, etc., in this application example.

This exclusion does not apply in cases of intentional or negligent loss of life, physical injury or damage to health, or any other damage if these are the result of intentional or grossly negligent misconduct.

Any form of duplication of these application examples or excerpts hereof is not permitted without the express consent of Siemens Industry Sector.

History

The following versions of this documentation have been released to date. The changes apply to the previous version:

Edition	Comment / change
09/2013	Initial release
10/2013	Small editorial improvements, defective Web links repaired
03/2014	Integration of additional application examples, content expansions, and corrections
09/2014	Supplements and corrections to the contents

Safety systems - General information 2

2.1 Basic terminology

Redundancy

With redundancy, more than one component is implemented for the same function, so the function of a faulty component is performed instead by the other component(s). A redundant configuration reduces the probability of a function failing due to a single defective component. This requirement is necessary for achieving Safety Integrity Level SILCL 3 per IEC 62061, SIL 3 per IEC 61508 and PL e per ISO 13849-1 (also necessary for SIL 2 / PL d under certain circumstances).

The simplest form of redundancy is two-channel redundancy. If a circuit fails, two-channel redundancy ensures that the safety function is maintained. In a redundant system configuration, the subsystems for detecting and reacting must also be implemented with two-channel redundancy.

Note

All SIRIUS Safety devices that comply with SILCL 3 per IEC 62061, SIL 3 per IEC 61508 and PL e per ISO 13849-1 are redundantly configured with regard to the internal logic as well as with regard to the output circuits.

Cross-circuit detection

Cross-circuit detection is a diagnostic function of an evaluation unit that detects short-circuits and cross-circuits between the input channels (sensor circuits) during two-channel detecting or reading. A cross-circuit can be caused, for example, by a cable casing being squashed. In devices without cross-circuit detection, this can mean that a two-channel emergency stop circuit does not trip even though only one NC contact is faulty (secondary error).

Enabling circuit

An enabling circuit provides a safety-related output signal. From an external viewpoint, enabling circuits usually act as NO contacts (however, in terms of functionality, safety-oriented opening is always the most important aspect). An individual enabling circuit that is redundantly configured internally in the safety relay can be used for SIL 3 / PL e. Note: Enabling current paths can also be used for signaling purposes.

Feedback circuit

A feedback circuit is used to monitor controlled actuators (e.g. relays or load contactors) with positively driven contacts or mirror contacts. The enabling circuits can only be activated with the feedback circuit closed.

When using a redundant shutdown path, the feedback circuit of both actuators must be evaluated. These may also be connected in series.

Automatic start

For an automatic start, the device is started without manual confirmation, but only after the input image has been checked and a positive test of the evaluation unit has been conducted. This function is also known as dynamic operation and is not permissible for emergency stop devices. Safety devices for prohibited danger zones (e.g. position switches, light arrays, safety mats) can use the automatic start function if this does not pose any risk.

Monitored start

For a monitored start, machine operation is initiated by actuating the the Start button, but only after the input image has been checked and a positive test of the evaluation unit has been conducted. The monitored start evaluates the signal change of the Start button. This means that the Start button cannot be manipulated/tampered with (misuse). For PL e (ISO 13849-1) as well as SIL 3 (IEC 62061), the monitored start must be used in the case of emergency stop. For other safety sensors/functions, the necessity for a monitored start command depends on the risk assessment.

Manual start

For a manual start, device operation is initiated by operating the Start button, but only after the input image has been checked and a positive test of the safety relay has been conducted. On a manual start, the Start button is not monitored for correct functioning. A positive edge of the Start button is sufficient for starting.

Note

Manual start is not permitted for emergency stop devices.

Two-hand operation / synchronism

Synchronous sensor operation is a special form of simultaneity of sensors. In this case, it is not sufficient for sensor contacts 1 and 2 to be switched to the closed state at different times. Instead, they must be closed within 0.5 seconds. Synchronism of sensors is required, in particular, in the case of two-hand operation of presses. This ensures that the presses only become active when the sensors are operated simultaneously with both hands. This minimizes the risk of the operator getting a hand in the press.

Positive opening operation

Positive-opening switches are designed in such a way that actuation of the switch always results in opening of the contacts. Welded contacts are opened by actuation (EN 60947-5-1).

Positively-driven contacts

A component with positively-driven contacts guarantees that the NC and NO contacts are never closed simultaneously (EN 60947-5-1).

Mirror contacts

A mirror contact is an NC contact that is guaranteed not to be closed at the same time as a main contact (EN 60947-4-1).

2.2 General Information

This chapter contains general and overall information on the topic of safety systems.

Details of regulations and standards, as well as the specification and design of safety-related parts of controllers, can be found at the end of the manual.

2.2.1 The objective of safety systems

The objective of safety systems is to keep potential hazards for both people and the environment as low as possible by means of design measures and suitable technical equipment, without restricting, more than absolutely necessary, industrial production, the use of machines and the production of chemical products. The protection of man and environment has to be put on an equal footing in all countries by applying rules and regulations that have been internationally harmonized. At the same time, the distortion of competition due to differing safety requirements in international trade are to be avoided.

2.2.2 Local legislation

The most important thing for machine manufacturers and plant builders is that the legislation and regulations in the country where the machine or plant is being operated always apply. For instance, the control system of a machine that is to be used in the US must fulfill the local US requirements even if the machine manufacturer (OEM) is based in Europe. Although the technical concepts with which safety is achieved are subject to the rules of technology, it is nevertheless important to note whether any legal specifications or restrictions apply.

2.2.3 Functional safety

From the perspective of the object to be protected, safety is indivisible. The causes of danger and also the technical measures to avoid them can vary widely. This is the reason that a differentiation is made between various types of safety, e.g. by specifying the particular cause of a potential hazard. Thus we speak of "electrical safety" when protection against hazards is to be implemented by electrical means, or "functional safety" when safety depends on correct functioning.

To ensure the functional safety of a machine or plant, the safety-related parts of the protection and control devices must function correctly. In addition, the systems must behave in such a way that either the plant remains in a safe state, or it is put into a safe state if a fault occurs.

In this case, it is necessary to use specially qualified technology that fulfills the requirements described in the relevant standards. The requirements for achieving functional safety are based on the following basic goals:

- Avoiding systematic faults
- Controlling systematic faults
- Controlling random faults or failures

The measure for the achieved functional safety is the probability of dangerous failures, the fault tolerance and the quality that is to be guaranteed as a result of freedom from systematic faults. It is expressed in the standards using different terms:

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

2.2.4 Objective of the standards

Manufacturers and operators of technical equipment and products are responsible for safety. This means that plants, machines, and other technical equipment must be made as safe as possible in accordance with the current state of the art. To ensure this, companies describe in the various standards the current state of the art regarding all aspects relevant to safety. Observance of the relevant standards ensures that state-of-the-art technology has been utilized and thus the plant builder or machine/device manufacturer has fulfilled his duty of care.

You can find details of regulations and standards in the chapter Regulations and Standards (Page 123).

Note

No claim to completeness

The standards, directives and legislation listed in this manual represent a selection to communicate the essential goals and principles. This list does not claim to be complete.

2.2.5 Safety-related functions

Safety-related functions encompass classic and more complex functions.

Classic functions:

- Stopping
- Procedures in an emergency situation
- Preventing unintentional start-up

More complex functions:

- Status-dependent interlocks
- Velocity limiting
- Position limiting
- Controlled stop
- Controlled holding (stopping the machine but maintaining power), and others

2.2.6 Stopping

Stopping (stop categories of EN 60204-1)

EN 60204-1 (VDE 0113 Part 1) defines three stop categories for stopping a machine. These describe the control sequence for stopping independently of any emergency situation:

Stop category	Description
0	Uncontrolled stopping by immediately switching off the power to the machine's drive elements
1	Controlled stopping; the power feed is only interrupted when the motor has come to a standstill.
2	Controlled stopping where the energy feed is still maintained even at standstill.

Note

Switching off only interrupts the energy feed that can cause the movement. Disconnection from the energy source does not take place.

2.2.7 Procedure in an emergency situation

EN 60204-1 / 11.98 has established and defined possible procedures for emergencies (EN 60204-1 Annex D). The terms in brackets correspond to implementation in the final draft of Edition 5.0 of IEC 60204-1.

A procedure in an emergency includes the following individually or in combination:

- Emergency stop
- Emergency start
- Emergency switching off
- Emergency switching on

In accordance with EN 60204-1 and ISO 13850, these functions are initiated exclusively by deliberate human action. We will concentrate below on "emergency switching off" and "emergency stop" only. The latter is defined in the EU Machinery Directive. For simplicity, we will use the terms "emergency off" and "emergency stop" below.

2.2.8 Emergency off

This is an operation in an emergency that is intended to disconnect the electrical energy to a complete installation or part of an installation if there is a risk of electric shock or another risk having an electrical cause (from EN 60204-1 Annex D).

Functional aspects for switching off in an emergency are defined in IEC 60364-4-46 (identical to HD 384-4-46 and VDE 0100 Part 460). Switching off in an emergency must be provided where

- protection against direct contact (e.g. with sliding contacts, slipring elements, switchgear in electrical operating areas) is only achieved by clearance or obstacles;
- There is a possibility of other hazards or damage caused by electrical energy.

The following still applies in 9.2.5.4.3 of EN 60204-1: Switching off in an emergency is achieved by shutting down the machine resulting in a Category 0 stop.

If Stop Category 0 is not permissible for a machine, it can be necessary to provide another form of protection, e.g. against direct contact, so that switching off in an emergency is not necessary.

This means the emergency off is only to be used where the risk analysis identifies a hazard from electrical voltage / energy requiring immediate and full disconnection of the electrical voltage.

2.2.9 Emergency stop

An emergency operation intended to stop a process or movement that has become hazardous (from EN 60204-1 Annex D). The following still applies in 9.2.5.4.2 of EN 60204-1:

In addition to the requirements for stopping (see 9.2.5.3 of EN 60204-1), the following requirements apply for stopping in an emergency:

- It must take priority over all other functions and operations in all operating modes
- The power to the machine drive elements, which could result in a potentially hazardous condition or potentially hazardous conditions, must be disconnected as quickly as possible without creating other hazards (e.g. using mechanical stopping devices which do not require an external supply, using counter-current braking for stop Category 1).
- Resetting must not initiate restart.

Stopping in an emergency must have the effect of either a Category 0 stop or a Category 1 stop (see 9.2.2 of EN 60204-1). The category for stopping in an emergency must be defined using the risk assessment for the machine.

Devices for stopping in an emergency must be available at all operating workstations and other locations where stopping in an emergency can be necessary.

To comply with the safety objectives of EN 60204-1, the following requirements apply:

- When switching the contacts, even briefly, the command device must latch.
- It must not be possible for the machine to be restarted from a remote main console without first eliminating the hazard. The emergency stop device must be released locally in the form of a conscious operator action.

2.2.10 Safety function

A safety function describes the reaction of a machine/plant to the occurrence of a specific event (e.g. opening of a protective door). Execution of the safety function(s) is carried out by a safety-related control system. This usually comprises three subsystems: detecting, evaluating, reacting.

Detecting (sensors):

- Detecting a safety requirement, e.g.: Emergency stop or a sensor for monitoring a danger zone (light array, laser scanner, etc.) is actuated.

Evaluating (evaluation unit):

- Detection of a safety requirement and the safe initiation of the reaction (e.g. switching off the enabling circuits).
- Monitoring the correct operation of sensors and actuators.
- Initiating a reaction upon detection of faults.

Reacting (actuators):

- Shutdown of the hazard in accordance with the switching command of the evaluation unit.

2.2.11 Mode selector switches

Machines often have several operating modes that can be changed using a mode selector switch. Every machine must be designed in such a way that it is safe in every operating mode. Since the mode selector switch can only change between these safe operating modes protected by safety functions, the mode selector switch itself does not have to be safe by design or included in the calculation of these safety functions.

The mode selector switch must not itself trigger any machine operation. This must be done by means of a separate operator action.

If an operating mode requires a safety function to be revoked (e.g. for setup or maintenance purposes), the safety function must be replaced by another safety function in accordance with EN 60204-1 Chapter 9.2.4.

In this case, the recommendation is that the electrical design of the mode selector switch should be similar to the highest safety level of all operating modes. But here too, it is not included in the calculation of the safety functions.

In addition, there are special requirements regarding mode switching for specific machine types. These requirements are mentioned in the C standards for these machine types and must be applied.

See also

More detailed FAQs on the subject of mode selection (http://support.automation.siemens.com/WW/view/en/89260861)

2.2.12 Connection of actuators

Note

To achieve the performance level / safety integrity level given in the following examples, the actuators shown must be monitored in the feedback circuit of the corresponding safety relay.

Note

For capacitive and inductive loads, we recommend an adequate protective circuit. In this way, electromagnetic interference can be suppressed and contact service life increased.

Actuator wiring up to PL c per ISO 13849-1, or SILCL 1 per IEC 62061

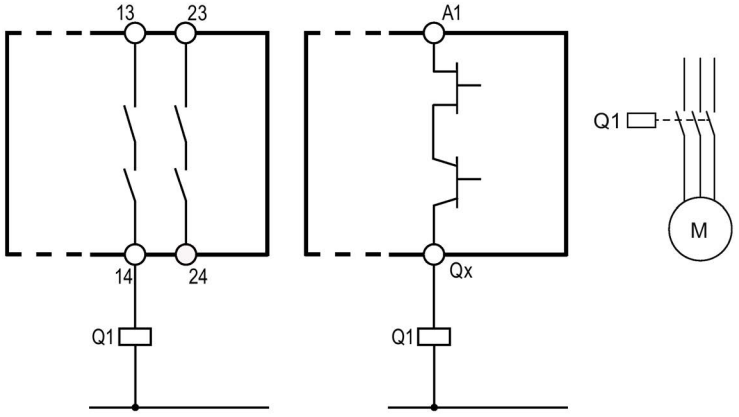


Figure 2-1 PL c per ISO 13849-1, or SILCL 1 per IEC 62061

Actuator wiring for protected laying up to PL e / Cat. 4 per ISO 13849-1, or SILCL 3 per IEC 62061

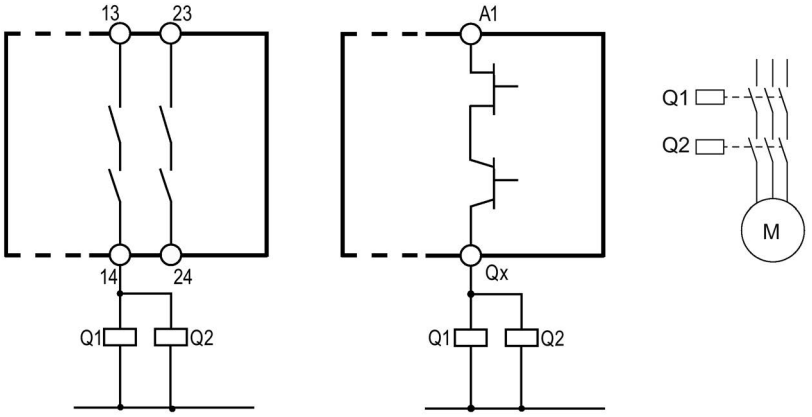


Figure 2-2 PL e per ISO 13849-1, or SILCL 3 per IEC 62061

⚠ WARNING

PL e per ISO 13849-1 or SILCL 3 per IEC 62061 can only be achieved with cross-circuit-proof/short-circuit to P-proof laying of the control cables from the relay output (e.g. 14) to the control relays/contactors (Q1 and Q2) (e.g. as a separately sheathed cable or in its own cable duct).

Some restrictions may apply with regard to the safety levels attainable in the individual controllers. Please refer to the specifications in the relevant device manuals.

Actuator wiring up to PL e per ISO 13849-1, or SILCL 3 per IEC 62061

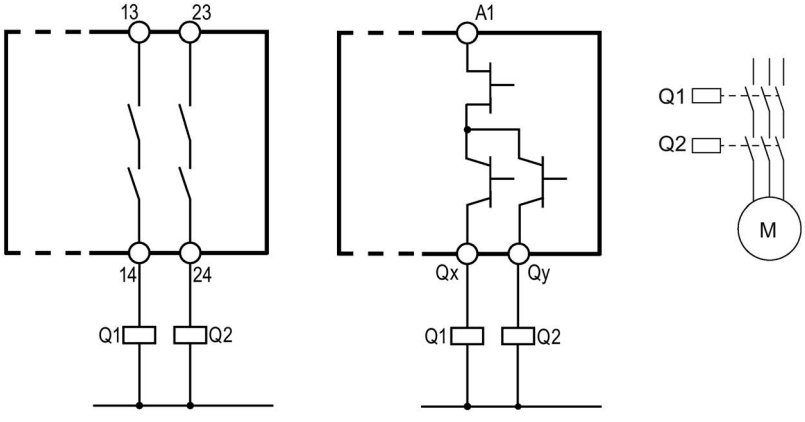


Figure 2-3 PL e per ISO 13849-1, or SILCL 3 per IEC 62061

2.2.13 Series connection of sensors

Series connection of emergency stop command devices

It is possible to connect emergency stop command devices in series up to the highest safety level (SILCL 3 per IEC 62061, SIL 3 per IEC 61508 and PL e per ISO 13849-1), because it is assumed that only one emergency stop is operated at a time. This ensures that errors and defects can be detected. See the "Stopping in an emergency" section - Introduction (Page 26).

Series connection of position switches

In general, position switches may be connected in series if measures ensure that multiple protective doors are not regularly opened simultaneously (otherwise a fault cannot be detected)

However, for safety level SILCL 3 per IEC 62061, SIL 3 per IEC 61508, and PL e per ISO 13849-1, they must never be connected in series, because every dangerous fault must be detected (independently of the operating personnel).

See the "Protective door monitoring" section - Introduction (Page 44).

Series connection of an emergency stop command device and a protective door monitor

In general, an emergency stop command device and a position switch may be connected in series if measures ensure that the two are not regularly opened/operated simultaneously (otherwise a fault cannot be detected).
However, for safety level SILCL 3 per IEC 62061, SIL 3 per IEC 61508, and PL e per ISO 13849-1, they must never be connected in series, because every dangerous fault must be detected (independently of the operating personnel).

See the chapter "Typical combinations of safety functions" - Introduction (Page 110).

Application examples

3

3.1 Introduction

People working near machinery (e.g. in the manufacturing industry) must be appropriately protected by means of technical equipment. This results in a host of safety functions designed to meet precisely this purpose. The implementation of some of the most essential safety functions is shown in the subsequent sections using easily understandable application examples. The examples are divided according to the type of safety function to be implemented:

- Stopping in an emergency
- Protective door monitoring
- Monitoring of open danger zones
- Speed/standstill monitoring
- Safe operator input
- Typical combinations of safety functions

Handling application examples

The application examples are easy to handle thanks to a uniform structure. The application is described briefly at the start of each example. This is followed with the design of the safety function using simple overview pictures.

Sensor signals and activation of the actuators are indicated by blue lines, while the feedback circuit for monitoring the actuators is represented by a broken line.

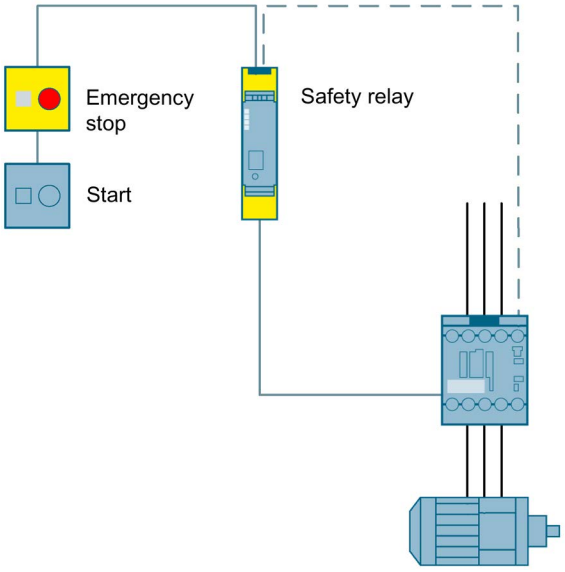
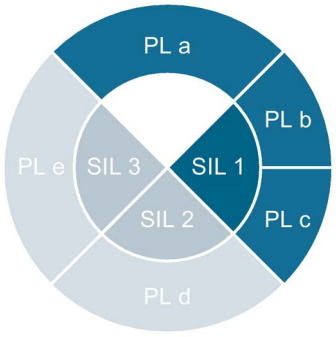
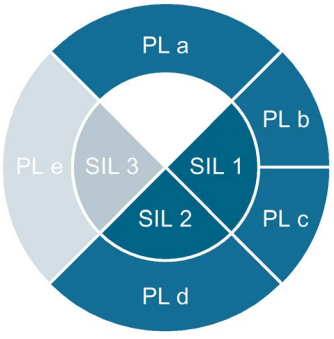
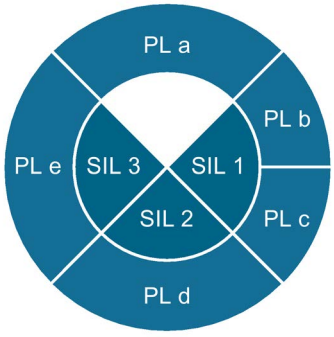


Figure 3-1 Example representation: Structure of a safety function

The precise functional principle is explained, as well as the maximum achievable safety level in SIL per IEC 62061 and PL per ISO 13849-1.

Representation of the maximum achievable safety level		
		
Suitability for up to SIL 1 / PL c	Suitability for up to SIL 2 / PL d	Suitability for up to SIL 3 / PL e

Some application examples contain several safety functions. The representation then describes the achieved safety level of the safety function given in the title. The achieved safety level of the additional safety functions is then explained in the text.

Note

The achieved safety level depends on the implementation of the application examples in each case. In particular, the assumptions made with regard to switching frequency or fault exclusions, for example, must be checked or observed.

The safety-related components used are listed for easy replication of the application.

The functions have been tested with the indicated hardware components. Other similar products not on this list can also be used. In this case, please note that changes in the wiring of the hardware components (e.g. different terminal assignment) may be necessary.

At the end of each example, there is an Internet link under which further information on the respective application example is stored. This encompasses, for example:

- Wiring diagrams
- The project files when using the modular safety system
- CAx data of the hardware components used

A detailed safety calculation with all key values can be found in the stored SET project file or the SET report. You must register (http://www.siemens.com/safety-evaluation-tool) to use the file.

You can conveniently download (http://www.siemens.com/cax) all the documentation on the hardware components used with just a few clicks at the CAx download link. This requires a Siemens Service & Support Portal or Siemens Industry Mall account.

The safety relays are parameterized using DIP switches. The relevant setting can be found in the circuit diagrams.

Note

Details of regulations and standards, as well as the specification and design of safety-related parts of controllers, can be found at the end of this manual.

3.2 Stopping in an emergency

3.2.1 Introduction

The emergency stop command device is a component that is widely used to protect people, equipment and the environment against possible hazards, and to initiate stopping in an emergency. This chapter describes applications with safety functions from precisely this application area.

Typical application

The emergency stop command device with its positive opening contact is monitored here using an evaluation unit. If emergency stop is actuated, the evaluation unit switches the downstream actuators off via safe outputs in accordance with Stop Category 0 per EN 60204-1. Before restarting or acknowledging the emergency stop switch-off by means of the Start button, a check is made as to whether the contacts of the emergency stop command device have been closed and the actuators switched off.

Note

- The sensor cables must be protected; only safety sensors with positive opening contacts must be used.
- Equipment, functional aspects and design guidelines for emergency stop are found in EN ISO 13850. The standard EN 60204-1 must also be observed.
- "Emergency stop" is not a way of reducing the risk.
- "Emergency stop" is a supplementary safety function. (When "emergency stop" is operated, the motor must be switched off.

Unintentional actuation

There is frequently a requirement to protect an emergency stop command device against unintentional actuation, and thus to enhance plant availability. The first step is to correctly position the emergency stop command device on the machine. The emergency stop command device must be easily accessible, free from obstruction and its actuation must not present a hazard. There is also the option of using a protective collar to prevent unintentional actuation. Here too, unhindered accessibility must be ensured.

Note

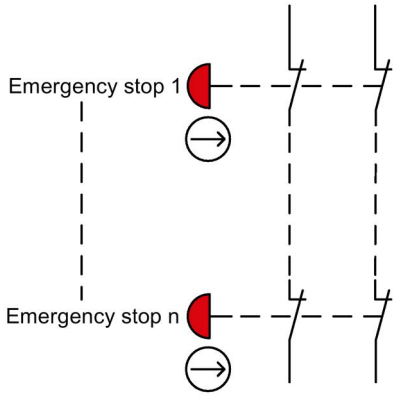
SIEMENS SIRIUS emergency stop command devices with protective collar correspond to the requirements of EN ISO 13850 "Safety of machinery. Emergency stop. Principles for design".

Special requirements for protective collars do not yet exist since these are not explicitly mentioned in any standard on functional safety. The acceptance of such collars for a specific machine is frequently at the discretion of the particular expert assessor.

Conditions in series connection

Up to PL e (per ISO 13849-1) or SIL 3 (per IEC 62061) emergency-stop command devices may only be connected in series if measures ensure that failure and simultaneous pressing of the emergency-stop command devices is not possible.

If multiple emergency stop command devices are electrically connected in series, each safety-related shutdown via an emergency stop command device is a single supplementary safety function. If identical emergency stop command devices are used, it is sufficient to regard one supplementary safety function as representing all supplementary safety functions.



See also

Explanation of series connection of emergency stop command devices (http://support.automation.siemens.com/WW/view/en/35444028)

3.2.2 Emergency stop shutdown to SIL 1 or PL c with a safety relay

Application

Single-channel emergency stop shutdown of a motor by a 3SK1 safety relay and a power contactor.

Design

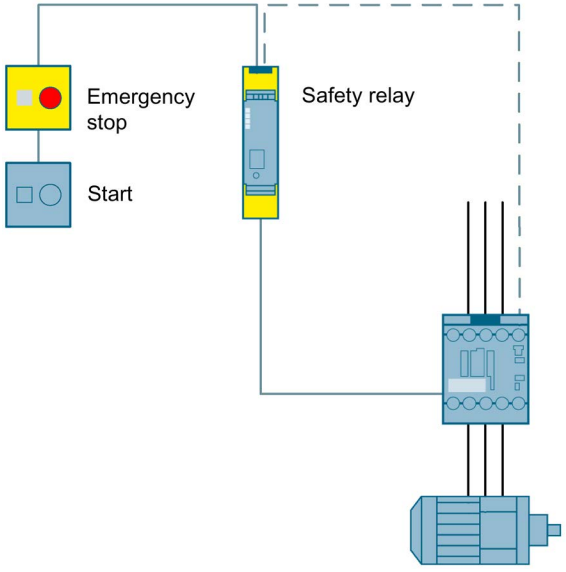
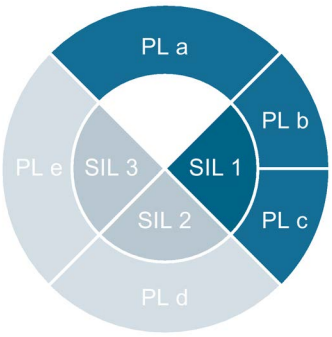


Figure 3-2 Emergency stop shutdown to SIL 1 or PL c with a safety relay

Operating principle

The safety relay monitors the emergency stop command device. When the emergency stop command device is actuated, the safety relay opens the enabling circuits and switches the power contactor off in a safety-related way. If the emergency stop command device is unlatched and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Emergency stop command device	Safety relay	Contactor
		
3SB3 (http://www.siemens.com/sirius-commanding)	3SK1 (http://www.siemens.com/safety-relays)	3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/73134129)

3.2.3 Emergency stop shutdown to SIL 1 or PL c with a Modular Safety System

Application

Single-channel emergency stop shutdown of a motor by a parameterizable 3RK3 Modular Safety System and a power contactor.

Design

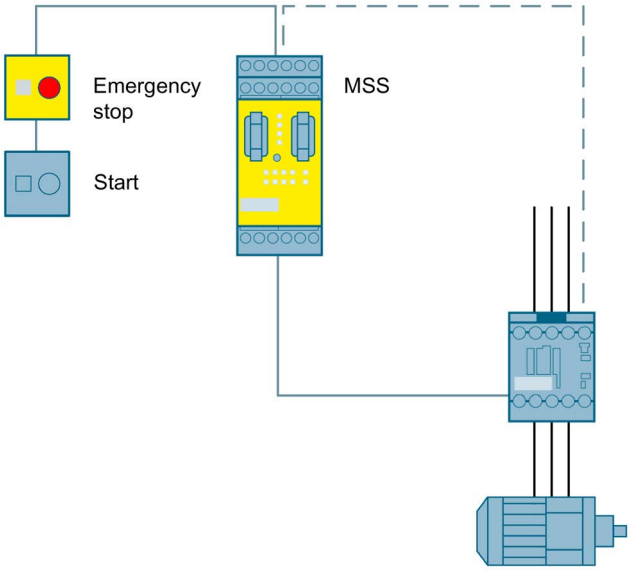
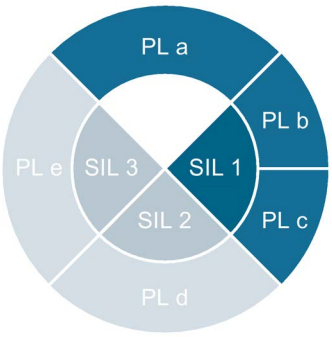


Figure 3-3 Emergency stop shutdown to SIL 1 or PL c with a Modular Safety System

Operating principle

The Modular Safety System monitors the emergency stop command device. When the emergency stop command device is actuated, the Modular Safety System opens the enabling circuits and switches the power contactor off in a safety-related manner. If the emergency stop command device is unlatched and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related component

Emergency stop command device	Modular Safety System	Contactor
		
3SB3 (http://www.siemens.com/sirius-commanding)	3RK3 (http://www.siemens.com/sirius-mss)	3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/69064058)

3.2.4 Emergency stop shutdown to SIL 3 or PL e with a safety relay

Application

Two-channel emergency stop shutdown of a motor by a 3SK1 safety relay and power contactors.

Design

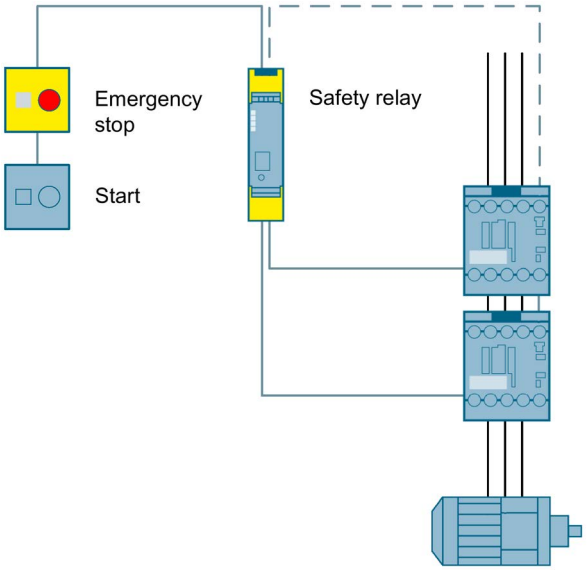
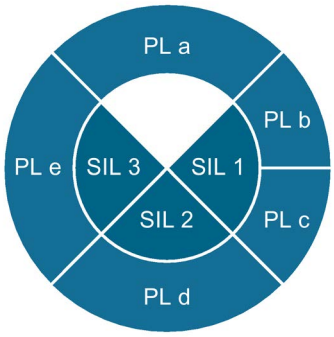


Figure 3-4 Emergency stop shutdown to SIL 3 or PL e with a safety relay

Operating principle

The safety relay monitors the emergency stop command device on two channels. When the emergency stop command device is actuated, the safety relay opens the enabling circuits and switches the power contactors off in a safety-related way. If the emergency stop command device is unlatched and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Emergency stop command device	Safety relay	Contactor
		
3SB3 (2-channel) (http://www.siemens.com/sirius-commanding)	3SK1 (http://www.siemens.com/safety-relays)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/73136378)

3.2.5 Emergency stop shutdown to SIL 3 or PL e with a Modular Safety System

Application

Two-channel emergency stop shutdown of a motor by a parameterizable 3RK3 Modular Safety System and power contactors.

Design

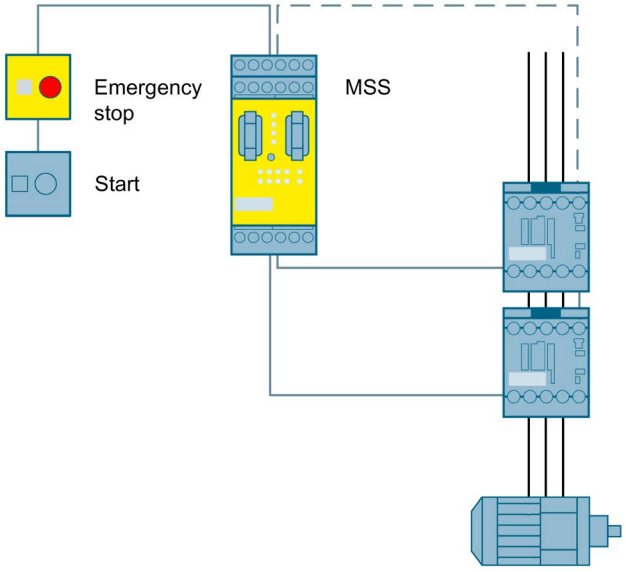
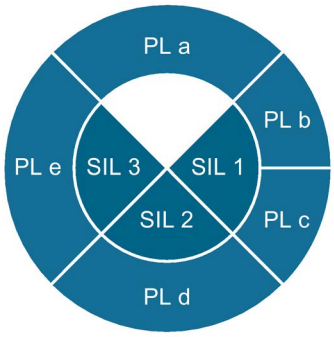


Figure 3-5 Emergency stop shutdown to SIL 3 or PL e with a modular safety system

Operating principle

The modular safety system monitors the emergency stop command device on two channels. When the emergency stop command device is actuated, the modular safety system opens the enabling circuits and switches the power contactors off in a safety-related way. If the emergency stop command device is unlatched and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Emergency stop command device	Modular safety system	Contactor
		
3SB3 (2-channel) (http://www.siemens.com/sirius-commanding)	3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/69064698)

3.2.6 Emergency stop shutdown to SIL 3 or PL e with fail-safe motor starters and a safety relay

Application

To be able to safely shut down a machine in an emergency, an emergency stop command device is attached and monitored by a safety relay. Safe shutdown takes place via fail-safe motor starters.

Design

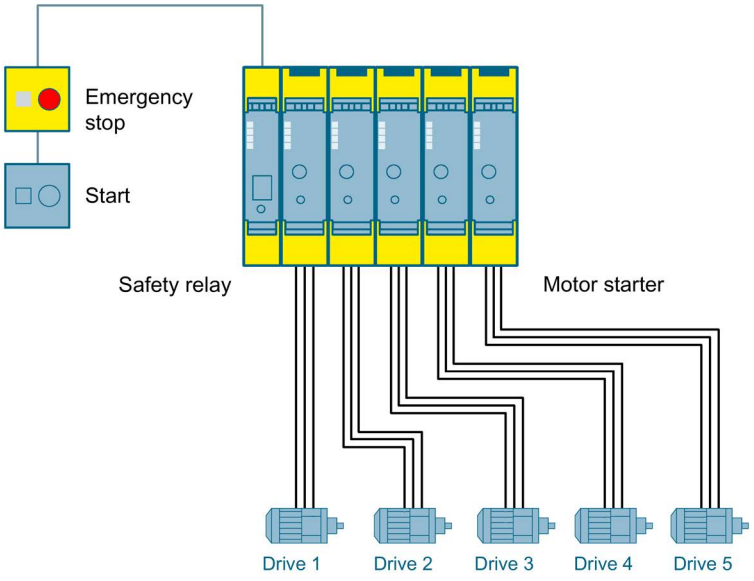
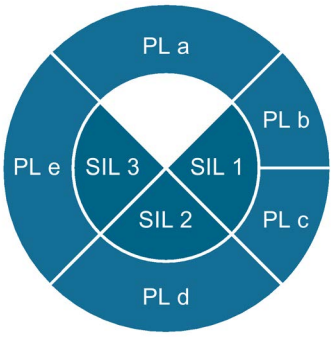


Figure 3-6 Emergency stop shutdown to SIL 3 or PL e with fail-safe motor starters and a safety relay

Operating principle

The safety relay monitors the emergency stop command device. When the emergency stop command device is actuated, the safety relay switches the fail-safe motor starters off via the device connectors. The motor starters then safely shut down the load. If the emergency stop command device is unlocked, the Start button can be used to switch on again.



Note

In this example, it is assumed that the hazard emanates from only one of the drives in each case, but that an emergency stop switches off a group of drives. For this reason, only a single motor starter is considered in the safety evaluation, and this is used as an example.

If the hazard emanates from the movement of several drives, all motor starters involved with this hazard must be taken into account in the safety evaluation.

Safety-related components

Emergency stop command device	Safety relay	Fail-safe motor starters
		
3SB3 (http://www.siemens.com/sirius-commanding)	3SK1 (http://www.siemens.com/safety-relays)	3RM1 (http://www.siemens.com/motorstarter/3rm1)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/88411471)

More detailed FAQs on: Safe shutdown with the 3RM1 motor starters
(http://support.automation.siemens.com/WW/view/en/67478946)

3.2.7 Emergency stop shutdown to SIL 3 or PL e with fail-safe motor starters and a modular safety system

Application

To be able to safely shut down a machine in an emergency, an emergency stop command device is attached and monitored by a modular safety system. Safe shutdown takes place via fail-safe motor starters.

Design

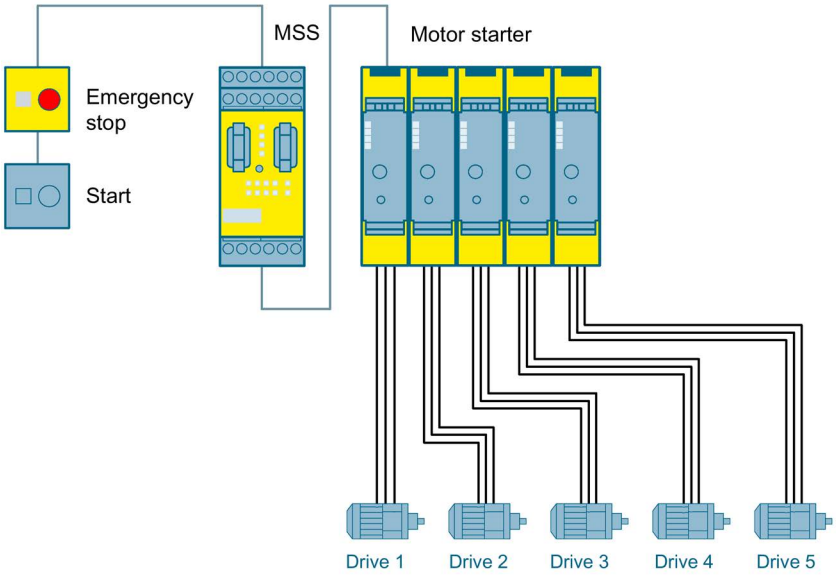
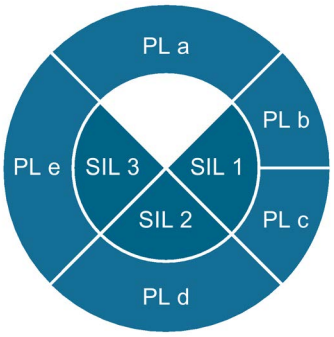


Figure 3-7 Emergency stop shutdown to SIL 3 or PL e with fail-safe motor starters and a modular safety system

Operating principle

The modular safety system monitors the emergency stop command device. When the emergency stop command device is actuated, the modular safety system switches the fail-safe motor starters off. The motor starters then safely shut down the load. If the emergency stop command device is unlocked, the Start button can be used to switch on again.



Note

In this example, it is assumed that the hazard emanates from only one of the drives in each case, but that an emergency stop switches off a group of drives. For this reason, only a single motor starter is considered in the safety evaluation, and this is used as an example.

If the hazard emanates from the movement of several drives, all motor starters involved with this hazard must be taken into account in the safety evaluation.

Note

This example applies to configurations within a control cabinet. If the logic components and the actuators are not located in the same control cabinet, other precautions must be taken, such as cross-circuit-proof laying of the shutdown signal.

Safety-related components

Emergency stop command device	Modular safety system	Fail-safe motor starters
		
3SB3 (http://www.siemens.com/sirius-commanding)	3RK3 (http://www.siemens.com/sirius-mss)	3RM1 (http://www.siemens.com/motorstarter/3rm1)

See also

Circuit diagram, MSS project and SET calculation
(http://support.automation.siemens.com/WW/view/en/88822643)

More detailed FAQs on: Safe shutdown with the 3RM1 motor starters
(http://support.automation.siemens.com/WW/view/en/67478946)

3.2.8 Emergency stop shutdown via AS-i to SIL 3 or PL e with a Modular Safety System

Application

Monitoring of multiple emergency stop command devices via AS-i with a 3RK3 Modular Safety System.

Design

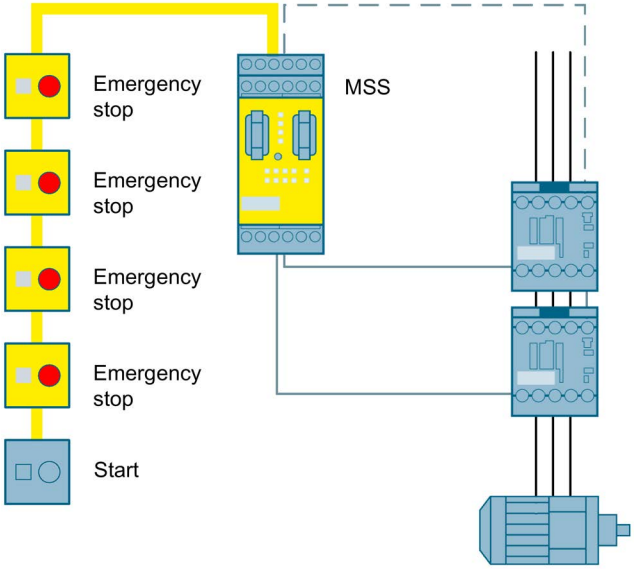
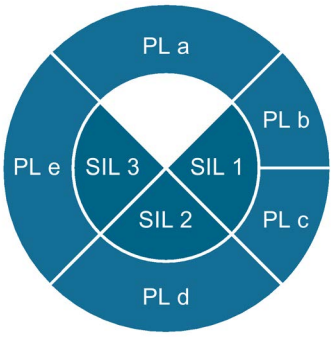


Figure 3-8 Emergency stop shutdown via AS-i to SIL 3 or PL e with a Modular Safety System

Operating principle

The Modular Safety System monitors each of the two-channel emergency stop command devices connected to AS-i. When one of the emergency stop command devices is actuated, the Modular Safety System opens the enabling circuits and switches the power contactors off in a safety-related way. If the emergency stop command device is unlatched and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Emergency stop command device	Modular Safety System	Contactor
		
3SB3 (2-channel) (http://www.siemens.com/sirius-commanding)	3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

Note

In addition to the safety-related components, operation of an AS-i network requires an AS-i master and an AS-i power supply.

See also

MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/73133559)

3.3 Protective door monitoring

3.3.1 Introduction

This section describes applications with separating protective devices in the form of a protective door. The most frequently used solution in the area of plants and machinery is to protect danger zones by means of protective devices or access flaps which ensure mechanical separation. The aim here is to monitor unauthorized access to parts of a plant or equipment and to prevent dangerous machine functions when the protective device is not in the closed position. Protective equipment can be monitored both with mechanical position switches or safety switches, as well as with non-contact safety switches based on solenoid or RFID technology.

A tumbler is frequently also implemented in conjunction with protective door monitoring. Interlocking devices with a tumbler are used to protect danger zones against undesired entry. There are usually two reasons for this:

1. To protect personnel against overtravel of dangerous machine movements, high temperatures, etc. ISO 14119 or EN 1088 provide guidelines for designing and selecting interlocking devices. These standards state that the danger zone must not be accessible until after the dangerous machine movement has been stopped.
2. A tumbler may be useful for reasons of process safety. This situation occurs when the hazard is stopped after opening the guard, but damage can occur to the machine or workpiece as a result. In this case, the machine is first moved to a controlled stop position before access is enabled.

Position switches

The position switches are normally used as positively operated switches on protective doors. If the protective door is opened, the position switch is actuated and the switch is reliably opened (see Basic terminology (Page 11): "Positive opening").

Mechanical safety switches (with separate actuator)

Unlike position switches, safety switches cannot simply be bypassed. The safety switch can only be operated with the associated coded actuator.

Mechanical safety switches (hinge switches)

Hinge switches are used in those areas where the position of swiveling protective devices such as doors or flaps must be monitored.

Mechanical safety switches (with tumbler)

Safety switches with tumblers are special safety engineering devices which prevent accidental or intentional opening of protective doors, guards or other covers while a dangerous state prevails. (e.g. overtravel of the machine). Independently of the tumbler, position detection is also implemented by means of this type of switch with the help of a separate actuator.

Non-contact safety switches (solenoid-operated switches)

Solenoid-operated switches comprise a coded solenoid and a switching element. They are intended for attachment to movable protective equipment. Their closed design makes them especially suitable for areas subject to heavy contamination, cleaning agents or disinfectants.

Non-contact safety switches (RFID)

RFID safety switches comprise a coded non-contact safety switch and an RFID actuator of the same design. They are extremely versatile, especially for use in areas subject to extreme environmental conditions. Their electronic operating principle also makes these switches ideal for metalworking machinery. The switches have a larger switching interval than mechanical switches, improve the mounting tolerance, and offer a wide range of diagnostics capabilities. They also offer maximum protection against tampering thanks to individual coding of switch and actuator.

Typical application

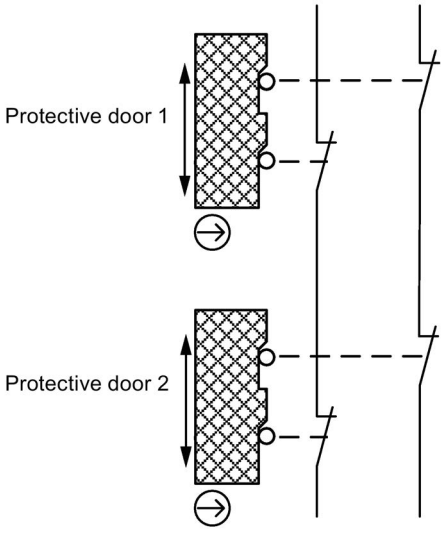
The protective door is monitored by an evaluation unit using SIRIUS position switches with positive opening contacts. If the protective door is opened, the evaluation unit switches the downstream actuators off via safe outputs in accordance with Stop Category 0 per EN 60204-1. If the protective door is closed, automatic starting takes place after the position switches and downstream contactors have been checked. In the case of manual start, this does not happen until the Start button is actuated.

Note

- Position switches are to be placed in such a position that they are not damaged when they are approached or passed. For this reason, it is not permissible to use them as a mechanical stop.
- Sensor cables must be protected; only safety sensors with positive opening contacts must be used.
- The tumbler represents a single, separate safety function alongside the safety function of the protective door monitor by means of position switches. The control can have a required safety integrity that is one stage lower than that resulting from the risk evaluation for the protective door monitor. (Reason: The probability that both safety functions will fail at the same time can be more or less ruled out. Example:
  The protective door monitor is required in PL d or SIL 2, tumbler control can be implemented in PL c or SIL 1

Conditions in series connection

Position switches may only be connected in series up to PL d (per ISO 13849-1) or SIL 2 (per IEC 62061) if it can be ensured that multiple protective doors will not be open simultaneously on a regular basis (otherwise faults could not be detected). Series connection in PL e (per ISO 13849-1) or SIL 3 (per IEC 62061) is not possible.



Possible combinations for position detection and achievable safety level

The application examples in this chapter can only cover a fraction of the possible combinations of detection units. However, the tables below show in a simple form the maximum safety level that can be achieved by a given method of position detection.

Table 3- 1 **Safe position monitoring with mechanical switches**

Evaluation units 			Position switches 	Safety switches, hinge switches 	Safety switches with separate actuator 	Safety switches with optional tumbler function 
Achievable safety level with ONE Position switches	**Monitoring an NC contact**		SIL 1 / PL c	SIL 1 / PL c	SIL 1 / PL c	SIL 1 / PL c
	Monitoring of 2 NC contacts or 1 NC contact + 1 NO contact		SIL 1 / PL c	SIL 2 / PL d	SIL 2 / PL d	SIL 2 / PL d
Achievable safety level with TWO position switches	Position switches		SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e
	Safety switches, hinge switches		SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e
	Safety switches with separate actuator		SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e
	Safety switches with optional tumbler function		SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e

Example 1:

A safety level of up to PL e or SIL 3 can be achieved by combining two mechanical safety switches (with separate actuator).

Example 2:

A safety level of up to PL d or SIL 2 can be achieved by using a mechanical safety switch (hinge switch).

Table 3- 2 Safe protective door tumbler

Safe evaluation units	Safety switches	
	Safety switches with tumbler 	Safety switches with tumbler 
 3RK3 Modular Safety System	SIL 2 / PL d	SIL 3 / PL e
 3TK2845 safety relay	SIL 2 / PL d	SIL 3 / PL e

Note

Generally, positive actuation by means of the design of the protective equipment must be ensured to use this position switch. The values listed in the table are only permissible under this condition.

Note

Taking account of certain fault exclusions (e.g. actuator breakage), use of just one hinge switch or a switch with separate actuator up to SIL 2 or PL d is possible as described in the table. Since the machine manufacturer must provide proof of fault exclusion, the component manufacturer is unable to carry out a definitive assessment of the measures taken.

For further information, refer to the letter under the following link:
http://support.automation.siemens.com/WW/view/en/35443942.

Note

With a two-channel design with electro-mechanical sensors, SIL 3 or PL e can only be achieved when the sensors are supplied by the evaluation unit. Only this guarantees adequate diagnostics.

Table 3- 3 **Safe position monitoring with non-contact safety switches**

Safe evaluation units	**Detection units Non-contact safety switches**	
	Solenoid-operated switches 3SE66 / 3SE67 	RFID safety switches 3SE63 
 3SK1 safety relay	SIL 3 / PL e	SIL 3 / PL e
 3RK3 Modular Safety System	SIL 3 / PL e	SIL 3 / PL e

Note

The achievable safety levels also depend on the type of the safety evaluation unit used (especially its diagnostics capability).

See also

Monitoring and locking a protective door with a Modular Safety System (MSS) (http://support.automation.siemens.com/WW/view/en/62837891)

Achievable safety level using only one SIRIUS position switch with or without tumbler (http://support.automation.siemens.com/WW/view/en/35443942)

3.3.2 Protective door monitoring to SIL 1 or PL c with a safety relay

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off.

Design

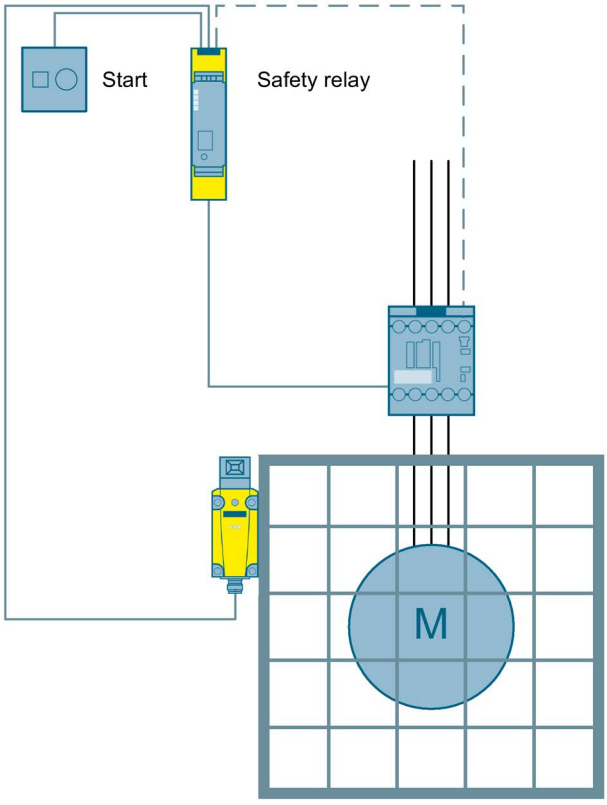
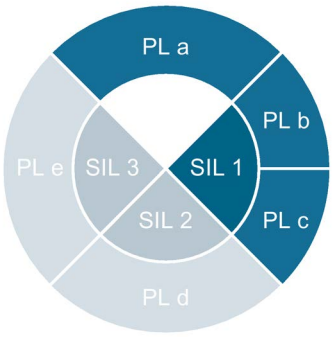


Figure 3-9 Protective door monitoring to SIL 1 or PL c with a safety relay

Operating principle

The position of a protective door is monitored via the contact of the safety switch. When the monitored door is opened, the safety relay triggers and opens the enabling circuits, switching off the power contactor in a safety-related manner. If the door is closed and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Safety switch	Safety relay	Contactor
		
3SE5 (http://www.siemens.com/sirius-detecting)	3SK1 (http://www.siemens.com/safety-relays)	3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation (http://support.automation.siemens.com/WW/view/en/73135973)

3.3.3 Protective door monitoring to SIL 1 or PL c with a Modular Safety System

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off.

Design

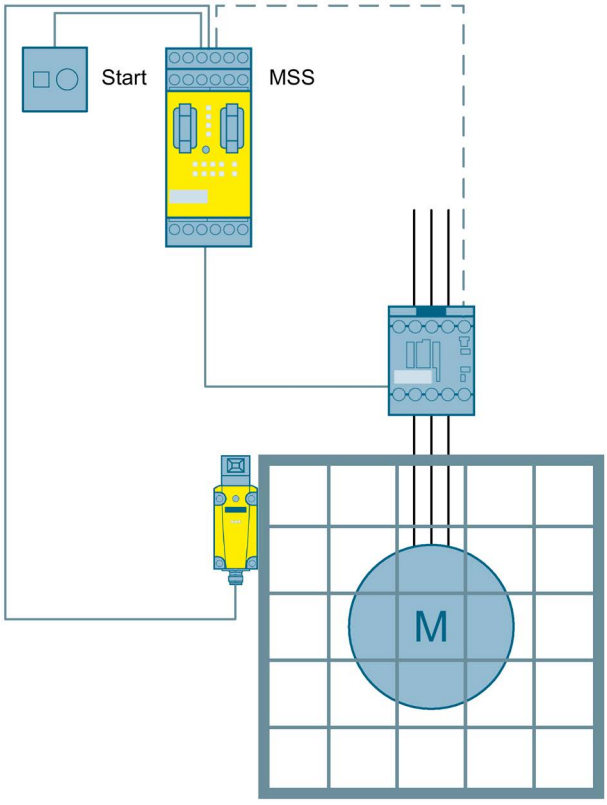
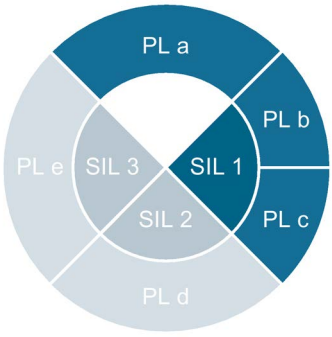


Figure 3-10 Protective door monitoring to SIL 1 or PL c with a Modular Safety System

Operating principle

The position of a protective door is monitored via the contact of the safety switch. When the monitored door is opened, the Modular Safety System triggers and opens the enabling circuits, switching off the power contactor in a safety-related manner. If the door is closed and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Safety switch	Modular Safety System	Contactor
		
3SE5 (http://www.siemens.com/sirius-detecting)	3RK3 (http://www.siemens.com/sirius-mss)	3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/69064060)

3.3.4 Protective door monitoring to SIL 3 or PL e with a safety relay

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off.

Design

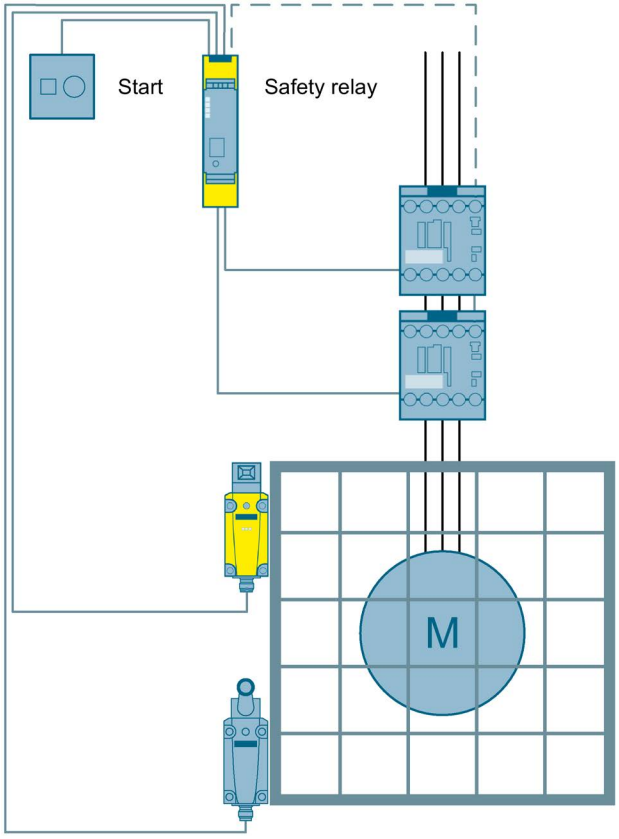
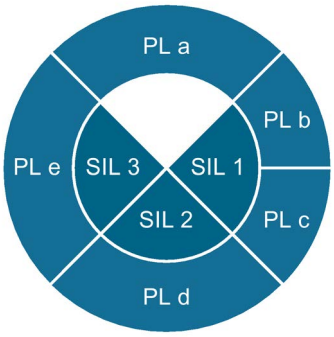


Figure 3-11 Protective door monitoring to SIL 3 or PL e with a safety relay

Operating principle

The position of a protective door is monitored via two safety switches. When the monitored door is opened, the safety relay triggers and opens the enabling circuits, switching off the power contactors in a safety-related manner. If the door is closed and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Position switches		Safety relay	Contactor
			
2x 3SE5 (http://www.siemens.com/sirius-detecting)		3SK1 (http://www.siemens.com/safety-relays)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation (http://support.automation.siemens.com/WW/view/en/73135309)

3.3.5 Protective door monitoring to SIL 3 or PL e with a Modular Safety System

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off.

Design

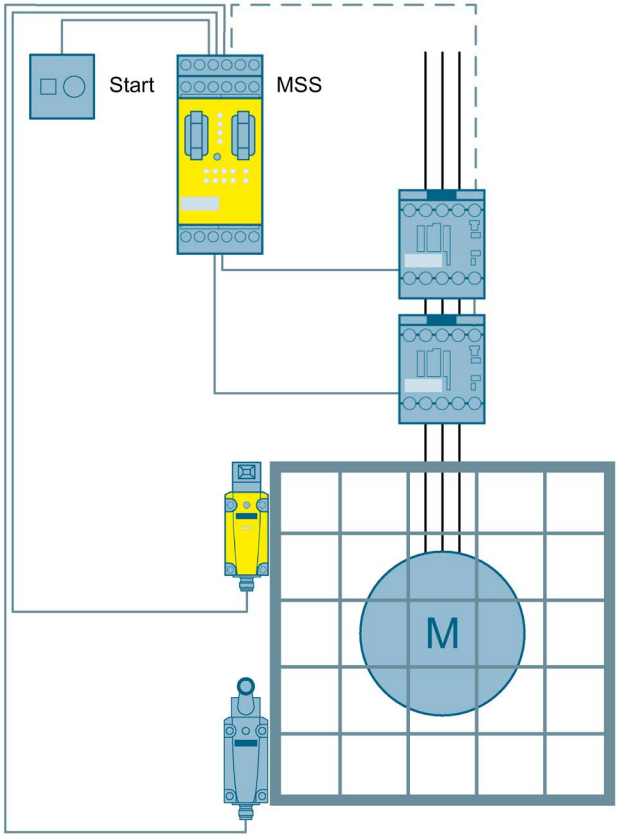
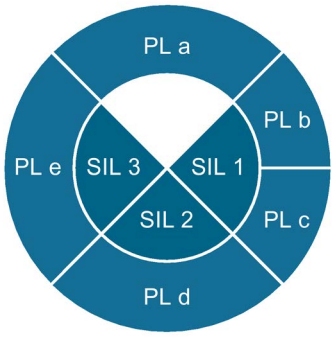


Figure 3-12 Protective door monitoring to SIL 3 or PL e with a Modular Safety System

Operating principle

The position of a protective door is monitored via two safety switches. When the monitored door is opened, the Modular Safety System triggers and opens the enabling circuits, switching off the power contactors in a safety-related manner. If the door is closed and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Position switches		Modular Safety System	Contactor
			
2x 3SE5 (http://www.siemens.com/sirius-detecting)		3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/69064861)

3.3.6 Protective door monitoring to SIL 3 or PL e with a fail-safe motor starter and a safety relay

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off.

Design

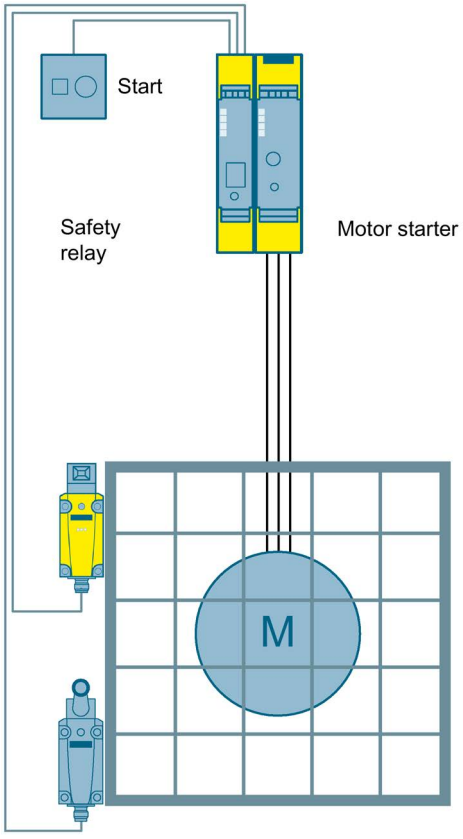
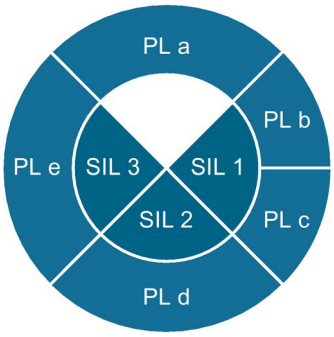


Figure 3-13 Protective door monitoring to SIL 3 or PL e with a fail-safe motor starter and a safety relay

Operating principle

The position of a protective door is monitored via the contact of the safety switch. When the monitored door is opened, the safety relay trips and switches the fail-safe motor starter off via the device connector. The motor starter then safely shuts down the load. If the door is closed, the Start button can be used to switch on again.



Safety-related components

Safety switch	Safety relay	Fail-safe motor starters
		
2x 3SE5 (http://www.siemens.com/sirius-detecting)	3SK1 (http://www.siemens.com/safety-relays)	3RM1 (http://www.siemens.com/motorstarter/3rm1)

See also

Circuit diagram and SET calculation (http://support.automation.siemens.com/WW/view/en/88822953)

More detailed FAQs on: Safe shutdown with the 3RM1 motor starters (http://support.automation.siemens.com/WW/view/en/67478946)

3.3.7 Protective door monitoring to SIL 3 or PL e with a fail-safe motor starter and a modular safety system

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off.

Design

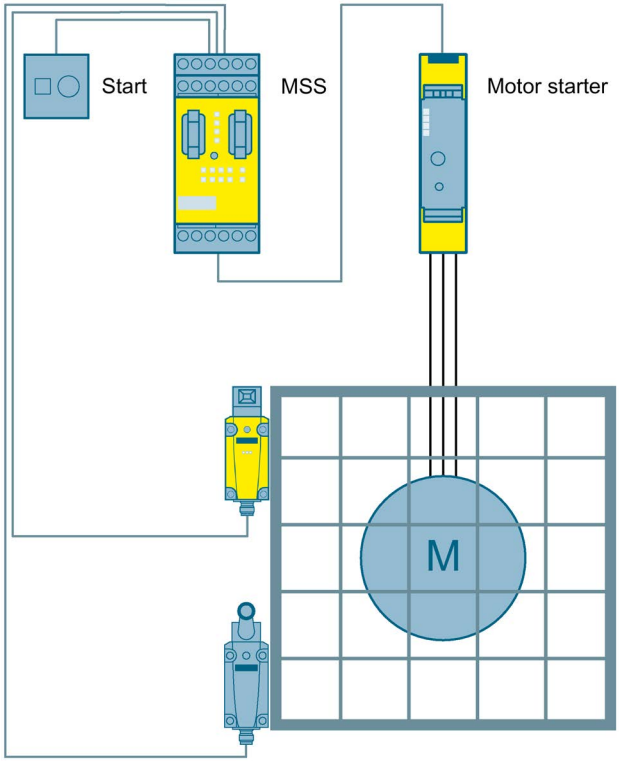
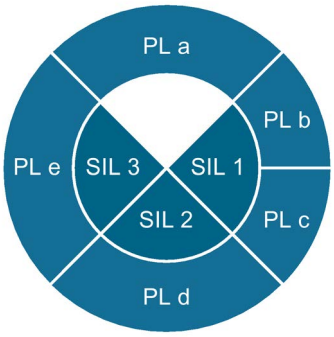


Figure 3-14 Protective door monitoring to SIL 3 or PL e with a fail-safe motor starter and a modular safety system

Operating principle

The position of a protective door is monitored via the contact of the safety switch. When the monitored door is opened, the modular safety system trips and switches the motor starter off safely. The motor starter then safely shuts down the load. If the door is closed and the feedback circuit is closed, the Start button can be used to switch on again.



Note

This example applies to configurations within a control cabinet. If the logic components and the actuators are not located in the same control cabinet, other precautions must be taken, such as cross-circuit-proof laying of the shutdown signal.

Safety-related components

Safety switch		Modular safety system	Fail-safe motor starters
			
2x 3SE5 (http://www.siemens.com/sirius-detecting)		3RK3 (http://www.siemens.com/sirius-mss)	3RM1 (http://www.siemens.com/motorstarter/3rm1)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/88822778)

More detailed FAQs on: Safe shutdown with the 3RM1 motor starters (http://support.automation.siemens.com/WW/view/en/67478946)

3.3.8 Protective door monitoring via AS-i to SIL 3 or PL e with a Modular Safety System

Application

Monitoring of multiple protective doors and control of the actuators via AS-i with a Modular Safety System.

Design

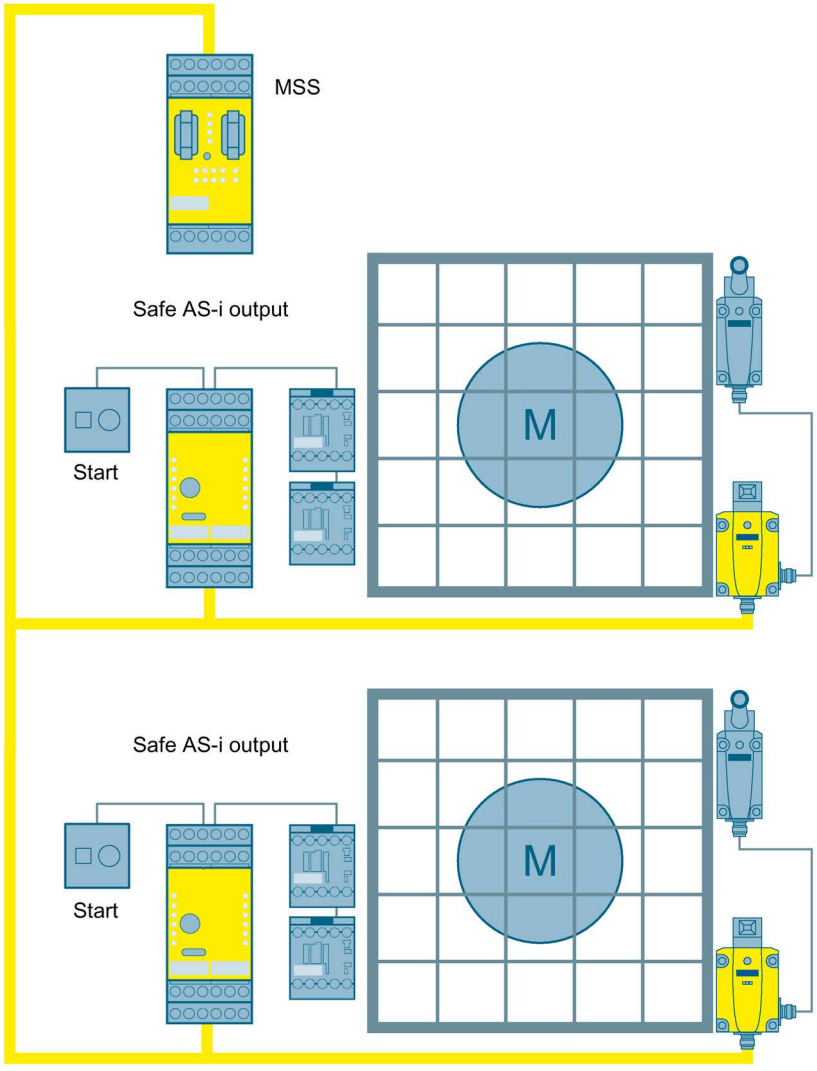
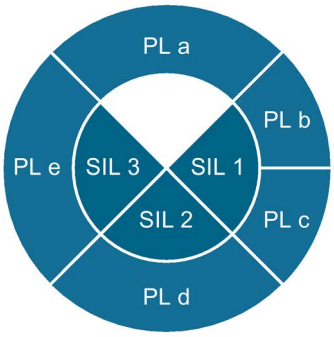


Figure 3-15 Protective door monitoring via AS-i to SIL 3 or PL e with a Modular Safety System

Operating principle

The Modular Safety System monitors the safety switches connected to AS-i, and transmits status signals via the AS-i bus in the form of simulated AS-i slaves. These simulated slaves are monitored by safe AS-i outputs. When one of the protective doors is opened, the Modular Safety System interrupts the respective status signal. The safe AS-i output then opens the enabling circuits and the power contactors switch off in a safety-related manner.

The signals from the start button and the auxiliary contacts of the contactors are sent from the safe AS-i output via the AS-i bus to the Modular Safety System, and evaluated there. If the respective door is closed and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Position switches	Modular Safety System	Safe AS-i output	Contactor
			
2x 3SE5 (http://www.siemens.com/sirius-detecting)	3RK3 (http://www.siemens.com/sirius-mss)	3RK1405 (www.siemens.com/as-interface)	2x 3RT20 (http://www.siemens.com/sirius-switching)

Note

In addition to the safety-related components, operation of an AS-i network requires an AS-i master and an AS-i power supply.

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/73135311)

3.3.9 Protective door monitoring by means of non-contact safety switch to SIL 3 or PL e with a safety relay

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off.

Design

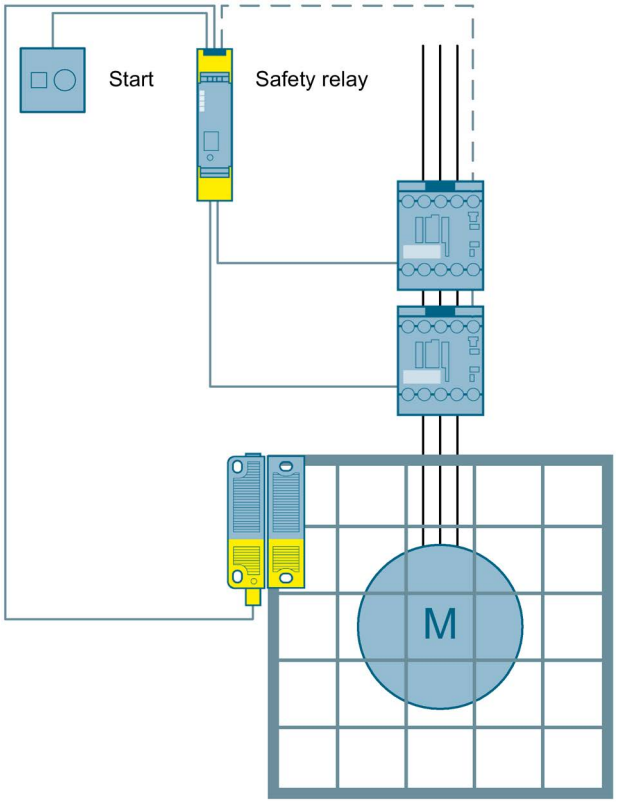
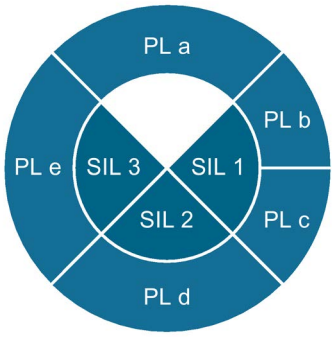


Figure 3-16 Protective door monitoring by means of non-contact safety switch to SIL 3 or PL e with a safety relay

Operating principle

The position of a protective door is monitored via the non-contact safety switch. When the monitored door is opened, the safety relay triggers and opens the enabling circuits, switching off the power contactors in a safety-related manner. If the door is closed and the feedback circuit is closed, the Start button can be used to switch on again.

The 3SE6315 non-contact safety switch has two channels internally and possesses its own diagnostics capability. Because of this, and because it is tamper-proof thanks to its RFID technology, a redundant safety switch is not required to achieve up to PL e per ISO 13849-1 or SIL 3 per IEC 62061.



Safety-related components

Non-contact safety switch	Safety relay	Contactor
		
3SE6315 (http://www.siemens.com/sirius-detecting)	3SK1 (http://www.siemens.com/safety-relays)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/73134150)

3.3.10 Protective door monitoring by means of non-contact safety switch to SIL 3 or PL e with a Modular Safety System

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off.

Design

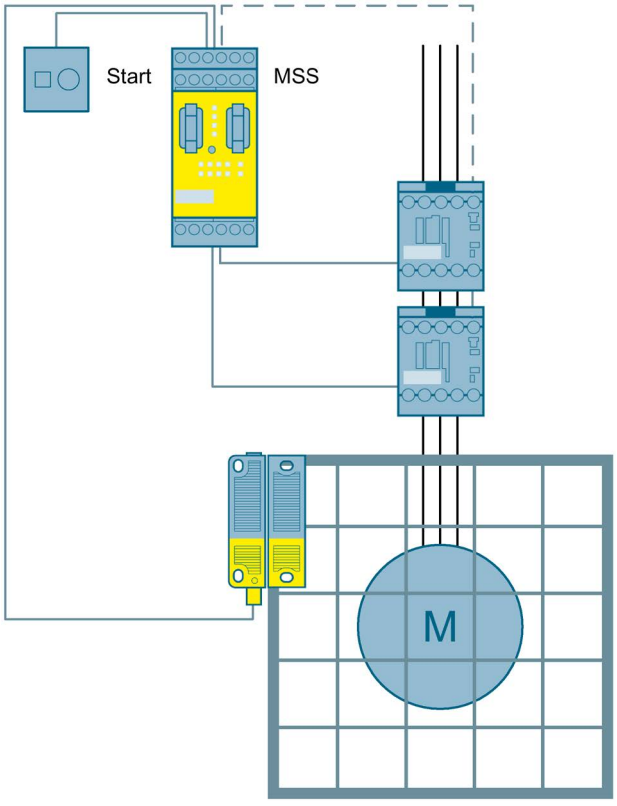
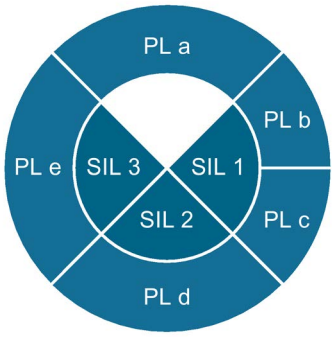


Figure 3-17 Protective door monitoring by means of non-contact safety switch to SIL 3 or PL e with a Modular Safety System

Operating principle

The position of a protective door is monitored via the non-contact safety switch. When the monitored door is opened, the Modular Safety System triggers and opens the enabling circuits, switching off the power contactors in a safety-related manner. If the door is closed and the feedback circuit is closed, the Start button can be used to switch on again.

The 3SE6315 non-contact safety switch has two channels internally and possesses its own diagnostics capability. Because of this, and because it is tamper-proof thanks to its RFID technology, a redundant safety switch is not required to achieve up to PL e per ISO 13849-1 or SIL 3 per IEC 62061.



Safety-related components

Non-contact safety switch	Modular Safety System	Contactor
		
3SE6315 (http://www.siemens.com/sirius-detecting)	3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/69064862)

3.3.11 Protective door monitoring with tumbler to SIL 2 or PL d with a safety relay

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off. If the machine continues to present a hazard even after switching off, access can be prevented for this period by a tumbler.

Design

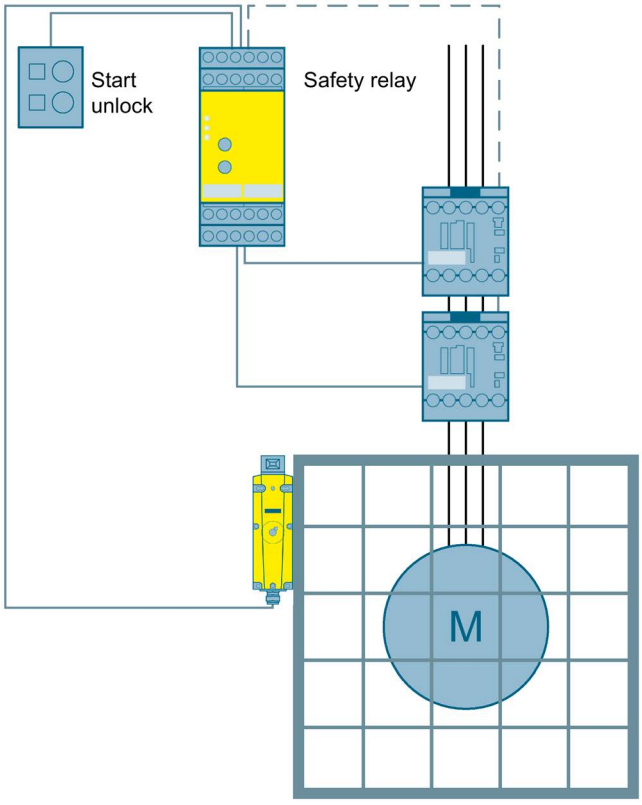


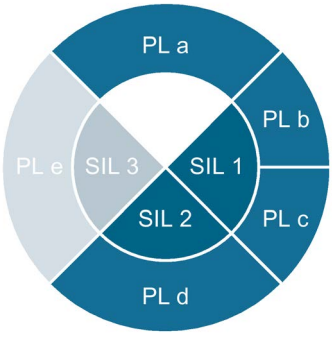
Figure 3-18 Protective door monitoring with tumbler to SIL 2 or PL d with a safety relay

Operating principle

The position of a protective door is monitored via one safety switch. In addition, the door is locked via the safety switch. If the command to unlock the door is issued, the safety relay triggers and opens the enabling circuits, switching off the power contactors in a safety-related manner. The tumbler is unlocked after expiry of a set time. If the door is closed and locked, and the feedback circuit is closed, the Start button can be used to switch on again.

The safety function "Protective door monitoring" and the safety function "Protective door tumbler" are designed for up to SIL 2 or PL d.

Taking account of fault exclusions, use of only one safety switch with or without tumbler is permissible to SIL 2 or PL d. For further information, refer to the letter given below.



Safety-related components

Safety switches with tumbler	Safety relay	Contactor
		
3SE5 (http://www.siemens.com/sirius-detecting)	3TK2845 (http://www.automation.siemens.com/mcms/industrial-controls/en/safety-systems/3tk28)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation (http://support.automation.siemens.com/WW/view/en/73136328)

Letter concerning the use of safety relays to SIL 2 or PL d (http://support.automation.siemens.com/WW/view/en/35443942)

3.3.12 Protective door monitoring with tumbler to SIL 2 or PL d with a Modular Safety System

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off. If the machine continues to present a hazard even after switching off, access can be prevented for this period by a tumbler.

Design

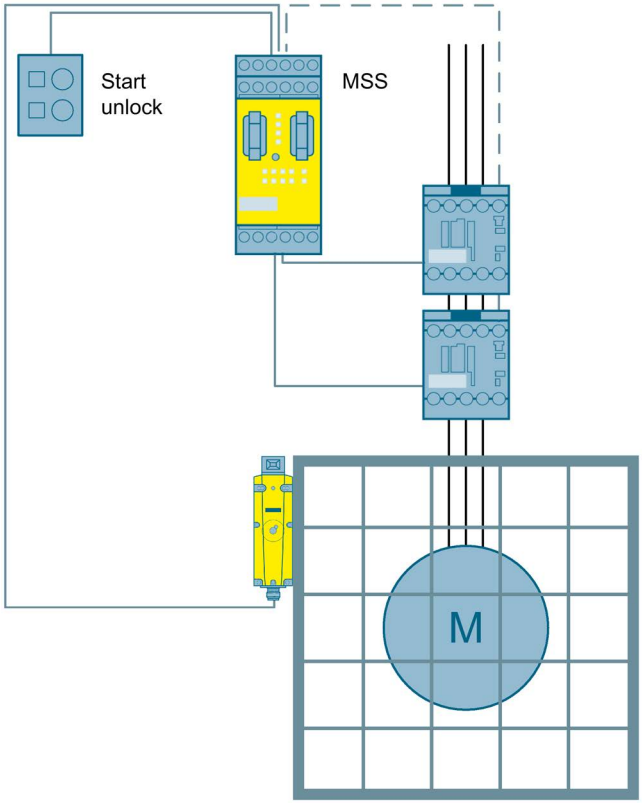
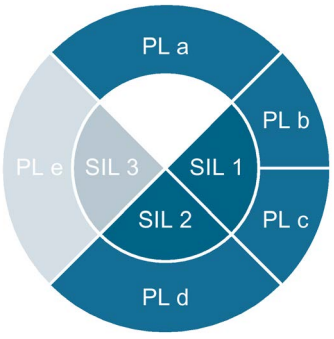


Figure 3-19 Protective door monitoring with tumbler to SIL 2 or PL d with a Modular Safety System

Operating principle

The position of a protective door is monitored via one safety switch. In addition, the door is locked via the safety switch. If the command to unlock the door is issued, the safety relay triggers and opens the enabling circuits, switching off the power contactors in a safety-related manner. The tumbler is unlocked after expiry of a set time. If the door is closed and locked, and the feedback circuit is closed, the Start button can be used to switch on again.



The safety function "Protective door monitoring" and the safety function "Protective door tumbler" are designed for up to SIL 2 or PL d.

Taking account of fault exclusions, use of only one safety switch with or without tumbler is permissible to SIL 2 or PL d. For further information, refer to the letter given below.

Safety-related components

Safety switches with tumbler	Modular Safety System	Contactor
		
3SE5 (http://www.siemens.com/sirius-detecting)	3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation
(http://support.automation.siemens.com/WW/view/en/73137468)

Letter concerning the use of safety relays to SIL 2 or PL d
(http://support.automation.siemens.com/WW/view/en/35443942)

3.4 Monitoring of open danger zones

3.4.1 Introduction

Within an industrial plant there are often areas that must be made inaccessible to personnel for certain periods due to the high level of hazard. There must, for example, be no parts of the body in the interior of a press during the downward movement of the press. Monitoring for such hazards is often implemented using light curtains.

At certain times, it might be necessary to suppress the protective function. Muting is the intentional, temporary suppression of the protective function. This "muting mode" is triggered by muting sensors (e.g. while transporting material into the danger zone).

Note

Light curtains can only perform their function if they are installed with sufficient safety clearance. The calculation formulas for the safety clearance depend on the type of protection. Positioning situations and calculation formulas can be found in the standard EN 13855 ("Positioning of safeguards with respect to the approach speeds of parts of the human body").

3.4.2 Access monitoring using a light curtain to SIL 3 or PL e with a safety relay

Application

To monitor access to an open danger zone, so-called non-contact protective equipment such as a light curtain can be used. If the light beam is interrupted, a shutdown signal is triggered.

Design

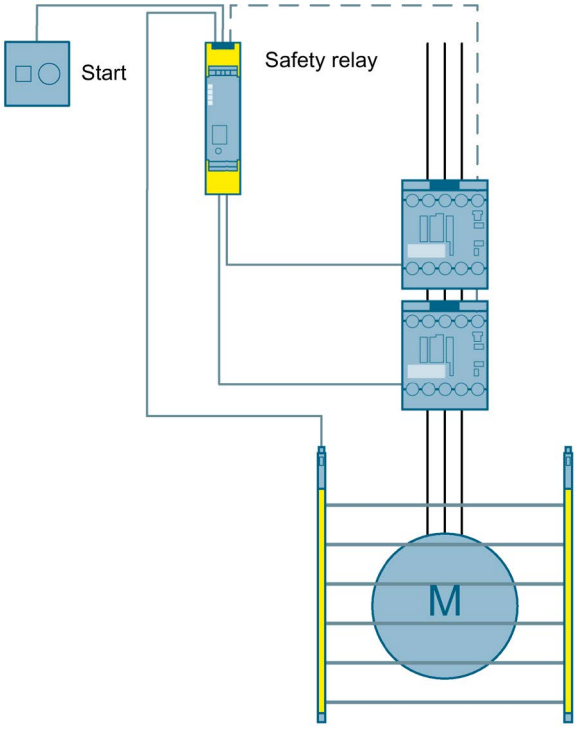
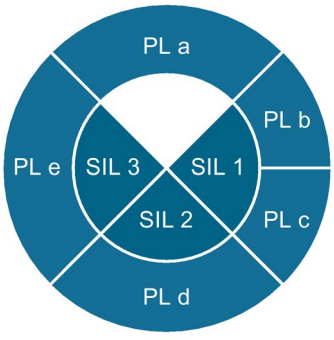


Figure 3-20 Access monitoring using a light curtain to SIL 3 or PL e with a safety relay

Operating principle

The light curtain consists of a send unit and a receive unit. Between the two is the protective zone. If the light beam is interrupted, outputs OSSD1 and OSSD2 carry voltage and are evaluated by the safety relay. When the light beam is interrupted, the two outputs switch off and the safety relay opens the enabling circuits, switching off the power contactors in a safety-related manner. If the light beam is uninterrupted and the feedback circuit is closed, you can switch on again. This can happen automatically or using a Start button, depending on the application.



Safety-related components

Light curtain	Safety relay	Contactor
		
SICK C4000	3SK1 (http://www.siemens.com/safety-relays)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation (http://support.automation.siemens.com/WW/view/en/73136329)

3.4.3 Access monitoring using a light curtain to SIL 3 or PL e with a Modular Safety System

Application

To monitor access to an open danger zone, so-called non-contact protective equipment such as a light curtain can be used. If the light beam is interrupted, a shutdown signal is triggered.

Design

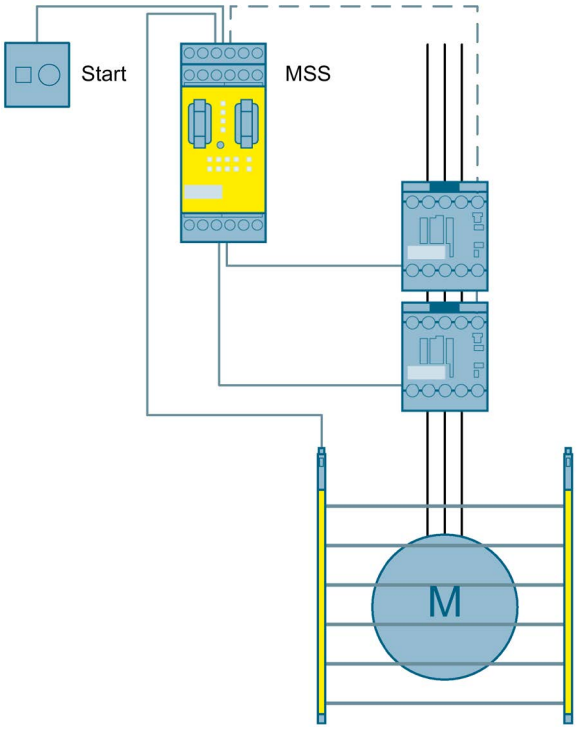
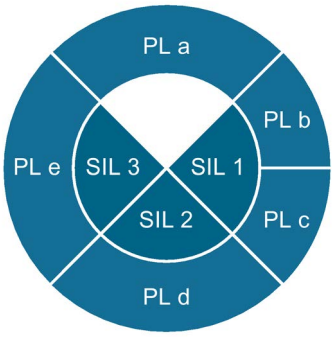


Figure 3-21 Access monitoring using a light curtain to SIL 3 or PL e with a Modular Safety System

Operating principle

The light curtain consists of a send unit and a receive unit. Between the two is the protective zone. If the light beam is interrupted, outputs OSSD1 and OSSD2 carry voltage and are evaluated by the Modular Safety System. When the light beam is interrupted, the two outputs switch off and the Modular Safety System opens the enabling circuits, switching off the power contactors in a safety-related manner. If the light beam is uninterrupted and the feedback circuit is closed, you can switch on again. This can happen automatically or using a Start button, depending on the application.



Safety-related components

Light curtain	Modular Safety System	Contactor
		
SICK C4000	3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/69064070)

3.4.4 Access monitoring using a safety mat to SIL 3 or PL e with a safety relay

Application

Safety mats that trigger a shutdown signal when stepped on can be used to monitor access to an open danger zone.

Design

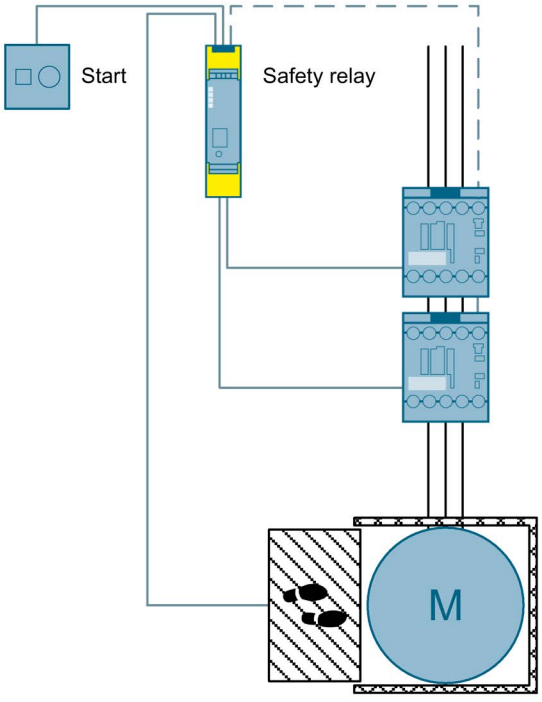
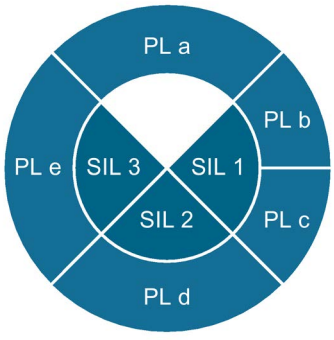


Figure 3-22 Access monitoring using a safety mat to SIL 3 or PL e with a safety relay

Operating principle

Safety mats based on the normally-closed (NC) principle (or NC-NO) can be evaluated with the 3SK1 safety relay. With this principle, the two-channel sensor circuit is interrupted if someone enters. The safety relay then opens the enabling circuits, switching the power contactors off in a safety-related manner. If the safety mat is free and the feedback circuit is closed, you can switch on again. This can happen automatically or using a Start button, depending on the application.



Safety-related components

Safety mat	Safety relay	Contactor
		
	3SK1 (http://www.siemens.com/safety-relays)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation (http://support.automation.siemens.com/WW/view/en/77262359)

3.4.5 Access monitoring using a safety mat to SIL 3 or PL e with a Modular Safety System

Application

Safety mats that trigger a shutdown signal when stepped on can be used to monitor access to an open danger zone.

Design

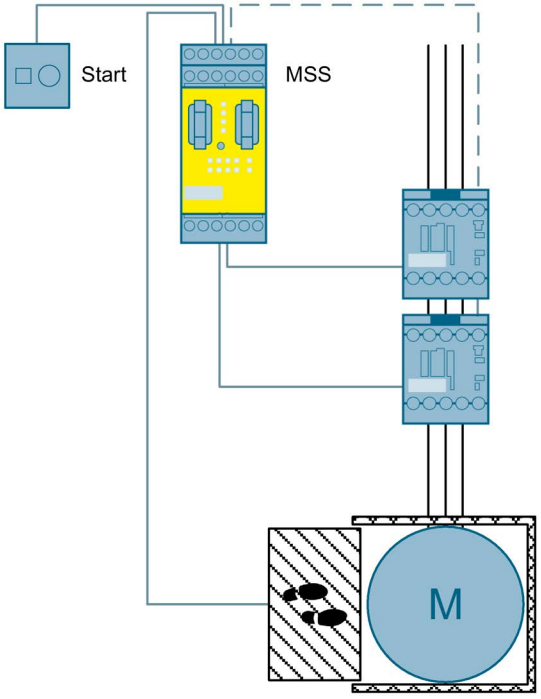
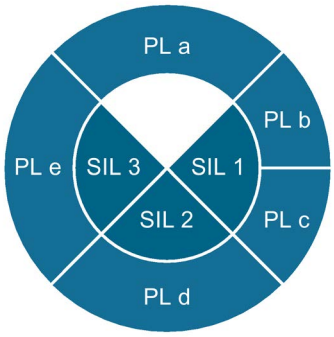


Figure 3-23 Access monitoring using a safety mat to SIL 3 or PL e with a Modular Safety System

Operating principle

Safety mats can be based either on the normally-closed principle or on the cross-circuit principle. With the normally-closed principle, the two-channel sensor circuit is interrupted if someone enters. With the cross-circuit principle, on the other hand, a cross-circuit between the two sensor circuits is triggered if someone enters. In both cases, the signal is evaluated by the Modular Safety System. The Modular Safety System then opens the enabling circuits, switching the power contactors off in a safety-related manner. If the safety mat is free and the feedback circuit is closed, you can switch on again. This can happen automatically or using a Start button, depending on the application.



Safety-related components

Safety mat	Modular Safety System	Contactor
		
	3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/77262361)

3.4.6 Area monitoring using a laser scanner to SIL 2 or PL d with a safety relay

Application

Laser scanners are frequently used to monitor entire areas for unauthorized access. These provide wide-area monitoring of a danger zone, and they trigger a shutdown signal when objects are detected.

Design

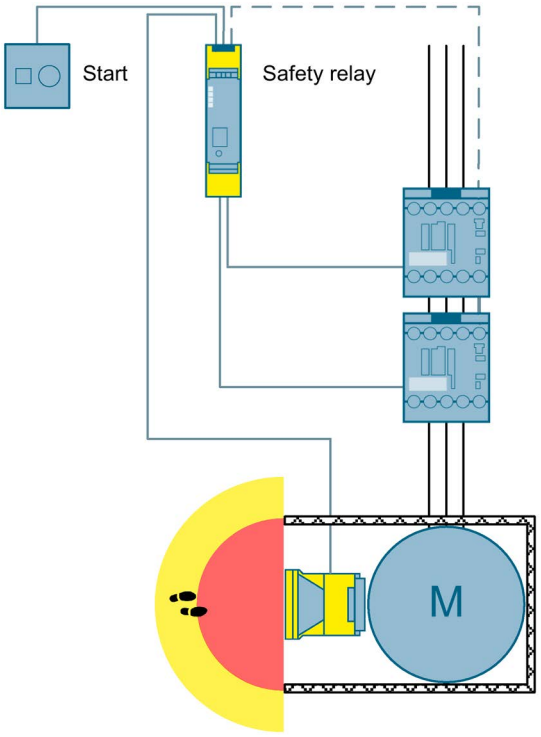
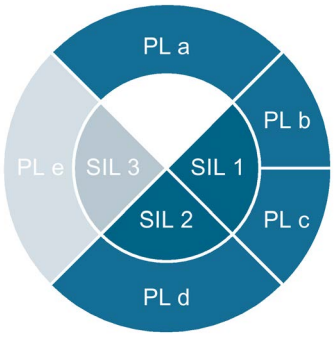


Figure 3-24 Area monitoring using a laser scanner to SIL 2 or PL d with a safety relay

Operating principle

The laser scanner provides wide-area monitoring of a safety area. This can usually be divided into a warning zone and a danger zone. When anyone enters the warning zone, a warning is output by means of an indicator light, for example. If anyone enters the safety zone on the other hand, the machine is switched off.

During operation, the outputs OSSD1 and OSSD2 carry voltage and are evaluated by the safety relay. When the light beam is interrupted, the two outputs switch off and the safety relay opens the enabling circuits, switching off the power contactors in a safety-related manner. If the light beam is uninterrupted and the feedback circuit is closed, you can switch on again. This can happen automatically or using a Start button, depending on the application.



Safety-related components

Laser scanner	Safety relay	Contactor
		
SICK S3000	3SK1 (http://www.siemens.com/safety-relays)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/77262367)

3.4.7 Area monitoring using a laser scanner to SIL 2 or PL d with a Modular Safety System

Application

Laser scanners are frequently used to monitor entire areas for unauthorized access. These provide wide-area monitoring of a danger zone, and they trigger a shutdown signal when objects are detected.

Design

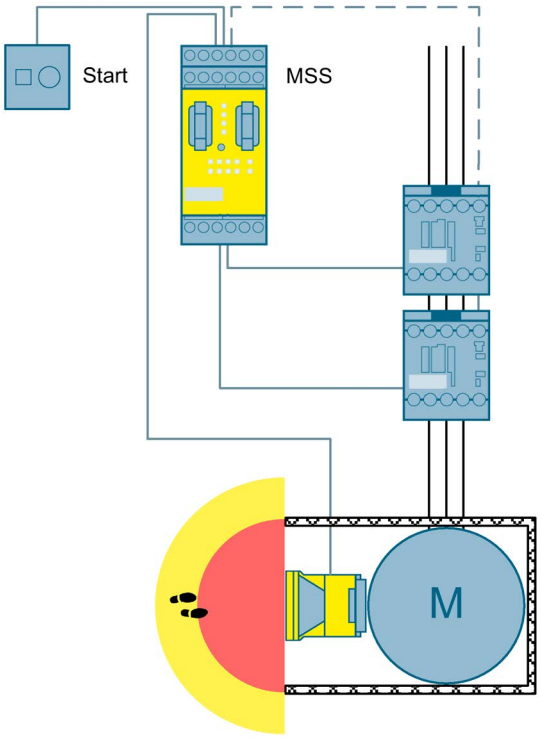
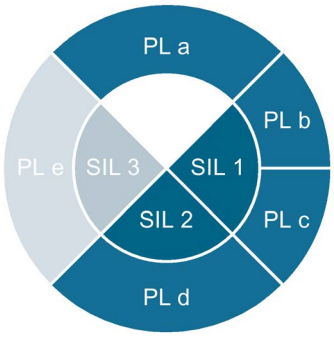


Figure 3-25 Area monitoring using a laser scanner to SIL 2 or PL d with a Modular Safety System

Operating principle

The laser scanner provides wide-area monitoring of a danger zone. This can usually be divided into a warning zone and a safety area. When anyone enters the warning zone, a warning is output by means of an indicator light, for example. If anyone enters the safety zone on the other hand, the machine is switched off.

During operation, the outputs OSSD1 and OSSD2 carry voltage and are evaluated by the safety relay. When the light beam is interrupted, the two outputs switch off and the safety relay opens the enabling circuits, switching off the power contactors in a safety-related manner. If the light beam is uninterrupted and the feedback circuit is closed, you can switch on again. This can happen automatically or using a Start button, depending on the application.



Safety-related components

Laser scanner	Modular Safety System	Contactor
		
SICK S3000	3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation
(http://support.automation.siemens.com/WW/view/en/77284304)

3.5 Safe speed and standstill monitoring

3.5.1 Introduction

In machines in which the machine movement or moving parts can pose a hazard to people and machinery, speed monitoring or standstill monitoring is frequently used.

These applications are frequently implemented in conjunction with guards (protective door) and a protective door tumbler.

Interlocking devices with a tumbler are used to protect danger zones against undesired entry. There are usually two reasons for this:

1. To protect personnel against overtravel of dangerous machine movements, high temperatures, etc. ISO 14119 or EN 1088 provide guidelines for designing and selecting interlocking devices. These standards state that the danger zone must not be accessible until after the dangerous machine movement has been stopped.
2. A tumbler may be useful for reasons of process safety. This situation occurs when the hazard is stopped after opening the guard, but damage can occur to the machine or workpiece as a result. In this case, the machine is first moved to a controlled stop position before access is enabled.

With speed monitoring, a protective door tumbler is only unlocked, for example, when the moving part has come to a stop or is running at a safe speed.

With standstill monitoring, in contrast to speed monitoring, the protective door tumbler, for example, is only unlocked when standstill is achieved.

3.5.2 Safe speed monitoring to SIL 2 or PL d with a safety relay and a speed monitoring relay

Application

To ensure that the speed of a motor is limited even in the event of a fault, and personnel are thus protected against possible falling tool parts, the speed is monitored with the help of two speed monitoring relays and a safety relay.

Design

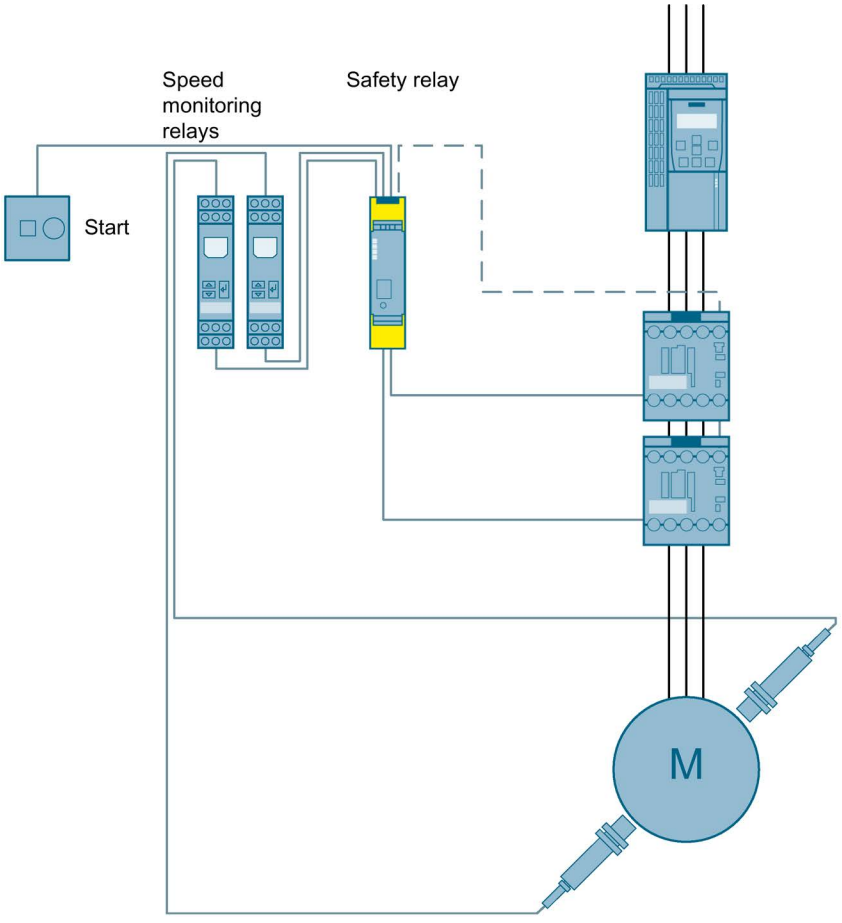
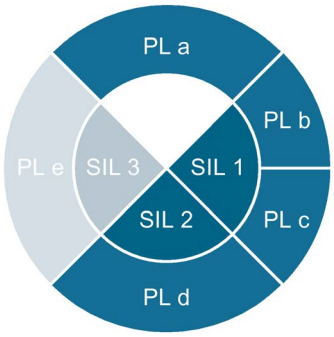


Figure 3-26 Safe speed monitoring to SIL 2 or PL d with a safety relay and a speed monitoring relay

Operating principle

It is possible to achieve up to SIL 2 or PL d with the redundant use of two standard speed monitoring relays. A specific speed or speed range (upper and lower limit) is set here on both speed monitoring relays. These monitor the speed of the motor continuously and indicate via relay contacts whether the speed limit or the speed range is maintained or exceeded.



The safety relay, in turn, monitors the signals of the speed monitoring relays for discrepancies and cross-circuits.
If the speed of the motor exceeds the speed limit or exits the speed range, the motor is switched off immediately in a safety-related manner.
If the speed of the motor has dropped again below the speed limit, is within the speed range, or is at a standstill, and the feedback circuit is closed, the Start button can be used to switch the motor on again.

Note

If two redundant monitoring relays are used in the sensor circuit to detect process variables, this can result in one monitoring relay detecting a limit overshoot before the other. This can be caused by setting or measuring deviations of the devices and the external sensors.

In the example given above, one monitoring relay could detect the limit overshoot shortly before the other in the case of a continuous increase in speed. In this case, the power supply to the drive is switched off. The speed decreases immediately. Due to the necessary cross-comparison of the inputs in safety-related evaluation, the discrepancy error remains active. The application can only be switched on again after zero crossing of both channels. In this case, the monitoring relays must be checked and manually reset.

This behavior can occur when monitoring slowly increasing process variables. Methods of avoiding a discrepancy error include:

- Empirical calculation of the setting parameters for synchronizing the monitoring relays
- Identical design of the external sensors (sensors of the same type, same cable lengths, etc.)

Safety-related components

Speed monitoring relays	Safety relay	Contactor
		
2x 3UG4651 (http://www.siemens.com/sirius-monitoring)	3SK1 (http://www.siemens.com/safety-relays)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/69065516)

Letter concerning the use of safety relays to SIL 2 or PL d
(http://support.automation.siemens.com/WW/view/en/35443942)

3.5.3 Safe speed monitoring to SIL 3 or PL e with a speed monitor

Application

To ensure that the speed of a motor is limited even in the event of a fault, and personnel are thus protected against possible falling tool parts, the speed is monitored with the help of a speed monitor.

Design

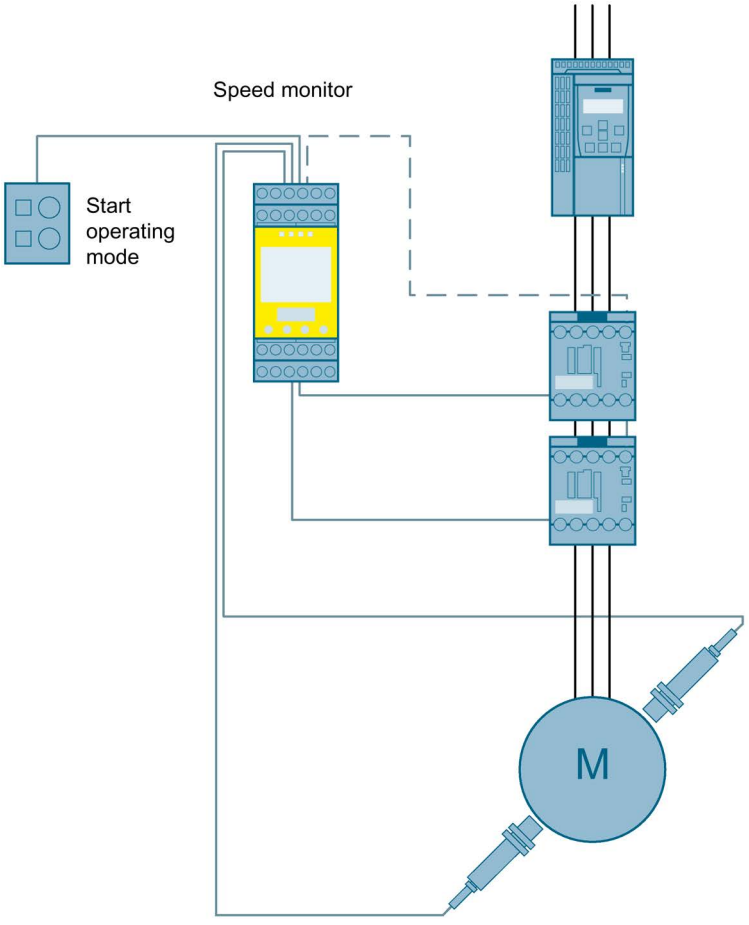
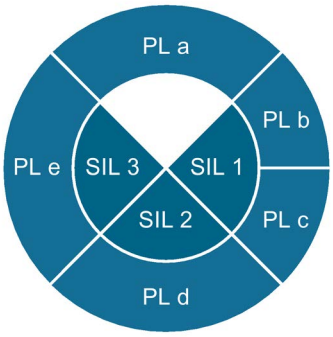


Figure 3-27 Safe speed monitoring to SIL 3 or PL e with a speed monitor

Operating principle

A specific speed limit or speed range (upper and lower limit) is set on the speed monitor.
You can change between setup mode and automatic mode with individual speed ranges using a mode switch.
If the respective speed window is overshot or undershot, the power contactors are switched off in a safety-related manner.

As soon as the actuators have switched off and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Speed monitor	Contactor
	
3TK2810-1 (http://www.automation.siemens.com/mcms/industrial-controls/en/safety-systems/3tk28)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/69065043)

3.5.4 Safe standstill monitoring including protective door tumbler to SIL 3 or PL e with a Modular Safety System

Application

The Modular Safety System monitors a protective door. The standstill monitor ensures access to the moving, dangerous machine parts is not permitted while the motor is operating.

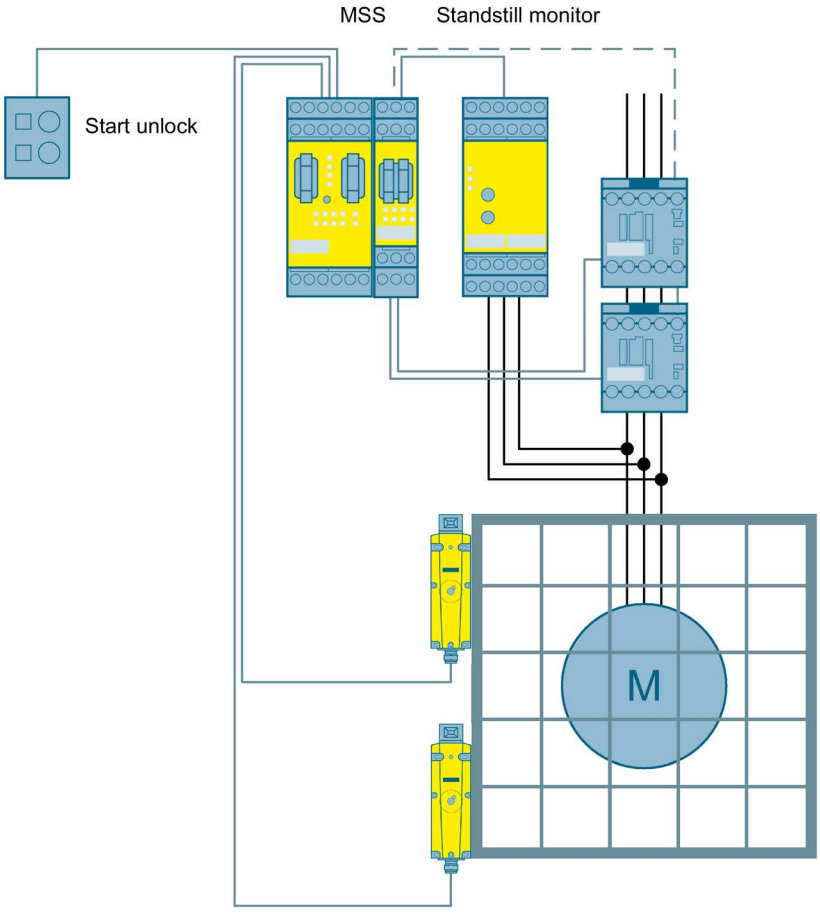
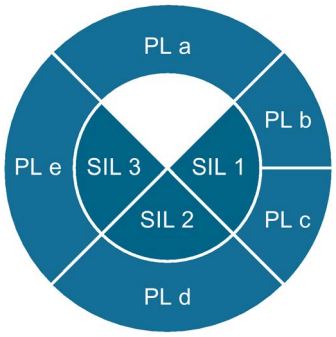


Figure 3-28 Safe standstill monitoring including protective door tumbler to SIL 3 or PL e with a Modular Safety System

Operating principle

The 3TK2810-0 safe standstill monitor measures a voltage of the coasting motor induced by residual magnetization at three terminals of the stator winding. If the induction voltage approaches 0, this means motor standstill for the device and the output relays are activated.



The Modular Safety System monitors this signal from the standstill monitor as well as the two safety switches.

If motor standstill is detected and the button for unlocking is pressed, the tumbler is unlocked and the protective door can be opened. At the same time, the contactors are shut down in a safety-related manner, thus preventing unexpected restart of the motor.

If the door is locked and the feedback circuit is closed, the Start button can be used to switch on again.

The emergency stop is an additional safety function that is not considered further here.

Safety-related components

Safety switches with tumbler	Standstill monitor	Modular Safety System	Expansion module	Contactor
				
2x 3SE5 (http://www.siemens.com/sirius-detecting)	3TK2810-0 (http://www.automation.siemens.com/mcms/industrial-controls/en/safety-systems/3tk28)	3RK3 (http://www.siemens.com/sirius-mss)	3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/69065515)

3.5.5 Safe speed monitoring, protective door monitoring, and tumbler monitoring to SIL 2 or PL d with a Modular Safety System and a speed monitoring relay

Application

The Modular Safety System ensures with the help of the speed monitoring relay that no access is permitted to the moving, dangerous machine parts above an adjustable speed.

Design

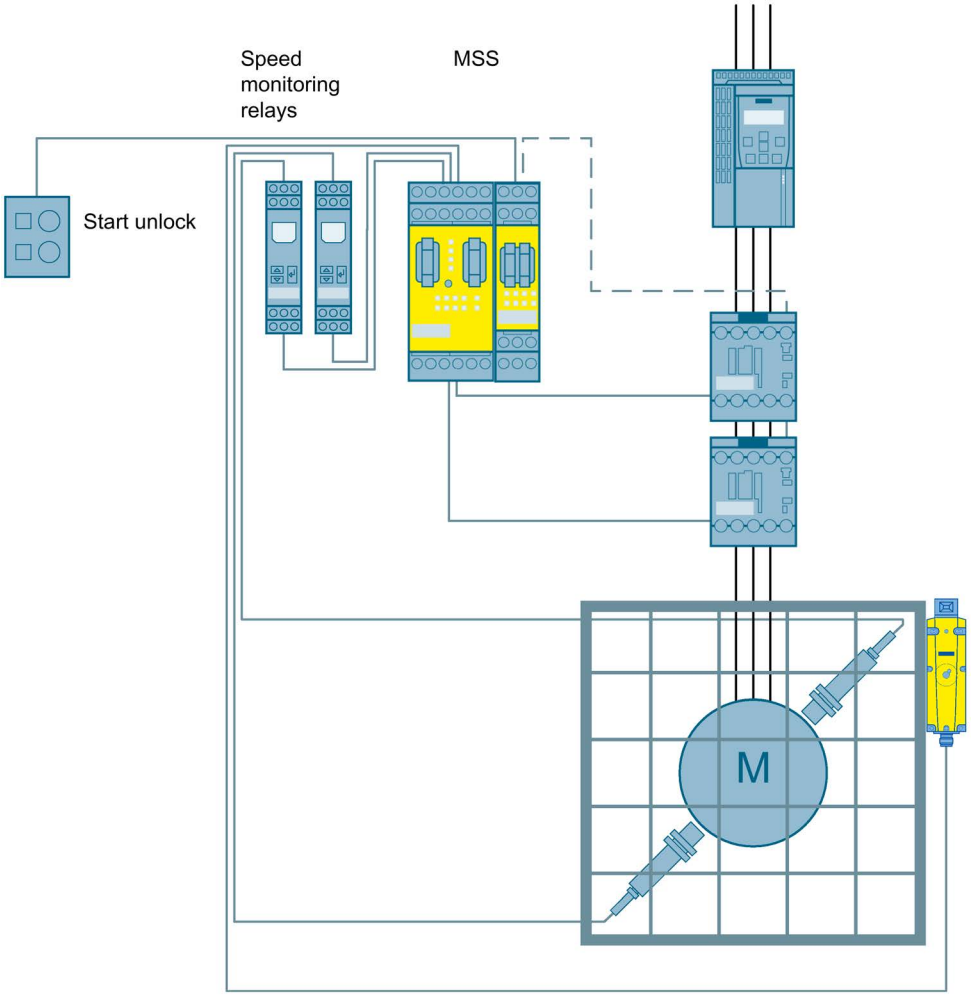
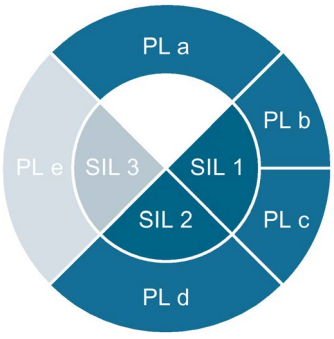


Figure 3-29 Safe speed monitoring, protective door monitoring, and tumbler monitoring to SIL 2 or PL d with a Modular Safety System and a speed monitoring relay

Operating principle

It is possible to achieve up to SIL 2 or PL d with the redundant use of two standard speed monitoring relays. A safe speed window is set on the speed monitoring relay. As long as the speed is outside this safe speed window, access to the moving, dangerous machine parts is prevented by a protective door with a tumbler. The Modular Safety System monitors the signals of the speed monitoring relay as well as the two safety switches.



While the speed of the motor is within the safe speed window, the tumbler can be unlatched and the protective door opened by pressing the unlatching button. If the speed of the motor exceeds the safe speed window while the door is opened, the motor is immediately switched off in a safety-related manner. If the door is locked and the feedback circuit is closed, the Start button can be used to switch on again.

In this example, the safety function "Protective door monitoring" and the safety function "Protective door tumbler" are designed for up to SIL 2 or PL d.

Taking account of fault exclusions, use of only one safety switch with or without tumbler is permissible to SIL 2 or PL d. For further information, refer to the letter given below.

Note

If two redundant monitoring relays are used in the sensor circuit to detect process variables, this can result in one monitoring relay detecting a limit overshoot before the other. This can be caused by setting or measuring deviations of the devices and the external sensors.

In the example given above, one monitoring relay could detect the limit overshoot shortly before the other in the case of a continuous increase in speed. In this case, the power supply to the drive is switched off. The speed decreases immediately. Due to the necessary cross-comparison of the inputs in safety-related evaluation, the discrepancy error remains active. The application can only be switched on again after zero crossing of both channels. In this case, the monitoring relays must be checked and manually reset.

This behavior can occur when monitoring slowly increasing process variables. Methods of avoiding a discrepancy error include:

- Empirical calculation of the setting parameters for synchronizing the monitoring relays
- Identical design of the external sensors (sensors of the same type, same cable lengths, etc.)

Safety-related components

Safety switches with tumbler	Speed monitoring relays	Modular safety system	Expansion module	Contactor
				
3SE5 (2-channel) (http://www.siemens.com/sirius-detecting)	2x 3UG4651 (http://www.siemens.com/sirius-monitoring)	3RK3 (http://www.siemens.com/sirius-mss)	3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation
(http://support.automation.siemens.com/WW/view/en/77284310)

Letter concerning the use of safety relays to SIL 2 or PL d
(http://support.automation.siemens.com/WW/view/en/35443942)

3.5.6 Safe speed monitoring, protective door monitoring and tumbler monitoring to SIL 3 or PL e with a speed monitor

Application

The speed monitor ensures that no access is permitted to the moving, dangerous machine parts above an adjustable speed.

Design

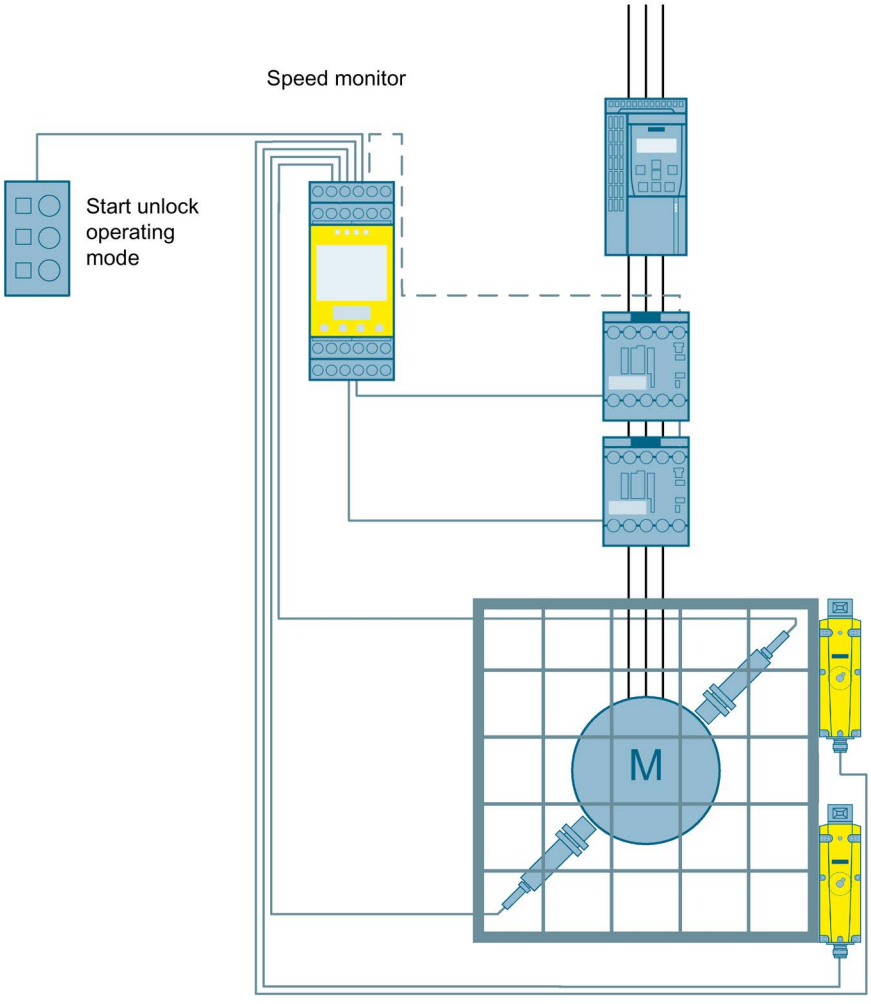
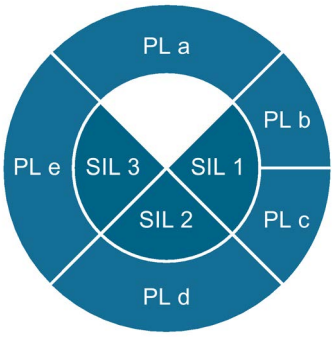


Figure 3-30 Safe speed monitoring, protective door monitoring and tumbler monitoring to SIL 3 or PL e with a speed monitor

Operating principle

A safe speed window is set on the speed monitor. As long as the speed is outside this safe speed window, access to the moving, dangerous machine parts is prevented by a protective door with a tumbler. At the same time, the speed monitor monitors the position of the protective door.

You can change between setup mode and automatic with individual speed windows using a mode switch. A detected standstill and observance of the set speed window are output via two relay outputs



In automatic mode, the protective door remains locked as long as no standstill is detected. If the automatic speed window is overshot or undershot, the power contactors are switched off in a safety-related manner.
In setup mode, the protective door is permanently enabled. If the setup speed window is overshot or undershot, the power contactors are switched off.

If the protective door is open, the speed monitor ensures that the motor cannot be switched on. If the door is closed and the feedback circuit is closed, the Start button can be used to switch on again.

Safety-related components

Safety switches with tumbler	Speed monitor	Contactor
		
2x 3SE5 (http://www.siemens.com/sirius-detecting)	3TK2810-1 (http://www.automation.siemens.com/mcms/industrial-controls/en/safety-systems/3tk28)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/77284316)

3.6 Safe operator input

3.6.1 Introduction

If an operator has to work within a danger zone, e.g. when positioning or removing workpieces for presses, stamping presses or similar machinery, safety functions must be implemented for the safe operation of the machine. Starting of the dangerous movement must only be allowed if, for example, no parts of the operator's body are within the danger zone. One method of implementing this is by using two-hand operation. This involves the operator pressing two pushbuttons almost simultaneously with both hands to start the machine or the dangerous movement. Releasing either of the pushbuttons causes the machine or the movement to stop.

The following chapter contains application examples with two-hand operation for safe operation of a machine.

Note

Selection of a two-hand control device as suitable safety equipment depends on the risk assessment.

3.6.2 Two-hand operation to SIL 3 or PL e with a safety relay

Application

Two-hand operation consoles comprise two pushbuttons that must be pressed simultaneously to operate a machine. This prevents the operator from reaching into the danger zone during operation.

Design

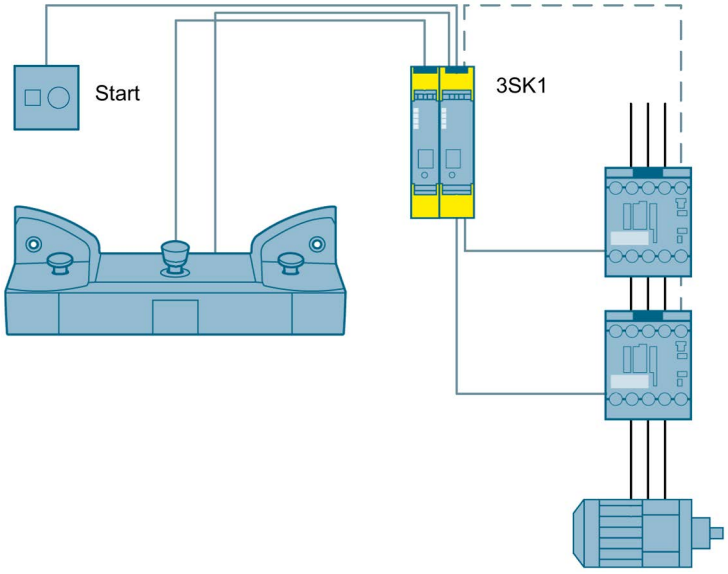


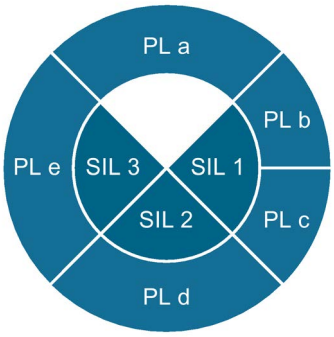
Figure 3-31 Two-hand operation to SIL 3 or PL e with a safety relay

Operating principle

By imposing the condition of simultaneous pressing of both pushbuttons, the operator is restricted to the two-hand operation console and is thus unable to reach into the danger zone. The safety relay only switches the enabling circuits when both signals are active within 500 ms and the feedback circuit is closed.

If one of the two pushbuttons is released, the safety relay immediately switches the machine off in a safety-related manner.

After the emergency stop is actuated, the Start button must be used to restart.



Safety-related components

Two-hand operation console	Safety relay	Input expansion	Contactor
			
3SB38 (http://www.siemens.com/sirius-commanding)	3SK1 (http://www.siemens.com/safety-relays)	3SK1 (http://www.siemens.com/safety-relays)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation (http://support.automation.siemens.com/WW/view/en/74562494)

3.6.3 Two-hand operation to SIL 3 or PL e with a Modular Safety System

Application

Two-hand operation consoles comprise two pushbuttons that must be pressed simultaneously to operate a machine. This prevents the operator from reaching into the danger zone during operation.

Design

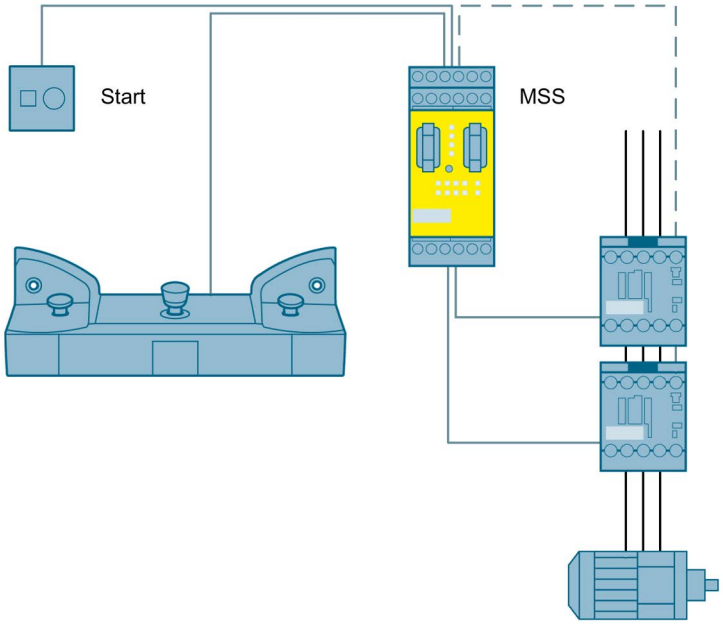
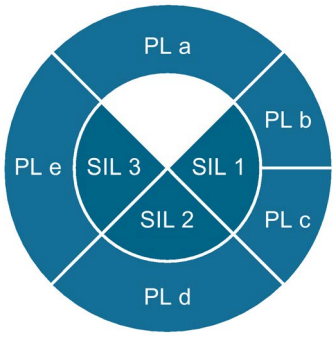


Figure 3-32 Two-hand operation to SIL 3 or PL e with a Modular Safety System

Operating principle

By imposing the condition of simultaneous pressing of both pushbuttons, the operator is restricted to the two-hand operation console and is thus unable to reach into the danger zone. The Modular Safety System only switches the enabling circuits when both signals are active within 500 ms and the feedback circuit is closed.



If one of the two pushbuttons is released, the Modular Safety System immediately switches the machine off in a safety-related manner.

The four-channel design in the two-hand operation console ensures that possible welding of one of the contacts is detected immediately.

After the emergency stop command devices are actuated, the Start button must be used to restart

Safety-related components

Two-hand operation console	Modular Safety System	Contactor
		
3SB38 (http://www.siemens.com/sirius-commanding)	3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/69064071)

3.7 Typical combinations of multiple safety functions

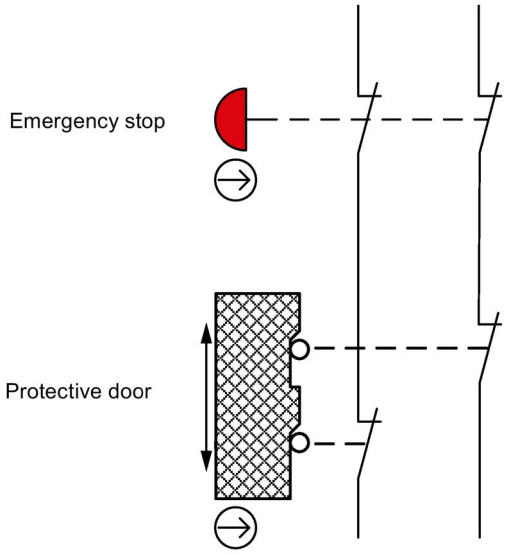
3.7.1 Introduction

Only in the rarest of cases is it sufficient to implement only one safety function on a machine. Different safety functions from the previous chapters are frequently implemented on one machine to achieve the required level of safety.

Application examples containing typical combinations of safety functions are shown in the following chapter.

Conditions for series connection of emergency stop command devices and protective door monitoring with position switches

Emergency stop command devices and position switches may only be connected in series up to PL d (per ISO 13849) or SIL 2 (per IEC 62061) if it can be ensured that the emergency stop command device and the protective door will not be actuated simultaneously (otherwise a fault cannot be detected).



Linking or cascading safety functions

If two or more plant sections are linked together, in other words, the requirement for a safety function in one plant section triggers the requirement for a safety function in the other plant section, transfer of the signal must meet the same safety function requirements in the affected plant section.

Example:

An emergency stop command device is monitored in both plant sections. The emergency stop function in plant section 1 is designed according to SIL 3 or PL e, and in plant section 2 according to SIL 2 or PL d.

Although an emergency stop command issued in plant section 2 only affects this plant section, an emergency stop command issued in plant section 1 must bring both plant sections to a safe standstill.

Since the risk assessment for plant section 2 requires SIL 2 or PL d, transfer of the signal for the emergency stop command from plant section 1 must correspond at least to this safety level. The signal lines must, therefore, be cross-circuit proof, or the signal must be transferred via a safe communication line (such as ASIsafe).

The hazard zone must always be clearly visible from the position from which the start/restart command is issued. Whether or not each plant section requires its own Start button depends on the plant and the risk assessment.

Note

Linking may be implemented within a control cabinet in a single-channel configuration. This is even permissible up to SIL 3 or PL e, because cable routing within a control cabinet is regarded as short-circuit-proof and proof against short-circuiting to P potential (fault exclusion in accordance with ISO 13849-2).

3.7.2 Emergency stop and protective door monitoring to SIL 3 or PL e with a safety relay

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off. An emergency stop command device is additionally monitored for shutting down the machine in an emergency.

Design

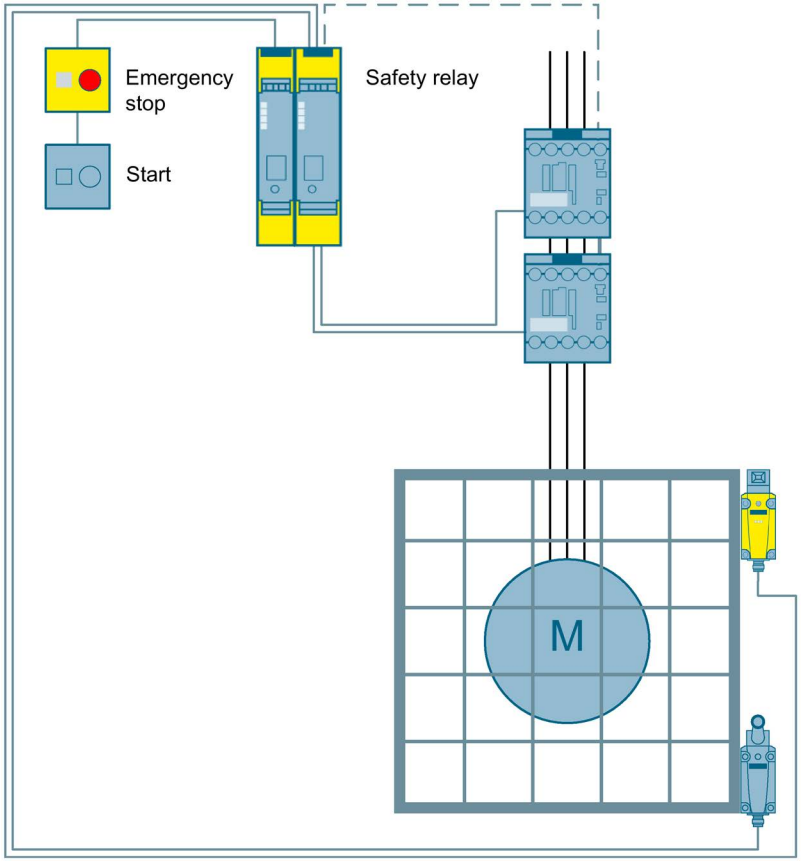
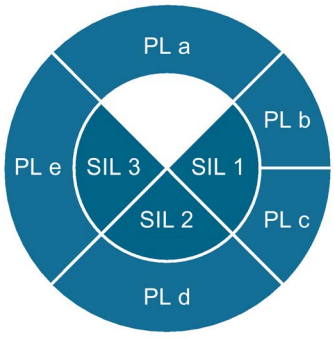


Figure 3-33 Emergency stop monitoring and protective door monitoring to SIL 3 or PL e with a safety relay

Operating principle

The safety relay monitors the two safety switches as well as the two emergency stop contacts via an additional input expansion. When the emergency stop command device is actuated or the protective door is opened, the safety relay opens the enabling circuits and switches the power contactors off in a safety-related way.

If the door is closed, the emergency stop command device is unlatched and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Emergency stop command device	Position switches		Safety relay	Input expansion	Contactor
					
3SB3 (2-channel) (http://www.siemens.com/sirius-commanding)	2x 3SE5 (http://www.siemens.com/sirius-detecting)		3SK1 (http://www.siemens.com/safety-relays)	3SK1 (http://www.siemens.com/safety-relays)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/74562495)

3.7.3 Emergency stop and protective door monitoring to SIL 3 or PL e with a Modular Safety System

Application

Protective doors are frequently used to fence off danger zones. These are monitored for position and, if necessary, the area from which the hazard emanates is switched off. An emergency stop command device is additionally monitored for shutting down the machine in an emergency.

Design

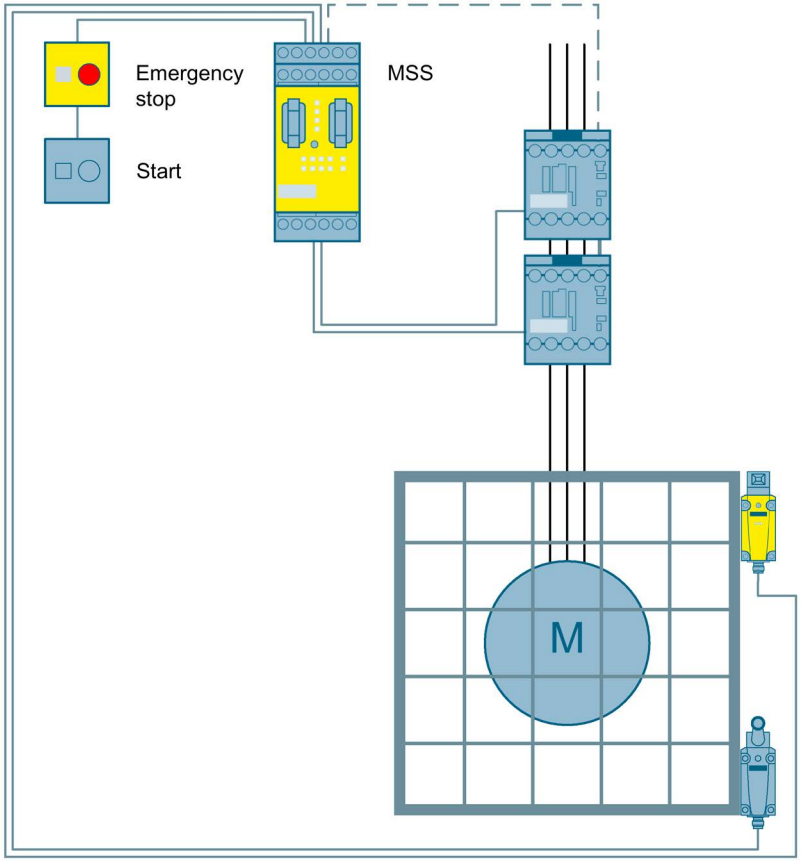
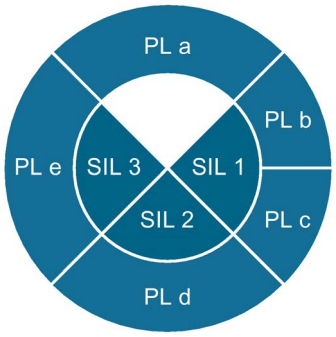


Figure 3-34 Emergency stop monitoring and protective door monitoring to SIL 3 or PL e with a Modular Safety System

Operating principle

The Modular Safety System monitors the two safety switches as well as the emergency stop command device on two channels. When the emergency stop command device is actuated or the protective door is opened, the Modular Safety System opens the enabling circuits and switches the power contactors off in a safety-related way.

If the door is closed, the emergency stop command device is unlatched and the feedback circuit is closed, the Start button can be used to switch on again.



Safety-related components

Emergency stop command device	Position switch		Modular Safety System	Contactor
				
3SB3 (2-channel) (http://www.siemens.com/sirius-commanding)	2x 3SE5 (http://www.siemens.com/sirius-detecting)		3RK3 (http://www.siemens.com/sirius-mss)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram, MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/74563943)

3.7.4 Emergency stop shutdown of multiple motors to SIL 3 or PL e with a safety relay

Application

If there is a safety requirement to switch off more than one drive simultaneously (e.g. with tool slides, machine tools, suction equipment, etc.), this can be done with the help of output expansions with additional enabling circuits.

Design

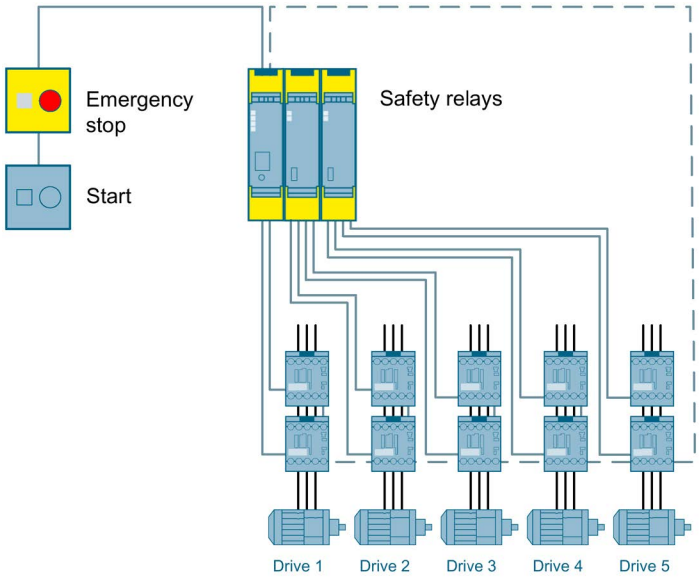
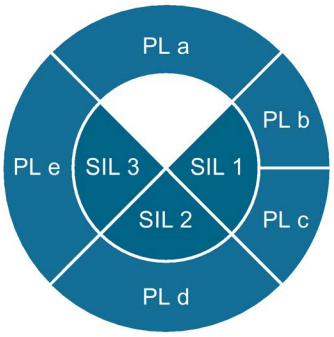


Figure 3-35 Emergency stop shutdown of multiple motors to SIL 3 or PL e with a safety relay

Operating principle

The safety relay monitors the emergency stop command device on two channels. When the emergency stop command device is actuated, the safety relay and the output expansions open the enabling circuits and switch the power contactors off in a safety-related way. If the emergency stop command device is unlatched and the feedback circuit of all actuators is closed, the Start button can be used to switch on again.

Shutdown of the individual drives represents a separate safety function in each case, even if the shutdown command originates in the same emergency stop device and safety relay.



Safety-related components

Emergency stop command device	Safety relay	Output expansion	Contactor
			
3SB3 (2-channel) (http://www.siemens.com/sirius-commanding)	3SK1 (http://www.siemens.com/safety-relays)	3SK1 (http://www.siemens.com/safety-relays)	3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/74563681)

3.7.5 Cascading of safety relays to SIL 3 or PL e

Application

Cascading of safety relays is used for tripping several safety relays in series. Multiple safety functions can then be logically connected to a shared shutdown path. At the same time, several enabling circuits can be created for selective shutdown of drive elements.

Design

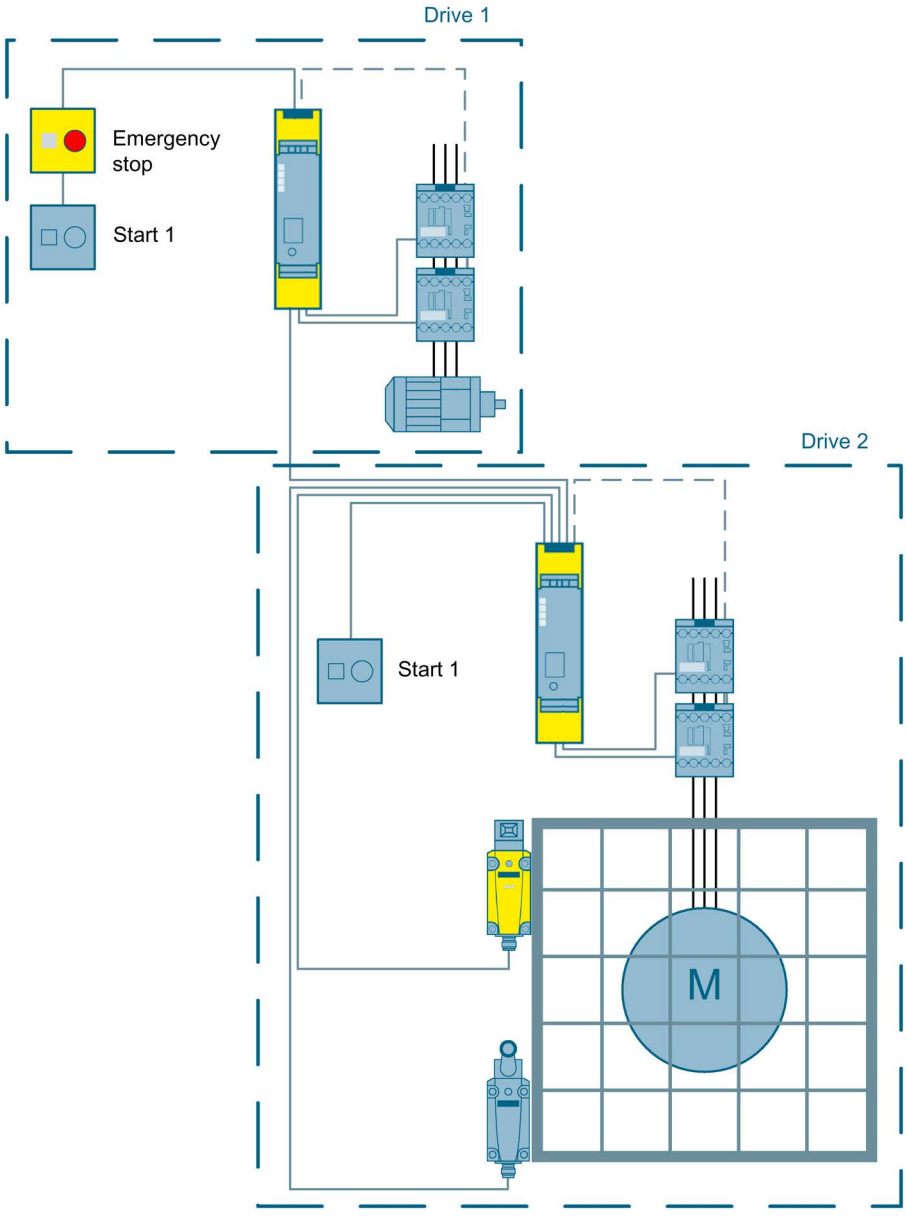
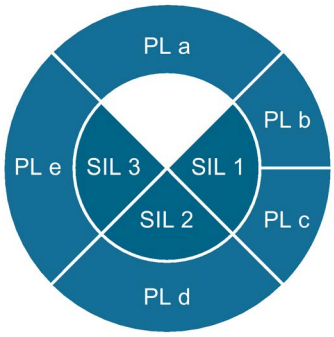


Figure 3-36 Cascading of safety relays to SIL 3 or PL e

Operating principle

The two safety relays represented are logically connected via the cascading input. If the emergency stop is triggered at the first safety relay, both safety relays then switch their actuators off. By contrast, if the protective hood shown is opened, only the associated actuators are switched off, for example.

If an emergency stop has been triggered by the higher-level safety relay, the lower-level safety relay must be switched on again manually using the Start button. A global Start button is only possible if all danger zones are visible from this Start button.



Note

This example applies to configurations within a control cabinet. If the two safety relays are not located in the same control cabinet, other precautions must be taken, such as cross-circuit-proof laying of the cascading signal.

Safety-related components

Emergency stop command device	Safety switch	Safety relay	Contactor
			
3SB3 (2-channel) (http://www.siemens.com/sirius-commanding)	2x 3SE5 (http://www.siemens.com/sirius-detecting)	3SK1 (http://www.siemens.com/safety-relays)	2x 3RT20 (http://www.siemens.com/sirius-switching)

See also

Circuit diagram and SET calculation
(http://support.automation.siemens.com/WW/view/en/77282496)

3.7.6 Safe slave-to-slave communication between several plant sections to SIL 3 or PL e via AS-i

Application

To link several plant sections logically to each other, slave-to-slave communication is required. This must be fail-safe in design to also enable transfer of safe shutdown signals. The modular safety system offers such an option with AS-i.

Design

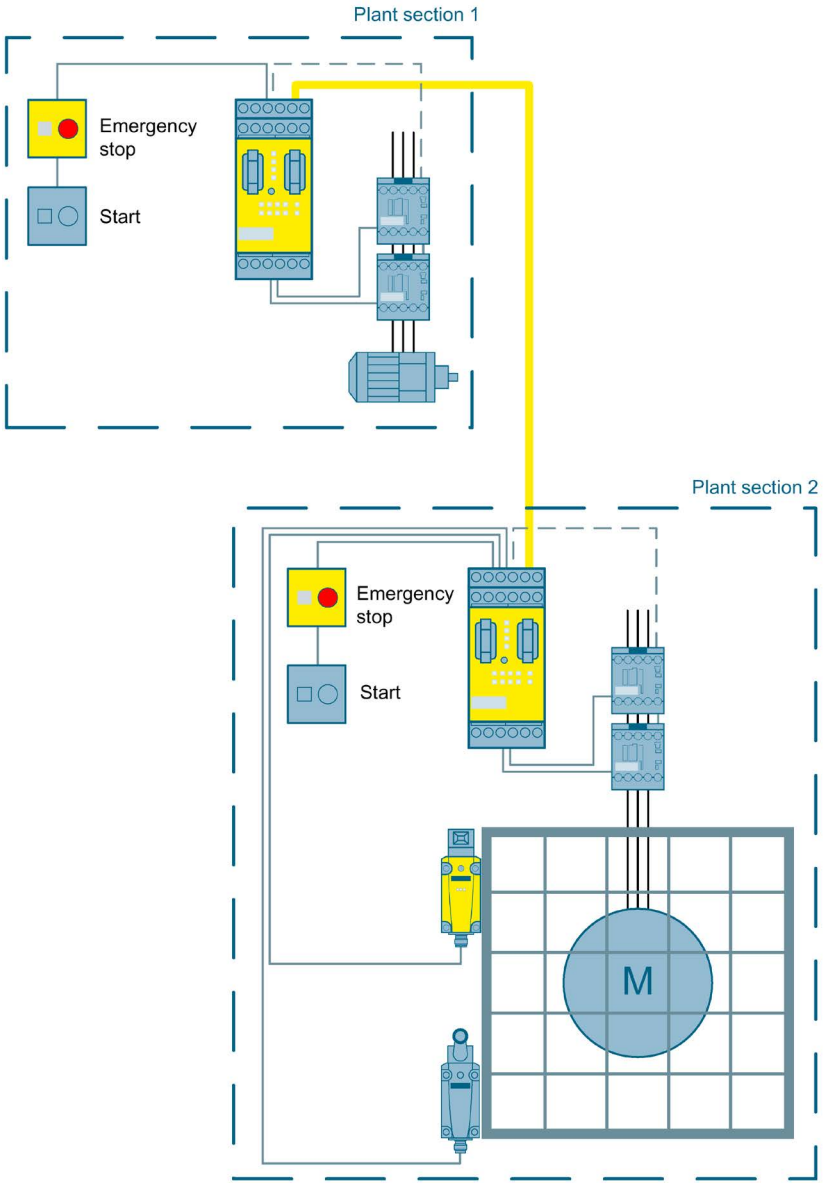
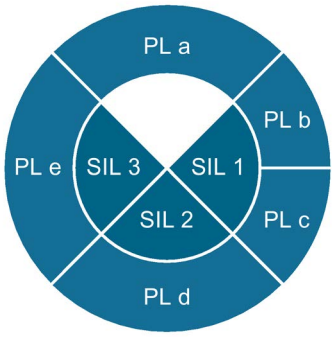


Figure 3-37 Safe slave-to-slave communication between several plant sections to SIL 3 or PL e via AS-i

Operating principle

Both plant sections are independent of each other due to the process. If the machine is shut down in one of the two plant sections, this shutdown command is forwarded to the modular safety system in the other plant section by means of safe slave-to-slave communication via AS-i.

In addition, diagnostics information and alarm signals can also be exchanged between the two plant sections.



Note

Whether both plant sections can be switched on again using the Start button, or whether each plant section requires its own Start button, depends on the plant and the risk assessment.

Safety-related components

Emergency stop command device	Safety switch		Modular safety system	Contactor
				
2x 3SB3 (2-channel) (http://www.siemens.com/sirius-commanding)	2x 3SE5 (http://www.siemens.com/sirius-detecting)		2x 3RK3 (http://www.siemens.com/sirius-mss)	4x 3RT20 (http://www.siemens.com/sirius-switching)

Note

In addition to the safety-related components, operation of an AS-i network requires an AS-i master and an AS-i power supply.

See also

MSS project and SET calculation (http://support.automation.siemens.com/WW/view/en/88823146)

More detailed FAQs on: Safe slave-to-slave communication (http://support.automation.siemens.com/WW/view/en/58512565)

Regulations and Standards

4

4.1 Regulations and standards in the European Union (EU)

4.1.1 Safety of machinery in Europe

4.1.1.1 Legal basis

Machinery Directive (2006 / 42 / EC)

When the European common market was launched, a decision was made to harmonize the domestic standards and regulations of all the EU Member States relating to the technical implementation of machines. This meant that, as an internal market directive, the content of the Machinery Directive had to be implemented by the individual member states as national legislation. In Germany, the content of the Machinery Directive was implemented as the 9th statutory instrument of the Product Safety Law (9. ProdSV). For the Machinery Directive, this was realized with the aim of achieving standard safety objectives and, in turn, removing technical trade barriers. In accordance with the definition of a machine ("an assembly of linked parts or components, at least one of which moves"), this directive has a very broad scope. The application area also extends to cover replaceable equipment, safety components, load carrying equipment, chains, belts, ropes, removable propshafts, and incomplete machines.

"Machine" also refers to an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole.

This means that the Machinery Directive is applicable from a basic machine up to a plant.

The basic safety and health requirements specified in Annex I of the Directive must be fulfilled for the safety of machines. The manufacturer must carefully observe the principles listed in Annex I, Paragraph 1.1.2 when it comes to integrating safety.

The safety objectives must be implemented responsibly to ensure compliance with the Directive. Manufacturers of a machine must verify that their machine complies with the basic requirements. This verification is facilitated by means of harmonized standards. In the case of machines that present an increased potential hazard as listed in Annex IV of the Machinery Directive, a certification procedure is demanded. (Recommendation: machines that are not listed in Annex IV can also present a significant potential hazard and must be dealt with accordingly.)

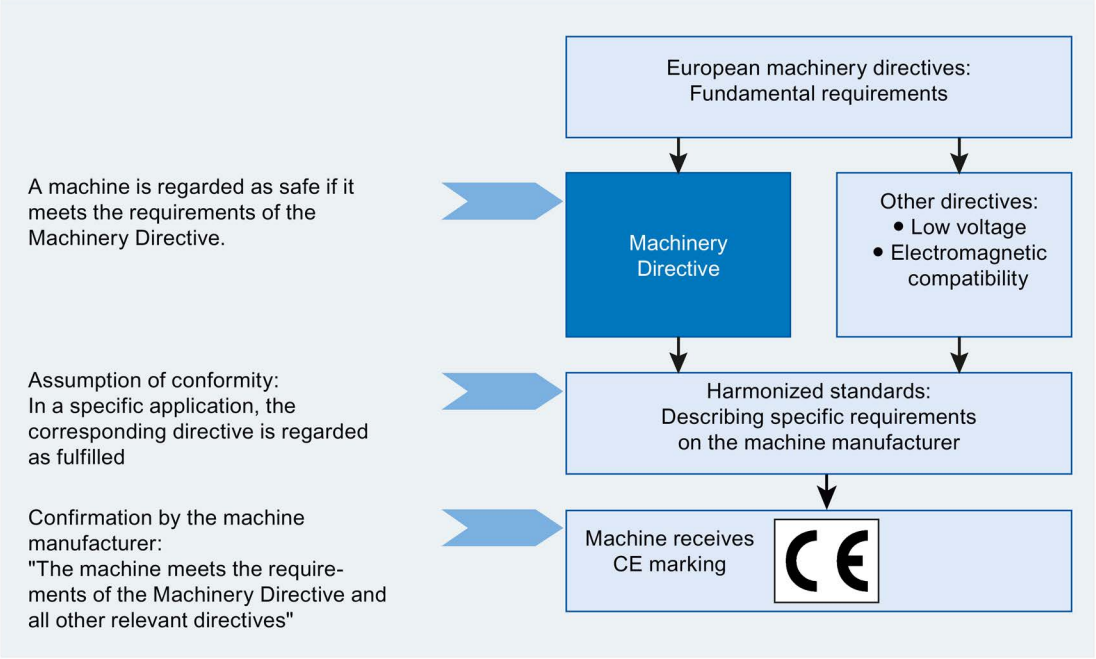


Figure 4-1 European Machinery Directives

Standards

Before any machines or plant can be put on the market or operated, they must meet the fundamental safety requirements of the EU Directives. Standards can be extremely helpful to achieving compliance with these safety requirements. In the EU, a distinction must be made here between standards that have been harmonized under an EU directive, and standards that have been ratified but not harmonized under a specific directive, as well as other technical rules also referred to as "national standards" in the directives.

Ratified standards describe the recognized state-of-the-art. In other words, by applying ratified standards, manufacturers can prove that the recognized state-of-the-art has been complied with.

All standards ratified as European standards must, in principle, be adopted unchanged as national standards of the member states, regardless of whether the standards have been harmonized under a directive or not. Existing national standards on the same subject must then be revoked. The intention is thus to create a uniform (consistent) body of standards in Europe over time.

Harmonized European standards

Harmonized European standards (EN standards) are published in the Official Journal of the European Communities and must be included in domestic standards without any revisions.

They are designed to fulfill basic health and safety requirements as well as the safety objectives specified in Annex I of the Machinery Directive.

When the harmonized standards are observed, it is "automatically assumed" that the directive is fulfilled, in other words, manufacturers can be confident that they have fulfilled the safety aspects of the directive in so far as they have been dealt with in the respective standard. However, not every European Standard is harmonized in this sense. The lists in the Official European Journal is decisive. These lists can be viewed, always up to date, on the Internet (http://www.newapproach.org/).

4.1.1.2 CE conformity process

CE conformity process

Phases in the CE conformity process

The CE conformity process is divided into different phases that must be carried out throughout the entire life cycle (planning, design, installation, operation, and maintenance).

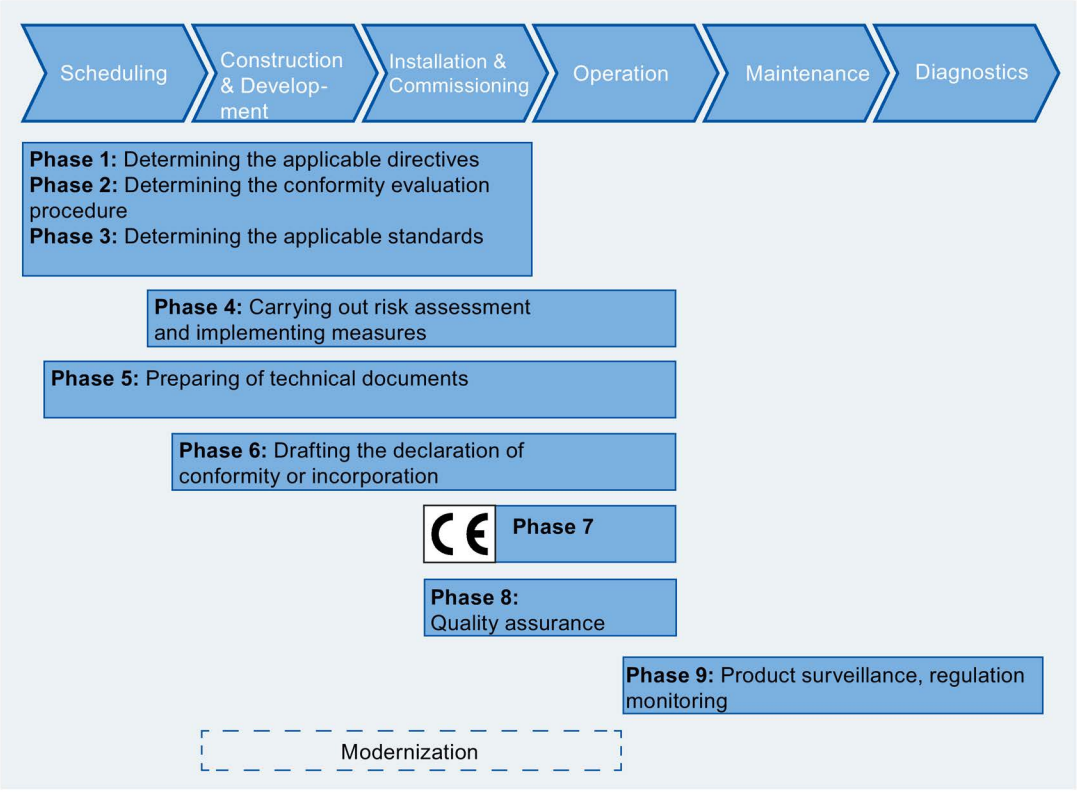


Figure 4-2 CE conformity process for machinery and plants

The applicable directives must be established in Phase 1 right back at the planning stage. This could involve one or more directives or none. (e.g. Machinery Directive, see Chapter 2.2.1)

In Phase 2, the conformity assessment procedure is established in accordance with the applicable directives from Phase 1.

Definition of the applicable standards follows in Phase 3.

Phase 4 then consists of risk assessment of the machine, risk reduction, and validation. This phase also includes assessment of the safety-related parts of the machine control. The individual steps of Phase 4 are explained in the sections below.

The technical documentation is created in parallel with planning, development and commissioning. This is also called Phase 5. The technical documentation must be available in full at the time of supplying the machine. This includes technical documentation (see Annex VII of the Machinery Directive), conformity certification, acceptance protocols (if applicable), transport documentation, etc.

If the validation procedure has been successfully completed, the declaration of conformity or declaration of incorporation can be drafted in Phase 6, and in Phase 7, the CE mark can be affixed to the machine.

All manufacturers have an obligation to monitor their products for possible hidden shortcomings after placing them on the market. This is covered by Phase 8 quality assurance and Phase 9 product monitoring. For example, information must be gathered about whether the product is actually used as originally intended, and how it behaves during its life cycle.

In particular, dangerous shortcomings, and misuse or incorrect handling of the product must be prevented by appropriate measures. If hidden shortcomings are discovered, the user must be informed.

Risk assessment

Risks are intrinsic in machines due to their design and functionality. For this reason, the Machinery Directive requires that a risk assessment be performed for each machine and, if necessary, the level of risk reduced until the residual risk is less than the tolerable risk. The standard EN ISO 12100 "Safety of machinery - General principles for design - Risk assessment and risk reduction" (03 / 2011) is to be used for the process of assessing these risks.

EN ISO 12100 mainly describes the risks and design principles to be considered, and the iterative process when assessing and reducing risks to achieve the appropriate degree of safety.

Risk assessment is a procedure that allows hazards resulting from machines to be systematically investigated. Where necessary, the risk assessment is followed by a risk reduction procedure. When the procedure is repeated, this is known as an iterative process. This can help eliminate hazards (as far as this is possible) and can act as a basis for implementing suitable protective measures.

Risk assessment involves the following steps:

- Risk analysis
  - Determining the machine limits
  - Identifying the hazards
  - Risk estimation
- Risk evaluation

As part of the iterative process to achieve the required level of safety, a risk evaluation is carried out after risk estimation. A decision must be made here as to whether the residual risk needs to be reduced. If the risk is to be further reduced, suitable protective measures must be selected and applied. The risk assessment must then be repeated.

Risks must be reduced by designing and implementing the machine accordingly (e.g. by means of controllers or protective measures suitable for the safety-related functions).

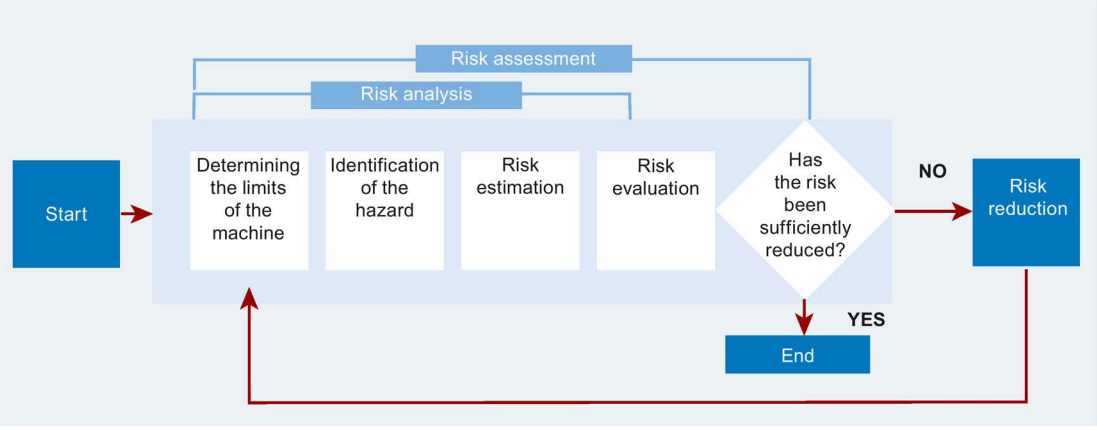


Figure 4-3 Iterative procedure for risk assessment in accordance with EN ISO 12100

Risk reduction

If the estimated risk appears to be too high, it must be reduced until the residual risk is less than the tolerable risk. For this purpose, an attempt must first be made to make the machine safe by modifying the design. If that is not possible, the risk must be reduced by applying suitable protective measures.

- The severity of possible injury can be reduced, for example, by reducing the speed of movement or power levels of the machine parts when personnel are present.
- The frequency with which personnel are present in the danger zone can be reduced by means of barriers.
- There is always a certain probability that a machine will not behave as intended, or that protective equipment will fail. This can be caused by faults in any parts of the machine. A reduction in the risk factor can be achieved by appropriate design of the safety-related parts. The safety-related parts also include the machine control if its failure can result in a hazard. The risk caused by failure of the control can be reduced by implementing the control in accordance with IEC 62061 or ISO 13849-1.
- The possibility of avoiding injury can be increased if hazard states can be detected in good time, by means of signal lamps, for example.

A common parameter in all these elements is the probability of the occurrence of an undesired event. Reducing this probability can reduce the risk.

Carry out the following steps for risk reduction:

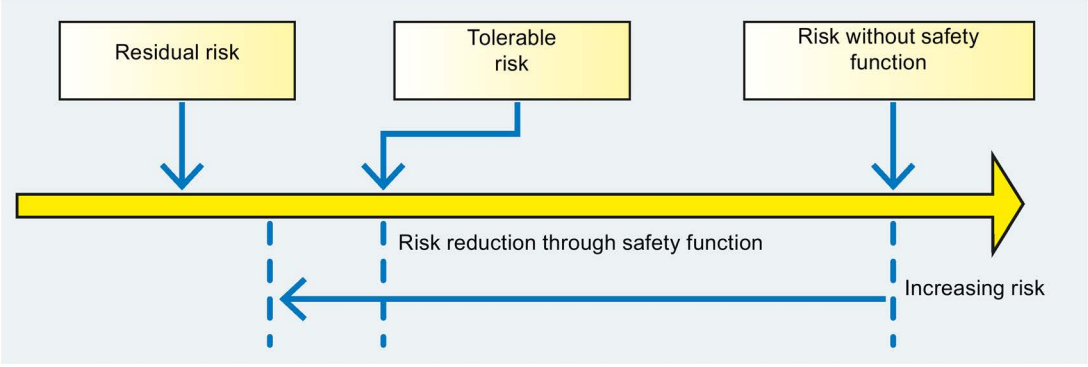


Figure 4-4 Risk reduction

Step 1: Inherently safe design

Inherently safe design removes hazards or reduces the associated risks by selecting appropriate design features of the machine itself and/or the interplay between personnel and the machine.

Safe design can be achieved, for example, by integrating safety into the machine (covers, barriers, etc.). These measures have top priority within the scope of risk reduction. They must:

- Avoid crush points
- Prevent electric shock
- Include concepts for stopping in an emergency
- Include concepts for operation and maintenance

Step 2: Technical protective measures and/or supplementary protective measures

Taking account of the intended use and reasonably foreseeable misuse, selected technical and supplementary protective measures can be suitably applied to reduce the risk if elimination of a hazard proves to be impossible, or if the associated risk cannot be sufficiently reduced by inherently safe design.

Step 2 also includes all the safety-related control functions of a machine. Special requirements apply to these. Compliance with these requirements must be tested.

Typical design of a safety-related control function:

- Sensing (position switch, emergency stop, light curtain, etc.)
- Evaluating (fail-safe controller, safety relay, etc.)
- Reacting (contactor, frequency converter, etc.)

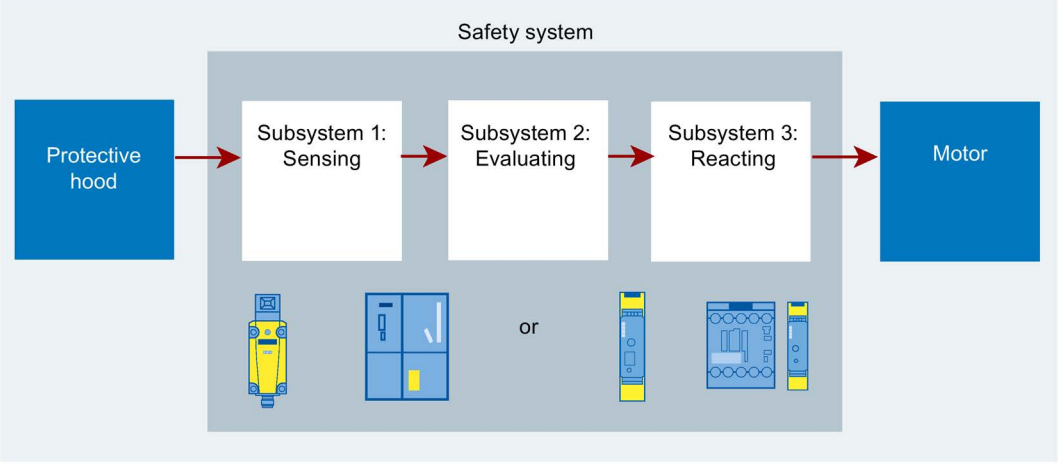


Figure 4-5 Safety system for the safety function

Step 3: User information

If risks remain despite inherently safe design and the use of technical and supplementary protective measures, the user information must draw attention to all residual risks.

This type of user information includes:

- Warning information in the operating instructions
- Special work instructions
- Pictograms
- Information on the use of personal protective equipment

Requirements regarding safety-related controller components are graded according to the magnitude of the risk and the level to which the risk needs to be reduced. EN ISO 13849-1 uses the hierarchically graded performance level (PL) for evaluation. IEC 62061 uses "safety integrity level" (SIL) to make this type of classification. Both are a measure of the safety-related performance of a control function.

It is always important - independent of which standard is applied - that all machine control parts involved in implementing these safety-related functions clearly fulfill these requirements.

Note

The control of a machine also includes the load circuits of the drives and motors.

When planning and implementing the controller, it is necessary to check whether the requirements of the selected PL or SIL are met. Since the requirements for achieving the necessary safety performance in EN ISO 13849 and IEC 62061 are structured differently, the requirements for checking are also structured differently. For design in accordance with EN ISO 13849, Part 2 (EN ISO13849-2) gives the details of validation and describes what must be taken into account. The requirements for validation of a design in accordance with IEC 62061 are described in the standard itself.

Validation

Validation means an evaluating test of the safety functionality aimed at. The purpose is to confirm the definitions and the level of conformity of the safety-related parts of the controller within the overall definition for safety requirements on the machine. The validation must also indicate that every safety-related part meets the requirements of the relevant standard. The following aspects are described here:

- Error lists
- Validation of the safety functions
- Validation of the demanded and achieved safety performance (category, safety integrity level or performance level)
- Validation of the environmental requirements
- Validation of the maintenance requirements

A validation plan must describe the requirements for carrying out validation for the defined safety functions.

Aim of the validation:

Establishment of conformity with the requirements

- of the European directives.
- that result from the customer order, the use of the machine, and, if applicable, further national requirements that apply for the machine.

All the machine-related information must be provided when the machine is made available. This includes: the customer order, the technical documentation (see Annex VII of the Machinery Directive), conformity certification, acceptance certificate (if applicable), shipping documents, etc.

4.2 Regulations and standards outside the European Union (EU)

4.2.1 Regulations and standards outside the European Union - Overview

The following description is intended to provide an overview of the regulations of some countries outside the European Union. It must not be regarded as a complete description. The precise requirements, as well as national and local rules for a special application, must be checked in detail in each individual case. For further information regarding the specifications for safety engineering in other countries, please contact the respective local approval authorities.

4.2.2 Legal requirements in the U.S.A.

With regard to the legal requirements for safety at work, a key difference between the U.S.A. and Europe is that in the U.S.A., no unified machinery safety legislation exists at the federal level that defines the responsibility of the manufacturer/supplier. Rather, there is a general requirement that employers must ensure safety at work. This is regulated by the Occupational Safety and Health Act (OSHA). The regulations of OSHA, relevant for safety at work, are described in OSHA 29 CFR 1910.xxx ("OSHA Regulations (29 CFR) PART 1910 Occupational Safety and Health"). (CFR: Code of Federal Regulations).

In addition to the OSHA Regulations, it is important to carefully observe the up-to-date standards of organizations such as NFPA and ANSI, as well as the extensive product liability legislation in the US. Two especially important standards for safety in industry are NPFA 70 (known as the National Electrical Code (NEC)) and NFPA 79 (Electrical Standard for Industrial Machinery). Both describe the fundamental requirements regarding the properties and implementation of electrical equipment. The National Electric Code (NFPA70) takes priority for buildings but also for the electrical connections of machines and machine parts. NFPA 79 applies to machines. This creates a gray area between the two standards when it comes to large machines that are made of machine parts. Large conveyor systems, for example, can be regarded as part of the building, making NFPA 70 and/or NFPA 79 applicable.

4.2.3 Legal requirements in Brazil

The Brazilian Ministry of Labor and Employment, responsible for employment relationships and other matters regarding health and safety at work, published a new version of regulatory standard NR 12 (Norma Regulamentadora Nº 12) in December 2010. Analogously to Article 137 of European Directives, this regulation applies both to new and existing machines, and has the aim of ensuring machine safety according to the state-of-the-art. Similar to international technical standards, this Brazilian regulation also covers the complete life cycle of the machine, including design, trade, transportation, operation, maintenance and disposal.

Although the new version of NR 12 is based on the European model, in which Directives are supported by international standards, it differs from them in terms of legal instruments for the assessment of conformity and in its use of harmonized standards. Instead of checks performed by third-party regulatory bodies, the Brazilian government inspects machines and installations through nominated authorities at the place of operation. Inspections only cover the requirements stipulated in the regulation, and for this reason, NR 12 has additional technical content (Annexes) for specific types of machine.

In terms of structure, NR 12 is similar to a safety standard. It has general requirements that can be fulfilled by performing a risk assessment in accordance with Type-A standards such as ISO 12100, technical requirements as given in some Type-B standards as well as specific requirements for specific machines similar to Type-C standards.

The Annexes of NR 12 are not harmonized with Type-C standards; however, most of them were either heavily influenced by Type-C standards or based on them in order to in turn comply with established international standards. Although a presumption of conformity with NR 12 is not possible, most requirements can be fulfilled by meeting the stipulations of Type-C standards.

A summary of NR 12 can be found below:

12.1 to 12.5: General principles and scope of the standard.

12.6 to 12.13: Environmental conditions for safe operation around the machinery.

12.14 to 12.23: Electrical installations – application of regular technical requirements for switchgear, control gears and electrical installations (concepts from EN 60204). This part of the standard makes reference to another regulatory standard for electrical installations (NR 10).

12.24 to 12.37: Control systems – application of concepts well defined in ISO 12100 referring to controls: arrangement and type of controls (two-hand control devices according to EN 574), mode selection, prevention of unexpected start-ups, manipulation, use of components that are 'proven-in-use' etc.

12.38 to 12.55: Safety Control Systems – general requirements, fault response and design based on categories (NRB 14153 or EN 954) in conformity with the risk assessment (ISO 12100). This part also includes requirements for fixed or movable guards (EN 953, EN 1088).

12.56 to 12.63: Emergency Stop Safety Systems – specific requirements (similar to ISO 13850).

12.64 to 12.76: Permanent means of access to parts of the machine

12.77 to 12.84: Pressurized systems

12.85 to 12.93: Conveyors and lifting systems

12.94 to 12.105: Ergonomic aspects

12.106 to 12.110: Additional risks

12.111 to 12.115: Maintenance, inspection and setup of machines

12.116 to 12.124: Signaling

12.125 to 12.129: Information for use, manuals, procedures

12.130 to 12.134: Safety procedures

12.135 to 12.147: Training and qualification

12.148 to 12.156: Supplementary requirements

ANNEX I: Safety clearances for the prevention of access to hazardous zones (ISO 13852, ISO 13853, ISO 13854 and ISO 13855)

ANNEX II: Training

ANNEX III: Means of permanent access (EN 14122)

ANNEX IV: Terms and definitions

ANNEX V: Portable saw machines

ANNEX VI: Machinery for production of bread, pastry and similar goods

ANNEX VII: Butcher shop and grocery machines

ANNEX VIII: Mechanical (EN 692), hydraulic presses (EN 693) and similar machines

ANNEX IX: Plastic injection molding machines (EN 201)

ANNEX X: Machinery for shoes production and similar goods

ANNEX XI: Machinery and devices for agricultural and forestry use

NOTE: NR 12 is currently under review and new Annexes may still be added.

4.2.4 Legal requirements in Australia

Health and safety at work also plays an essential role in Australia.
The January 2013 revision of the directives has also resulted in new requirements for machinery. The Directives "Work Health and Safety Act 2012" and "Work Health and Safety Regulations 2012" play a decisive role in conjunction with the corresponding Codes of Practice. The Directives define measures for specific hazards (such as protective fences) for the purpose of guaranteeing a safe workplace. The Codes of Practice also include practical implementations and aids for using Directives, but they are not themselves binding.

Specification and design of safety-related controls for machines

5

5.1 Safety-related parts for the machine control

5.1.1 Four risk elements

Four risk elements

Risk assessment allows determination of the risk by means of four risk elements:

- Severity of the possible harm
- Frequency with which personnel are present in the danger zone
- Probability of a hazardous event occurring
- Possibility of avoiding or minimizing the harm

These risk elements then form the input parameters for implementing a safety-related control function: They enable assignment of the risk to the requirements of the safety-related control. For this reason, the IEC 62061 offers procedures for evaluating the risk elements and grading the safety performance.

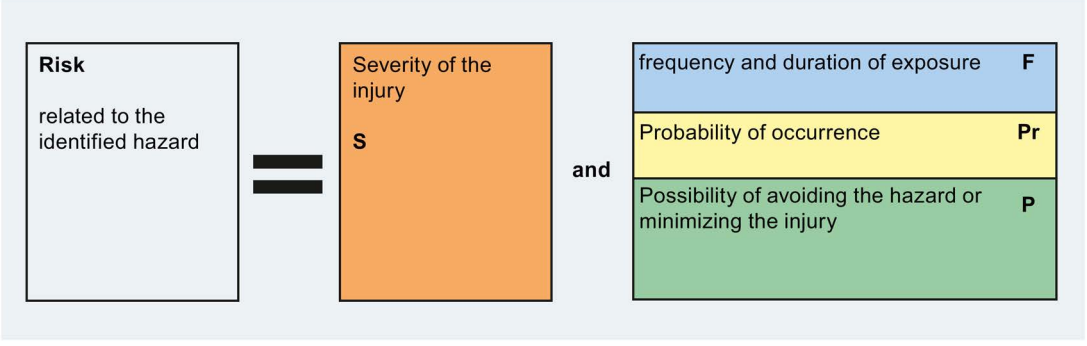


Figure 5-1 Risk related to the identified hazard

Determining the necessary safety performance (safety integrity)

If the risk assessment establishes that malfunctions of the controller or failure of the protective equipment can result in an excessively high risk, their probability must be reduced to the point where the residual risk is tolerable. In other words, the controller must achieve a sufficient "safety performance."

IEC 62061 provides a procedure that uses a system of safety performance grading that is probability-oriented, quantified and thus hierarchical. The result of the risk analysis is then the safety integrity level (SIL) for the related safety functions.

ISO 13849-1 contains a similar quantified and thus hierarchical grading of safety performance. The measure called performance level (PL) there correlates with the SILs of IEC 62061 via the assigned probabilities of failure.

By applying the EN ISO 13849-1 and IEC 62061 standards, machine manufacturers comply with the new Machinery Directive and thus also achieve export capability and liability security. These standards have introduced quantitative aspects as well as qualitative considerations. Protective measures for reducing the risk by applying the appropriate safety functions are derived from the process of risk assessment. The solution of the safety function is then checked and evaluated with hardware components and, if applicable, software components, until the safety integrity required by the risk assessment is achieved.

Note

If a C standard exists for the machine type under consideration, the protective measures described there take precedence. However, a check must be made to ensure that the specifications are up to date with regard to later technical developments.

Risk graph acc. to ISO 13849-1

The aim is to use the risk elements to calculate the required performance level PL_r, in other words, the probability of dangerous system failures.

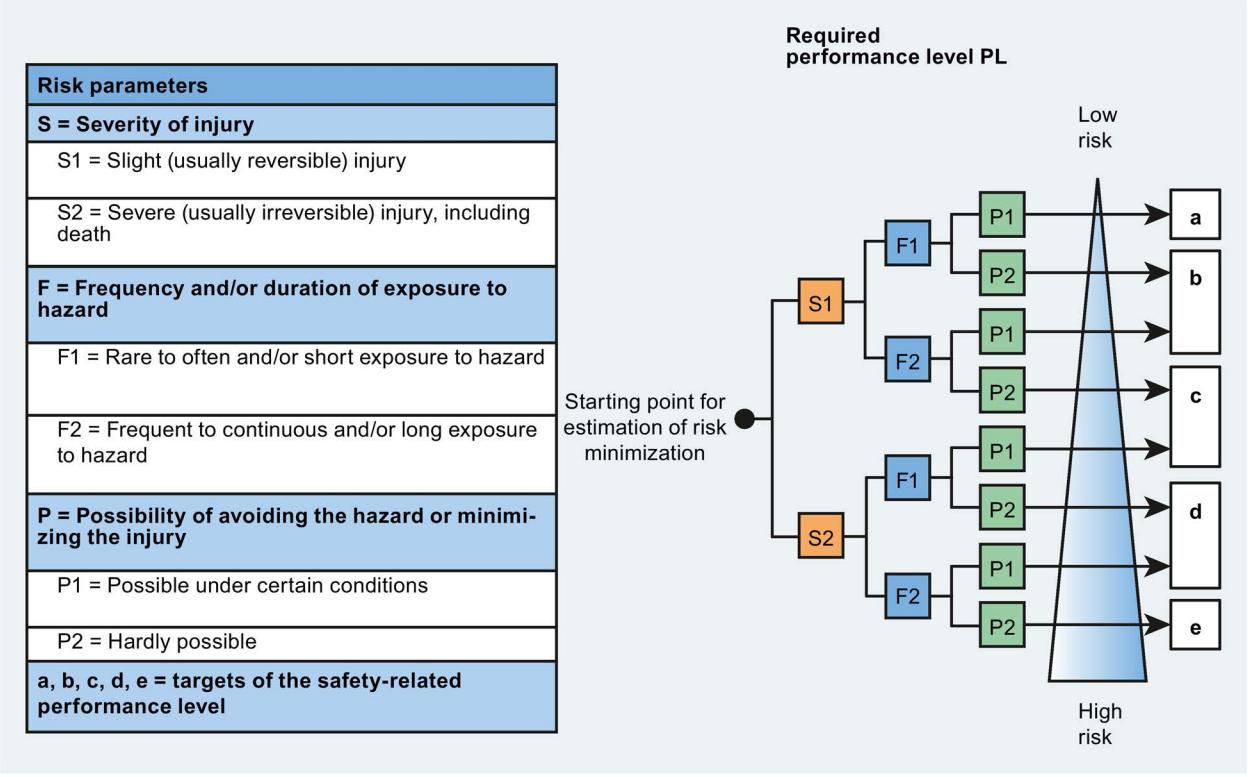


Figure 5-2 Risk graph in accordance with ISO 13849-1 for determining the required performance level

To determine the necessary performance level, the parameters **S** (severity of the injury), **F** (frequency/duration of exposure to the hazard), and **P** (possibility of avoidance) are used.

The severity of injury (S) is divided into reversible (e.g. crushing or flesh wounds) and irreversible (amputation, death).

There are no generally valid time periods for the frequency and duration of exposure to the hazard (F). If a person is exposed to the hazard more frequently than once per hour (e.g. to install workpieces), F2 (frequently to continuously) must be selected. It is also irrelevant whether the same person or different persons are exposed to the hazard. If access is only necessary from time to time, F1 (rarely to less frequently) can be selected.

The possibility of avoidance (P) is influenced by different aspects. The training and level of knowledge of the operator must be considered here, as well as the possibilities of avoidance by means of, for example, escape or operation with or without supervision. The parameter **P1** (possible under certain conditions) must only be selected if there really is the possibility of avoiding an accident or of significantly reducing the level of injury caused.

The performance levels (PLs) are a quantitative measure of the safety performance, just like the safety integrity levels (SILs) in IEC 61508 and IEC 62061.

Safety performance for implementing the controller in accordance with IEC 62061

The procedure described in IEC 62061, Annex A uses tables that can be used direct to document the executed risk assessment and SIL assignment.

For the individual risk parameters, the associated weighting is selected using the values given in the header of the table. The total of the weightings of all parameters provides the probability class of the injury.

C = F + Pr + P

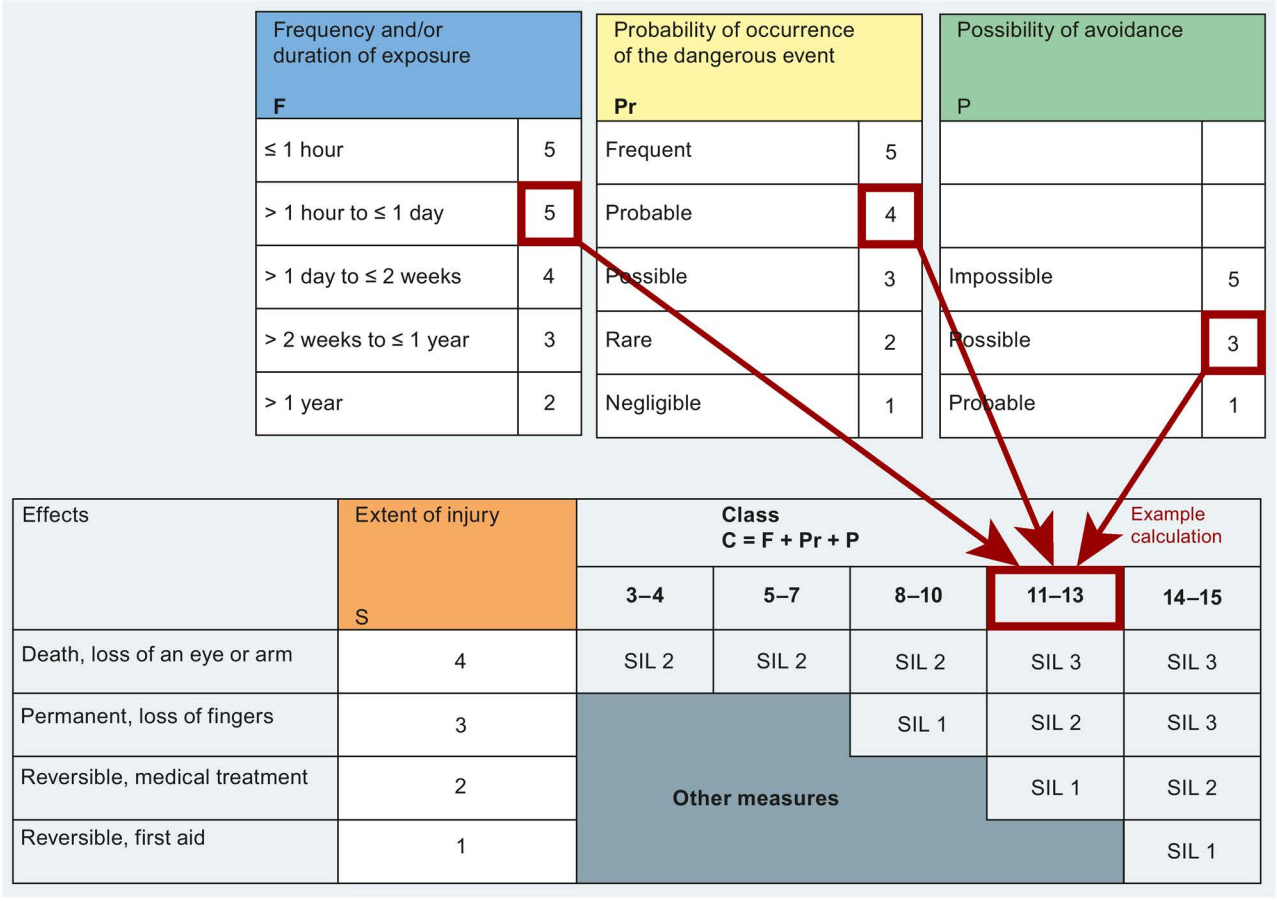
The frequency and duration of exposure is expressed by the parameter "F." The necessity of access to the danger zone can vary in the individual operating modes (automatic, maintenance mode, etc.). The type of access (setting tools, delivering materials, etc.) also plays a role and must be considered under this aspect. The applicable frequency and duration is selected from the associated table. If the duration of exposure is less than 10 minutes, the value can be reduced to the next stage down. However, the frequency value ≤1 h must never be reduced.

The probability of occurrence of the hazardous event is expressed by the parameter "Pr". This must be estimated independently of the other parameters. Human behavior (conditioned, for example, by pressure of time, lack of awareness of the hazard, etc.) must also be taken into account here. Under normal production conditions, and taking account of the worst case, the probability is "extremely high." When using a low value, a detailed reason must be provided (e.g., operator abilities very high).

The possibility of avoidance or limitation of the injury is expressed by the parameter "P." Aspects must be taken into account here that affect both the machine (e.g., possibility of removing oneself from the hazard) and the possibility of detecting the hazard (e.g. detection impossible due to high surrounding noise levels). Grading is carried out in accordance with the table (probable, possible, impossible).

With the help of this probability class and the potential severity of injury of the considered hazard, the necessary SIL for the associated safety function can be read from the table.

The aim is to determine a required safety integrity level SIL of the system from the risk elements.



Frequency and/or duration of exposure F	
≤ 1 hour	5
> 1 hour to ≤ 1 day	5
> 1 day to ≤ 2 weeks	4
> 2 weeks to ≤ 1 year	3
> 1 year	2

Probability of occurrence of the dangerous event Pr	
Frequent	5
Probable	4
Possible	3
Rare	2
Negligible	1

Possibility of avoidance P	
Impossible	5
Possible	3
Probable	1

Effects	Extent of injury S	Class C = F + Pr + P				Example calculation
		3–4	5–7	8–10	11–13	14–15
Death, loss of an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, loss of fingers	3	Other measures		SIL 1	SIL 2	SIL 3
Reversible, medical treatment	2				SIL 1	SIL 2
Reversible, first aid	1					SIL 1

Figure 5-3 Determination of the required SIL

5.2 Specification of the safety requirements

Specification of the safety requirements

If control functions have been identified as safety-related, or if protective measures are to be implemented with controller resources, the precise requirements for these "safety functions" ("safety-related control functions") must be defined in the safety requirements specification. This specification includes descriptions of the following for each safety-related function:

- its functionality, that is, all the required input information, its logical combination, and the associated output states or actions, as well as the frequency of use
- the necessary response times
- the required safety performance

The specification of the safety requirements contains all the information required for designing and implementing the controller. It is the interface between the machine designer and the manufacturer/integrator of the controller, and can thus also be used to demarcate responsibilities.

5.3 Design and implementation of the (safety-related) controller in accordance with IEC 62061

5.3.1 Philosophy/theory

Structuring principle for a safety-related control system

Correct design is an essential prerequisite for the correct and intended functioning of a controller. To achieve this aim, IEC 62061 has defined a systematic top-down design process:

A safety-related electrical control system (SRECS) encompasses all components from information acquisition, through information combination, up to and including the execution of actions. To enable a simple systematic procedure for the design, safety-related assessment, and implementation of an SRECS that is to meet the requirements of IEC 61508, IEC 62061 uses a structuring principle based on the following architectural elements (see the figure below).

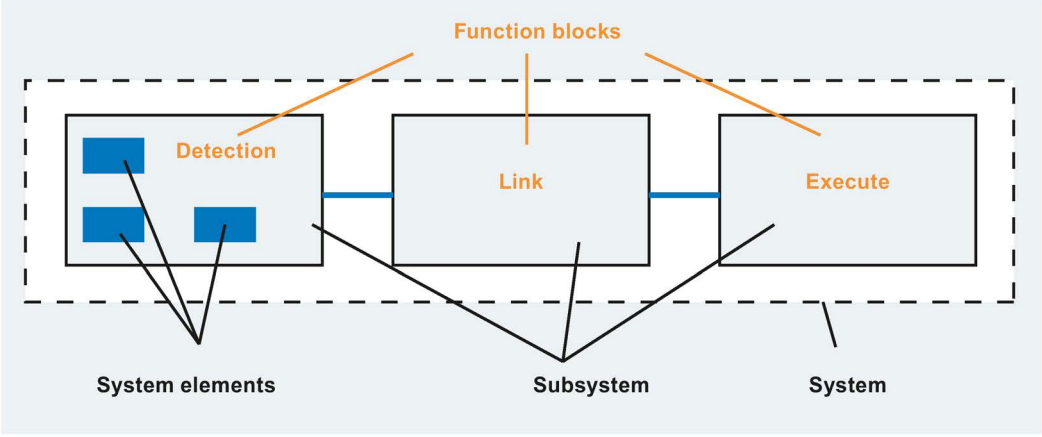


Figure 5-4 Structuring elements of the system architecture

Initially, a distinction is made between a "virtual" (that is, functional) view, and the "real" (that is, system) view. The functional view considers only the functional aspects, regardless of the hardware and software implementation. The virtual view only considers, for example, the information to be acquired, how that information is to be combined, and which action is to result. However, no statement is yet made about whether, for example, redundant sensors are required for gathering the information, or how the actuators are implemented. Only with the "real view" is implementation by the SRECS considered. A decision must then be made here as to whether, for example, one or two sensors are required to capture specific information to achieve the required safety performance. The following terms are defined.

Terms for structuring the functions (functional view)

- **Function block**
  Smallest unit of a safety-related control function (SRCF) whose failure results in the failure of the safety-related control function.
  Remark: In IEC 62061, an SRCF (F) is regarded as a logic "and" combination of the functions blocks (FBs), e.g. F = FB1 & FB2 & ... & FBn. The definition of a function block differs from the definition used in IEC 61131 and other standards.
- **Function block element**
  Part of a function block.

Terms for structuring the real system (system view)

- **Safety-related electrical control system**
  Electrical control system of a machine whose failure leads to a direct increase in the risk.
  Remark: An SRECS encompasses all the parts of an electrical control system whose failure can lead to a reduction in, or the loss of, functional safety. This can encompass both energy and control circuits.
- **Subsystem**
  Part of the SRECS architecture design on the topmost level. The failure of any one subsystem leads to a failure of the safety-related control function.
  Remark: In contrast to general usage whereby "subsystem" can mean any subordinate unit, the term "subsystem" in IEC 62061 is used within a strictly defined hierarchy of terminology. "Subsystem" means subdivision at the topmost level. The parts resulting from further subdivision of a subsystem are called "subsystem elements"
- **Subsystem element**
  Part of a subsystem that encompasses an individual component or group of components. With these structuring elements, control functions can be structured in accordance with a clear procedure in such a way that defined parts of the function (function blocks) can be assigned to specific hardware components, the subsystems. This results in clearly defined requirements for the individual subsystems so that they can be designed and implemented independently of each other. The architecture for implementing the full control system results from arranging the subsystems in the same way as the function blocks are arranged (logically) within the function.

5.3.2 Design process of a safety-related control system (SRECS)

Design process

If the safety requirements specification is available, the designated control system can be designed and implemented. A control system that meets the specific requirements of a specific application cannot generally be purchased off the shelf, but instead must be designed and built from available devices, individually for the machine in question.

The design process takes a step-by-step approach and starts by finding a suitable control system architecture for each safety function. The architectures of all the safety functions of the machine in question can then be integrated to form a control system.

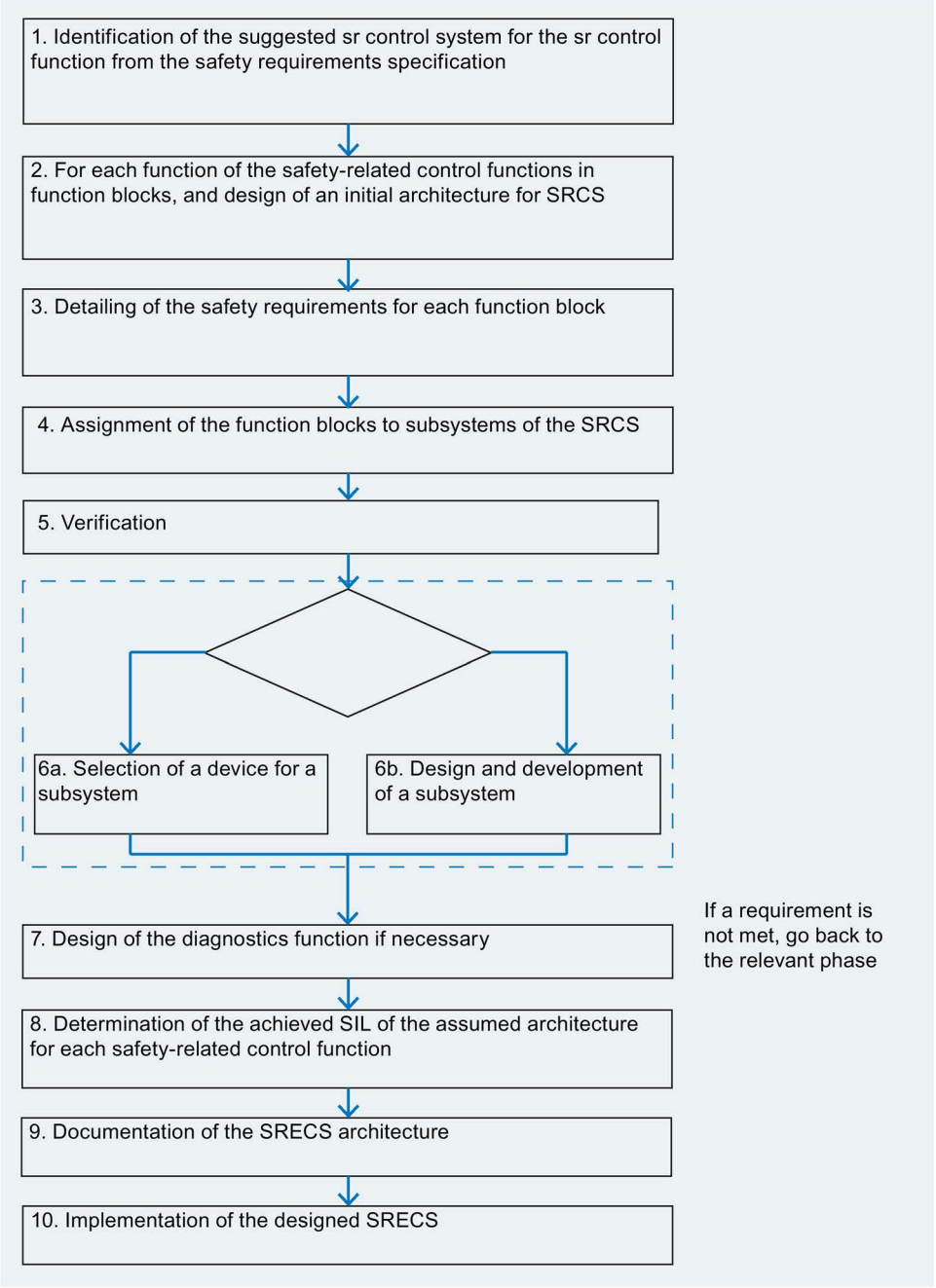


Figure 5-5 Design process of a safety-related control system

Structuring the safety function

The basic principle of structured design involves subdividing each control function into (conceptual) function blocks in such a way that these can be assigned to specific subsystems. The demarcation of the individual function blocks is selected in such a way that they can be fully executed by specific subsystems. It is important here that each function block represents a logical unit that must be executed correctly for the correct execution of the overall safety function.

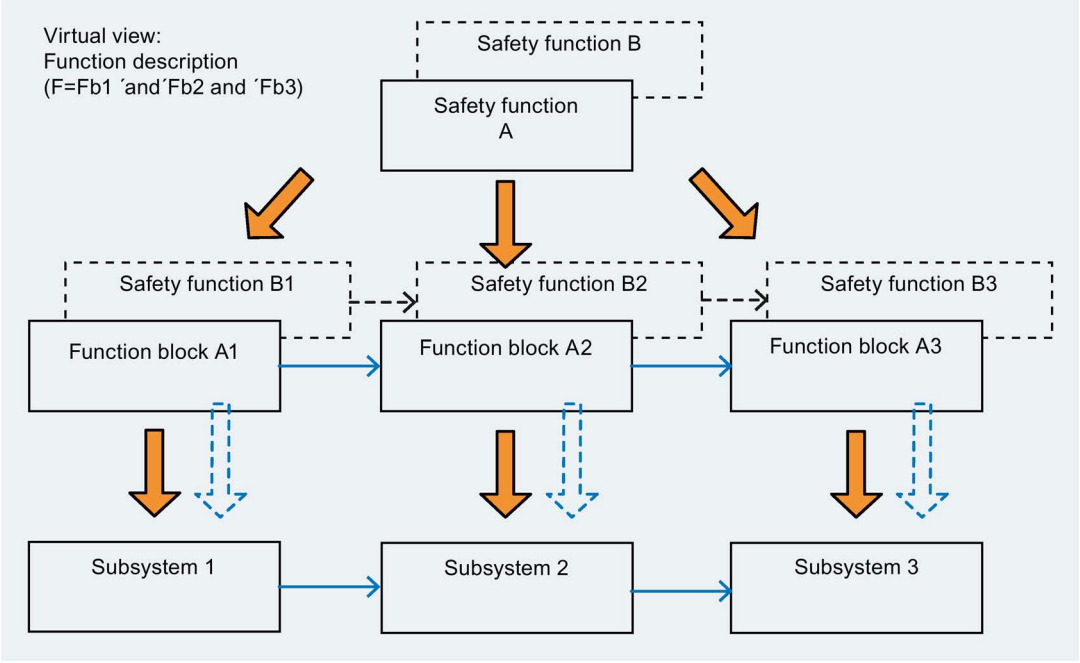


Figure 5-6 Subdivision of a safety function into function blocks and assignment to subsystems

Safety performance of a subsystem in accordance with IEC 62061

"Safety integrity" in accordance with IEC 62061 requires the fulfillment of the three basic requirements that are graded according to the SIL:

1. Systematic integrity
2. Structural constraints, in other words, fault tolerance, and
3. Limited probability of hazardous, random (hardware) failures (PFH_D).

The systematic integrity (1) of the system required for the whole function, and the structural constraints (2) apply for the individual subsystems just as for the system. In other words, if each individual subsystem meets the required systematic integrity and the structural constraints of a specific SIL, the system also meets them. However, if a subsystem meets only the lower requirements of a lower SIL, this limits the SIL that the system can achieve. We therefore refer to the "SIL claim limit" (SIL CL) of a subsystem.

- Systematic integrity: SIL SYS <= SIL CL_{lowest}
- Structural constraints: SIL SYS <= SIL CL_{lowest}

Limiting the probability of hazardous, random faults (3) applies for the overall function; in other words, it must not be exceeded by all subsystems together. The following therefore applies:

$PFH_D = PFH_{D1} + ...+ PFH_{Dn}$

5.3.3 System design for a safety function

Architectural design

The architecture of a control system for a specific safety function corresponds in its logical structure to the previously determined structure of the safety function. To define the real system structure, the function blocks of the safety function are assigned to specific subsystems. The subsystems are then interconnected in such a way that the connections specified by the function structure are established. The physical interconnection takes place in accordance with the properties of the selected technology, e.g. by means of single wiring (point-to-point) or bus connection.

The same procedure is used for further safety functions of the machine or plant. However, in doing so, function blocks that correspond to those of other safety functions can be assigned to the same subsystems. So if, for example, the same information has to be acquired for two different functions (the position of the same protective door, for example), the same sensors can be used for the purpose.

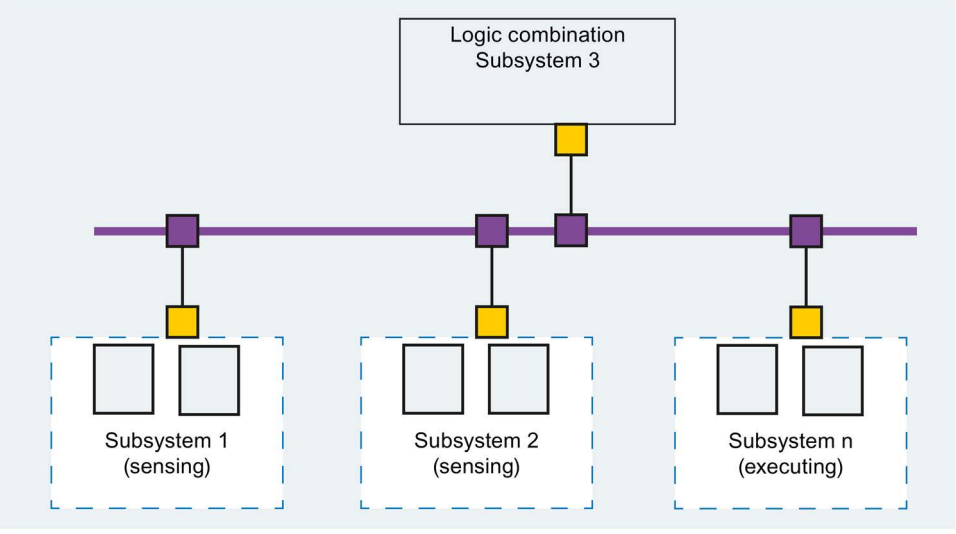


Figure 5-7 Example of a system architecture for a safety function

Selection of suitable devices (subsystems)

A subsystem that is to be used for implementing a safety function must have the required functionality and must meet the relevant requirements of IEC 62061. Microprocessor-based subsystems must comply with IEC 61508 for the relevant SIL.

The individual subsystems must meet the safety parameters (SIL CL and PFH_D) required in the specification.

In many cases, devices require additional fault detection measures (diagnostics) to actually achieve the safety performance specified for their use as a subsystem. This fault detection can, for example, can be carried out by means of additional devices (such as SIRIUS 3SK1 safety relays) or corresponding software diagnostics blocks in the logic processing. For such cases, the device description must include the corresponding information.

If a suitable device that meets the requirements of a subsystem specified in this way is not available, it must be assembled by combining available devices. This requires a subsequent design step. For details, see section "Design and implementation of subsystems (Page 154)."

5.3.4 Implementation of the safety-related control system

A safety-related control system must be implemented in such a way that it meets all the requirements in accordance with the demanded SIL. The aim is to sufficiently reduce the probability both of systematic and random faults that can result in dangerous failure of the safety function. The following aspects should be noted:

- Hardware integrity, in other words, architectural constraints, (fault tolerance) and limited probability of failure
- Systematic integrity, in other words, requirements for avoiding and controlling faults
- Behavior when a fault is detected, and software design / software development

Hardware integrity

Each subsystem must possess adequate fault tolerance for the SIL of the system. This depends on the proportion of faults tending toward a safe state related to the probability of all possible faults of the subsystem. Potentially dangerous faults of a subsystem detected in good time by the diagnostics are among the faults tending toward a safe state.

The permitted probability of failure of a safety function is limited by the SIL defined in the specification.

Systematic integrity

Measures must be applied both for avoiding systematic faults and for controlling faults remaining in the system.

Avoiding systematic faults:

- The system must be installed in accordance with the safety plan
- The manufacturer's specifications for the devices used must be followed
- The electrical installation must be carried out in accordance with IEC 60204-1 (7.2, 9.1.1 and 9.4.3)
- Check the design for suitability and correctness
- Use of a computer-aided tool that uses pre-configured and tested elements.

Controlling systematic faults:

- Use of the principle of energy shutdown
- Measures for controlling temporary subsystem failures or faults, due to voltage interruptions, for example
- When connecting the subsystems by means of a bus, the data communication requirements of IEC 61508-2 must be fulfilled (e.g. PROFIsafe and ASIsafe)
- Faults in the connection (wiring) and the interfaces of the subsystems must be detected, and appropriate responses must be initiated. For systematic handling, the interfaces and the wiring are regarded as a component part of the relevant subsystem.

For details, see IEC 62061 6.4

Behavior when a fault is detected

If subsystem faults can result in a dangerous failure of a safety function, the faults must be detected in good time, and an appropriate response must be initiated to avoid the hazard. The extent to which automatic fault detection (diagnostics) are necessary depends on the failure rate of the devices used, and the SIL to be achieved (or the required PFH of the subsystem).

How the system or subsystem must behave when a fault is detected depends on the fault tolerance of the relevant subsystem. If the detected fault does not result directly in the failure of the safety function, in other words, fault tolerance > 0, a fault response is not necessary immediately, but only when the probability of the occurrence of a second fault becomes high (usually after hours or days). If the detected fault results directly in the failure of the safety function, in other words, fault tolerance = 0, a fault response is necessary immediately, that is, before a hazard occurs.

5.3.4.1 Achieved safety performance

Achieved safety performance

The specification of every safety function defines the safety performance the function requires. This must be fulfilled by the safety-related control system.

Which safety performance a system achieves must be determined for each safety function. This is done using the architecture of the system and the safety parameters of the subsystems involved in executing the safety function under consideration.

Design according to IEC 62061

The achieved SIL is limited by the "SIL suitability" of its subsystems. The lowest value of the subsystems used limits the SIL of the system to this value. (The chain is only as strong as its weakest link.)

- Systematic integrity: SIL SYS <= SIL CL_{lowest}
- Structural constraints: SIL SYS <= SIL CL_{lowest}

For connecting the subsystems together, the same requirements must be met. For this, individual wiring is regarded as a component part of each of the two connected subsystems. In the case of bus connection, send and receive hardware and software are component parts of the subsystems.

Apart from this basic suitability, the probability of a dangerous failure of every safety function must be considered. This value is derived from the simple addition of the failure probabilities of the subsystems involved in the function:

$PFH_D = PFH_{D1} + ... + PFH_{Dn}$

In the case of bus connections, the probability of possible data transmission errors (PTE) must also be added.

The value determined in this way for a specific safety function must be less than (or equal to) the value determined by the associated SIL.

Table 5- 1 Limits to the probabilities of dangerous faults of a safety function

Probability of a dangerous failure per hour (PFH_D)			
	SIL 1	**SIL 2**	**SIL 3**
PFH_D	$< 10^{-5}$	$< 10^{-6}$	$< 10^{-7}$

5.3.5 System integration for all safety functions

After the architectures for all safety functions have been designed, the next step is the integration of these function-specific architectures to form the complete safety-related control system.

Wherever multiple safety functions have identical function blocks, shared subsystems can be used for their implementation:

- For example, you need only one safety PLC to implement the logic of all safety functions.
- If the status of the same protective door has to be sensed to eliminate a number of different hazards (in other words, for different safety functions), only one sensor only has to be installed on this door for them all.

This does not affect the safety integrity that has already been determined for the individual functions. This only has to be taken into account when determining the switching frequency of the electromechanical (wear-prone) devices.

5.3.6 Design and implementation of subsystems

As an alternative to the selection of an existing subsystem, a subsystem can also be assembled by combining devices that do not on their own meet the safety requirements, but that achieve the necessary safety performance when combined. This is the SIL claim limit (SIL CL) dictated by the SIL of the safety function with regard to systematic integrity and structural restrictions. For the probability of dangerous, random faults (PFH_D), the maximum PFH values for the individual subsystems has been defined when designing the system architecture.

Redundancy is generally required, at least for SIL 2 and SIL 3, whether to achieve the necessary fault tolerance, or to enable fault detection (diagnostics). However, the combination of two devices to form one subsystem can also be required to reduce the probability of a dangerous failure.

The precise requirements for designing and implementing subsystems are described in IEC 62061, Section 6.7 and 6.8. The following description provides an overview.

Subsystem architectural design

A special subsystem architecture must always be designed when the necessary safety integrity (safety performance) cannot be achieved direct with the devices provided for a specific task (subfunction, "function block"). In general, the safety-related features

- Low probability of failure
- Fault tolerance, fault control
- Fault detection

can only be achieved by means of special architectural measures. The extent to which specific measures are necessary depends on the required safety performance (safety integrity).

A specific (sub)function, the function block (e.g. locking of a door), is assigned to the subsystem. This function block is initially (conceptually) subdivided into individual elements (function block elements) that can then be assigned to specific devices, the subsystem elements. In general, the same function can be assigned to two function block elements (the function has been effectively doubled). If these function block elements are then implemented using separate devices, the subsystem has single fault tolerance (single redundancy).

Detecting faults in a subsystem (diagnostics)

For a subsystem without fault tolerance, every fault results in a loss of function. The failure of the function can result in a dangerous or safe machine state, depending on the type of fault. Faults that result in a dangerous machine state are critical. They are called "dangerous faults." To avoid a dangerous fault actually resulting in a hazard, you can detect certain faults by means of diagnostics, and put the machine into a safe state before the hazard occurs. A dangerous fault detected by diagnostics can thus be converted to a "safe fault."

In a redundant subsystem, the first fault does not yet result in failure of the function. Only a further fault can cause the loss of the function. To avoid failure of the subsystem, the first fault must therefore be detected before a second fault occurs. Fault detection must, of course, be linked to an appropriate system response. In the simplest case, the machine is stopped, for example, to bring it to a safe state that does not require the (faulty) safety function.

As a result of fault detection (diagnostics) linked to an appropriate fault response, the probability of a dangerous failure of the relevant safety function is reduced in both cases. The degree to which the probability is reduced depends, among other things, on how many of the possible hazardous faults are detected. The measure for this is the diagnostic coverage (DC).

Fault detection in a subsystem can be carried out in the relevant subsystem itself or by another device, e.g. the safety PLC.

Systematic integrity of a subsystem

When designing and implementing a subsystem, measures must be taken both to avoid and to control systematic faults, for example:

- The devices used must comply with the relevant international standards.
- The manufacturer's conditions of use must be observed.
- The design and the materials used must be such that they withstand all expected environmental conditions.
- Behavior in response to environmental influences must be pre-defined so that a safe state of the machine can be maintained.
- Online fault detection
- Positive actuation to initiate a protective measure

The requirements described in IEC 62061 refer only to the design of electrical subsystems of a low level of complexity, in other words, not to subsystems with microprocessors. The required measures apply equally for all SILs.

Probability of failure (PFH_D) of a subsystem

Possible failures are differentiated according to whether they are "safe" or "dangerous." Dangerous failures of a subsystem are defined as follows.

Dangerous failure

Failure of an SRECS, a subsystem, or subsystem element with the potential to cause a hazard or non- functional state.

Note: Whether such a state occurs or not can depend on the system architecture; in systems with multiple channels for improving safety, the probability of a dangerous hardware failure resulting in a dangerous overall state or a functional failure is low.

This means, for example: In a redundant subsystem (that is, fault tolerance 1), a fault in a channel is said to be dangerous if it is potentially dangerous, in other words, if it can result in a dangerous state of the machine in the absence of a second channel.

For the safety requirements, only the probability of dangerous failures is significant. Although "Safe faults" impair the availability of the system, they do not cause a hazard.

The probability of failure of a subsystem depends on the failure rates of the devices that make up the subsystem, the architecture and the diagnostics measures. For the two most commonly used architectures, the formulas are specified in IEC 62061.

Structure without fault tolerance with diagnostics

With this structure (see the figure below), the subsystem fails if any one of its elements fails, in other words, a single fault results in the failure of the actual safety function. But this does not yet necessarily mean a dangerous loss of the safety function. Depending on the type of the fault, the machine can go to a safe or a dangerous state, in other words, the subsystem has a "safe" or a "dangerous" fault. If the probability of dangerous failure per hour (PFHd) is greater than given in the specification, these faults must be detected by means of diagnostics, and a fault response must be initiated before a hazard arises. This turns dangerous faults into safe faults, and consequently the probability of a dangerous failure of the subsystem is reduced, so that the probability of failure permitted in the specification can possibly be achieved.

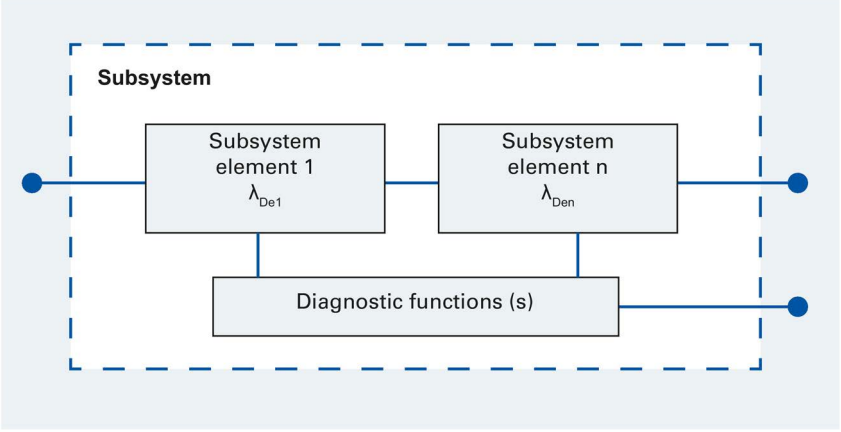


Figure 5-8 Logic structure of a subsystem without fault tolerance with diagnostics

Structure with simple fault tolerance and diagnostics

With this structure (see the figure below), the first fault does not yet result in failure of the function. However, the fault must be detected before the probability of occurrence of a second fault, that is, the failure of the subsystem, exceeds the limit given in the specification.

As well as independent, random faults, the possibility of common cause failures must be noted in redundant subsystems. Homogenous redundancy does not help against such faults. At the design stage, systematic measures must therefore be taken to make their probability sufficiently low. Since common cause faults can never be completely ruled out, they must be taken into account in calculating the probability of failure of a subsystem. This is done with the help of the common cause factor (β) with which the effectiveness of the adopted measures is evaluated. Annex F of IEC 62061 contains a table for determining the achieved common cause factor.

With this structure, a single failure of any subsystem element does not result in the failure of the safety-related control function.

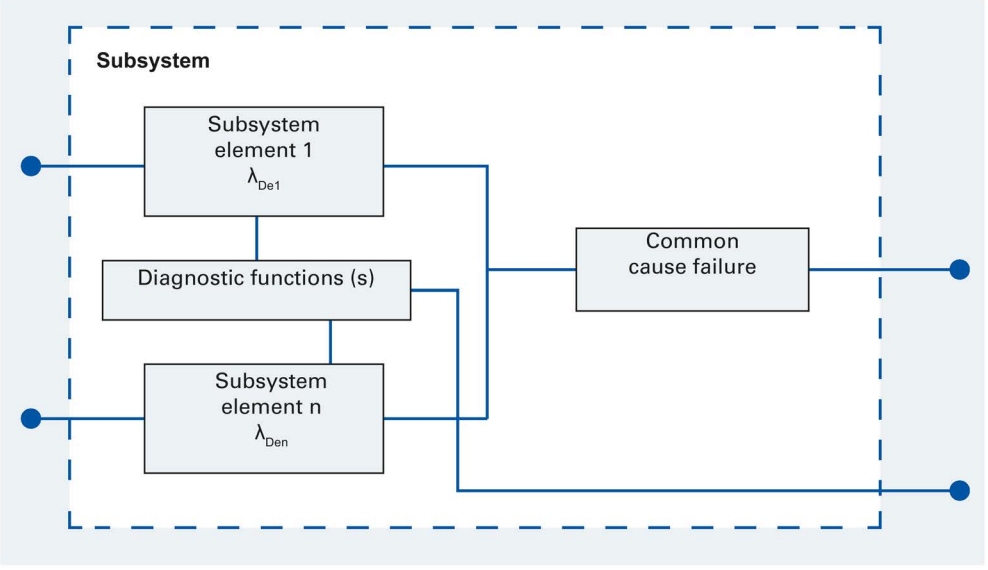


Figure 5-9 Logic structure of a subsystem with simple fault tolerance with diagnostics

Structural constraints of a subsystem

The structural constraints demand a minimum of fault tolerance depending on the type of the possible faults of the subsystem. The greater the proportion of "safe" faults, the lower is the required fault tolerance for a specific SIL.

The table below shows the relevant limits. "Safe faults" in this context are also potentially dangerous faults that are detected by diagnostics.

Table 5- 2 Structural constraints of a subsystem

Proportion of safe faults	Hardware fault tolerance	
	0	1
< 60 %	Not permissible (see the standard for exceptions)	SIL 1
60% to < 90%	SIL 1	SIL 2
90% to < 99%	SIL 2	SIL 3
≥ 99 %	SIL 3	SIL 3
Note: A hardware fault tolerance of N means N+1 faults can result in the loss of the function.		

So for a subsystem, for example, that is to be used for SIL 2, no fault tolerance is required (FT = 0) if the proportion of its faults that tend toward a safe state is more than 90%. Most devices do not achieve this value on their own. However, you can reduce the proportion of dangerous faults by detecting the faults by means of diagnostics and initiating an appropriate response in good time.

The safe failure fraction of a subsystem is the proportion of faults that result in a safe state of the machine as a percentage of all faults of the subsystem weighted according to the probability of their occurrence.

5.4 Design and implementation of safety-related parts of a controller in accordance with ISO 13849-1

Purpose

A safety-related (control) system must execute a safety function correctly. Even in the event of a fault, it must behave in such a way that the machine or plant remains in, or is brought to, a safe state.

Determining the necessary safety performance (safety integrity)

The requirements of the safety function have been determined by means of the process of risk assessment (see chapter "Safety-related parts for the machine control (Page 137)").

ISO 13849-1 prescribes a required performance level PL_r. See chapter "Safety-related parts for the machine control (Page 137)."

Design process of the safety-related parts of a controller

The categories in accordance with ISO 13849-1 refer equally to the system (safety function) and its subsystems. When implementing in accordance with ISO 13849-1, the same principle of structuring the safety-related system can be used as that described in IEC 62061. Each subsystem separated in this way must then achieve the performance level demanded for the protective function. The requirements of the relevant category also apply for wiring of the subsystems together.

In ISO 13849-1, the performance level PL_r is additionally introduced at the design stage as the quantitative variable for the probability of failure alongside the categories.

The figure below shows the iterative process for structuring the safety-related parts of the controllers (SRP / CS):

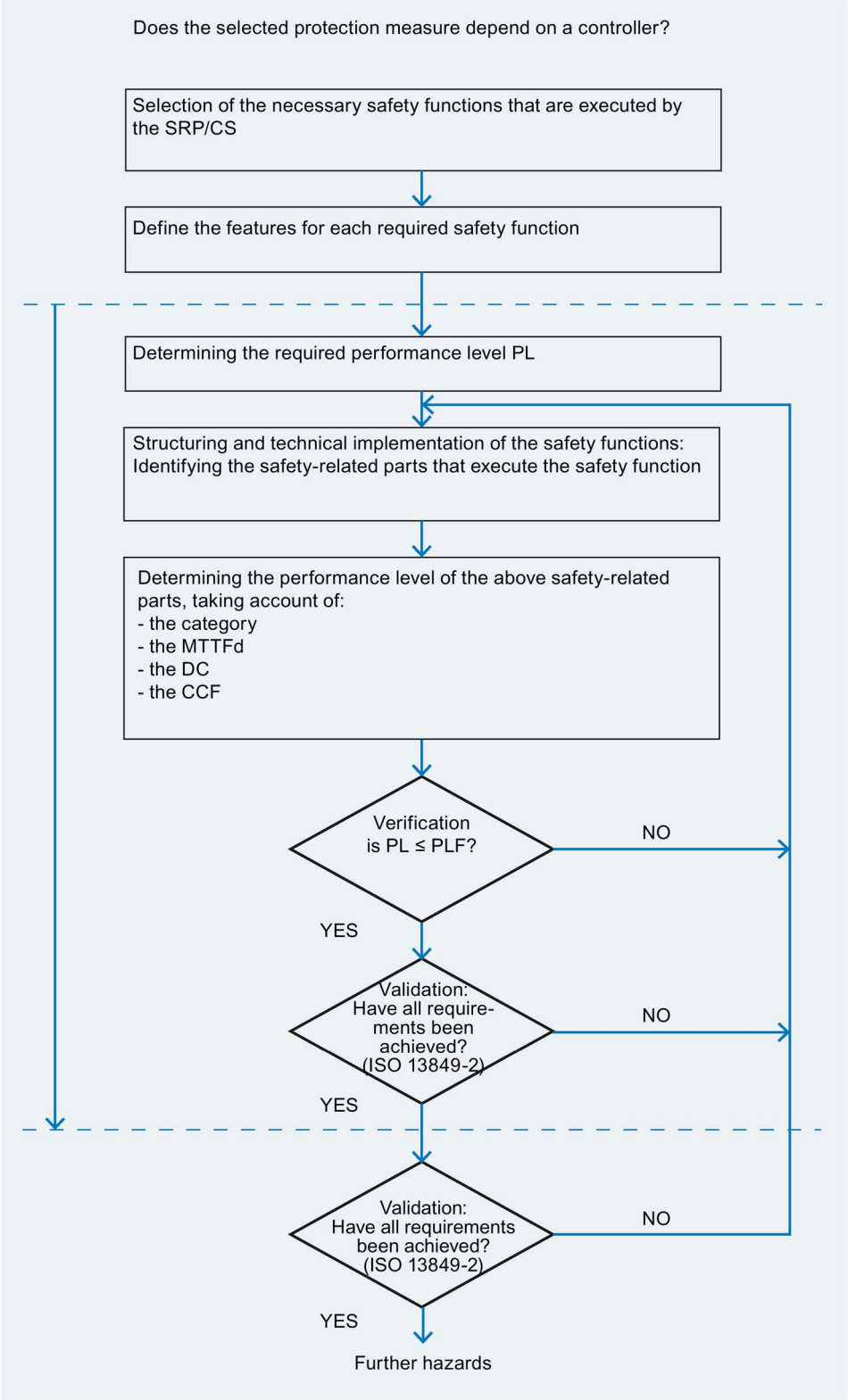


Figure 5-10 Iterative process for structuring the safety-related parts of controllers

Design in accordance with ISO 13849-1

The architecture design is oriented around the required performance level PL_r.

The design concept of ISO 13849-1 is based on specially pre-defined architectures of the safety-related parts of the controller.

A safety function can comprise one or more safety-related parts of a controller (SRP / CS).

A safety function can also be an operating function such as a two-hand control device for initiating a process.

A typical safety function comprises the following safety-related parts of a controller:

- Input (SRP/CS_a)
- Logic / processing (SRP/CS_b)
- Output / energy transmission element (SRP/CS_b)
- Connections (i_{ab}, i_{ac}) (e.g. electrical, optical)

Note: Safety-related parts comprise one or more components; components can comprise one or more elements.

All connecting elements are included in the safety-related parts.

If the safety functions of the controller have been determined, the safety-related parts of the controller must be identified. Their contribution to the process of risk reduction (ISO 12100) must also be assessed.

Performance level PL

When using ISO 13849, the ability of safety-related parts to execute a safety function is expressed by determining a performance level.

The PL must be estimated for each selected SRP/CS and/or combination of SRP/CS that executes a safety function.

The PL of the SRP/CS must be determined by estimating the following aspects:

- $MTTF_d$ (mean time to dangerous failure)
- DC (diagnostic coverage)
- CCF (common cause failure)
- Structure
- Behavior of the safety function under fault condition(s)
- Safety-related software
- Systematic failures

Mean time to dangerous failure of each channel ($MTTF_d$)

The value of the $MTTF_d$ of each channel is specified in three stages, and must be taken into account for each channel individually (e.g. single channel or each channel of a redundant system). A maximum value of 100 years can be fixed with regard to the $MTTF_d$.

$MTTF_d$	
Low	3 years ≤ $MTTF_d$ < 10 years
Average	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ ≤ 100 years

Diagnostic coverage (DC)

The value for DC is specified in four stages. To estimate the DC, failure mode and effects analysis (FMEA), or similar procedures, can be used in most cases. In this case, all relevant faults and/or failure modes must be taken into account, and the PL of the SRP/CS combination that is to execute the safety function must be tested against the required performance level (PL_r). For a simplified approach to estimating the DC, see ISO 13849-1 Annex E.

Diagnostic coverage (DC)	
None	DC < 60%
Low	60% ≤ DC < 90%
Average	90% ≤ DC < 99%
High	99% ≤ DC

5.4.1 Design and implementation of categories

Category B

To achieve Category B, the safety-related parts of the controller must meet the following requirements and they must be structured, selected and combined in accordance with these requirements.

- Application of the fundamental safety principles
- Ability to withstand the expected operating demands, including switching capacity or the frequency of operations of the components
- Robustness in respect of the influences of the material to be processed and the environmental conditions, including, for example, substances such as oils, cleaning agents, salt spray
- Robustness in respect of other relevant external influences, including mechanical vibration, electromagnetic interference, and interruptions or faults in the energy supply.

In a Category B system, the $MTTF_d$ of each channel can be low to average. There is no diagnostics coverage (DC avg = none). Since the structure is usually single-channel, CCFs are not considered in this category since they are not relevant. The maximum achievable performance level of a Category B system is PL = b.
The single-channel design means a fault can result in the loss of the safety function.

Example of a designated Category B architecture:

- I1: Sensor 1 (e.g. a position switch)
- L1: Logic unit 1 (e.g. a safety relay)
- O1: Actuator 1 (e.g. a contactor)

The structural features are:

- Single-channel design

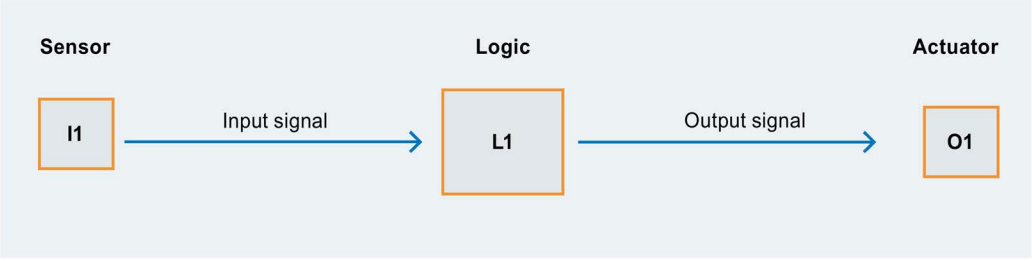


Figure 5-11 Designated architecture for Category B

Category 1

To achieve Category 1, the requirements for Category B must be met.
In addition, the following requirements must be met:

Field-proven components must be used for the safety-related parts of the controller, and field-provensafety principles must be adhered to (see ISO 13849-2).

In a Category 1 system, the MTTFd of each channel must be high.

The maximum achievable performance level is PL = c.

Example of a designated Category 1 architecture:

- I1: Sensor 1 (e.g. a position switch)
- L1: Logic unit 1 (e.g. a safety relay)
- O1: Actuator 1 (e.g. a contactor)

The structural features are:

- Single-channel design
- Use of field-proven components

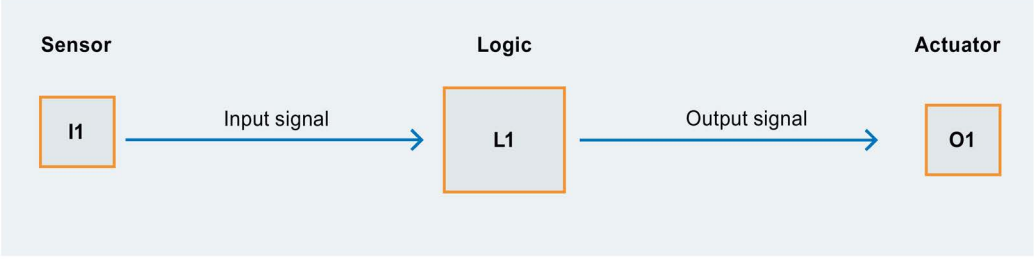


Figure 5-12 Designated architecture for Category 1

Category 2

To achieve Category 2, the requirements for Category B must be met. Field-proven safety principles must also be adhered to. The following requirements also apply:

The safety-related parts of the controller of a Category 2 system must be tested by the machine controller at appropriate intervals. This test of the safety function by the machine controller must be carried out:

- During machine start-up, and
- Before initiation of each dangerous situation, e.g. at the start of a new machine cycle, or the initiation of other movements, etc.

As the result of the test by testing equipment

- An appropriate fault response must take place if a fault is detected
- Operation must not be permitted if a fault is detected

The fault response must initiate a safe state whenever possible. Only when the fault has been remedied may normal operation be resumed. If the safe state cannot be entered (e.g. if the contacts have welded), a warning against the hazard must be provided.

In a Category 2 system, the MTTFd of each channel must be low to high depending on the required PLr. The safety-related parts of the control system must have low to average diagnostic coverage. At the same time, CCF measures must be used (see ISO 13849-1 Annex F).

In addition, the test itself must not result in any further hazards. The test equipment may be one of the safety-related parts of the control system, or it can be implemented separately.

The maximum achievable performance level of a Category 2 system is PL = d.

Note

Category 2 is a single-channel tested system as defined in the simplified procedure of ISO 13849-1: if a dangerous fault occurs, fault detection is only (meaningfully) effective if the fault-detecting test takes place before the next demand for the safety function. Against this background, a test rate is demanded that is 100 times faster than the demand rate of the safety function.

Example of a designated Category 2 architecture

- I1: Sensor 1 (e.g. a position switch)
- L1: Logic unit 1 (e.g. a safety relay)
- O1: Actuator 1 (e.g. a contactor)
- TE: Test equipment

The structural features are:

- Single-channel design
- Monitoring by the test equipment

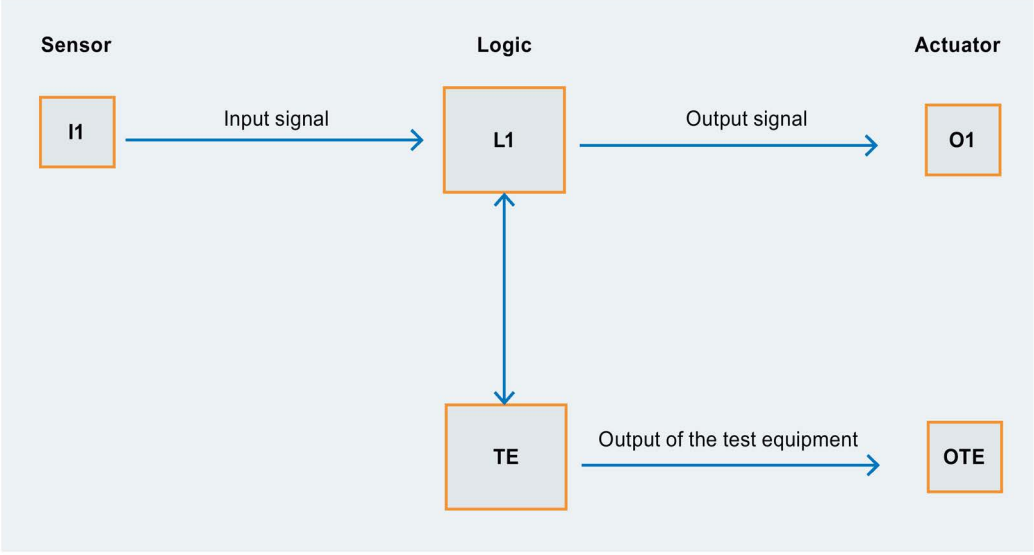


Figure 5-13 Designated architecture for Category 2

Category 3

To achieve Category 3, the requirements for Category B must be met. Field-proven safety principles must also be adhered to. The following requirements also apply:

The safety-related parts of the control system of Category 3 must be designed in such a way that the safety function is not lost if a single fault occurs. The single fault must be detected at or before the next demand for the safety function whenever possible.

In a Category 3 system, the MTTFd of each redundant channel must be low to high depending on the required PLr. The safety-related parts of the control system must have low to average diagnostic coverage. At the same time, CCF measures must be used (see ISO 13849-1 Annex F).

Example of a designated Category 3 architecture:

- I1 and I2: Sensor 1 and 2 (e.g. two position switches with positive opening contacts)
- L1 and L2: Logic unit 1 and 2 (a safety relay, for example, already includes these two units)
- O1 and O2: Actuator 1 and 2 (e.g. two contactors)

The structural features are:

- Redundant design
- Monitoring of the sensors (discrepancy monitoring)
- Monitoring of the enabling circuits (monitoring, comparable with the feedback circuits today)

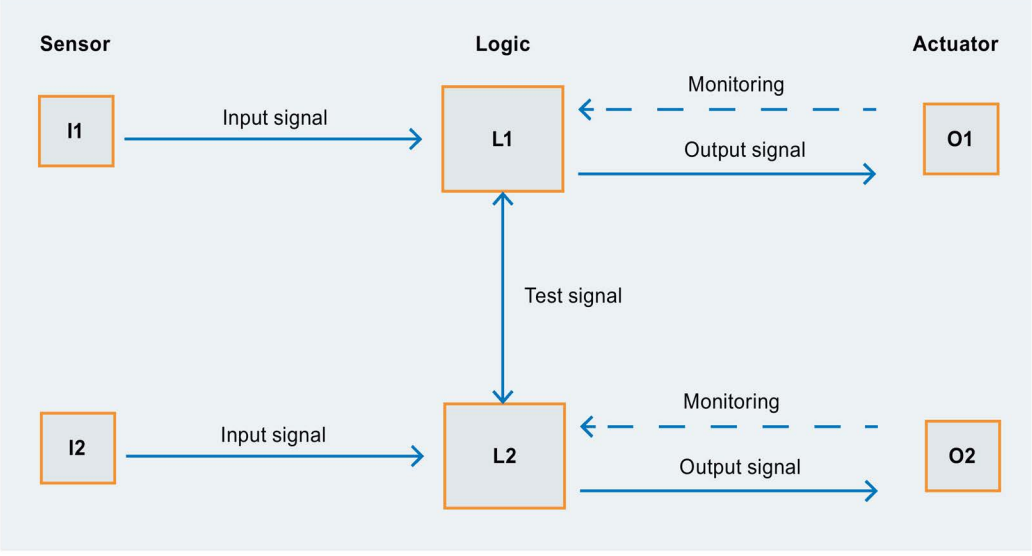


Figure 5-14 Designated architecture for Category 3

Category 4

To achieve Category 4, the requirements for Category B must be met. Field-proven safety principles must also be adhered to. The following requirements also apply:

The safety-related parts of the control system of Category 4 must be designed in such a way that the safety function is not lost if a single fault occurs. The single fault must be detected at or before the next demand for the safety function. If a fault cannot be detected, an accumulation of these faults must not result in the loss of the safety function.

In a Category 3 system, the MTTFd of each redundant channel must be high. The safety-related parts of the control system must have high diagnostic coverage. At the same time, CCF measures must be used (see ISO 13849-1 Annex F).

Example of a designated Category 4 architecture:

- I1 and I2: Sensor 1 and 2 (e.g. two position switches with positive opening contacts)
- L1 and L2: Logic unit 1 and 2 (a safety relay, for example, already includes these two units)
- O1 and O2: Actuator 1 and 2 (e.g. two contactors)

The structural features are:

- Redundant design
- Monitoring of the sensors (discrepancy monitoring)
- Monitoring of the enabling circuits (monitoring, comparable with the feedback circuits)
- High diagnostic coverage in all subsystems

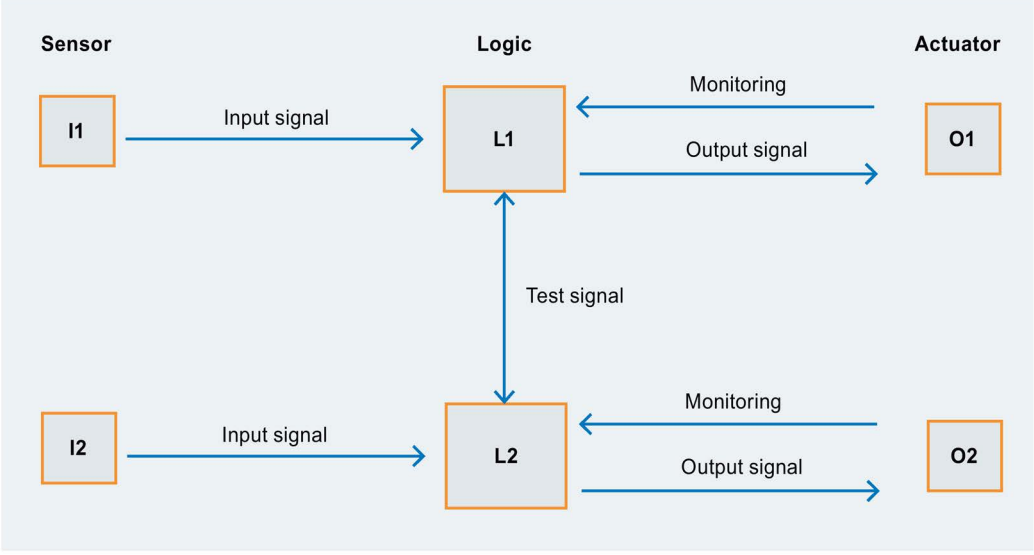


Figure 5-15 Designated architecture for Category 4

Evaluation of the safety functions

Each provided safety function and its implementation and evaluation must be documented in accordance with the specifications of the standard.

When evaluating safety functions on machines and in plants, the fast and simple handling of the SIEMENS Safety Evaluation Tool offers you valuable support.

The TÜV-tested online tool guides the user step by step from defining the structure of the safety system, through the selection of components, to the calculation of the achieved safety integrity in accordance with ISO 13849-1 and IEC 62061.

The integrated and extensive libraries also support you here. Users receive a standard-compliant report that can be integrated into the documentation as a safety verification.

Online access to the Safety Evaluation Tool ensures that the calculations are always carried out with the current standard, and the latest technical data for all safety-related components from SIEMENS are accessed.

You can find the Safety Evaluation Tool on the Internet (http://www.siemens.com/safety-evaluation-tool).

Service & Support

6

6.1 Service & Support

Safety Integrated on the Internet

Our online presence offers you up-to-date information on all aspects of safety engineering. Here you can find helpful documents, links, films and tools about Safety Integrated products and solutions, and about applying the standards.
Safety Integrated on the Internet (http://www.siemens.com/safety-integrated)

Functional Safety Services

We support you in carrying out risk assessments, for example. Or we handle SIL or PL verification for your existing concept, programming of the safety function, or verification of the engineering.

Functional Safety Services on the Internet (http://www.siemens.com/safety-services)

SITRAIN Training for Safety Integrated

Risk assessment, standards, CE marking, product training: You can find everything worth knowing about our extensive training program SITRAIN on the Internet.

SITRAIN Training for Safety Integrated on the Internet (http://www.siemens.com/sitrain-safetyintegrated)

Catalogs and information material

In the Information and Download Center, you will find all the up-to-date catalogs, customer magazines, brochures, demo software, and special-offer packages for downloading. Including our "Safety Integrated" Catalog.

Information and Download Center (http://www.siemens.com/safety-infomaterial)

Functional examples

You can find on the Internet further practice-oriented functional examples covering typical requirements within industrial safety engineering. They contain typical applications with product examples including wiring diagram, programming code, and evaluation in accordance with EN 62061 and EN ISO 13849.

Functional examples on the Internet (http://www.siemens.com/safety-functional-examples)

Safety Integrated Newsletter

Our regular Newsletter offers you up-to-date information on all aspects of safety engineering.

Safety Integrated Newsletter (http://www.industry.siemens.com/newsletter)

On-site service

Siemens supports its customers worldwide with product-, system-, and application-related services throughout the entire life cycle of a plant. From planning and development, through operation, right up to modernization, customers profit from the service, and also from the extensive technology/product know-how and industry competence of the Siemens experts.

Industry Services (http://www.siemens.com/industry-service)

Configurators

Assemble products and systems simply with the help of our configurators.

Industry Mall

Then order online in the Industry Mall – it's as simple as that.

Industry Mall (http://www.siemens.com/industrymall/)

Consulting

To be able to handle the growing demands in the area of safety engineering, Siemens uses selected Siemens Solution Partners Automation as well as its own safety experts. These highly qualified partner companies offer professional consulting and active support with all the relevant safety aspects of your automation projects.

Solution Partner Internet (http://www.siemens.com/automation/solutionpartner)

Index

T

U

V

W