SPECIAL INFORMATION

Guide for Safe Machinery

SIX STEPS TO A SAFE MACHINE

EU version

SICK
Sensor Intelligence.

Contents

Foreword

Figure 1: Machine safety inspection

Safe machines increase legal certainty for the manufacturer and user. Machine operators expect to be offered only safe machinery or devices. This expectation exists worldwide. There are also regulations on the protection of operators of machinery worldwide. Such regulations are different depending on countries and regions. However, there is broad agreement on the process to be applied during the manufacture and upgrade of machinery:

During the design and manufacture of machinery, the machine manufacturer shall identify and evaluate all possible hazards and hazardous points by undertaking a risk assessment.

Based on this risk assessment, the machine manufacturer shall take suitable design measures to eliminate or reduce the risk. If the risk cannot be eliminated by these design measures or the remaining risk is not tolerable, the machine manufacturer shall select and apply suitable protective devices, and provide information on the residual risks if necessary.

To ensure the intended measures work correctly, overall validation is necessary. This overall validation shall evaluate the design and technical measures, as well as the organizational measures in context.

About this guide

What does the guide contain?

You have before you a comprehensive guide on machine safety requirements and on the selection and use of protective devices. We will show you various ways in which you can safeguard machinery and protect persons against accidents taking into account the applicable European directives, regulations, and standards. The examples and statements given are the result of our many years of practical experience and are to be considered typical applications.

For better orientation and guidance through the guide, we have divided the path to a safe machine into 6 main steps. Two additional chapters describe the regulatory requirements for the machine manufacturer and the requirements for the machine user.

This guide describes the legal requirements on the safety of machinery in the European Union and their implementation. The legal requirements relating to machinery in other regions (e.g., North America, Asia) are described in separate versions of this guide.

It is not possible to derive any claims whatsoever from the following information, irrespective of the legal basis, as every machine requires a specific solution against the background of national and international regulations and standards.

We refer to the latest published standards and directives at the time of publishing. If, in the event of new standards, the use of the predecessor standard is permitted for a transition period, we have noted this situation in the relevant chapters of this guide.

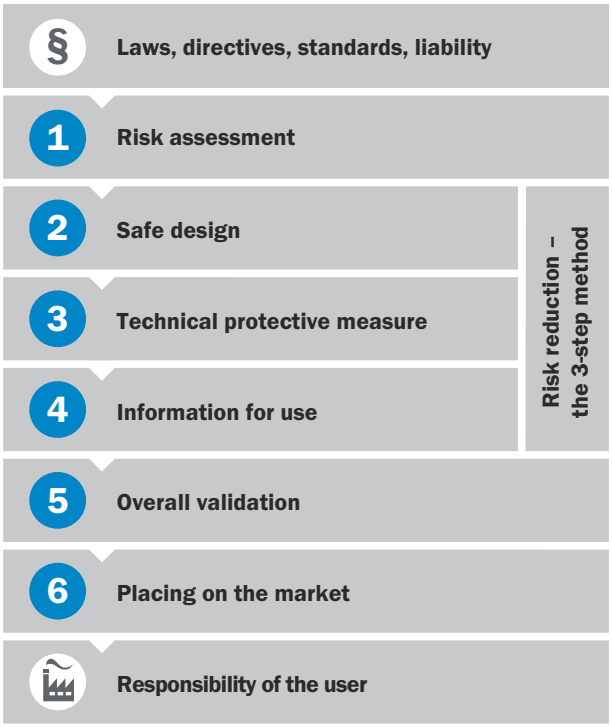


Figure 2: Structure: “Six steps to a safe machine”

Who is this guide for?

This guide is aimed at manufacturers, users, designers, system engineers, and all individuals who are responsible for machine safety.

Use of the terms “safety” and “safe” in this document

According to ISO Guide 51, "The term “safe” is often understood by the general public as the state of being protected from all hazards. However, this is a misunderstanding: “safe” is rather the state of being protected from recognized hazards that are likely to cause harm”.

Some level of risk is inherent in all products or systems (so-called residual risk). Absolute certainty is therefore not possible.

In this guide, the terms “safety” and “safe” are used as qualifiers for better understanding and readability. The terms are defined, as in ISO Guide 51, as “freedom from unacceptable risks” and are not to be understood as absolute protection against hazards.

SICK assumes no liability for the interpretation of the terms “safe” and “safety” in this document.

Your editorial team

Figure 3: From left to right: Otto Görnemann, Rolf Schumacher, Stephanie Kaiser, Hans-Jörg Stubenrauch, Matthias Kurrus, Harald Schmidt.

Machine safeguarding in the work process

The requirements on the safeguarding of machinery have changed more and more with the increasing use of automation. In the past, protective devices in the manufacturing process were something of a nuisance; for this reason, they were often not used at all.

Today, innovative technologies make it easy to integrate protective devices into the manufacturing process. As a result, they are no longer a hindrance for the operator and even help productivity in many cases.

For this reason, reliable protective devices that are integrated into the manufacturing process are indispensable.

Figure 4: Development of a safety concept

Safety is a basic need

Safety is a basic human need. Studies show that people continuously subjected to stressful situations are more susceptible to psychosomatic illnesses. Even though it is possible to adapt to extreme situations over the long term, they will place a great strain on the individual.

It is often said, however, that more “safety” results in lower productivity – the opposite is actually the case: Higher levels of safety result in increased motivation and satisfaction and, as a result, higher productivity.

The following requirement on the machine manufacturer and user can be derived from this: **Operators and maintenance personnel shall be able to rely on the safety of a machine!**

Safety is a management task

Employers in industry are responsible for their employees as well as for smooth, cost-effective production. Only if managers make safety part of everyday business activities will employees be receptive to the subject.

To improve sustainability, experts are therefore calling for the establishment of a wide-ranging “safety culture” in the respective companies.

Involvement of the employees results in acceptance

It is extremely important that the needs of operators and maintenance personnel are taken into consideration in the planning at concept level. Only an intelligent safety concept matched to the work process and the personnel will result in the required acceptance.

Expert knowledge is required

In the European Union, national legal requirements are harmonized by European legislation such as the Machinery Directive. Directives describe general requirements that are specified in more detail by standards.

The safety of machinery depends to a large extent on the correct application of such standards. European standards are often also accepted outside the European Union.

Implementing all these requirements in practice requires extensive specialist knowledge, application expertise, and many years of experience.

§ – Laws, directives, standards

European directives

One of the goals of the European Community is the protection of the health of its citizens both in the private and in the professional sphere. A further goal is the creation of a single market with free movement of goods. In order to achieve such goals, the functioning of the European Union is regulated by treaty as follows: The EU Commission or the Council of the European Union issues legal acts, including so-called directives, which define the basic objectives and requirements. The directives are kept technology-neutral as far as possible. The Member States then have to implement these directives in their national legislation.

The following directives have been published in the area of health and safety at work and machine safety:

- The Machinery Directive, which addresses the manufacturers of machines
- The Work Equipment Directive, which addresses the users of machines
- Additional directives, e.g., Low Voltage Directive, EMC Directive, ATEX Directive

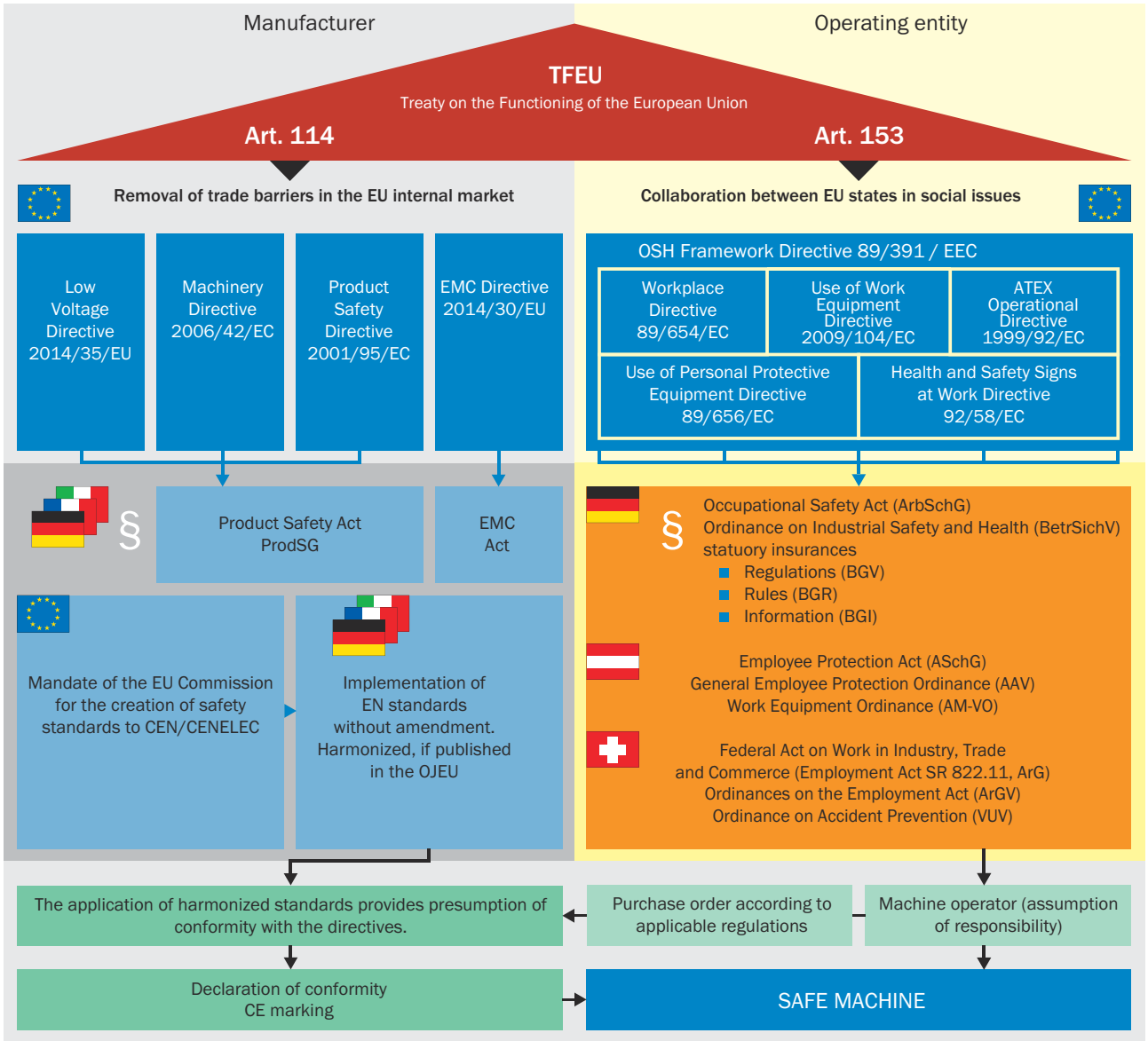


Figure 5: EU directives for manufacturers and users regarding machine safety and occupational health and safety

NOTE
The directives are freely available, e.g., at eur-lex.europa.eu.

NOTE
European directives apply to manufacturers and organizations that place machinery on the market in the European Union.

The Machinery Directive

Machinery Directive 2006/42/EC addresses the manufacturers and distributors of machines and safety components. It establishes the necessary tasks for new machines to meet health and safety requirements in order to dismantle trade barriers within Europe and to guarantee a high level of health and safety for users and operators.

It applies to machines and to safety components individually placed on the markets, as well as to used machines and safety components from third-party countries which are placed on the market in the European Economic Area for the first time (e.g., from the USA or Japan).

- In 1989, the Council of the European Community passed the directive on the approximation of the laws of the Member States relating to machinery, known as the Machinery Directive (89/392/EEC).
- By 1995, this directive had to be applied in all EC Member States.
- In 1998, various amendments were summarized and consolidated in the Machinery Directive 98/37/EC.
- in 2006, the Machinery Directive 2006/42/EC, which replaced the previous version, was passed. All EC member states were obliged to adopt the new directive by December 29, 2009.

NOTE
As of December 29, 2009 only Machinery Directive 2006/42/EC is to be implemented!

NOTE
The Machinery Directive was implemented in the German-speaking countries as follows:

- Germany: Ninth Ordinance (Machinery Ordinance / 9. ProdSV) to the Product Safety Act (ProdSG) dated November 8, 2011
- Switzerland: Federal law on product safety (PrSG) dated June 12, 2009 and Ordinance on the safety of machinery (Machinery Ordinance) dated April 2, 2008
- Austria: Federal act on protection against dangerous products (Product Safety Act 2004 [PSG 2004]) and Machine safety ordinance 2010

If machinery and safety components comply with the Machinery Directive, member states may not prohibit, restrict or impede their being placed on the market and put into service. It is also forbidden for them to apply national laws, ordinances, or standards to impose more stringent requirements!

The Work Equipment Directive

The obligations for employers are set out in the Work Equipment Directive, which applies to the use of machinery and equipment in the workplace. The directive contains minimum requirements that must be met when using work equipment in order to improve occupational health and safety. Each member state may add its own national requirements: e.g., regarding equipment testing, service and maintenance intervals, the use of personal protective equipment, or the layout of the workplace. The requirements of the Work Equipment Directive as well as national requirements and operating regulations are in turn implemented in national laws.

Figure 6: Validation

NOTE

- Germany: Occupational Safety and Health Act (Arbeitsschutzgesetz (ArbSchGes)), Ordinance on Industrial Safety and Health (Betriebssicherheitsverordnung (BetrSichV))
- Switzerland: Federal legislation on work in industry, commerce and trade (Bundesgesetz über die Arbeit in Industrie, Gewerbe und Handel (SR 822.11, ArG))
- Austria: Labor Protection Act (ArbeitnehmerInnenschutzgesetz (ASchG))

Work Equipment Directive 2009/104 / EC: **eur-lex.europa.eu**

Obligations of the machine manufacturer

Safe design of machinery

Manufacturers are obliged to design and build their machines such they are compliant with the essential safety and health requirements of the Machinery Directive. Manufacturers shall take account of the safety integration already during the design phase. In practice, this means that the designer shall perform a risk assessment already at the design phase of the machine. The resulting measures shall be incorporated directly into development. Steps 1 to 5 of this guide describe in detail how to proceed here.

Preparing technical documents

The machine manufacturer shall prepare a technical files according to Annex VII of the Machinery Directive. The technical files are subject to the following criteria:

- It shall contain all diagrams, calculations, test reports and documents that are relevant to the conformity with the essential health and safety requirements of the Machinery Directive.
- It shall be archived for at least ten years from the last day of manufacture of the machine (or the machine type).
- Shall be submitted to the authorities on duly reasoned request.

NOTE
It is not possible to derive from the Machinery Directive an obligation on the manufacturer to supply the complete technical documentation to the purchaser (user) of the machine.

Issuing the declaration of conformity

After the machine manufacturer has built his machine according to the requirements of the Machinery Directive, he shall declare, in a legally binding manner, conformity with these requirements by issuing a declaration of conformity and marking the machine (CE marking). It is then permitted to place the machine on the market in the European Union.

The Machinery Directive explains the process for the conformity assessment. There are two procedures for machinery (see "EU conformity assessment procedure for machinery and safety components", page 16):

- Standard procedure:
  Machines that are not explicitly listed in Annex IV of the Machinery Directive are subject to the standard process. The “Essential health and safety requirements” described in Annex I must be met. The manufacturer shall then compile the technical files and apply the CE marking. This process does not require the involvement of a third party (test body or authority). The technical files shall be provided to the national market authorities upon duly reasoned request.

Figure 7: Safeguarding of a machine and diagnostics on the protective device

- Procedure for machinery that is listed in Annex IV:
  Machines that are particularly hazardous are subject to special procedures. Annex IV of the Machinery Directive contains a list of particularly hazardous machinery and also safety components; this list includes electro-sensitive protective equipment such as photoelectric safety switches and safety laser scanners. The “Essential health and safety requirements” in Annex I of the Machinery Directive must be met first.
  If applicable harmonized standards covering all relevant health and safety requirements are available for the machinery or safety components, the declaration of conformity can then be obtained in one of the following three ways:
  - Self-certification by the standard procedure
  - EC type examination by a notified body: A notified body tests whether the machine meets the relevant essential health and safety requirements applicable to the machinery or the safety component. On compliance with those requirements, the notified body issues an EC type examination certificate containing the results of the tests.
  - Use of a full quality management system that has been assessed (QMS): The full QMS shall ensure conformity with the requirements of the Machinery Directive and be assessed by a notified body. The manufacturer is responsible for the effective and appropriate use of the QMS. See also Annex X of the Machinery Directive.

  If no applicable harmonized standards exist for the machinery or parts of the machinery or if harmonized standards have not been applied, conformity can only be achieved as follows:
  - EC type examination by a notified body
  - Use of a full quality management system (QMS) that has been assessed

Marking of the machine as conforming to the European directives (“CE conform”)

Once all the requirements have been met and before the machine within the scope of the Machinery Directive is placed on the market, the CE marking shall be applied to the machine.

NOTE
The CE marking can only be affixed if the machine meets all applicable European directives. Only a machine with the CE marking is allowed to be placed on the market in the European Union.

Special case: Partly completed machinery

In many cases, parts of machines, machine assemblies, or machine components are manufactured and delivered that are very close to the definition of a machine but cannot be considered complete machines in the context of the Machinery Directive. The Machinery Directive defines as “partly completed machinery” an assembly of components that almost form a machine, but that on their own cannot perform any specific function. An individual industrial robot, for example, is a partly completed machine. A partly completed machine is only intended to be installed in other machinery or in other partly completed machinery or equipment, or to be combined with such machinery or equipment in order to form a machine in the context of the Directive.

Partly completed machinery cannot meet all requirements of the Machinery Directive. Therefore, the Machinery Directive regulates their free trade using a special procedure:

- The manufacturer shall meet all reasonably achievable essential health and safety requirements of the Machinery Directive.
- The manufacturer shall issue a declaration of incorporation. It describes which essential requirements of the Machinery Directive are applied and met. Technical documentation, similar to that for a machine, is to be prepared as appropriate and archived.
- Instead of operating instructions, the manufacture shall prepare assembly instructions in the same manner and supply them with every “partly completed” machine. The language used in these assembly instructions can be agreed between the manufacturer and user (integrator).

NOTE
See also section "Test bodies", page 20.

EU conformity assessment procedure for machinery and safety components

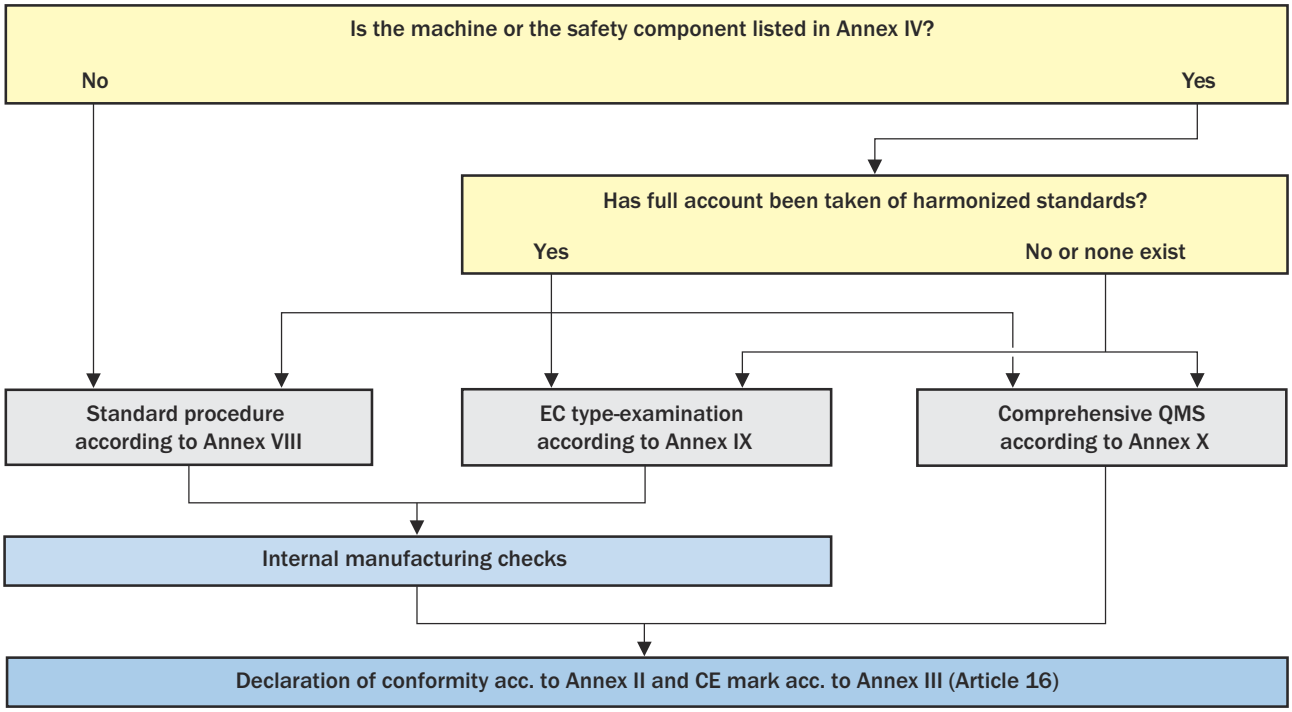


Figure 8: Conformity assessment procedure according to Article 12 of the Machinery Directive 2006/42/EC

Summary: Laws, directives

As the manufacturer of a machine, among other requirements, the Machinery Directive applies to you:

- You shall meet all essential health and safety requirements of the Machinery Directive.
- You shall take account of safety integration during the design process.
- For the declaration of conformity, you shall use either the standard procedure or the procedure for machinery in Annex IV of the Machinery Directive.
- You shall compile a technical documentation file for the machine; in particular, this shall include all safety-related design documents.
- You shall supply operating instructions with the product in an official language of the country of use. If these operating instructions are not “original operating instructions” in an official EU language, then such a version must also be supplied.
- You shall issue a declaration of conformity and mark the machine or the safety component with the CE marking.

As a machine user, the Work Equipment Directive applies to you:

- Observe the requirements of the Work Equipment Directive and its national implementations. These may also include more stringent requirements!
- You shall find out whether further national requirements (e.g., testing of work equipment, service or maintenance intervals, etc.) exist and comply with them.

Standards

Standards are technical agreements made between the various interested parties (manufacturers, users, test bodies, occupational health and safety authorities, and governments). Contrary to popular opinion, standards are not prepared or agreed by governments or authorities. Standards describe the state-of-the-art at the time they are drafted. Over the last 100 years, a change from national standards to globally applicable standards has taken

place. Depending on the place the machine or product is to be used, different legal stipulations may apply that make it necessary to apply different standards. The correct selection and application of standards supports the machine manufacturer to ensure compliance with legal requirements.

This guide makes reference to international standards (ISO, IEC). An overview of the relevant standards is provided in the annex, page 166.

The overview also contains their regional equivalents (e.g. EN) or equivalent national standards to the referenced international standards.

Global standardization organizations and structures

ISO (International Standardization Organization)
ISO is a worldwide network of standardization organizations from 165 countries. ISO prepares and publishes international standards focused on non-electrical technologies.

IEC (International Electrotechnical Commission)
The International Electrotechnical Commission (IEC) is a global organization that prepares and publishes international standards in the area of electrical technology (e.g., electronics, communications, electromagnetic compatibility, power generation), and related technologies.

Types of standards

There are three types of standards:

Type-A

Type-A standards, also called basic safety standards, contain basic terminology, principles of design and general aspects that can be applied to all machinery.

Type-B

Type-B standards, also called generic safety standards, address a safety aspect or protective device that can be used for a wide range of machinery. Type-B standards are in turn divided into:

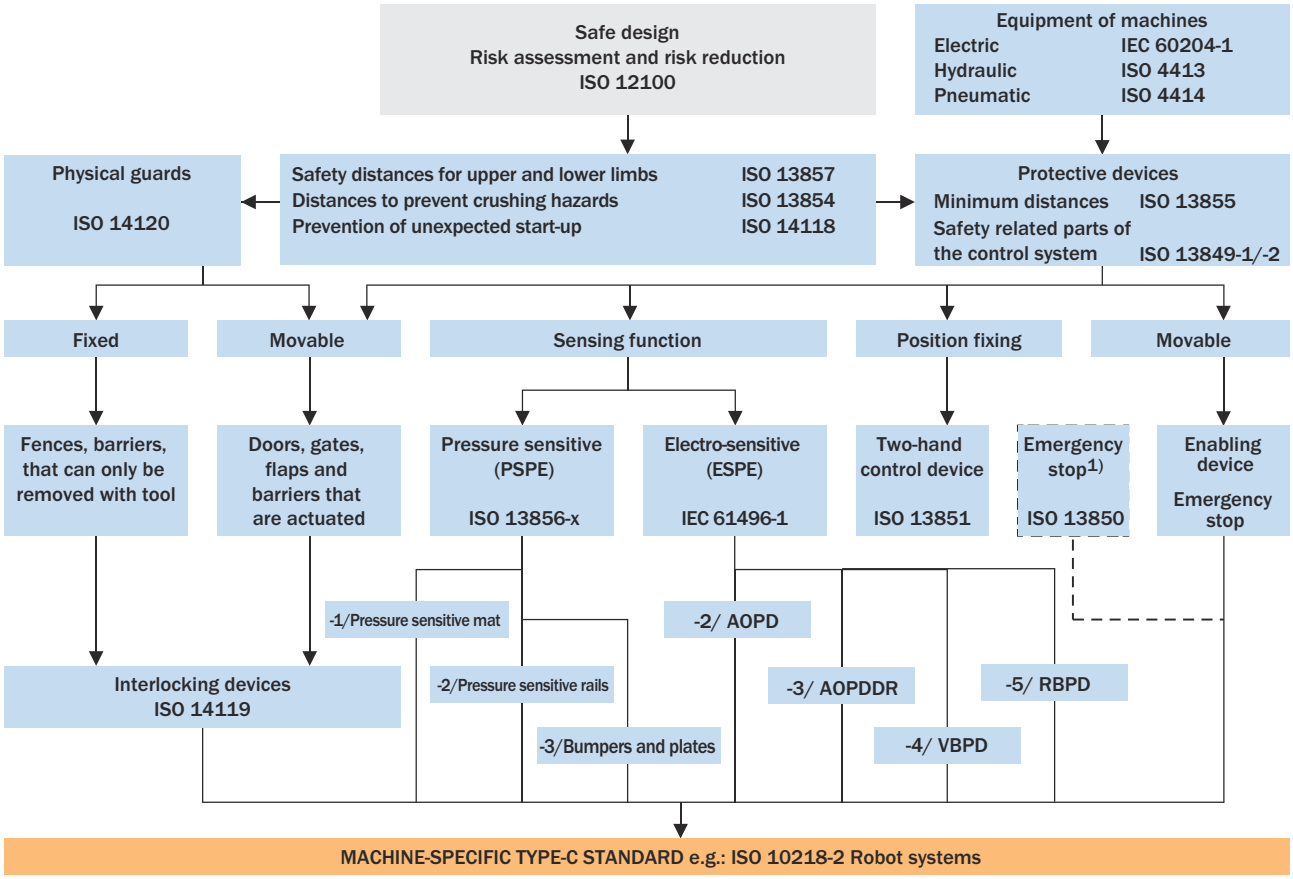
- Type-B1 standards on specific safety aspects, e.g., the electrical safety of machinery, the calculation of safety distances, requirements for control systems
- Type-B2 standards on protective devices, e.g., two-hand control devices, physical guards and electro-sensitive protective equipment

Type-C

Type-C standards contain all safety requirements for a specific machine or a type of machine. If this standard exists, it has priority over the type-A or type-B standard. A type-C standard may, however, refer to a type-B or type-A standard. In all circumstances the requirements of the Machinery Directive shall be met.

NOTE
A list of important standards is provided in the annex (page 166).

Overview of protective devices, physical guards and associated standards



1) Emergency stop is a safety measure but it is not a protective device!
AOPD Active optoelectronic protective device
AOPDDR Active optoelectronic protective device responsive to diffuse reflection
VBPD Vision based protective device
RBPD Radar based protective device

Type-A standard
Type-B standard
Type-C standard

Figure 9: Protective devices and related standards

European standardization organizations and structures

CEN (Comité Européen de Normalisation/European Committee for Standardization)
CEN is a group of standardization organizations from EU member states, the EFTA countries as well as future members from CEN or EFTA. CEN prepares the European Standards (EN) in non-electrical areas. To prevent these standards representing barriers to trade, CEN collaborates with ISO. Using a voting procedure, CEN determines whether ISO standards are adopted and publishes them as European standards.

CENELEC (Comité Européen de Normalisation Electrotechnique/European Committee for Electrotechnical Standardization)
CENELEC is the comparable institution to CEN in the area of electrical technology, and prepares and publishes European standards (EN) in this area. CENELEC is increasingly adopting IEC standards and their numbering system.

National standardization organizations and structures

As a rule each EU member state has its own standardization organization, e.g., DIN, ON, BSI, AFNOR. These prepare and publish national standards in accordance with the legal requirements of the respective member states. To provide harmonized health and safety in the European Community and to remove trade barriers, the European standards are adopted by the national standardization organizations.

The following principles apply to the relationship between national and safety standards:

- If similar national standards exist for adopted European standards, the national standards shall be withdrawn.
- If no applicable European standards exist for specific aspects or machinery, existing national standards can be applied.
- A national standardization organization is only allowed to draft a new national standard if this intention has been announced and there is no interest at European level (at CEN or CENELEC).

European standards for machinery safety

Standards that describe the requirements of European directives in concrete detail in such a way that compliance with the standards provides presumption of conformity with the directives are referred to as “harmonized standards”.

The status of the standard is indicated by various abbreviations:

- A standard with the prefix “EN” is recognized and can be applied in all EU states.
- A standard with the prefix “prEN” is currently in preparation.
- A document that also has “TS” as a prefix is a technical specification and is used as a preliminary standard. These documents exist as CLC/TS or as CEN/TS.
- A document that also has “TR” as a prefix is a report on the state of the art.

A harmonized European standard is prepared as follows:

1. The EU Commission, as the executive organ of the EU, issues a mandate to CEN or CENELEC to draft a European standard to specify in detail the requirements of a directive.
2. The preparatory work is undertaken in international technical committees in which the technical specifications to meet the essential safety requirements in the directive(s) are defined.
3. Once the standard has been approved by the responsible technical committee in a final vote, it is reviewed by the European Commission to determine whether the requirements contained in the standard sufficient to fulfill the requirement of Annex I of the Machinery Directive listed in its Annex ZA. Annex ZA may list one, several or all of the essential health and safety requirements.
4. If the European Commission considers that the standard adequately supports the relevant requirements of Annex ZA, the standard is listed in the Official Journal of the European Union as a harmonized standard.

NOTE

- A harmonized European standard is used as a reference and replaces all national standards on the same subject.
- The compliance of a safety component or a machine with the applicable harmonized standards provides presumption of conformity with the essential health and safety requirements defined in directives, e.g., in the Machinery Directive.

NOTE

A list of the standards with presumption of conformity with the directives is available at ec.europa.eu.

NOTE

- The application of standards, independent of whether they are harmonized or not, is not a requirement of the Machinery Directive. However, if harmonized standards are applied, the so-called “presumption of conformity” applies, according to which it is assumed that the machine meets the relevant essential safety and health requirements of the Machinery Directive.
- If a type-C standard exists for a machine type, it takes precedence over type-A and type-B standards. In this case, only the type-C standard applied justifies the presumption of conformity for meeting the requirements of the Machinery Directive.

Summary: Standards

- European standards specify in more detail the objectives defined in the European directives.
- The application of harmonized standards provides the “presumption of conformity”, i.e., the presumption the machine meets the requirements of the directive. In other words, if you select and apply the right standards for your machine or system, you can assume that you will meet the legal requirements. In specific cases the obligations on the manufacturer can go beyond the content of the standards if, for example, a standard no longer reflects the state of the art.
- There are type-A standards (basic safety standards), type-B standards (generic safety standards), and type-C standards (standards on the safety of machinery). If a type-C standard exists, it has priority over the type-A or type-B standard.

Test bodies, insurance providers and market surveillance

Test bodies

Test bodies providing safety advice

Companies that want to know whether their machines are compliant with the applicable European directives and standards can obtain advice on safety aspects.

Accredited test bodies

Accredited test bodies are test bodies that certify compliance with the test procedures and test criteria from recognized national institutions. These test bodies may include institutions for occupational safety and health which generally employ highly competent specialists.

Notified bodies

Each EU member state has the obligation to nominate test bodies as per the minimum requirements defined in the Machinery Directive, and to notify the European Commission in Brussels of these test bodies for listing.

Only these test bodies are authorized to perform EU-type examinations and to issue EU type examination certificates for the machinery and safety components listed in Annex IV of the Machinery Directive. Not all notified test bodies can test every type of product or machine. Many test bodies are only notified for specific areas.

Insurance providers

Berufsgenossenschaften (statutory OSH insurance bodies)/IFA – Institute for Occupational Safety and Health of the German Social Accident Insurance

In Germany, the Berufsgenossenschaften and other organizations cover the legal accident insurance obligation. The Berufsgenossenschaften are organized by branches so that specific requirements in the individual sectors of the economy can be better met.

Insurance companies

Many insurance companies have departments that offer expert specialist advice, particularly in relation to the prevention of liability risks that may result from ignorance or failure to comply with legal requirements.

Market surveillance

In the states of the EU and EFTA, work safety and market surveillance are the responsibility of national authorities.

- In Germany, this is the responsibility of the “Länder” agencies for occupational health and safety.
- Austria has a range of occupational safety inspectorates. Machine manufacturers can also contact national authorities for expert advice in relation to questions about the safety of machinery and safety at work.
- In Switzerland, market supervision is the responsibility of the State Secretariat for Economic Affairs (SECO). The Swiss National Accident Insurance Fund (Suva), noted for its high levels of technical expertise, is responsible for enforcement.

NOTE
Important addresses can be found in the annex in section "Useful links", page 168.

1 – Risk assessment

When designing a machine, the possible risks must be assessed and, where necessary, protective measures must be applied to protect the operator from any hazards that may still be present.

The process of risk assessment supports the machine manufacturer in this task. A risk assessment is a sequence of logical steps that facilitate the systematic analysis and evaluation of risks. The results of the risk assessment must be taken into account when designing and constructing the machine (risk reduction).

The risk assessment should help to reduce or avoid risks. As a consequence it may identify necessary measures to protect the operator from hazards. If necessary, the risk assessment process must be repeated several times. The first process steps are intended to identify and assess hazards. This is followed by an evaluation and, if necessary, risk mitigation. If the measure triggers a new hazard, the repeated risk assessment reveals this. Being machine-related and application-specific, the risk assessment is already specified in many type-C standards. If this is not the case or not applicable, the requirements of the type-A and type-B standards can be used.

NOTE

➜ Safe design, risk assessment and risk reduction type-A standard: ISO 12100

The risk assessment process

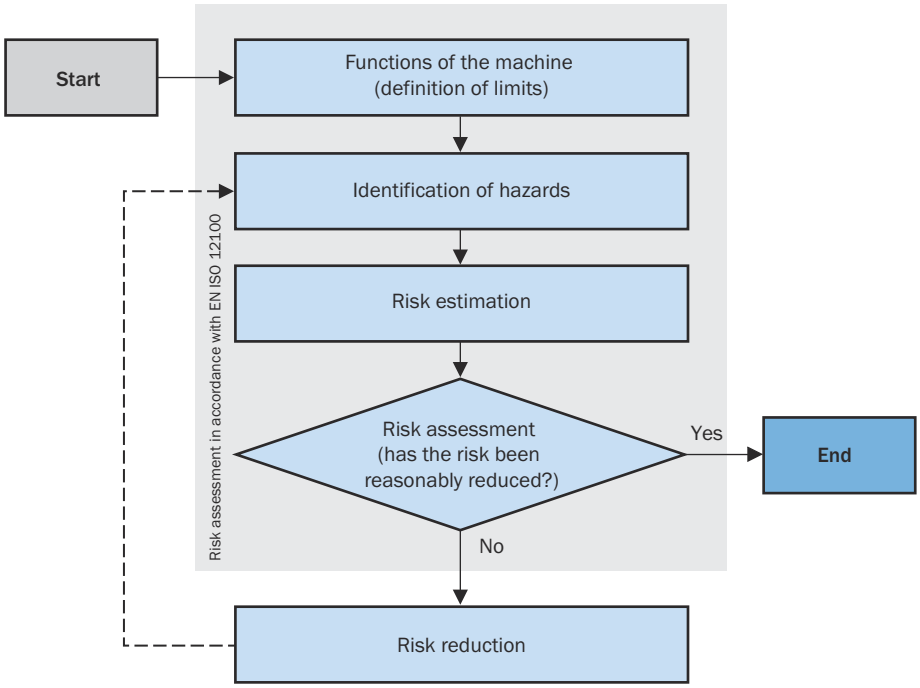


Figure 10: Risk assessment process

NOTE

- The process shall be performed for all hazards. It must be repeated (iterative process) until the remaining residual risk is acceptably low.
- The results achieved during the risk assessment and the procedure applied shall be documented.

Functions of the machine (definition of limits)

The risk assessment starts with the definition of the functions of the machine. These may include:

- The specification for the machine (what is produced, maximum production performance, materials to be used)
- Physical limits and expected location
- Planned service life
- The intended functions and operating modes
- The malfunctions and disruptions to be expected
- The people involved in the machine process
- The products related to the machine
- Intended use but also the unintentional actions of the operator or the reasonably foreseeable misuse of the machine

Reasonably foreseeable misuse

Reasonably assumable, unintentional actions of the operator or foreseeable misuse may include:

- Loss of control of the machine by the operator (particularly on hand-held or portable machinery)
- Reflex actions by individuals in the event of a malfunction, a fault, or a failure during the use of the machine
- Human error due to lack of concentration or carelessness
- Human error due to the selection of the “path of least resistance” in the performance of a task
- Actions under pressure to keep the machine in operation whatever happens
- Actions by certain groups of people (e.g., children, youths, the disabled)

Expected malfunctions and faults

There is significant potential for hazards due to malfunctions and faults in the components relevant to functionality, in particular components of control systems. Examples:

- Reversing of a roller movement (with the result that hands are drawn in)
- Movement of a robot outside its programmed working area

Identification of hazards

After defining the function of the machine comes the most important step in the risk assessment on the machine. This step comprises the systematic identification of foreseeable hazards, hazardous situations, and/or hazardous events.

Table 1: Example of hazards during the life cycle of a machine

In particular the machine manufacturer should take into account the hazards listed below...	**... in all phases of the service life of the machine.**
• Mechanical hazards • Electrical hazards • Thermal hazards • Noise hazards • Vibration hazards • Radiation hazards • Hazards generated by materials and substances • Hazards generated by neglecting ergonomic principles during the design of machinery • Slipping, tripping, and falling hazards • Hazards associated with the environment in which the machine is used • Hazards resulting from a combination of the aforementioned hazards	• Transport, assembly, and installation • Commissioning • Setup • Normal operation and troubleshooting • Maintenance and cleaning • Decommissioning, dismantling, and disposal

Table 2: Examples of hazards and their impacts on machines/systems

	Cutting due to moving parts		Crushing due to moving parts		Shearing due to moving parts with sharp edges

	Piercing due to sharp, rotating parts		Drawing in or entrapment due to rotating moving parts		Drawing-in or entrapment
	Capturing due to protruding rotating parts		Striking due to moving parts		Impact from broken parts
	Impact from ejected chips		Burning due to objects at high temperature		Electric shock due to live parts
	Eye damage due to optical radiation		Crushing, impact due to falling objects		Being run over, struck, crushed due to moving large machines

Risk estimation and risk assessment

After the hazards have been identified, a risk estimation is to be undertaken for each hazardous situation considered.

Risik **is a function of** **Extent of harm** **and** **Probability of occurrence**

The risk related to each hazardous situation considered is determined by the following risk parameters:

- The extent of harm that can be caused by the hazard (minor injury, serious injury, etc.)
- The probability of occurrence of this harm. This is determined by:
  - The exposure of a person/persons to the hazard
  - The occurrence of the hazardous event
  - The technical and human possibilities for the prevention or limitation of harm

There are a variety of tools available for assessing risks, e.g., tables, risk graphs, numerical methods.

Based on the results of the risk estimation, the risk assessment determines whether the application of protective measures is required and when the necessary risk reduction has been achieved.

NOTE
➜ Tools and tables: Technical Report – ISO/TR 14121-2

Scalable Risk Analysis and Evaluation Method (SCRAM)

The method is used to evaluate the initial risk and to estimate the risk after applying inherently safe design measures. It also assists with estimating the effectiveness of the implemented technical protection measures and/or the information for use.

This method, developed by SICK on the basis of ISO 12100, has proven itself over many years through its practicality, plausibility, and reliability in preventing errors.

All 3 levels of risk reduction (3-step method) are considered by SCRAM:

- Safe design
- Technical protective measures
- Information for use

table 3 and table 5 on the following pages provide the basic framework for SCRAM. table 3 makes it possible to consider both the extent of the damage and the probability of occurrence of that damage. The risk elements used in SCRAM include:

- the severity of the injury
- the exposure of the person to the hazard
- the possibility of avoiding the hazard
- the probability of occurrence of the hazard

*Table 3: SCRAM, **Step 1** (main table for determining the risk index)*

Severity	Exposure	Avoidance	Occurence			
			01 – 03	01	02	03
S1	E0	÷	< 1			
	E1 – E3	A1, A2		< 1	< 1	< 1
S2	E0	÷	≤ 1			
	E1	A1		< 1	< 1	1
		A2		< 1	1	1
	E2	A1		1	2	2
		A2		1	2	2
	E3	A1		2	3	3
		A2		2	3	3
S3	E0	÷	1			
	E1	A1		3	4	4
		A2		3	4	4
	E2	A1		4	5	5
		A2		5	5	5
	E3	A1		5	6	6
		A2		6	6	6
S4	E0	÷	1			
	E1	A1		6	7	7
		A2		7	7	7
	E2	A1		7	8	8
		A2		8	8	8
	E3	A1		8	9	9
		A2		9	10	10
			Risk index			

S Severity of injury: negligible (1), mild (2), severe (3), critical (4)
E Hazard exposure prevented (0), low (1), medium (2), high (3)
A Possibility of avoidance: avoidable (1), not avoidable (2)
O Probability of occurrence: low (1), medium (2), high (3)

For all risk elements, this method provides parameters derived from practical experience to make classification easier and to improve the quality of the estimate.

The result is a so-called risk index. This is mapped to the safety levels of ISO 13849-1 (PL) and IEC 62061 (SIL) (see table 4, page 26). A separate risk estimation in accordance with ISO 13849-1, Annex A is not required when using SCRAM.

Table 4: Correspondence of the SCRAM risk index to the required safety level

Risk index	< 1	1	2 – 3	4 – 7	8 – 10
PLr (ISO 13849-1)	a	b	c	d	e
SIL (IEC 62061)	÷		1	2	3

The table 5 allows the estimation of the effectiveness of the implemented technical protective measures and/or information for use provided.

Table 5: Estimation of the effectiveness of the implemented technical protection measures and/or the information for use provided

	IN	Risk Reduction Measures			OUT
	Risk index	MSE and/or CSE	SIG and/or INS	ORG and/or PPE	Risk index
Step 2	8 – 10	M	n/a	n/a	1
	4 – 7	M			
	2 – 3	M			
	1	HR			< 1
	< 1	R			
Step 3	1	n/a	M	n/a	< 1
	< 1		HR		
	< 1	n/a	n/a	to be implemented by the employer	AR

MSE Mechanical safety precautions
CSE Control-related safety precautions
SIG Information on the machine (e.g., an indicator or sign)
INS Information in the operating instructions
ORG Safe work procedures
PPE Personal protective equipment
M Measure or a combination of these measures is mandatory for this risk level
HR Measure or a combination of these measures is highly recommended for this risk level
R One measure or a combination of these measures is recommended for this risk level, although less urgent than an HR recommendation
AR Acceptable risk
n/a Not applicable

For more detailed explanations of the method and how to use SCRAM, see the SICK whitepaper „SCALABLE RISK ANALYSIS AND EVALUATION METHOD (SCRAM)“, 8024038.

Documentation

The risk assessment documentation shall include the procedure applied and the results obtained, as well as the following information:

- Information about the machine such as specifications, limits, intended use, etc.
- Important assumptions that have been made, such as loads, strengths, safety coefficients
- All hazards and hazardous situations identified and hazardous events considered
- Data used and its sources as well as the accident histories and experience relating to risk reduction on comparable machinery
- A description of the protective measures applied
- A description of the risk reduction objectives to be achieved using these protective measures
- The residual risks relating to the machine
- All documents drafted during the risk assessment

NOTE

It is not possible to derive from the Machinery Directive an obligation on the manufacturer to supply the complete technical documentation to the purchaser (user) of the machine.

Risk assessment using Safexpert®

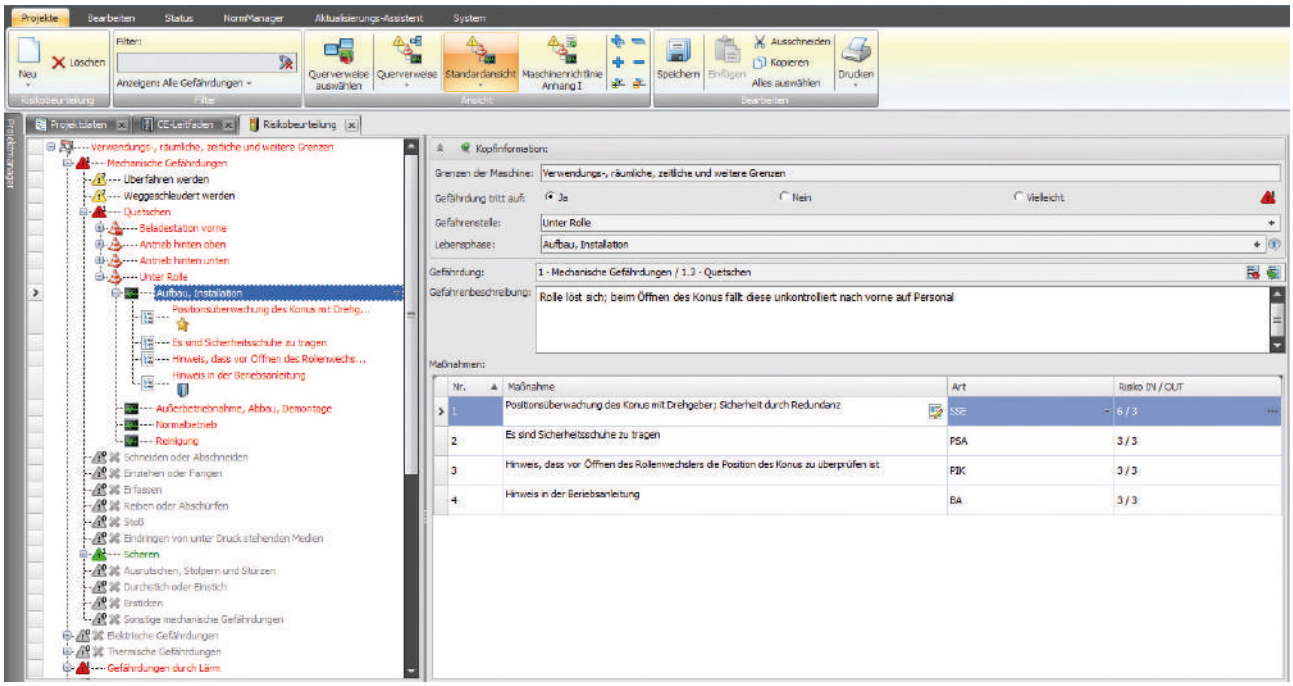


Figure 11: Risk assessment using the Safexpert® software from company ibf

The risk assessment process is also included in Safexpert®, a CE management software from company ibf. The user is guided through the legal requirements and the requirements in the standards. This task is simplified by the pre-defined list of hazards, the CE management software from ibf for structured risk assessment, and the scheme for evaluating both the risk and the level of safety necessary in control systems. The necessary standards are always kept up to date with the StandardManager and the update assistants. The hazards are evaluated separately at each hazardous point and for each phase of the machine's life cycle. Evaluating hazards individually enables the ideal measures for risk reduction to be selected in each case. Safexpert® uses a combination of risk graphs and matrices (tables). The estimation is made before (IN) and after (OUT) the protective measure (e.g., protective device) has been selected. The risk is categorized on a scale from 0 (no risk) to 10 (highest risk).

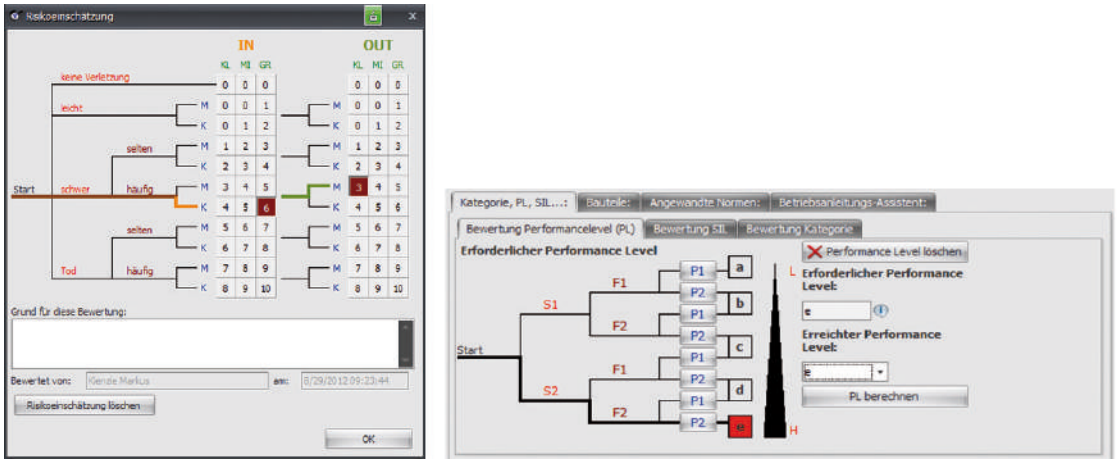


Figure 12: Risk graph for evaluating hazards using the Safexpert® software from ibf

NOTE

Safexpert® is not only used for risk assessment. Using Safexpert®, every aspect of the conformity process according to the Machinery Directive can be completed and documented efficiently.

Summary: Risk assessment

General

- Perform a risk assessment for all hazards. This iterative process must take into account all hazards and risks until there are no residual risks or only acceptable residual risks remain.

Risk assessment process

- Start the risk assessment by establishing the functions and the limits of the machine.
- During the risk assessment, take into account in particular reasonably foreseeable misuse and malfunctions.
- Then identify the hazards (mechanical, electrical, thermal,etc.) derived from the operation of the machine. Take into account these hazards in all life phases of the machine.
- Then estimate the risks derived from the hazards. These depend on the extent of harm and the probability of occurrence of the harm.
- Document the results of your risk assessment.

Risk reduction strategy

If the risk assessment shows that measures are required to reduce the risk, the 3-step method shall be used.

The 3-step method

The machine manufacturer must apply the following principles in the specified order when selecting risk reduction measures:

1 Safe design: elimination or minimization of residual risks as far as possible (integration of safety in the design and construction of the machine)
2 Technical protective measures: Take the necessary protective measures against risks that cannot be eliminated by design
3 Information for use about residual risks

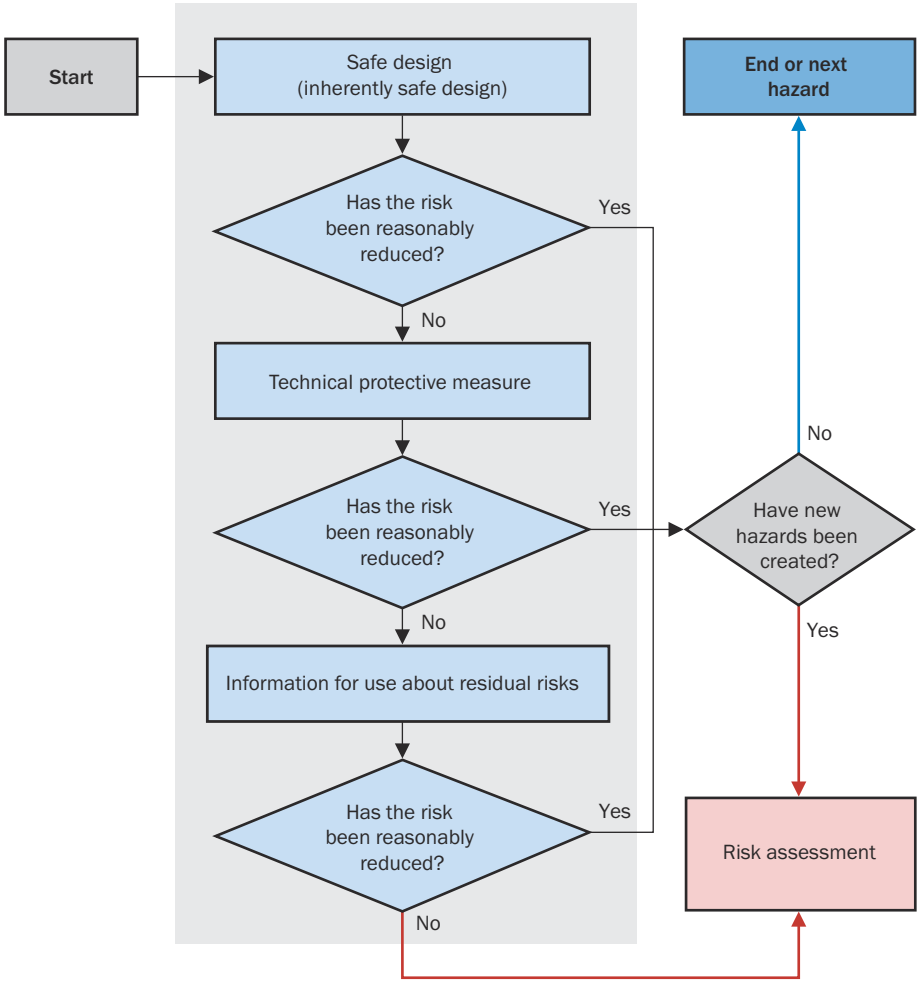


Figure 13: Process of the 3-step method for risk reduction

NOTE

➜ General principles of risk reduction: ISO 12100 (type-A standard)

2 Safe design (inherently safe design)

Safe design is the first and most important step in the risk reduction process. During this process, possible hazards are excluded by design. Safe design is therefore the most effective approach.

Aspects of safe design relate to the machine itself and the interaction between the person at risk and the machine.

Examples:

- Mechanical design
- Operating and maintenance concept
- Electrical equipment (electrical safety, EMC)
- Strategies for emergency stop in an emergency situation
- Equipment involving fluids
- Materials and resources used
- Machine function and production process

All components should be selected, applied and adapted in such a way that the safety of persons is maintained in the event of a machine error. The prevention of harm to the machine and the environment shall also be considered. All elements of the machine shall be designed to operate within the specified limits. The design should be as simple as possible. Safety-related functions shall be separated from other functions as far as possible.

Mechanical design

The following measures are examples of how mechanical design can prevent the arising of hazards:

- Avoiding sharp edges, corners, and protruding parts
- Avoiding crushing points, shearing points, and entanglement points
- Limiting kinetic energy (mass and speed)
- Considering ergonomic principles

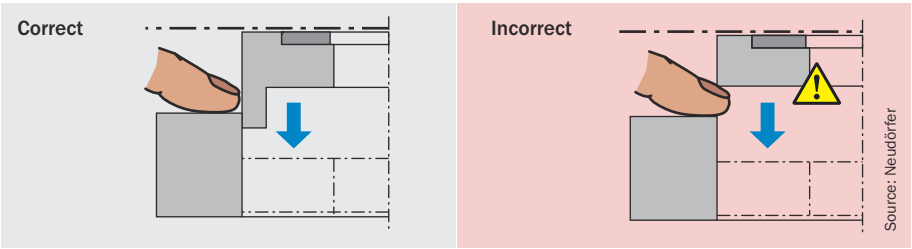


Figure 14: Example: Avoiding shearing points

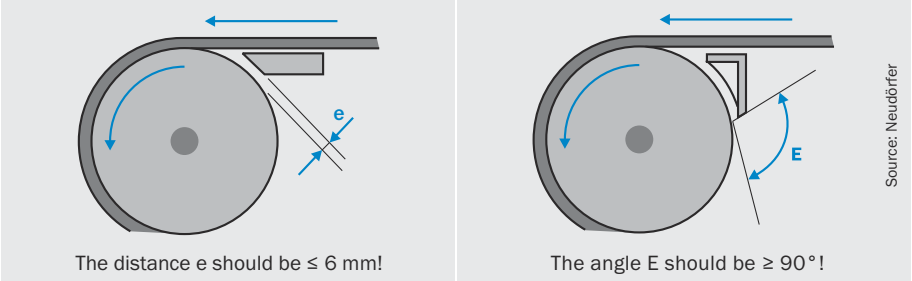


Figure 15: Avoiding entanglement points

NOTE

➜ Alfred Neudörfer: Konstruieren sicherheitsgerechter Produkte, Springer-Verlag, Berlin u. a., ISBN 978-3-662-62703-7 (8th edition 2020)

Operating and maintenance concept

The need for exposure to the hazard should be kept as low as possible. This can be achieved, for example, by:

- Automatic loading and unloading stations
- Setup and maintenance work from the “outside”
- Use of reliable, available components to prevent maintenance work
- Clear and unambiguous operating concept, for example grouping operating elements according to related functions (e.g., for setup operation)

Color marking

Manual control devices, indicators and information displayed on monitors shall be color-coded. The various colors have different meanings.

Table 6: Meaning of the colors of operating elements and indicator lights according to IEC 60204-1

General meaning of the colors for manual control devices

Color	Meaning	Explanation
White Gray Black	Non-specific	Initiation of functions
Green	Safe	Actuate during safe operation or to prepare the normal state
Red	Emergency	Actuate in case of dangerous state or in emergency
Blue	Mandatory	Actuate in case of state requiring mandatory action
Yellow	Abnormal	Actuate in case of abnormal state

General meaning of the colors for indicators

Color	Meaning	Explanation
White	Neutral	Use when uncertain about whether to use green, red, blue or yellow
Green	Normal status	
Red	Emergency	Dangerous state, respond with immediate action
Blue	Mandatory	Indicates a state requiring mandatory action by the operator
Yellow	Abnormal	Abnormal state, imminent critical state

NOTE

➜ Electrical equipment of machines: IEC 60204-1

Electrical equipment

Measures are required to exclude electrical hazards on machines. It is necessary to distinguish between two types of hazard:

- Hazards arising from electrical power, i.e., hazards due to direct or indirect contact
- Hazards arising from situations indirectly due to errors in the control system

NOTE

➜ In the following sections you will find important information on the design of the electrical equipment.

➜ Electrical equipment of machines: IEC 60204-1

Power supply connection

The electrical power supply connection is the interface between the electrical equipment in the machine and the supply grid. The regulations of the respective electricity grid operator on the connection must be observed.

A stable power supply is particularly important in safety-related applications. For this reason, the power supply should be able to bridge brief power outages.

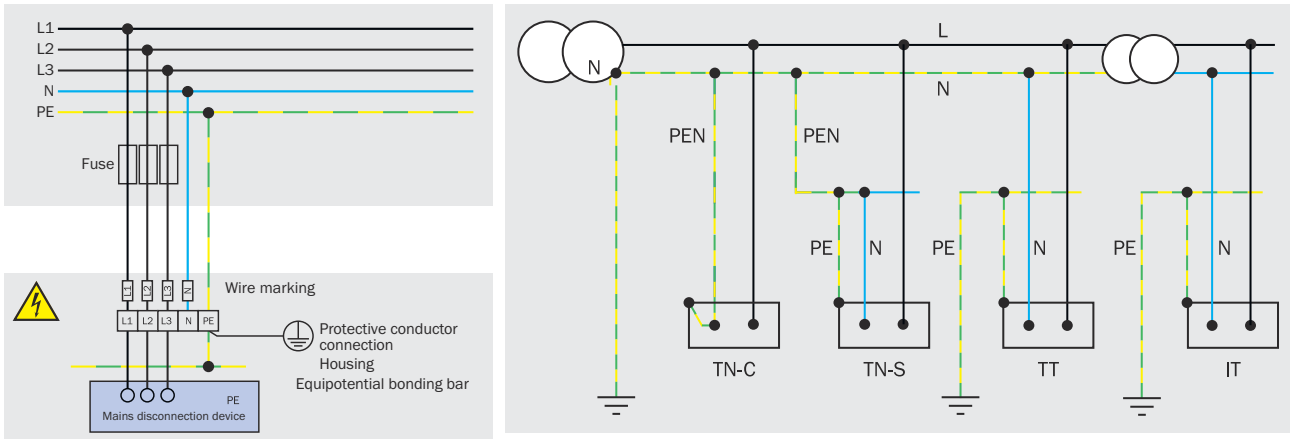
Earthing system

The earthing system characterizes both the type of connection on the secondary side of the supply transformer to earth and the type of earthing for the electrical equipment's chassis. Three earthing systems are standardized internationally:

- TN system
- TT system
- IT system

Earthing is an electrically conductive connection to the earth. A differentiation is made between protective earthing (PE), which is related to electrical safety, and functional earthing (FE), which is used for other purposes. The protective conductor system comprises earth electrodes, connecting cables, and the related terminals. For equipotential bonding, all conductive and accessible parts of the machine must be connected to the protective conductor system. Equipotential bonding is a basic means of protection in the event of a fault.

Table 7: Protective conductor system for different earthing systems



TN system

The TN system is the most common form of network in low voltage systems. In the TN system, the star point of the transformer is directly connected to earth (system earthing). The chassis of the equipment connected are connected to the transformer's star point via the protective conductor (PE).

Depending on the wire cross-section laid, PE and N conductors are laid as a common conductor (TN-C system) or as two independent conductors (TN-S system).

TT system

In a TT system, the star point of the supply transformer is earthed in the same way as in a TN system. The protective conductor connected to the electrically conductive equipment housing is not connected to this star point, but is earthed separately. The chassis of the equipment can also be earthed using a common protective earth electrode.

TT systems are usually only used in connection with residual current circuit breakers.

The advantage of the TT system lies in its increased reliability for remote areas.

IT system

The conductive housings of the equipment in an IT system are earthed in the same way as in a TT system, but the star point of the feeding transformer is not. Systems in which a shutdown will result in a hazardous situation and which should therefore not be shut down yet in the event of a single short-circuit or earth fault are designed as IT systems.

In the low-voltage area, IT systems are required, for example, to supply operating rooms and intensive care stations in hospitals.

NOTE

➜ Protective measures: Basic standard IEC 61140 and IEC 60364-4-41 with varying national amendments.

Mains disconnection device

According to IEC 60204-1, a mains disconnection device must be provided for every power supply connection to one or more machines. It must be able to isolate the electrical equipment from the power supply.

The following disconnection devices can be used for this purpose:

- Power circuit breaker for use category AC-23B or DC-23B
- Isolating switch with auxiliary contact for leading load shedding
- Circuit breaker
- Plug/socket combination up to 16 A / 3 kW

Certain circuits such as control circuits for interlocking functions do not need to be shut down by the isolation device. In this case special precautions must be taken to ensure the safety of operators.

Power isolation to prevent unexpected start-up

When working on the machine (maintenance, cleaning, servicing, etc.), a machine start or the restoration of power shall not result in a hazard for the persons involved. When mains disconnection devices are used, means shall be provided to prevent unintentional and/or mistaken switching of the power supply isolation device. This can be achieved, for example, by blocking the main switch in the “OFF” position with a padlock.

NOTE

This power isolation device is not suitable for use as a protective measure for brief interventions into the hazardous area for operational purposes.

Protection against electric shock

Protection classes

The classification into different protection classes describes the means by which single-fault safety is achieved. This categorization does not provide an indication of the level of protection.

Table 8: Symbols and explanations of protection classes

	**Protection class I** All devices with simple insulation (basic insulation) and a protective conduction connection are in protection class I. The protective conductor must be connected to a terminal marked with the earthing symbol or PE and be green-yellow.
	**Protection class II** Equipment in protection class II has increased insulation or double insulation and is not connected to the protective conductor. This protective measure is also known as protective insulation. There shall be no connection of a protective conductor.
	**Protection Class III** Equipment in protection class III operates with a safety extra-low voltage and, therefore, does not require any explicit protection.

Safety extra-low voltage SELV/PELV

AC voltages up to 50 volts (V_{RMS}) and DC voltages up to 120 volts are allowed as safety extra-low voltages. Above 75 volts DC, the requirements of the Low Voltage Directive must also be observed.

In the case of applications in normally dry rooms, it is not necessary to provide protection against direct contact (basic protection) if the rms value of the AC voltage does not exceed 25 V or the harmonic-free DC voltage does not exceed 60 V. A harmonic-free state exists when the DC voltage is superimposed with a sinusoidal AC voltage component of no more than 10% effective.

The safety extra-low voltage circuit shall be safely separated from other circuits (adequate air and creepage distances, insulation, connection of circuits to the protective conductor, etc.).

Two safety extra-low voltages are distinguished:

- SELV (safety extra-low voltage)
- PELV (protective extra-low voltage)

NOTE

A safety extra-low voltage shall not be generated from the mains using autotransformers, voltage dividers, or series resistors.

Table 9: Safety extra-low voltages SELV/PELV

		ELV (AC < 50 V rms, DC < 120 V)	
		SELV	**PELV**
Type of isolation	**Power sources**	Power sources with safe isolation, e.g., a safety transformer or equivalent power sources	
	Circuits	• Circuits with safe isolation from other non-SELV or non-PELV circuits • Circuits with basic insulation between SELV and PELV circuits	
Reference to earth potential or to a protective earth conductor	**Circuits**	Unearthed circuits	Earthed or unearthed circuits
	Housing	Housings cannot be intentionally earthed and also not connected to a protective conductor.	Housings can be intentionally earthed or connected to a protective conductor.
Additional measures	**Nominal voltage:** **AC > 25 V or** **DC > 60 V or** **Equipment in water**	Basic protection by means of insulation or sheathings in accordance with standards	
	Nominal voltage in normal dry environment: **AC ≤ 25 V or** **DC ≤ 60 V**	No additional measures required	Basic protection by means of: Insulation or sheathings in accordance with standards or Body and active parts connected to main earthing rail

NOTE

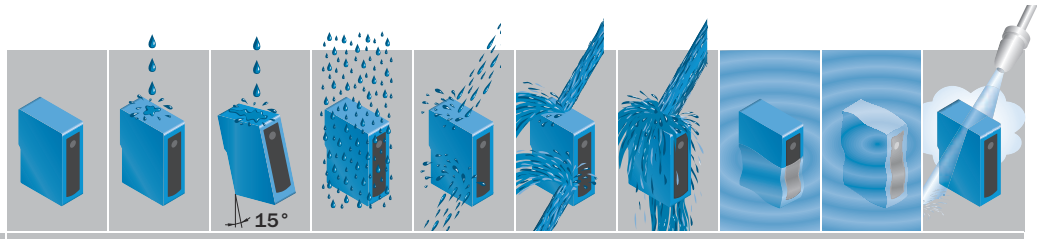
➜ Protection classes: IEC 60364-4-41

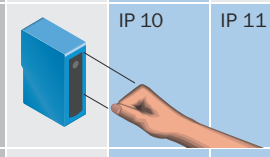
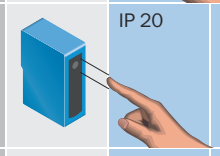
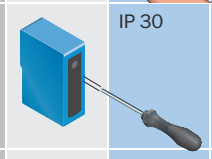
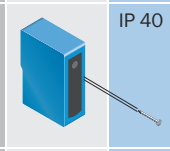
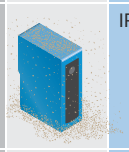
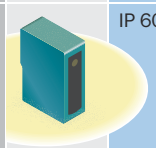
➜ Safety of transformers: EN 61558-x

Protective measures/enclosure ratings

The enclosure ratings describe the protection of a component against the ingress of water (not steam) and foreign objects (dust). In addition, they describe protection against direct contact with live parts. This protection is always required, even at low voltages. All parts that remain live after the isolation of the power shall be designed to at least enclosure rating IP 2x, control cabinets shall be designed to at least enclosure rating IP 54.

Table 10: Overview of protection classes according to IEC 60529



1st digit: Protection against ingress of solid foreign bodies		2nd digit: Protection against ingress of water (no steam, no other liquids!)									
		IP ...0	IP ...1	IP ...2	IP ...3	IP ...4	IP ...5	IP ...6	IP ...7	IP ...8	IP ...9K
		No protection	Dripping water vertical	Dripping water at an angle	Spraying water	Spraying water	Jet water	Jet water, heavy	Immersion temporary	Immersion continuous	100 bar, 16 l/min., 80 °C
IP 0... No protection		IP 00									
IP 1... Size of the foreign body ≥ 50 mm Ø		IP 10	IP 11	IP 12							
IP 2... Size of the foreign body ≥ 12 mm Ø		IP 20	IP 21	IP 22	IP 23						
IP 3... Size of the foreign body ≥ 2.5 mm Ø		IP 30	IP 31	IP 32	IP 33	IP 34					
IP 4... Size of the foreign body ≥ 1 mm Ø		IP 40	IP 41	IP 42	IP 43	IP 44					
IP 5... Protected against dust		IP 50			IP 53	IP 54	IP 55	IP 56			
IP 6... Dust-tight		IP 60					IP 65	IP 66	IP 67		IP 69K

Stopping

Besides stopping a machine during normal operation, it shall also be possible to stop a machine in an emergency situation.

Requirements:

- All machinery shall be fitted with one or more emergency stop control devices, that bring the machine to a shutdown in an emergency.
- Every machine shall be equipped with a control for stopping the machine in normal operation.

- At least one category 0 stop function shall be available. Additional category 1 and/or 2 stop functions may be necessary for safety-related or function-related reasons on the machine.
- A command to stop the machine shall have a higher priority than the commands for putting the machine into operation.

Stop categories according to IEC 60204-1

Safety-related and function-related aspects in machines result in stop functions in various categories. Stop categories shall not to be confused with the categories according to ISO 13849-1.

Table 11: Stop categories according to IEC 60204-1

Stop category 0	Supply of power to the drive elements is isolated (uncontrolled stopping)
Stop category 1	Machine is placed in a safe state, only then the supply of power to the drive elements is isolated
Stop category 2	Machine is placed in a safe state but the supply of power to the drive elements is not disconnected

NOTE

➜ See also section "Emergency stop", page 49.

NOTE

➜ Stop categories, see “Electrical equipment of machines: IEC 60204-1”.

Electromagnetic compatibility (EMC)

Electromagnetic compatibility is “the ability of a device, unit of equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment”.

The machine and the components used shall be selected and verified so that they can withstand or are immune to the expected disturbances. Increased requirements apply to safety components.

Electromagnetic disturbances can arise from the following causes:

- Fast, transient, electrical disturbances (burst)
- Surge voltages, e.g., caused by lightning strikes to the grid
- Electromagnetic fields
- High-frequency disturbance (neighboring cables)
- Electrostatic discharge (ESD)

The limits for interference immunity and interference emission are different for industrial and residential applications. More stringent requirements apply to components in the industrial sector. On the one hand they must withstand stronger disturbances, but on the other hand they are allowed to interfere more strongly. Components that meet the RF interference requirements in the industrial sector may cause RF interference in residential areas.

The following table shows examples of the typical interference immunity in a number of areas of application, in each case in the frequency range from 900 to 2 000 MHz.

Table 12: Typical interference immunity by area of application

Area of application	Minimum interference field strength for immunity
Entertainment electronics	3 V/m
Household electrical appliances	3 V/m
Information technology equipment	3 V/m
Medical equipment	3 ... 30 V/m
Industrial electronics	10 V/m
safety components	10 ... 30 V/m
Vehicle electronics	Up to 100 V/m

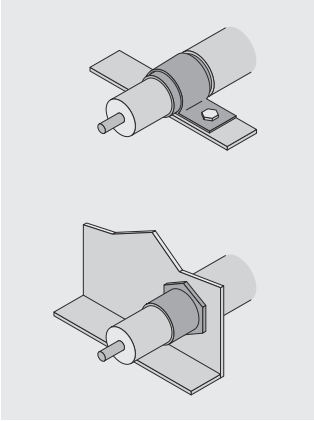
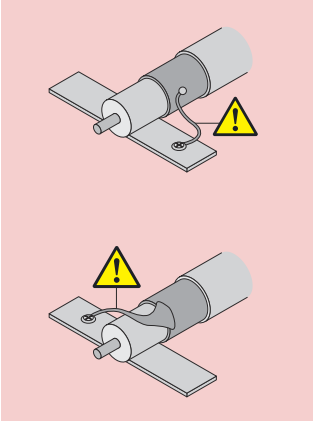
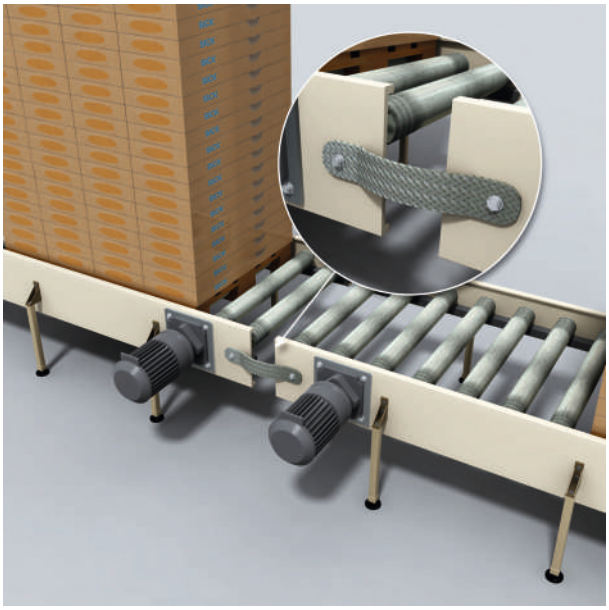
Table 13: Example of typical distances from mobile phone systems for different field strengths

Area of application	3 V/m	10 V/m	100 V/m	Note
DECT station	Approx. 1.5 m	Approx. 0.4 m	≤ 1 cm	Base station or hand-held unit
GSM mobile phone	Approx. 3 m	Approx. 1 m	≤ 1 cm	Maximum sender power (900 MHz)
GSM base station	Approx. 1.5 m	Approx. 1.5 m	Approx. 1.5 m	Sender power approx. 10 W

Basic design rules to avoid EMC problems

- Ensure continuous equipotential bonding by means of conductive connections between parts of machinery and systems.
- Apply physical separation of the control and measuring components from the supply unit, e.g., power supply units, contactors, actuators, inverters.
- Do not use the shielding to carry equipotential bonding currents.
- Use short shields and apply to the full surface area.
- Connect any functional earth (FE) provided.
- Terminate existing communication lines properly according to the manufacturer's specifications, e.g., using a terminator.

Twisted cables are often required to transmit data (fieldbus).

Example: Connecting shield correctly		Example: Providing equipotential bonding
		
Correct: Shield is short and fully tethered	Wrong: So-called “pig tails”	

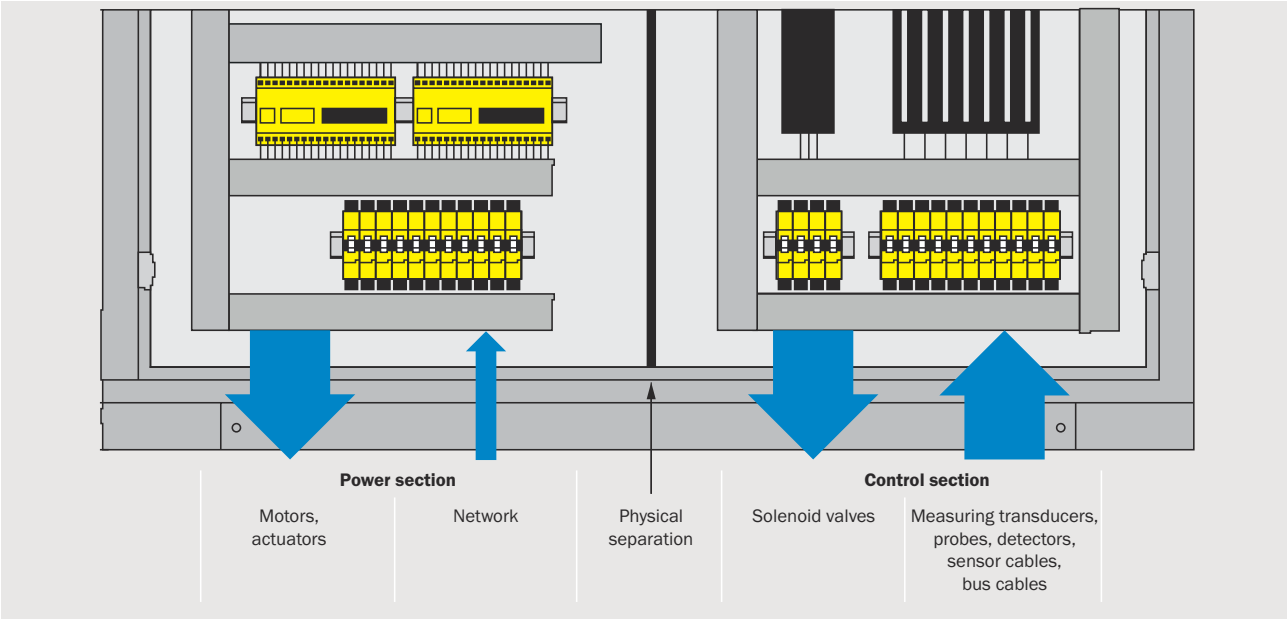


Figure 16: Example of physical separation

NOTE

➜ EMC standards: IEC 61000-1 to -4

➜ EMC requirements on safety components: IEC 61496-1, IEC 62061

Fluid technology

Fluid technology is the generic term used for all processes where energy is transmitted using gases or liquids. The generic term is used because liquids and gases behave similarly. Fluid technology describes processes and systems for the transmission of power using fluids in closed pipe systems.

Subsystems

Every fluid-related system comprises the following subsystems:

- Compressing: compressor/pump
- Conditioning: filters
- Pumping: pipework/hoses
- Controlling: valve
- Driving: cylinder

Pressure is established in any fluid-related system by pumping the fluid against loads. If the load increases, the pressure also increases.

Fluid technology is applied in engineering in hydraulics (energy transmission using hydraulic oils) and in pneumatics (energy transmission using compressed air). Oil-based hydraulics required a circuit for the fluid (feed and return), while in pneumatics the exhaust air is discharged to the environment using acoustic attenuators.

Design principles

The basic principles for the safe application of fluid technology are described in ISO 4413 (hydraulics) and ISO 4414 (pneumatics). All parts of a fluid-related system are to be protected against pressures that exceed the maximum operating pressure of a subsystem or the rated pressure of a component. A danger shall not be caused by leaks in a component or in the pipework/hoses. Acoustic attenuators are to be used to reduce the noise caused by escaping air. The use of acoustic attenuators shall not produce any additional hazard; acoustic attenuators shall not cause any harmful back-pressure.

Use in potentially explosive atmospheres

Protection against explosions is a particularly safety-related task. People are placed at risk in the event of an explosion, e.g., due to uncontrolled radiation of heat, flames, pressure waves, and flying debris, as well as due to harmful reaction products and the consumption of the oxygen in the ambient air necessary for breathing. Explosions and fires are not among the most common causes of industrial accidents. They often result, however, in serious injuries and death as well as major economic damage.

Where dust, flammable gases, or liquids are manufactured, transported, processed, or stored, a potentially explosive atmosphere may be produced, i.e., a mixture of fuel and atmospheric oxygen within the limits for explosions. If a source of ignition is present, an explosion will occur.

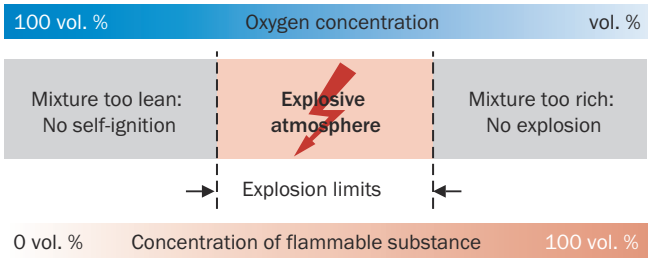


Figure 17: Conditions for an explosive atmosphere

Assessing the scope of the required protective measures

To assess the scope of the required protective measures, operators/employers need to divide potentially explosive-hazardous areas into zones based on the probability of the creation of a hazardous explosive atmosphere, see the ATEX Operational Directive 1999/92/EC, Annex I.

The information in the following table does not apply to mining (underground or surface).

Table 14: ATEX zone definition and equipment categories for equipment group II: Equipment for use in explosive dust and gas atmospheres

Zone definition				
For gases	**G**	Zone 2	Zone 1	Zone 0
For dusts	**D**	Zone 22	Zone 21	Zone 20
Explosive atmosphere		Seldom, short duration (< 10/year)	Occasional (10 – 100 h/year)	Continuous, frequent, long duration (> 1,000 h/year)
Safety measure		Normal	High	Very high
Device category that can be used (ATEX)				
1		II 1G/II 1D		
2		II 2G/II 2D		
3		II 3G/II 3D		

Labels

Equipment must be designed, tested, and suitably marked for use in these zones in accordance with the ATEX Product Directive 2014/34/EU.

Table 15: Marking of equipment for use in zones with explosive atmospheres

Ex	II	2G	Ex ia	IIC	T4	**Example: Marking of an item of equipment as per ATEX**
					Temperature class Can be used at ignition temperature > 135 °C	
				Explosive group Acetylene, carbon disulfide, hydrogen		
			Protection principle i = intrinsically safe a = two-fault-safe			
		Device category (ATEX) Can be used in zone 1				
	Equipment group Not for use in areas where there is a risk of firedamp					
Explosion protection marking						

NOTE

➜ ATEX Operational Directive: 1999/92/EC

➜ ATEX Product Directive: 2014/34/EU

➜ Standard: EN 1127-1 Explosive atmospheres - Explosion prevention and protection - Part 1: Basic concepts and methodology

➜ Standard: EN IEC 60079-0 Explosive atmospheres - Part 0: Equipment - General requirements

Summary: Safe design

Mechanics, electronics, operation

- The most effective and important measure is safe design to prevent hazards from occurring in the first place.
- Design so that the operators are exposed to the hazardous area as little as possible.
- Avoid dangers produced directly due to electrical power (direct and indirect contact) or produced indirectly due to faults in the control system.

Stopping

- Plan a control device for stopping the machine in normal operation.

EMC

- Design machines that meet applicable EMC requirements. The components used must be selected and verified so as to meet the following criteria:
  - Comply with electromagnetic disturbance limits to not interfere with other equipment or devices
  - Ensure immunity to the expected disturbances
  - Comply with limit values for the area of application

3 – Technical protective measures

A technical protective measure is implemented by means of one or more safety functions. Each safety function comprises at least one protective device. There are three types of protective devices:

- Mechanical protective devices that retain parts, substances, or radiation or permanently prevent entry/ access.
- Protective devices that are integrated into the controller of the machine to initiate the safe state as soon as persons or parts of the human body are detected.
- Protective devices that are integrated into the controller of the machine to initiate the safe state as soon as the monitored safety-related limits of machine parameters (position, speed, force, etc.) are exceeded.

All these protective devices implement safety functions, but not every protective device has to be integrated into the machine controller for this purpose. Fixed physical guards (fences, barriers, covers), for example, are not integrated into the machine controller but if designed correctly, such guards fulfill the requirement of the safety function.

Functional safety

When protective devices are integrated into the machine controller, the risk reduction relies on the correct functioning of the controller. In this case, we refer to this as functional safety. When implementing functional safety, the required safety level must be determined for each safety function. The requirements of each particular protective measure must be implemented using suitable components.

Validation

The validation of all technical protective measures ensures that the safety functions reliably reduce the risk.

The design of technical protective measures and safety functions and the methodology for their implementation in the control system form the content of the next chapter (sub-steps 3a to 3e).

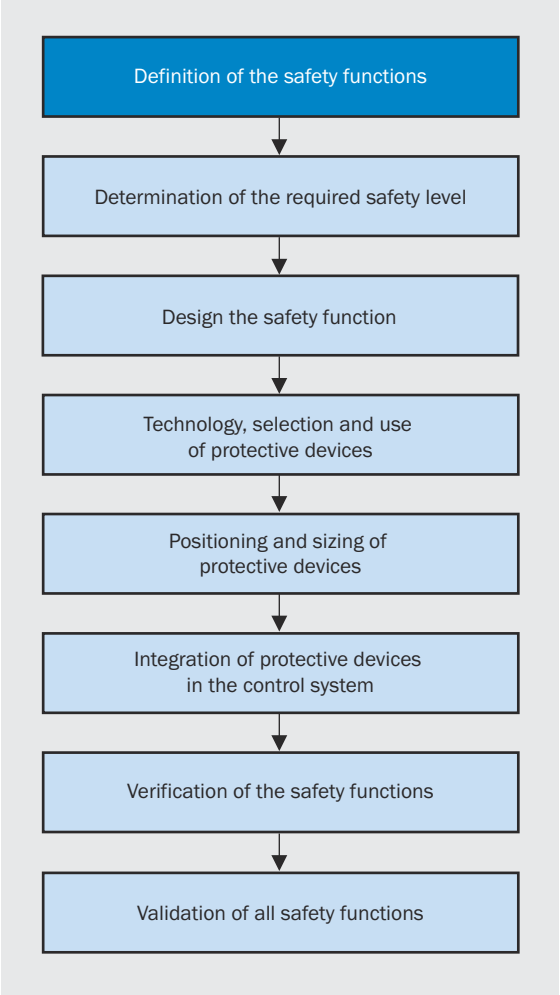


Figure 18: From definition to validation of the safety functions

3a – Defining the safety functions

The safety functions describe how risks are reduced by protective measures. At least one safety function must be defined for each hazard that has not been eliminated by the design.

It is necessary to precisely describe the safety function in order to achieve the required safety with reasonable effort. The type and number of components required for the function are derived from the definition of the safety function.

NOTE

➜ Examples for the definition of safety functions: IFA Report 2/2017, “Functional safety of machine controls”

Permanently preventing entry/access

Access to a hazardous point is prevented by means of mechanical covers, barriers, or obstacles (referred to as physical guards).

Examples:

- Prevention of direct access to hazardous points using covers (see figure)
- Distancing protective devices (e.g., tunnels) to prevent access to the hazardous points and allow the passage of materials or goods (see figure)
- Prevention of access to hazardous areas using physical guards

Figure 19: Preventing access to the hazardous point in a packaging machine by means of a tunnel

Temporarily preventing access

Access to a hazardous point is prevented until the machine is in a safe state.

Examples:

- On request, a machine stop is initiated. When the machine reaches the safe state, the blocking of access by the safety locking device is released.
- After disconnecting the power, a transfer key that allows access (opening the movable physical guard) is enabled.

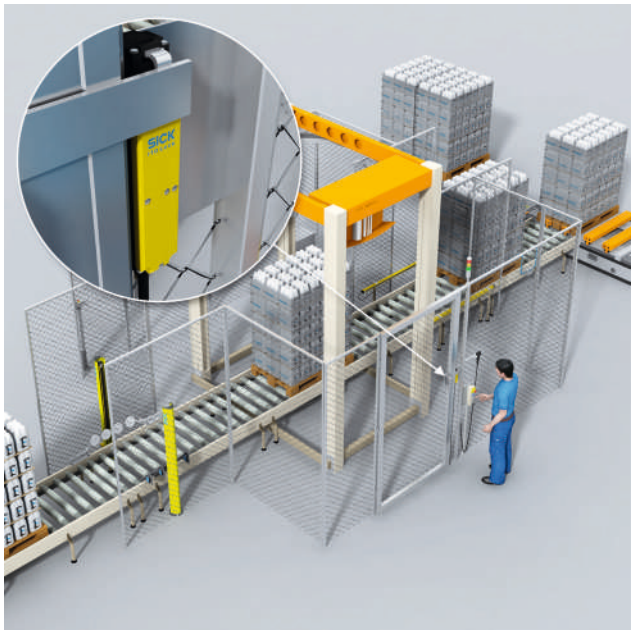


Figure 20: Temporarily preventing access to the hazardous point in a stretch film wrapper by means of a safety locking device

Retaining parts/substances/radiation

If parts can be ejected out of machines or radiation can arise, mechanical protective devices (physical guards) must be used to prevent these hazards.

Examples:

- Protection hood with special viewing window on a milling machine to protect against ejected shavings and tool parts
- Fence that can hold back a robot

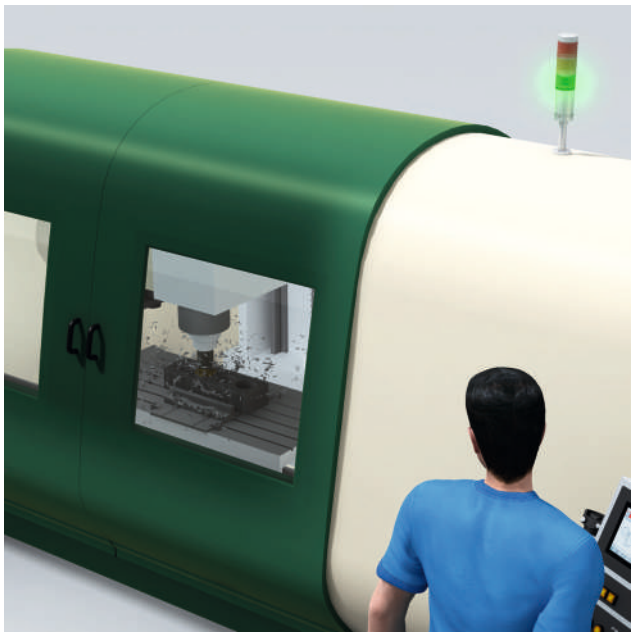


Figure 21: Retention of shavings in a processing machine by means of a protection hood

Initiating a stop

The purpose of a safety-related stop function is to place the machine in a safe state when requested (e.g., if a person approaches). To reduce the required stopping time, it may be advisable to implement a stop function that complies with stop category 1 (IEC 60204-1 "Stopping", page 35). Additional safety functions may be necessary to prevent an unexpected restart.

Examples:

- Opening a protective door with an interlock that has no locking device
- Interruption of the light beam of a safety light-beam sensor that protects against access

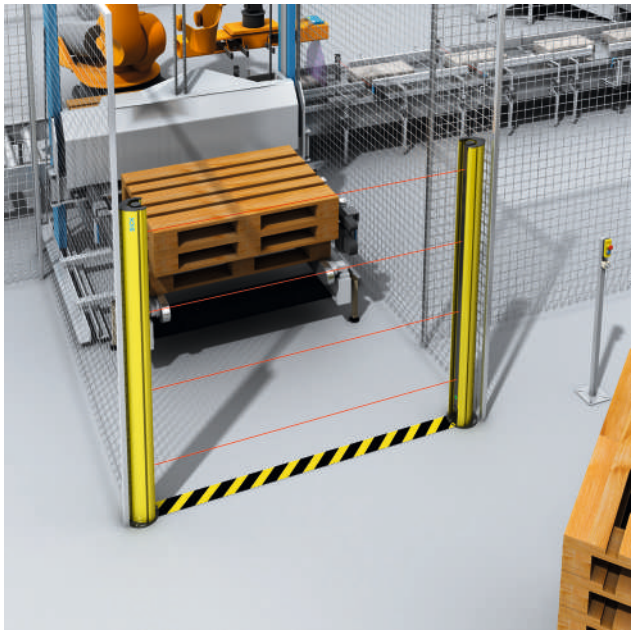


Figure 22: Initiating a stop by a safety multibeam sensor on a pallet handling machine when a person approaches

Avoiding an unexpected start-up

After the “Initiating a stop” function is triggered or the machine is switched on, it should require deliberate actions to put the machine into operation. These actions include manually resetting a protective device to prepare for restarting the machine (see also section "Application of reset and restart", page 110)

Examples:

- Resetting a safety light curtain (see figure: blue “Reset” button)
- Resetting the emergency stop device

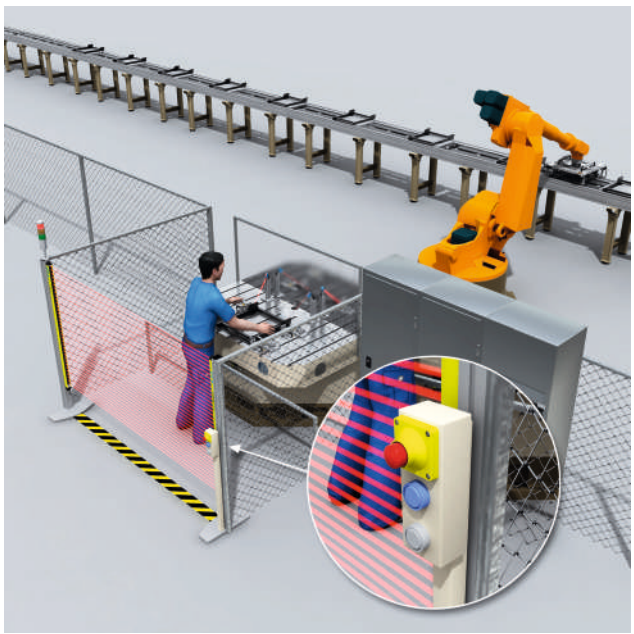


Figure 23: Avoiding the unexpected start-up by deliberate resetting the safety light curtain

Preventing start

After the “Initiating a stop” function, technical measures should be used to prevent the machine from starting or being put back into operation as long as there are persons in the hazardous area.

Examples:

- Use of a trapped key system: Restoration of power is only possible using the transfer key. The transfer key is only available when the means of access (movable physical guard) is closed and locked.
- Detection in the active protective field of a horizontally arranged safety light curtain. The “Initiating a stop” function is implemented by means of the vertical protective field of the safety light curtain.

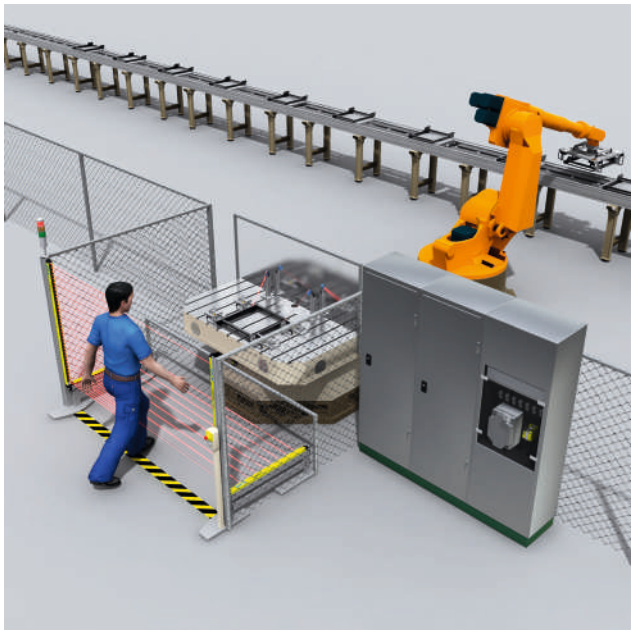


Figure 24: Preventing start-up by means of a horizontal safety light curtain

Combination of initiating a stop/preventing start

Restart is prevented using the same protective device that initiates the stop as long as there are persons or parts of the body in the hazardous area.

Examples:

- A two-hand control on single-person workplaces
- Use of a safety light curtain so that standing behind or reaching around is not possible (hazardous point protection)
- Use of a safety laser scanner for area protection

Figure 25: Initiating a stop and preventing start using a safety laser scanner (hazardous area monitoring)

Allowing material passage

To move materials in or out of the hazardous area, specific features of the materials moved are used for material detection or to automatically differentiate between material and people. The protective device is then not actuated during material transport; however, people are detected.

Examples:

- Selecting suitable sensors and placing them in appropriate positions enables the material to be detected and the safety function to be temporarily suspended while the material passes through (muting).
- Protective field switching on a safety laser scanner
- Horizontal light curtains with integrated algorithm for **human-material differentiation**

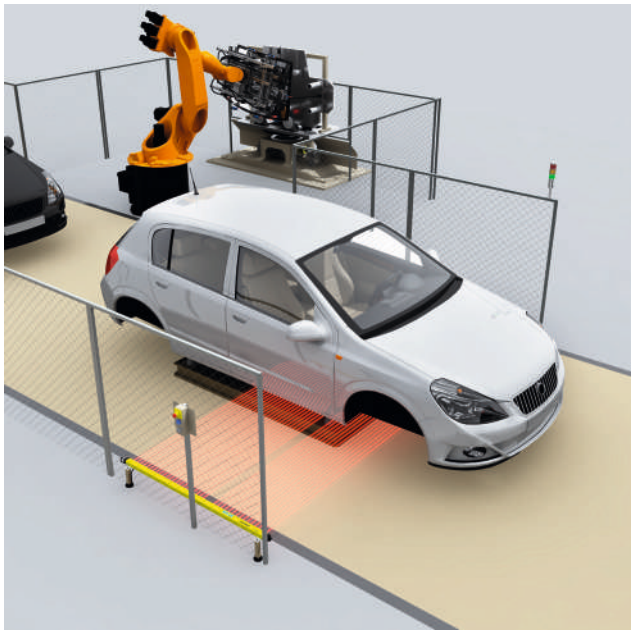


Figure 26: Access monitoring and allowing a car body to be transferred through a horizontal safety light curtain with integrated human-material differentiation

NOTE

➜ For more detailed information, see section see "Automatic material passage using ESPE", page 78.

Monitoring machine parameters

In some applications, it is necessary to monitor various machine parameters for safety-related limits. If a limit is exceeded, suitable measures are initiated (e.g., stop, warning signal).

Examples:

- Monitoring of speed, temperature, or pressure
- Position monitoring for collision avoidance

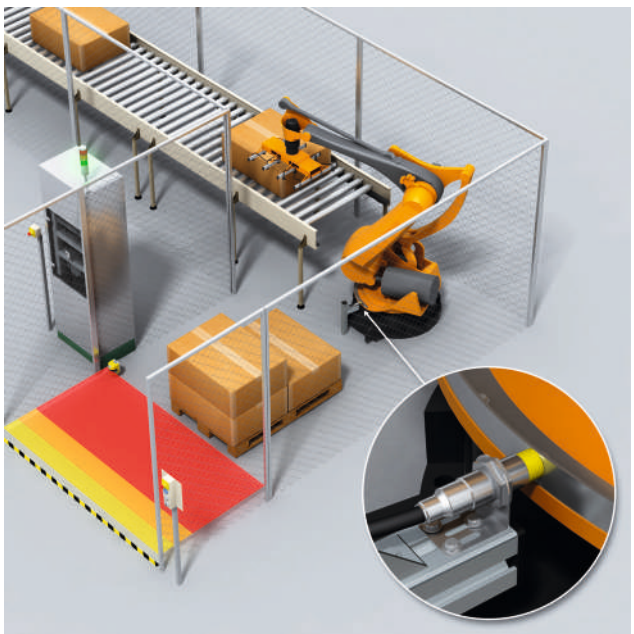


Figure 27: Monitoring the robot position using an inductive proximity sensor

Safeguarding work areas shared by humans and machines

If the operation of a machine requires a workspace to which both a worker and hazardous parts of the machine (e.g., a robot) need access at different times, it must be ensured that any contact or collision is avoided.

Additional safety functions may be necessary to avoid an unexpected restart.

Figure 28: Safeguarding a shared work area for humans and robots using safety light curtains

Disabling safety functions manually and for a limited time

If it is necessary for setup work or process monitoring to operate the machine with the protective function of the protective devices disabled, a suitable operating mode should be provided that meets the following requirements:

- Operating mode is only activated when an operating mode selector switch is in the corresponding position.
- Operating mode locks all other control and operating modes of the machine.
- Operating mode does not allow machine movements due to direct or indirect action on sensors or linked sequences.
- Operating mode allows dangerous machine functions only while command devices (e.g., enabling switch) are continuously actuated and under reduced risk conditions (e.g. limitation of speed, movement path, function duration).

Figure 29: Safe changing of the film roll on a stretch film wrapper with the movable guard (door) open through a combination of enabling switch and safely reduced speed

Combining or switching safety functions

A machine can adopt various states or work in various operating modes. Within this context, different safety measures may be effective or different safety functions may be coupled together. The process of switching between operating modes, or the selection and adjustment of different safety measures, is not allowed to lead to a dangerous state. When combining or changing safety functions, an appropriate safety level must also be determined and implemented.

Examples:

- After a change of operating mode between setup and normal operation, the machine is stopped. A new manual start command is necessary.
- Adapting the monitored area of a safety laser scanner according to the vehicle speed

Figure 30: Adapting the monitored area of a safety laser scanner according to the vehicle speed

Emergency stop

Emergency stop is a complementary protective measure and not a protective device.

The safety level of this function shall be defined based on the risk assessment of the machine. In particular, influencing environmental factors (e.g., vibration, method of actuation, etc.) shall be considered (see also section "Emergency operation", page 89).

Figure 31: Emergency stop by means of an emergency stop pushbutton

NOTE

➜ See IEC 60204-1 and ISO 13850

Safety-related indications and alarms

Safety-related indications are means of providing the user with information about impending hazards (e.g., overspeed) or possible residual risks. These kind of signals can also be used to warn the operator before automatic protective measures are initiated.

The following should be noted:

- Warning devices must be designed and arranged so that they can easily be checked and inspected.
- The information for use shall include the prescription of the regular inspection of warning equipment.
- Sensorial saturation should be avoided, in particular where audible alarms are concerned.

Examples:

- Interlocking indications
- Startup warning devices
- Muting lamps

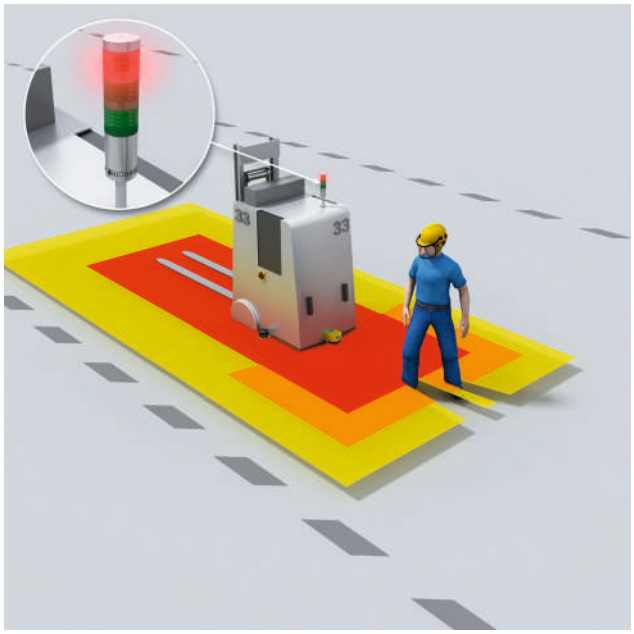


Figure 32: Safety-related indications on an autonomous fork-lift truck

Other functions

Safety devices can also perform other functions. The actual safety functions must not be impaired as a result of this.

Examples:

- Tool and machine protection
- PSDI mode (cycle initiation - see "Additional functions of ESPE", page 81 ff)
- Using the measurement data of a safety laser scanner to navigate an autonomous vehicle

Summary: Defining the safety functions

Define which safety functions are required for risk reduction:

- Permanently preventing entry/access
- Temporarily preventing access
- Retaining parts/substances/radiation
- Initiating a stop
- Avoiding an unexpected start-up
- Preventing start
- Combination of initiating a stop/preventing start
- Allowing material passage
- Monitoring machine parameters
- Safeguarding work areas shared by humans and machines
- Disabling safety functions manually and for a limited time
- Combining or switching safety functions
- Emergency stop
- Safety-related indications and alarms

3b – Determining the required safety level

As a rule, type-C standards (machine-specific standards) shall specify the required safety level.

The required safety level must be defined separately for each safety function, and applies for all devices involved, for example ...

- the sensor/the protective device
- the evaluating logic unit
- the power control element(s)

If no type-C standard exists for the particular machine or the type-C standard does not contain any requirements relating to this, the required safety level can be determined on the basis of one of the following standards:

NOTE

➜ ISO 13849-1

➜ IEC 62061

By applying these standards it can be ensured that the effort required to reduce the risk is reasonable for the risk that has been determined. The protection of an operator who manually inserts and removes parts at a metal press requires a different risk reduction compared to the protection of an operator who works on a machine on which the maximum risk is the trapping of a finger. Safety functions shall be specified individually for each phase of the machine's life cycle and hazard, since one and the same machine can have different hazardous points with different risks during different phases of the lifecycle.

The risk assessment is based on the following parameters:

- The severity of the possible injury/damage to health
- Frequency and/or duration of exposure
- The possibility of preventing the hazard

By combining these parameters, the required safety level can be determined. Some standards contain suitable methods for this determination. The risk assessment always starts without considering risk reduction measures.

Required performance level (PLr) according to ISO 13849-1

This standard uses a risk graph to determine the required risk reduction level. The parameters S, F and P are used to determine the magnitude of the risk.

The result of the procedure is a "required performance level" (PLr).

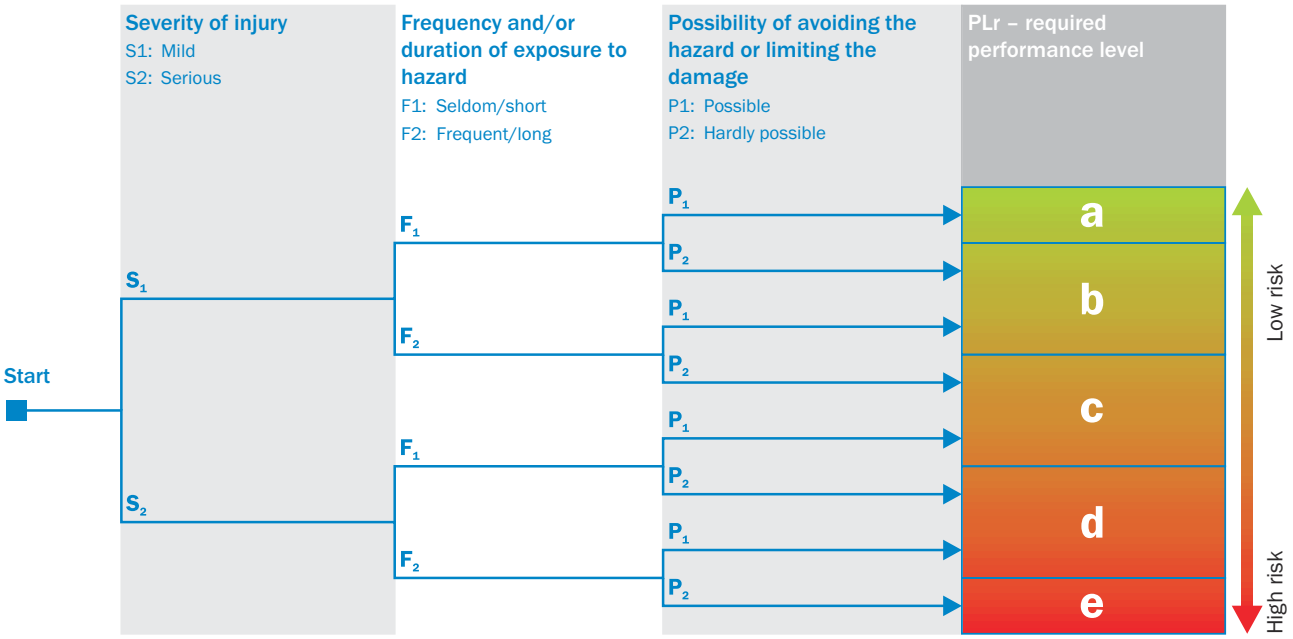


Figure 33: Risk graph according to ISO 13849-1

The performance level is defined in five discrete steps. The performance level depends on the structure of the control system, the reliability of the components used, the ability to detect faults as well as the resistance to common cause faults in multi-channel controllers (see section "Safety-related aspects of subsystems", page 56). In addition, further measures to avoid design faults are required.

If the probability of occurrence of a hazardous event can be assessed as low, the PLr may be reduced by one level. This method is described in Annex A of the standard. This annex is informative and not normative. It is not necessary, therefore, to apply the process described there in order to fully comply with the requirements of the standard.

The SCRAM method from SICK can also be used as an alternative. The advantage is the universal applicability and the finer granularity of the decision parameters see "Scalable Risk Analysis and Evaluation Method (SCRAM)", page 24.

Required safety integrity level (SIL) according to IEC 62061

The procedure used here is a numerical procedure. The severity, the frequency and duration of exposurein the hazardous area, and the probability of avoiding or limiting harm are evaluated. In addition, the probability of occurrence of the hazardous event is taken into consideration. The result is the required safety integrity level (SIL).

Table 16: Required safety integrity level depending on the impact of the hazard according to IEC 62061

Effects	Severity Se	Class Cl = Fr + Pr + Av				
		4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing finger(s)	3			SIL 1	SIL 2	SIL 3
Reversible, medical attention	2				SIL 1	SIL 2
Reversible, first aid	1					SIL 1

Table 17: Influencing variables for SIL determination according to IEC 62061

Frequency[1] of exposure Fr		Probability of occurrence of the hazardous event Pr		Probability of avoidance of the hazardous event Pv	
Fr ≥ 1 × per hour	5	Very high	5		
1 × per hour > Fr ≥ 1 × per day	5	Likely	4		
1 × per day > Fr ≥ 1 × in 2 weeks	4	Possible	3	Impossible	5
1 × in 2 weeks > Fr ≥ 1 × per year	3	Rarely	2	Rarely	3
1 × per year > Fr	2	Negligible	1	Probable	1

1) Applies for durations > 10 minutes

The SIL is determined as follows:

- Determine the severity Se.
- Determine values for the Frequency Fr, Probability Pr, and Avoidance Pv.
- Calculate the Class Cl from the sum of Fr + Pr + Pv.
- The required SIL is the intersection between the row “Severity Se” and the column “Class Cl”

The SIL is defined in three discrete steps. The SIL implemented depends on the structure of the control system, the reliability of the components used, the ability to detect faults as well as the resistance to multiple common cause faults in multiple channel control systems. In addition, further measures to avoid design faults are required (see "Safety-related aspects of subsystems", page 56).

Summary: Determining the required level of safety

General

- Define the necessary level of safety for each safety function.
- The parameters “severity”, “probability of occurrence” and “probability of avoiding damage” determine the required safety level.

Applicable standards

- ISO 13849-1 uses a risk graph to determine the required safety level. The result of the procedure is a “required performance level” (PLr).
- ISO 13849-1 is also applicable to hydraulic, pneumatic, and mechanical systems.
- IEC 62061 uses a numerical method to determine the required safety level. The result is a required safety integrity level (SIL).

3c – Designing the safety function

Steps 3c and 3d describe the design and verification of the safety functions. These steps may need to be performed several times in an iterative process.

Step 3c includes the development of the safety concept, the selection of the protective devices, the integration into the controller, and the verification of the safety function.

NOTE

During this process it is necessary to repeatedly check whether the selection of the technology offers sufficient safety and is also technically feasible, or whether other risks or additional risks are produced by the use of a specific technology.

Safety concept

Develop a concept for the required safety functions.

A machine or system consists of several components that interact and ensure the functionality of a machine or system.

A distinction must be made here between components that perform pure operating tasks and ones that are responsible for safety-related functions.

NOTE

➜ For details on this: IFA Report 2/2017, “Functional Safety of Machine Controls” at www.dguv.de/ifa/publikationen

Functional structure of a machine controller

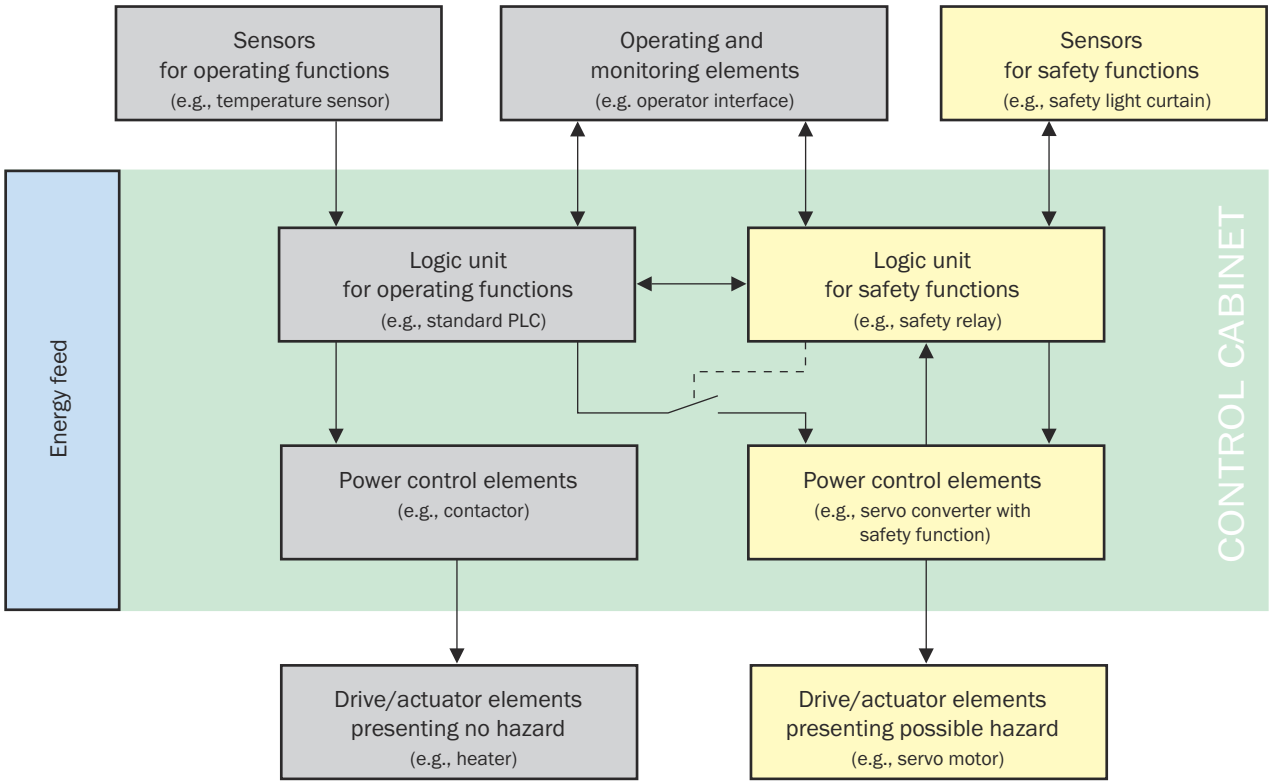


Figure 34: Functional structure of a machine controller

The safety-related parts of control systems shall be selected to suit the safety functions and the necessary level of safety. These parts include sensors, logic units, power control elements, for example, as well as drive and work elements. This selection is usually made while developing the safety concept.

A safety function can be implemented using one or more safety-related component(s). Several safety functions can share one or more components. Control systems shall be designed to avoid hazardous situations. It must be possible to start machinery only by voluntary actuation of a control device provided for the purpose.

If a machine restart will pose a hazard, then restarting on switching on the supply voltage shall be excluded by technical means.

If a machine restart will not pose a hazard, then restarting without operator intervention (automatic restart) is permitted.

Subsystems of the safety-related part of a machine control system

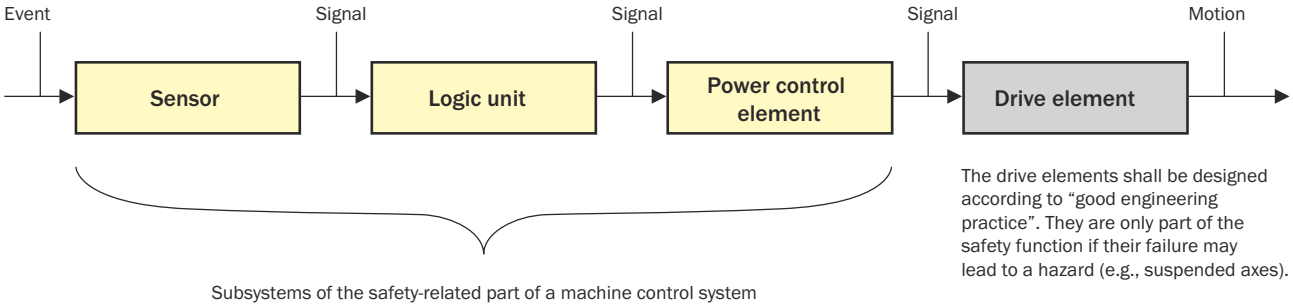


Figure 35: Subsystems of a machine controller

Decisive factors

The following features shall be considered when developing the safety concept:

- Features of the machine
- Features of the surroundings
- Human aspects
- Features of the design
- Features of protective devices (see "Technology, selection and use of protective devices", page 60)

Which protective devices are to be integrated and how they are to be integrated must be defined based on the above features.

Features of the machine

The following features of the machine shall be considered:

- Ability to stop the dangerous movement at any time (if not possible, use guards or impeding devices)
- Ability to stop the dangerous movement without additional hazards (if not possible, select different design/ protective device)
- Possibility of hazard due to ejected parts (if yes: use physical guards)
- Stopping times (knowledge of stopping times is necessary to ensure the protective device is effective)
- Possibility of monitoring stopping time/overrun (this is necessary if changes could occur due to aging/wear)

Features of the surroundings

The following features of the surroundings shall be considered:

- Electromagnetic disturbances, radiated interference
- Vibration, shock
- Ambient light, light interfering with sensors/welding sparks
- Reflective surfaces
- Contamination (mist, chips)

- Temperature range
- Moisture, weather

Human aspects

The following human aspects shall be considered:

- Expected qualification of the machine's operator
- Expected number of persons in the area
- Approach speed (K)
- Possibility of defeating the protective devices
- Reasonably foreseeable misuse

Features of the design

A safety function is performed by several subsystems. It is always advisable to implement safety functions with certified safety components. Certified safety components will simplify the design process and subsequent verification.

It is often not possible to implement a subsystem using only certified safety components that readily provide the level of safety (PL/SIL). In fact, the subsystem frequently has to be assembled from a number of discrete elements. In this case, the safety level depends on various safety-related aspects, see "Safety-related aspects of subsystems", page 56.

Safety-related aspects of subsystems

The safety level of a subsystem is dependent on various safety-related aspects, for example:

- Structure
- Reliability of the components/devices
- Diagnostics for detecting faults
- Resistance to common cause failures
- Process

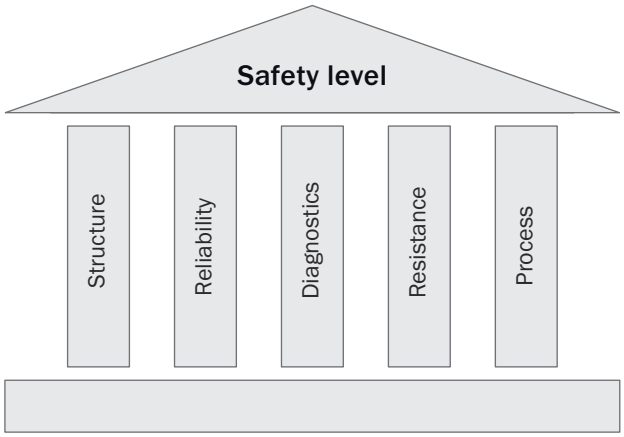
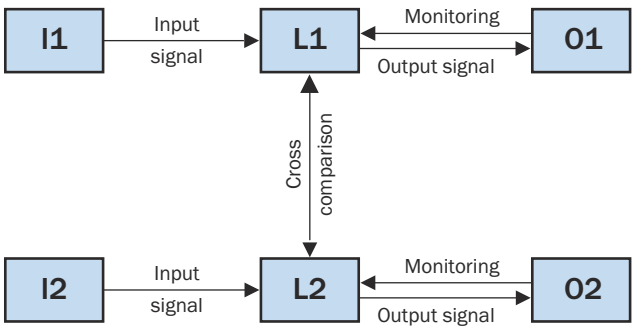


Figure 36: Aspects for determining the safety level of a subsystem

Structure

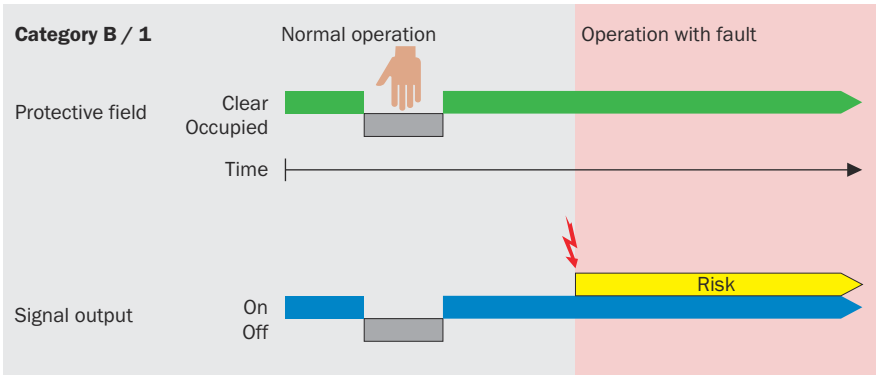
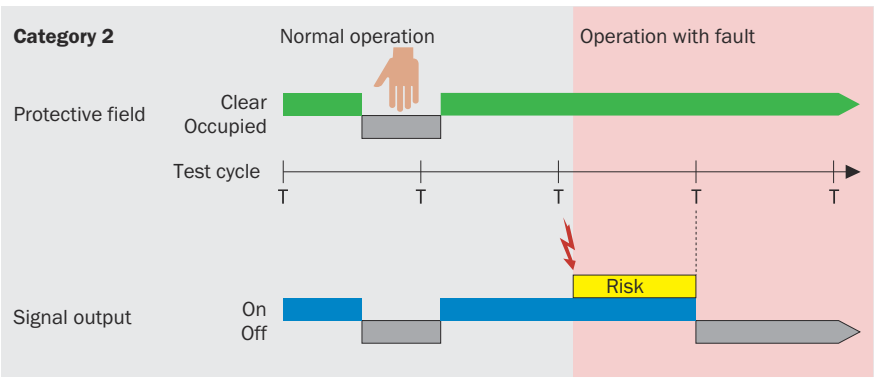
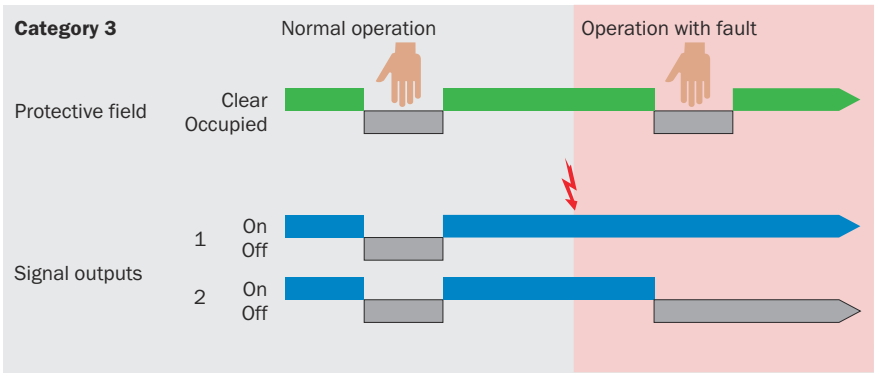
To reduce the susceptibility of a safety component to fault by means of a better structure, the safety-related functions can be executed in parallel on more than one channel. Dual-channel safety-related systems are common in the machine safety sector (see figure below). Each channel can perform the intended safety function. The two channels can be of diverse design (e.g., one channel uses electromechanical components, the other only electronics). Instead of a second equivalent channel, the second channel can also have a pure monitoring function.

Table 18: Structure of single-channel and dual-channel safety-related systems

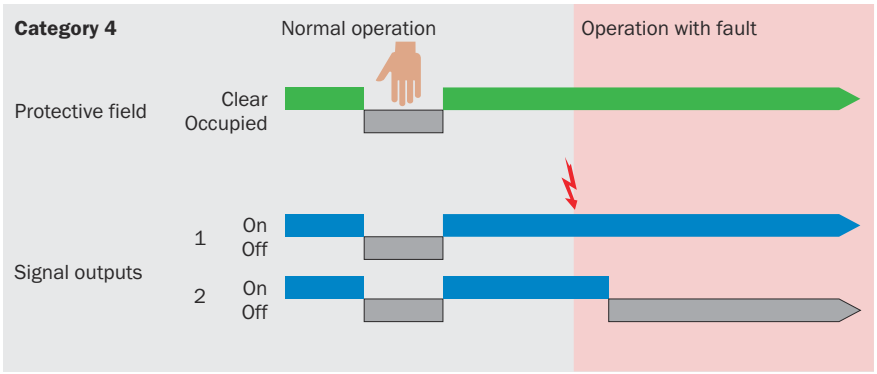
Single-channel safety-related systems	Dual-channel safety-related systems
	

The structure is described in the standard ISO 13849-1[1)] according to the categories described below.

Table 19: Categories according to ISO 13849-1 with description

	**Category B/Category 1** No fault detection. The occurrence of a fault will result in a risk. The risk can be minimized with reliable and proven components (Category 1).
	**Category 2** Faults are detected by carrying out a test. A risk prevails during the time between the occurrence of the fault and the next test. The test rate must be observed.
	**Category 3** In the event of a fault, the safety function is retained. The fault is detected either when the safety function is executed or when the next test is carried out. An accumulation of faults may lead to the loss of the safety function.

1) Note: A safety function is defined as a function whose failure can result in an immediate increase in risk.



Category 4
Despite a fault, the safety function is retained.
Contrary to Category 3, consequential faults following failure to detect the initial fault shall not result in a risk (loss of the safety function).

Reliability of the safety components/devices

The failure of safety-related components or devices may lead to disturbances in the machine process and to hazards. These components should therefore offer a high level of reliability. The higher the reliability, the lower the probability of a dangerous failure. The data for reliability describe the number of random failures during the service life of the components. These values are usually specified as:

- **B_{10} value** for electromechanical or pneumatic components. Here, service life is determined by switching frequency. The **B_{10} value** indicates the number of switching cycles until 10% of components fail.
- **Failure rate λ** (lambda value) for electronic components. The failure rate is often expressed in FITs (Failures In Time). One FIT is one failure per 10^9 hours.

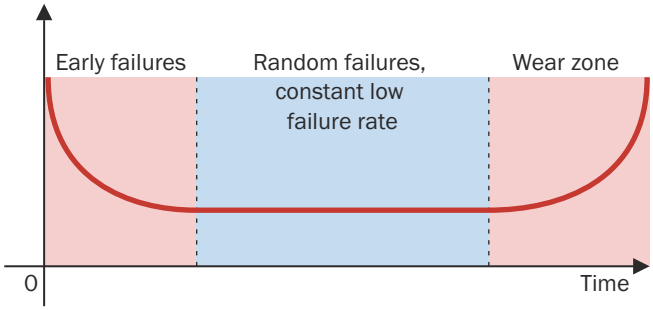


Figure 37: Failure rate λ (bathtub curve)

Diagnostics for detecting faults

Some faults can be detected by diagnostic measures. Diagnostic measures include plausibility monitoring, current and voltage monitoring, watchdog functionality, brief function test.

Since all faults cannot always be detected, the degree of fault detection must be defined. A Failure Mode and Effects Analysis (FMEA) should be performed for this purpose. For complex designs, measures and empirical values from standards provide assistance.

Resistance to common cause faults

The term common cause fault is used, for example, to refer to both channels failing simultaneously due to interference.

Appropriate measures must be taken to prevent this, e.g., isolated cable routing, suppressors, diversity of components.

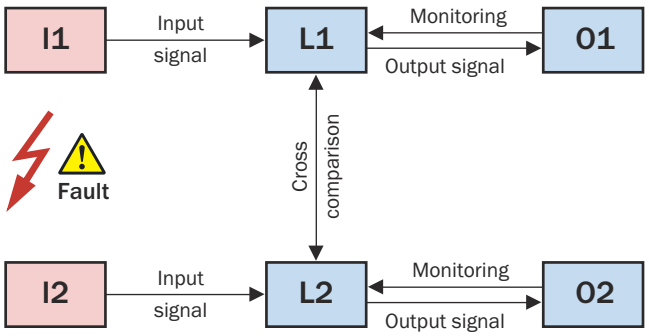


Figure 38: Structure of a dual-channel safety component with a fault

Process

The process brings the following influencing elements together:

- Organization and competence
- Design rules (e.g. specification templates, coding guidelines)
- Test concept and test criteria
- Documentation and configuration management

In the safety technology area, a process based on the V-model has proven particularly effective in practice for software (see figure).

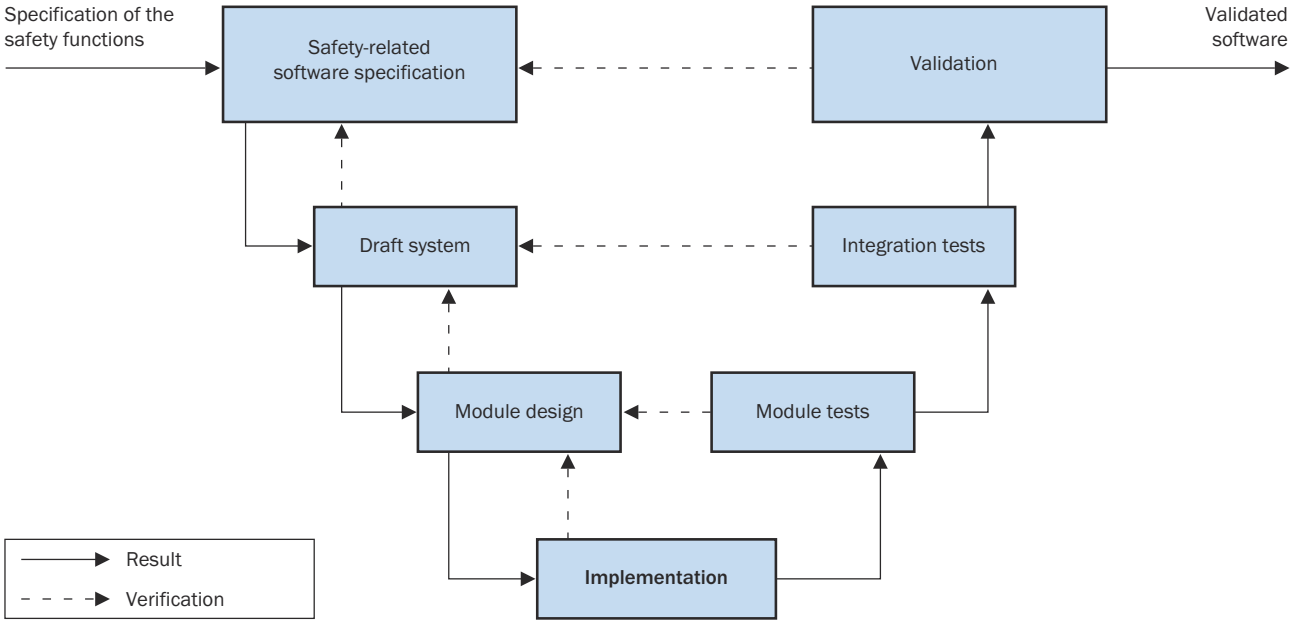
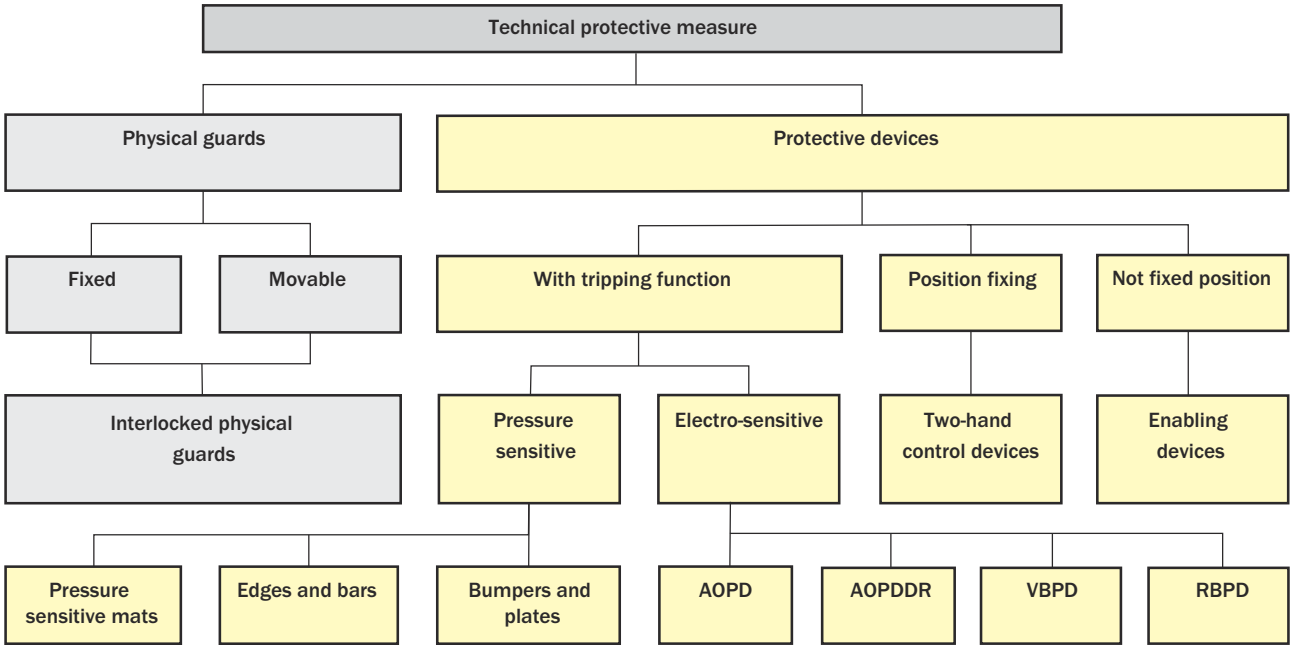


Figure 39: V-model with the development and testing concept for safety-relevant software

Technology, selection and use of protective devices



AOPD Active opto-electronic protective device, safety light curtains and safety light-beam sensors
AOPDDR Active opto-electronic protective device responsive to diffuse reflection, safety laser scanner
VBPD Vision based protective device, image-based protective devices
RBPD radar based protective devices, Radarbasierte Schutzeinrichtungen

Figure 40: Technology, selection and use of protective measures

Physical guards

Physical guards are mechanical protective devices that prevent hazardous points from being reached directly using parts of the body. They can be fixed or movable. Physical guards include, for example, covers, fences, barriers, flaps and protective doors. Covers and hoods prevent access from all sides. Fences are generally used to prevent full body access while barriers can only prevent unintentional or unconscious access to the hazardous points.

The safety function is essential for the design of guards. Must, for example, the physical guard only prevent access, and/or also retain parts and radiation?

Examples of ejected parts:

- Breaking/bursting tools (grinding wheels, drills)
- Emitted materials (dust, chips, slivers, particles)
- Blown out materials (hydraulic oil, compressed air, lubricant, materials)
- Parts ejected after the failure of a clamping or handling system

Examples of radiation sources:

- Thermal radiation from the process or the products (hot surfaces)
- Optical radiation from lasers, IR or UV sources
- Particle or ion radiation
- Strong electromagnetic fields, high frequency equipment
- High voltages from test systems or systems for discharging electrostatic charges (paper and plastic webs)

NOTE

The mechanical requirements for guards intended to contain radiation or ejected materials are generally higher than those for fixed guards intended to prevent access of persons.

Damage (breakage or deformation) to a physical guard is permitted in cases in which the risk assessment determines that no hazards will result.

General requirements on physical guards

- Protective devices (guards) shall be designed to be adequately robust and durable to ensure they withstand the environmental conditions to be expected during operation. The properties of guards shall be maintained during the entire period of use of the machines.
- They shall not cause any additional dangers.
- It shall not be possible to easily bypass the guards or render them ineffective.
- Guards shall not restrict observation of the working process more than necessary, insofar that observation is necessary.
- Guards shall be firmly held in place.
- They shall be fastened either by systems that can only be opened with tools, or they shall be interlocked with the dangerous movement.
- As far as possible, they should not remain in the protective position if unfastened.

NOTE

➜ Physical guards: ISO 14120

➜ Principles for safe machine design: ISO 12100 (type-A standard)

Mounting guards

Guards that are not removed or opened very often or are only removed or opened for maintenance work shall be fastened to the machine frame so that they can only be removed with tools (e.g., spanner, key). The process to remove them must be similar to a mounting operation and tools must be required.

Fastening elements on guards that are disassembled or removed regularly shall be designed so that they cannot be lost (e.g., captive screws).

Other types of fastening such as quick-release fasteners, screws with knobs, knurled screws, and wing nuts are only allowed if the guard is interlocked.

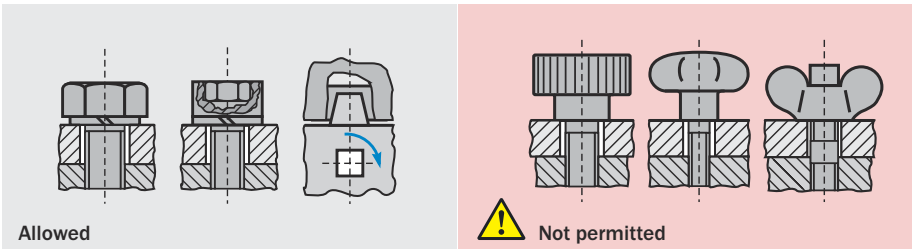


Figure 41: Example: Types of fastening for physical guards

Movable physical guards

Movable guards that need to be opened frequently or regularly without tools (e.g., for setup work) must be functionally linked to the dangerous machine function (interlocking, locking device). The term frequent opening is used, e.g., if the guard is opened at least once during a shift.

If hazards are to be expected when a guard is opened (e.g., very long stopping time), locking devices are required.

Ergonomic requirements to be met by movable physical guards

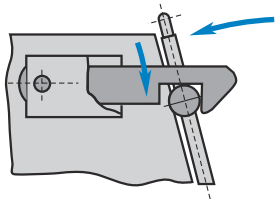
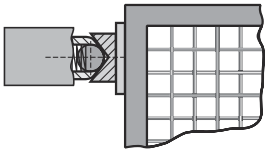
Ergonomic aspects are also significant during the design of protective devices. Guards will only be accepted by employees if they do not hinder setup, maintenance, and other similar activities any more than necessary. Movable physical guards must meet the following ergonomic criteria:

- Easy (e.g., one-handed) opening and closing, lifting, or moving
- Functional handle
- Opened guards should allow convenient access.

Mechanical locking of movable physical guards

As far as feasible, movable physical guards must be joined to the machine so that they can be securely held in the open position by hinges, guides, etc. Positive-fit mountings are preferred. Friction mountings (e.g., ball fasteners) are not recommended due to their diminishing effectiveness (wear).

Table 20: Example: Locking guards

	
Good	Possible

Interlocking physical guards

Physical guards must be interlocked if they have the following characteristics:

- Are actuated cyclically or opened regularly (doors, flaps)
- Can be removed without tools or easily (e.g., covers)
- Protect against a potentially serious hazard

Interlocking means that the opening of the guard is converted into an electrical signal that stops the dangerous movement. Physical guards are normally interlocked using position switches.

The interlocking of a physical guard should fulfill the following functions:

- The dangerous machine function cannot be initiated with the guard open (missing) (preventing start).
- The dangerous machine functions are stopped when the guard is opened (removed) (initiating a stop).

The following section describes the essential requirements on interlocking devices associated with physical guards according to ISO 14119.

There are four types of interlocking device:

Table 21: Types of interlocking devices according to ISO 14119

Designation	Actuation		Actuator		SICK product	
	Principle	Examples	Principle	Examples	Example	
Type 1	Mechanical	Physical contact, force, pressure	Not coded	Switching cam	i10P	
				Turning lever	i10R	
				Hinge	i10H	
Type 2			Coded	Shaped actuator (switching rod)	i16S	
				Key	–	
Type 3	Non-contact	Inductive	Not coded	Suitable ferromagnetic materials	IME2S	
		Magnetic		Magnets, electromagnets	MM12 [1]	
		Capacitive		All suitable materials	CM18 [1]	
		Ultrasound		All suitable materials	UM12 [1]	
		Optical		All suitable materials	WT 12 [1]	
Type 4		Magnetic	Coded	Coded magnet	RE1/2	
		RFID		Coded RFID transponder	STR1	
		Optical		Coded optical actuator	–	

1 These sensors are not designed for safety applications. If they are used in interlocking devices, the designer must give very careful consideration to systematic and common cause failures and take additional measures accordingly.

NOTE

Type 3 interlocking devices should only be used if the risk assessment shows that manipulation is not foreseeable or additional measures have been applied to prevent it.

Safety switches, position switches and interlocking devices

The commonly used term “safety switch” does not appear in the standards because the multitude of technologies and suitable sensor designs for interlocking devices does not allow general requirements to be defined.

Regardless of the technology used (mechanical, electrical, pneumatic, hydraulic), the following definitions apply:

- An interlocking device consists of an actuator and a position switch.
- A position switch consists of an actuator and an output signal element.

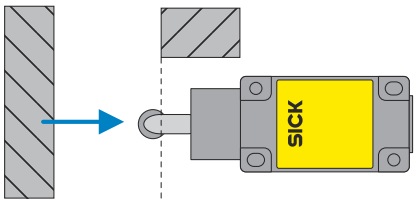
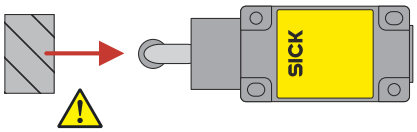
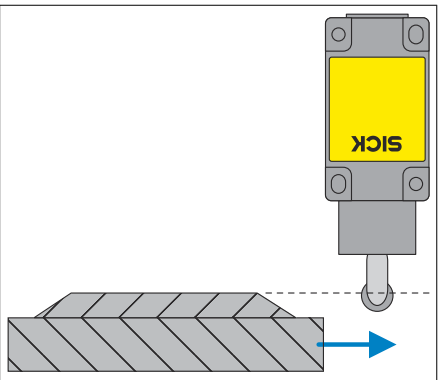
Depending on the technology of the position switch used and the functional safety requirements, either one or more interlocking devices will be required for a physical guard.

Mechanical attachment

Reliable mechanical attachment of the position switches and actuators is crucial for their effectiveness. The elements of interlocking devices

- shall be fitted such that they are protected against damage due to foreseeable external effects.
- shall not be used as a mechanical stop.
- shall be secured against unintentional operation and damage by means of their arrangement and design.
- shall be secured against unintentional changes in position by their arrangement, design and fastening. secured. If necessary, the switch and the actuating element must be secured by means of positive locking, e.g., with round holes, dowel pins, stops.
- shall be protected by their actuation method, or their integration in the control shall be such that they cannot be easily bypassed.
- shall be possible to check the switches for correct operation and, if possible, they shall be easily accessible for inspection.

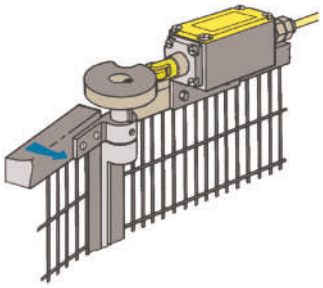
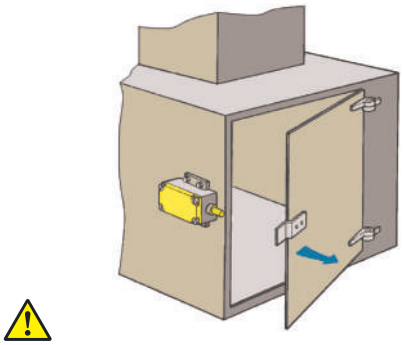
Table 22: Example: Mechanical attachment of position switches

		
Correct mounting: The position switch is protected by a mechanical stop.	**Incorrect mounting:** The position switch is used as a stop.	**Correct mounting:** The height of the cam has been matched to the position switch.

Positive mechanical actuation or interlocking arrangement

When using mechanical interlocking devices, reliable actuation is important. The use of positive mechanical actuation in an interlocking device ensures that the position switch is actuated when the guard is opened and reduces possibilities for manipulation. Positive mechanical actuation is the forced movement of the mechanical components of the interlocking device (safety switch) through direct contact with mechanical components or with the physical guard (e.g., protective door).

Table 23: Example: Positive mechanical actuation

	
Safe: Opening the protective door moves the mechanical plunger of the position switch (positive mechanical actuation). This opens the safety circuit.	**Faulty design:** The position switch may not always open the safety circuit, e.g., if the plunger is sticking due to incrustations or lubricating oil that has solidified.
Source: BG Feinmechanik und Elektrotechnik, BGI 575	

Positive opening

A contact element is positive-opening if the switching contacts are isolated immediately by a defined movement of the actuating element by non-elastic parts (e.g., springs). The use of positive opening normally closed contacts in position switches with positive mechanical actuation ensures that electrical circuit is still isolated even if the contacts are worn or other electrical faults have occurred.

The following requirements also apply where positive-opening mechanical position switches are concerned:

- The actuating travel shall be set to suit the positive-opening travel.
- The minimum plunger travel specified by the manufacturer shall be observed in order to provide the switching distance required for positive opening.

Figure 42: Symbol for positive opening normally closed contacts in accordance with IEC 60947-5-1, Annex K

NOTE

The use of both redundantly monitored electronic outputs from electro-sensitive position switches is considered equivalent to positive opening. If a type 3 or type 4 interlocking device is the only interlocking device on a physical guard, it must meet the requirements of IEC 60947-5-3.

Manipulation prevention

When designing interlocking devices, designers shall consider the possible motivation for manipulation of the protective device and foreseeable manipulation into account.

Measures to counter manipulation with simple means shall be applied.

Simple means include screws, needles, sections of sheet steel, coins, bent wire or the like.

Possible means of avoiding simple attempts to manipulate interlocking devices include:

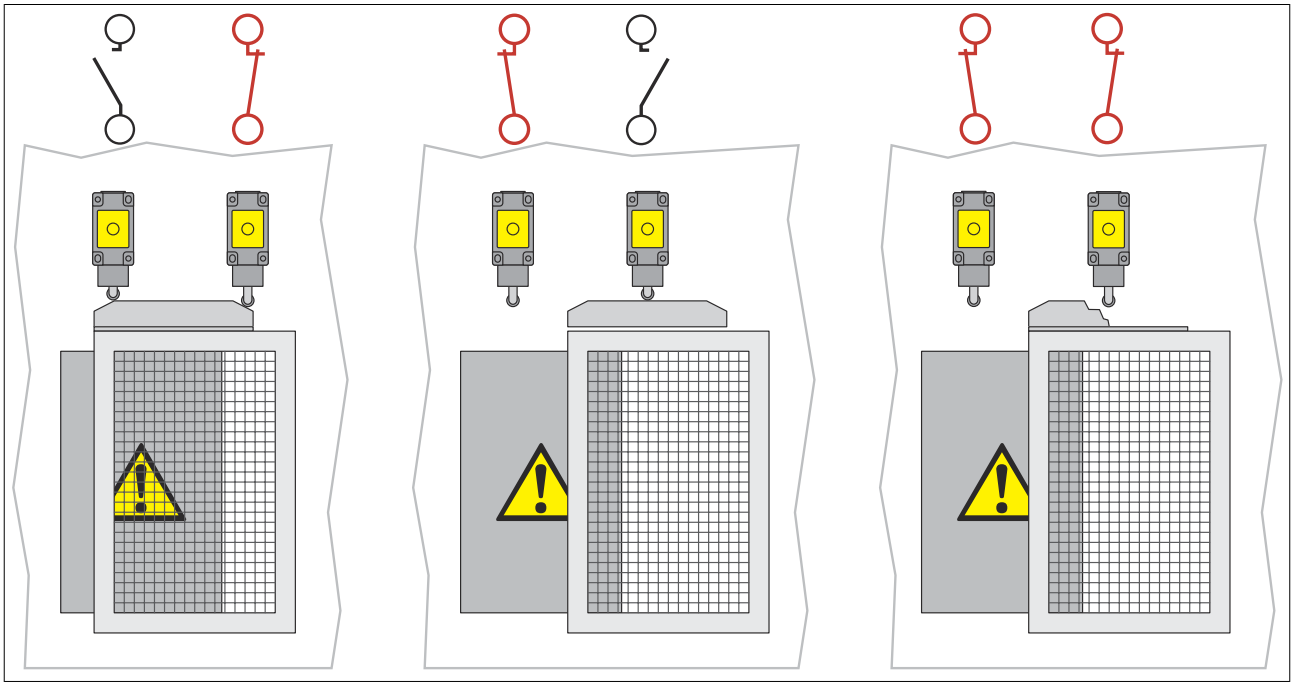
- Making interlocking devices difficult to access by using concealed assembly or assembly out of reach
- Using position switches with coded actuators
- Mounting the elements of the interlocking switches with “one-way” fasteners (e.g., safety screws, rivets)
- Manipulation monitoring in the control system (plausibility checks, testing)

Redundant design

The critical failure of an individual safety switch can be caused by manipulation, a mechanical error on the actuator or position switch (e.g., aging), or the effects of extreme ambient conditions (food industry example: stuck roller plunger due to contamination with flour). In particular at higher safety levels it is necessary to use an additional position switch, e.g., with the opposite function to that of the first position switch, and to have both switches monitored by the control system.

Example: An injection molding machine with cyclically actuated front protective doors. This application requires two mechanical switches.

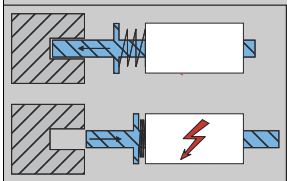
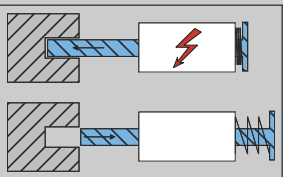
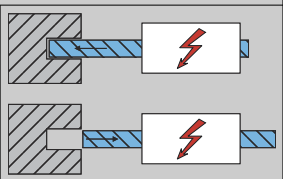
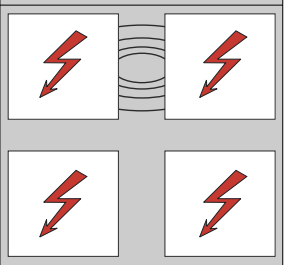
Table 24: Example: Detection of mechanical faults by means of a diverse redundant arrangement



Locking devices

Locking devices are devices that prevent guards from opening. They shall be applied if the stopping time of the dangerous machine state is longer than the time a person needs to reach the hazardous area (safety function "Temporarily preventing access", page 44). Locking devices shall prevent access to hazardous areas until the dangerous machine state has passed. Locking devices are also required if a process shall not be interrupted (process protection only, not a safety function). The figure below shows the possible designs of locking devices.

Table 25: Principles of operation of locking devices

Principle	Shape			Force
				
Functionality	Spring applied and power ON released	Power ON applied and spring released	Power ON applied and power ON released	Power ON applied and power ON released
Name	Mechanical locking device (preferred for safeguarding)	Electrical locking device (preferred for process protection)	Pneumatic/hydraulic locking device Bistable coil	Electromagnetic locking device

Releasing the locking device using power can be performed as follows:

- Time-control: In the case that a timer is used, the failure of this device shall not reduce the delay.
- Automatic: Only if there is no dangerous machine condition (e.g., due to standstill monitoring devices).
- Manual: The time between unlocking and the release of the protective device shall be greater than the time it takes for the dangerous machine function to stop.

Mechanical and electrical integration of locking devices

The same rules generally apply to locking devices as to interlocking devices. In relation to the principle of positive opening, attention is to be paid to which contacts should be positively opened. Guard signaling contacts indicate when the actuator has been withdrawn, that the guard is open. These contacts may be positive opening, but this is not always required.

Auxiliary and escape release, emergency release

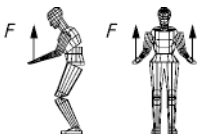
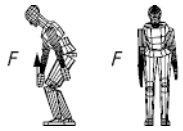
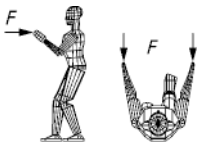
The risk assessment may show that in the case of a fault or in an emergency situation, measures are required for freeing personnel trapped in the hazardous area. A distinction must be made between concepts for auxiliary release (using a tool) and for emergency release or escape release (without a tool), as follows:

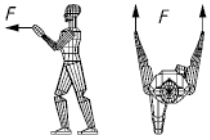
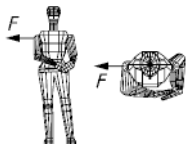
- Emergency release of a locking device
  Possibility of manually unlocking the locking device without tools from outside the protected area in case of emergency. A locking device with emergency release may be required, for example, to free trapped persons or to fight a fire.
- Auxiliary release of a locking device
  Possibility of manually unlocking the locking device using a tool or a key from outside the protected area in case of malfunction. A locking device with auxiliary release is not suitable for emergency release or escape release of the locking device.
- Escape release of a locking device
  Possibility of manually unlocking the locking device without the use of tools within the protected area in order to leave the area.

Locking force required

An essential criterion when selecting a locking device is the force required to hold the guard. Annex I of the ISO 14119 standard specifies the maximum force that can be applied to the most commonly used movable physical guards.

Table 26: Required locking force for physical guards according to Annex I of the ISO 14119 standard

Direction of force		Position	Application of force	Force [N]
	Horizontal pulling (dragging)	Sitting	Single handed	600
	Vertical upward	Standing, torso and legs bent, feet parallel	Bi-manual horizontal grips	1400
	Vertical upward	Standing, free	Single-handed horizontal grips	1200
	Horizontal, parallel to body symmetry plane backward pulling	Standing upright, feet parallel or in step posture	Bi-manual vertical grips	1100

Direction of force		Position	Application of force	Force [N]
	Horizontal, parallel to body symmetry plane forward pushing	Standing upright, feet parallel or in step posture	Bi-manual vertical grips	1300
	Horizontal, normal to body symmetry plane body off	Standing, torso bent sideward	Shoulder pushing on the metal plate side	1300
	Horizontal, normal to body symmetry plane	Standing, feet parallel	Single-handed vertical grip	700

Trapped key systems

One way of preventing unintentional starting is to use trapped key systems. Keys must be used to activate specific functions and operating modes, see table 27, page 68.

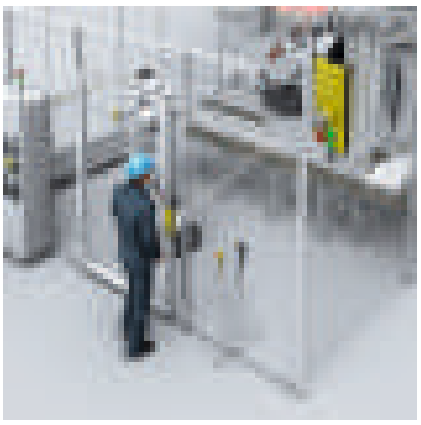
Figure ①: When a key is removed, a stop signal is generated and the dangerous state is stopped.

Figure ②: In the safe state (machine stopped), the safety locking device is unlocked and the door can be opened.

Figure ③: The service technician takes the key inside the plant. Inside, the inserted key enables the “setup mode” operating mode. Dangerous machine movements can now be made at reduced speed (turning the robot sideways) by means of an enabling switch. Automatic operation is disabled in this situation.

The key is then removed again, the service technician leaves the hazardous area, closes the door, and finally reinserts the key into the adapter. The door is locked and automatic operation is now possible again.

Table 27: Example: Trapped key system

		
①	②	③

Fault masking for series connection of interlocking devices with volt-free contacts

The ISO 14119 standard and the ISO TR 24119 technical report define, among other things, the requirements for the logical series connection of position switches. The risk of possible “fault masking” in the conventional series connection of the safety switches limits the achievable performance level and makes such series connection impermissible in some applications.

Fault masking can occur when switches with volt-free contacts are connected in series. Since the evaluation unit only evaluates the signals of the complete series, fault detection can be prevented. The fault, e.g. a short-circuit or cross-circuit, is either not detected at all or reset (masked) after detection as a result of the actuation of another

protective device with a fault-free switch. This means that operation of dangerous machine functions is possible despite the presence of an isolated fault. The accumulation of masked faults may then lead to the loss of the safety function.

Example for the development of fault masking

If it is assumed that, during foreseeable troubleshooting, one of the movable physical guards (e.g. protective door, maintenance flap) is operated by the machine operator and the fault is masked thereby, the corresponding reduction in the diagnostic coverage DC (fault recognition rate) has to be taken into account. This may lead to the performance level being reduced to PL d or PL c.

NOTE
For more information, see the special information "Safe series connection" from SICK.

Electro-sensitive protective equipment (ESPE)

With electro-sensitive protective equipment (ESPE), in contrast to "guards", protection is not based on the physical separation of persons at risk from the hazard itself. Protection is achieved through temporal separation. As long as there is somebody in a defined area, no dangerous machine functions are initiated, and such functions are stopped if already underway. A certain amount of time, referred to as the "stopping/run-down time", is required to stop these functions.

The ESPE must detect the approach of a person to the hazardous area in a timely manner and depending on the application, the presence of the person in the hazardous area.

The international standard IEC 61496-1 defines safety-related requirements for ESPE independent of their technology or principle of operation.

What are the benefits of electro-sensitive protective equipment?

If an operator frequently or regularly has to access a machine and is therefore exposed to a hazard, the use of an ESPE instead of (mechanical) physical guards (covers, safety fencing, etc.) is advantageous thanks to:

- Reduced access time (operator does not have to wait for the guard to open)
- Increased productivity (time savings when loading the machine)
- Improved workplace ergonomics (operator does not have to operate a physical guard)

In addition, operators and others alike are protected.

Against what hazards does electro-sensitive protective equipment not protect?

Since an electro-sensitive protective equipment does not represent a physical barrier, it is not able to protect persons against emissions such as ejected machine parts, workpieces or chips, ionizing radiation, heat (thermal radiation), noise, sprayed coolant and lubricant, etc. Similarly, ESPE cannot be used on machines on which long stopping/run-down times require minimum distances that cannot be achieved.

In such cases, physical guards must be used.

ESPE technologies

Electro-sensitive protective equipment can implement detection of persons through various principles: optical, capacitive, ultrasound, microwaves (radar) and passive infrared detection.

In practice, optical protective devices have been proven over many years and in large numbers (see figure 43, page 70).

Opto-electronic protective devices

The most common electro-sensitive protective devices are optoelectronic devices such as:

- Safety light curtains and safety light-beam sensors (AOPD: active optoelectronic protective devices)
- Safety laser scanners (AOPDDR: active optoelectronic protective devices responsive to diffuse reflection)
- Camera-based protective devices (VBPD: vision based protective devices)

Figure 43: Examples of optoelectronic protective devices

NOTE
An optoelectronic protective device can be used if the operator is not exposed to any danger of injury due to ejected parts (e.g., splashes of molten material).

Safety light curtains and safety light-beam sensors (AOPD)

AOPDs are protective devices that use optoelectronic transmission and reception elements to detect persons in a defined two-dimensional area. A series of parallel light beams (normally infrared) transmitted from the sender to the receiver form a protective field that safeguards the hazardous area. Detection occurs when an opaque object fully interrupts one or more beams. The receiver signals the beam interruption by a signal change (OFF state) to its output signal switching devices (OSSDs).

These signals from the OSSDs are used to stop the dangerous machine functions.

The international standard IEC 61496-2 defines safety requirements for AOPDs.

Typical AOPDs include safety single-beam sensors, safety multibeam sensors, and safety light curtains. AOPDs with a detection capability of more than 40 mm are called safety multibeam sensors. They are used to protect access to hazardous areas (see figure 44, page 70).

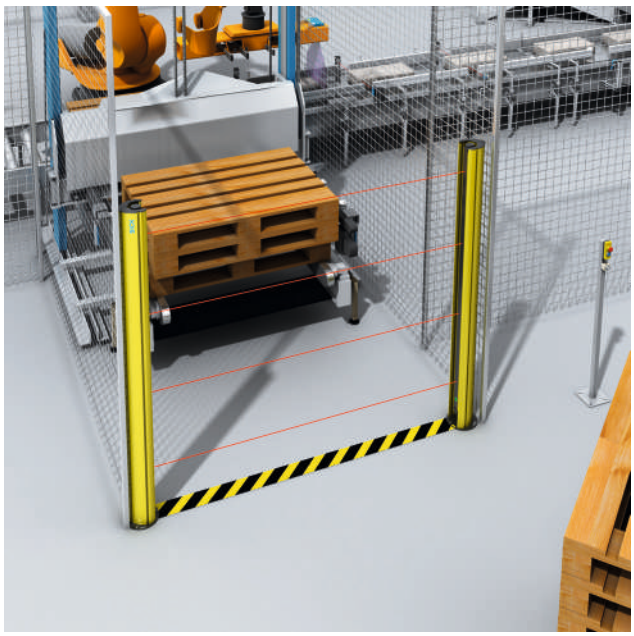


Figure 44: Access protection using a safety multibeam sensor

AOPDs with a detection capability of 40 mm or less are called safety light curtains and are used to safeguard hazardous points directly (see figure 45).

With both safety multibeam sensors and safety light curtains, rather than all light beams being activated at the same time, they are usually activated and deactivated in rapid sequence one after the other. This increases resistance to interference from other sources of light and increases their reliability accordingly. On state-of-the-art AOPDs, there is automatic synchronization between sender and receiver through an opti-

cal link. By using microprocessors, the beams can be evaluated individually. This enables additional ESPE functions to be implemented in addition to the protective function itself ("Additional functions of ESPE", page 81).

Figure 45: Hazardous point protection using a safety light curtain

Safety laser scanners (AOPDDR)

AOPDDRs are protective devices that use optoelectronic sender and receiver elements to detect the reflection of optical radiation generated by the protective device. This reflection is generated by an object in a predefined two-dimensional area.

Detection is signaled by a signal change (OFF state) to its output signal switching devices (OSSDs). These signals from the OSSDs are used to stop the dangerous machine functions.

A safety laser scanner is an optical sensor which monitors a hazardous area on a machine or vehicle by scanning the area around it on a single plane with infrared light beams.

The safety laser scanner operates on the principle of optical time-of-flight measurement. The scanner sends very short light pulses (S) while an “electronic stopwatch” runs simultaneously. If the light strikes an object, it is reflected and received by the scanner (R). The scanner calculates the distance from the object from the difference between the send and receive times.

A uniformly rotating mirror (M) in the scanner deflects the light pulses such that a sector of a circle is covered. The scanner then determines the exact position of the object from the measured distance and the angle of rotation of the mirror.

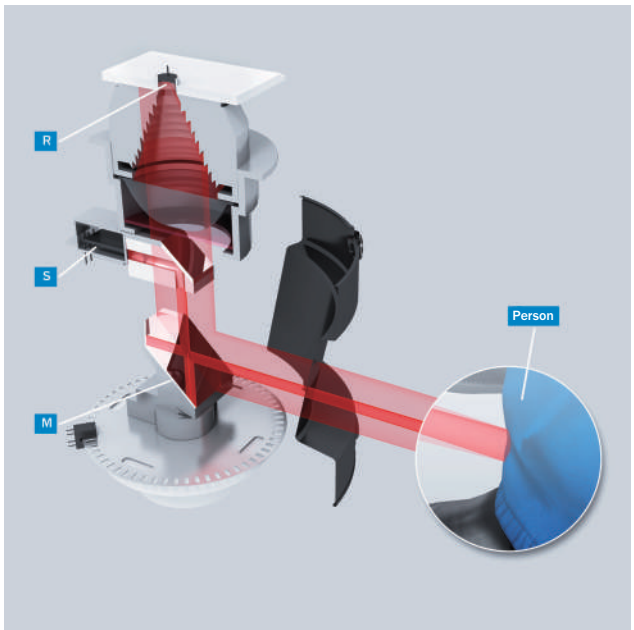


Figure 46: Basic structure of a laser scanner

The area in which object detection leads to triggering (protective field) can be configured by the user via a graphical user interface. Modern scanners support simultaneous and separate monitoring of multiple areas by evaluating fields simultaneously and by communicating with the controller through multiple safe cut-off paths. This feature can be used, for example, to adapt the monitored area to the speed of a vehicle.

Safety laser scanners use individually emitted pulses of light in precise directions and do not continuously cover the area to be monitored. Resolutions (detection capabilities) up to 20 mm are achieved through this operating principle. With the active scanning principle, safety laser scanners do not need external receivers or reflectors. Safety laser scanners also have to be able to reliably detect objects with extremely low reflectivity (e.g., black work clothing). The international standard IEC 61496-3 states the safety requirements for AOPDDRs.

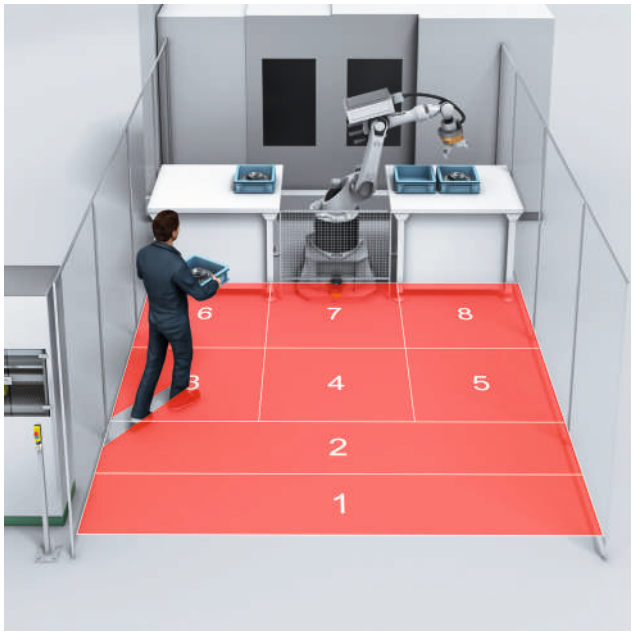


Figure 47: Simultaneous monitoring of multiple protective fields

Camera-based protective devices (VBPD)

VBPDs are camera-based protective devices and use image capturing and processing technologies for safety detection of persons (see figure 48).

Various principles can be used to detect persons, including:

- Interruption of the light retro-reflected by a retro-reflector
- Travel time measurement of the light reflected by an object
- Monitoring of changes from background patterns
- Detection of persons based on human characteristics

The various technical specifications (TS) and technical reports (TR) of the IEC 61496-4 series of standards contain the requirements and characteristics of VBPDs.

Figure 48: Protecting people when leaning into the hazardous area of a collaborative robot using a 3D vision-based camera system

Detection capability (resolution) of optoelectronic protective devices

The detection capability is defined as the limit for the sensor parameter that causes the electro-sensitive protective equipment (ESPE) to trigger.

In practice, this is about the size of the smallest object detected by the ESPE within the defined monitored area (protective field).

The detection capability is specified by the manufacturer. In general, the detection capability is determined from the sum of the beam separation and effective beam diameter. This ensures that an object of this size always covers a light beam and is always detected regardless of its position in the protective field.

For safety laser scanners (AOPDDR), the detection capability is dependent of the distance to the object, the angle between the individual beams of light (pulse), and the shape and size of the transmitted beam.

The reliability of the detection capability is determined by the type classification in the IEC 61496 series of standards (see table 28, page 75).

Preventing reflections from AOPDs

For AOPDs, the light beam is focused from the sender. The aperture angle of the lens is reduced as far as possible so that disturbance-free operation can even be ensured in the event of minor alignment errors. The same applies to the aperture angle of the receiver (effective aperture angle according to IEC 61496-2). But even for smaller aperture angles, there is the possibility for light beams from the sender to be deflected from reflective surfaces, thus leading to a failure to detect an object (see figure 49, see figure 50).

Therefore, all reflective surfaces and objects (e.g. material containers, reflective floors) have to maintain a minimum distance **a** from the protective field of the system (see table 28, page 75).

This minimum distance **a** depends on the distance **D** between the sender and receiver (protective field width). The minimum distance must be maintained on all sides of the protective field.

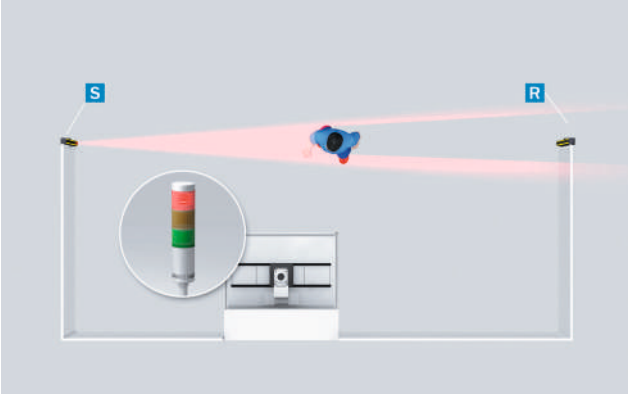


Figure 49: The person is detected reliably and the dangerous movement is stopped.

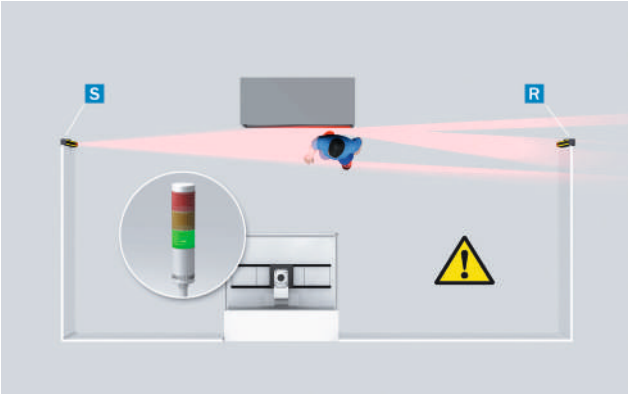


Figure 50: Reflection hinders detection by the ESPE and the dangerous movement is not stopped.

Preventing mutual interference from AOPDs

If several AOPDs are operated in close proximity to each other, the sender beams from a system (S1) can affect the receiver of another system (R2). There is a danger that the affected AOPD will lose its ability to provide protection (see figure 51).

Assembly situations of this kind must be avoided. If this is not possible, suitable measures must be taken to prevent mutual interference (assembly of opaque partitions or reversing the direction of transmission of a system, for example).

Type 4 AOPDs either have to have suitable external sender detection and change to a safe state (outputs in OFF state) when affected or have technical means to prevent interference. Beam coding is normally used so that the receiver only responds to light beams from the assigned (identically coded) sender (see figure 52).

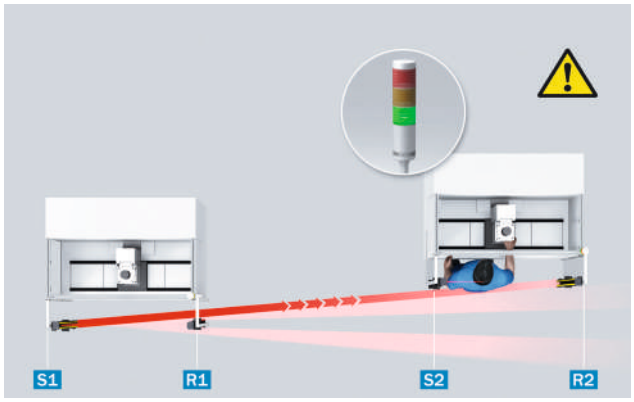


Figure 51: Mutual interference impedes detection by the ESPE (S2-R2) and the dangerous movement is not stopped.

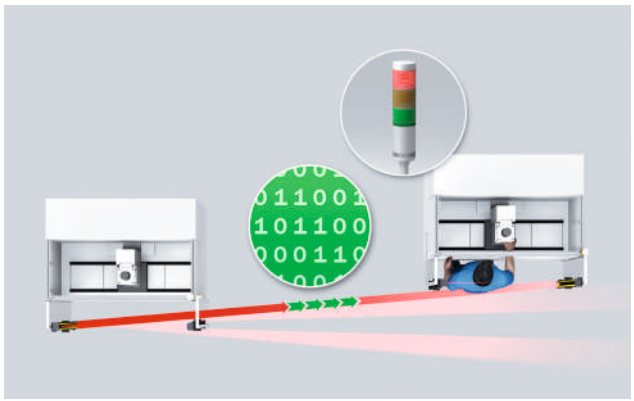


Figure 52: No mutual interference of protective devices due to the use of light beam coding – person is reliably detected and the hazardous movement is stopped.

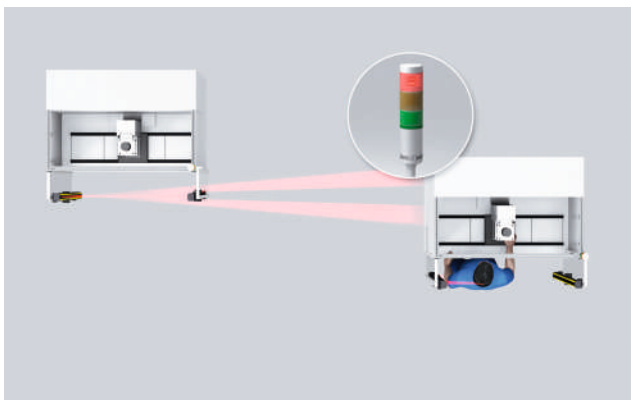


Figure 53: No mutual interference of protective devices due to suitable arrangement of the machine or ESPE systems

Selection of a suitable ESPE

Criteria can include:

- Specifications from harmonized standards, in particular type-C standards
- The space available in front of the hazardous area
- Ergonomic criteria, e.g., machine loading and unloading cycles

- Resolution
- Response time
- Ambient conditions

What safety function is the ESPE expected to perform?

- Initiating a stop ("Initiating a stop", page 45)
- Avoiding unexpected start-up ("Avoiding an unexpected start-up", page 45)
- Preventing start ("Preventing start", page 46)
- Combination of initiating a stop/preventing start (see "Combination of initiating a stop/preventing start", page 46)
- Allowing material passage ("Allowing material passage", page 47)
- Monitoring machine parameters ("Monitoring machine parameters", page 47)
- Safety-related indications and alarms (see "Safety-related indications and alarms", page 50)
- Other functions, e.g., PSDI mode, blanking, protective field switching, etc. (see "Additional functions of ESPE", page 81)

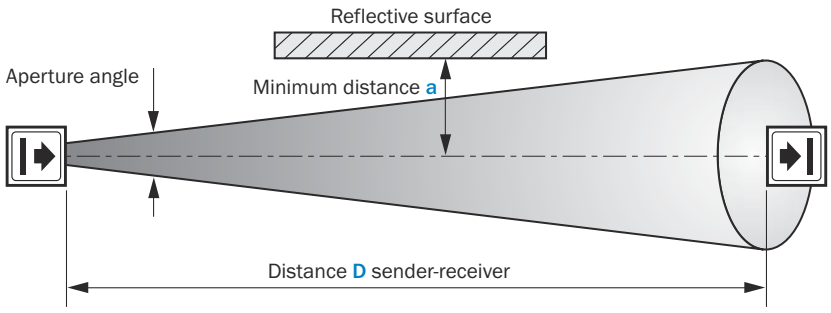
NOTE
➜ Requirements on ESPE: IEC 61496 series of standards

Safety level

For ESPE, the safety-related parameters have been implemented in a type classification (Type 2, Type 3, Type 4).

Type 3 is defined for AOPDDR. Types 2 and 4 are defined for AOPD.

Table 28: Main differences between type 2 and type 4 AOPDs according to IEC 61496-2

	Type 2	Type 4
Functional safety	The protective function may be lost if a fault occurs between test intervals	The protective function is maintained even if multiple faults occur
EMC (electromagnetic compatibility)	Basic requirements	Increased requirements
Maximum aperture angle of the lens	10°	5°
Minimum distance a to reflective surfaces, for distance D ≤ 3 m	262 mm	131 mm
		
Minimum distance a to reflective surfaces, for distance D > 3 m	= distance x tan (10°/2)	= distance x tan (5°/2)
Several senders of the same type of construction in one system	No special requirements (beam coding is recommended)	No effect or OSSDs shut down if they are affected

In addition to structural aspects (categories according to ISO 13849-1), the type classification also defines the requirements that shall be met with regard to electromagnetic compatibility (EMC), environmental conditions, and the optical properties. These include in particular their behavior in the presence of interferences (sun, lamps, similar types of device, etc.) but also the opening angle of optics in safety light curtains or safety light-beam sensors (the requirements to be met by a type 4 AOPD are more stringent than those for a type 2 AOPD).

NOTE
The aperture angle is decisive in determining the minimum distance in relation to reflective surfaces (see table 28).

Achievable reliability of safety functions with optoelectronic protective devices

Table 29: Comparison of the safety levels of ISO 13849-1 and IEC 62061

		ISO 13849-1					Example devices
		a	b	c	d	e	
ESPE type acc. to EN 61496-1	2						Safety light curtains, safety single-beam sensors, safety multibeam sensors
	3						Safety laser scanners, safe camera sensors
	4						Safety light curtains, safety single-beam sensors, safety multibeam sensors
			1		2	3	
			SIL (IEC 62061)				

NOTE
Always follow the additional application notes, information, and instructions in the instruction handbook for the optoelectronic protective devices!

Types of protection and required detection capability of the ESPE

This section describes the types of protection and which parts of the body should be detected by the ESPE.

Hazardous point protection with finger or hand detection

Hazardous point protection is used to detect when a person comes very close to the hazardous point. This allows the smallest minimum distance to be implemented. This may be necessary for ergonomic operation of the machine, e.g., for insertion work on a press, or to keep the space requirement of the machine low. Fingers/hands must therefore be detected, which requires ESPE with a detection capability up to 40 mm (ISO 13855). If a person can pass the detection zone of the protective device, prevention of unexpected start-up is necessary, e.g., by means of a reset function of the ESPE.

Figure 54: Hazardous point protection on an automatic assembly machine with safety light curtain

Access protection: detection of a person when accessing a hazardous area

Access protection is used to detect when a person enters the **hazardous area**. Detection of the largest body part (torso) is sufficient for this purpose. Access protection is particularly suitable for protecting large areas and **areas with large access points**. A person who has passed the detection zone of the protective device is no longer detected. Access protection therefore always requires prevention of unexpected start-up.

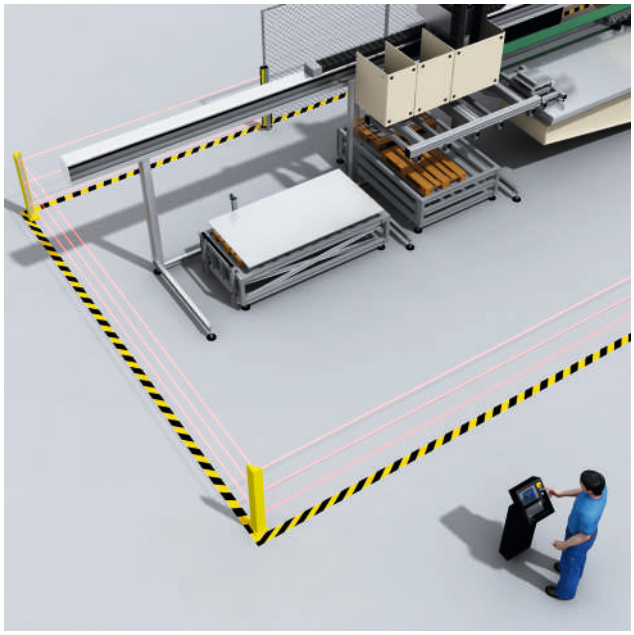


Figure 55: Access protection of a machine using safety multibeam sensors and deflector mirrors

Hazardous area protection: detection of the presence of a person in the hazardous area

Hazardous area protection is used to detect when a person approaches or is present **in the hazardous area**. This requires detection of the lower **limbs** or torso. Hazardous area protection is particularly suitable for machines where, for example, the **hazardous area** cannot be fully seen from the position of the reset pushbutton. Hazardous area protection does not require a reset function if the detection zone cannot be exited in the direction of the hazardous point. When entering the **hazardous area**, the dangerous state of the machine is stopped and starting is prevented.

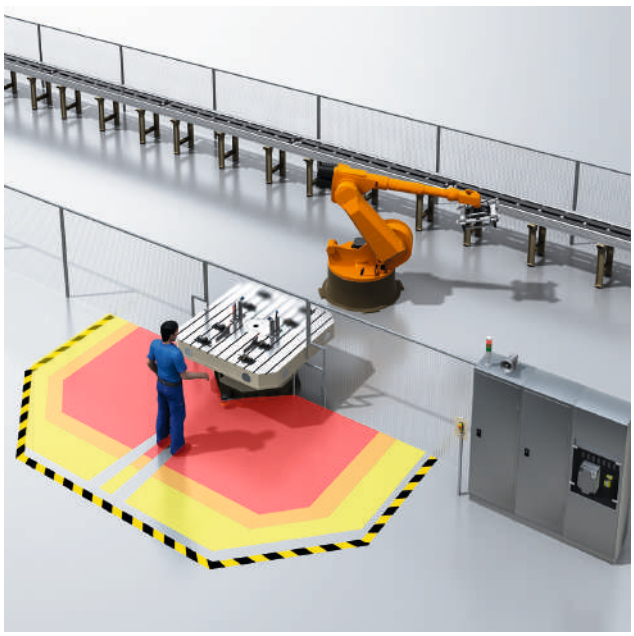


Figure 56: Hazardous area protection of a rotating table using a safety laser scanner

Mobile hazardous area protection: detection of a person approaching the hazardous area

Mobile hazardous area protection is used to detect when a person **approaches** or is present in the **hazardous area** of a moving hazardous point. This requires the detection of the lower limbs. The application may require that people lying down are detected.

Mobile hazardous area protection is particularly suitable for autonomous vehicles (e.g., cranes and forklifts).

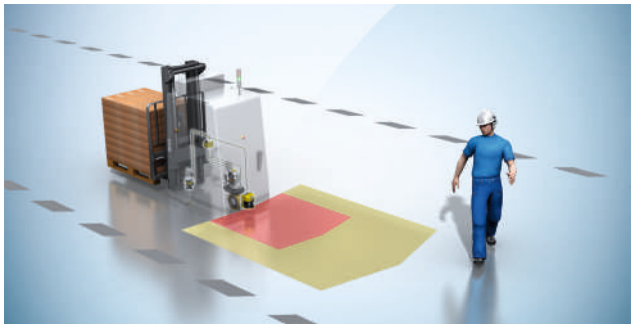


Figure 57: Mobile hazardous area protection of an autonomous forklift truck using a safety laser scanner

Automatic material passage using ESPE

The following safety functions can be integrated either in the logic unit or directly in suitable ESPE.

Automatic protective field switching

When large openings of machines are secured using ESPE, changing the shape of the active protective field can allow the passage of materials or packages with different contours. This prevents persons accessing the hazardous zone above or behind these materials. Some types of ESPE (AOPD) allow preprogrammed protective fields to be activated by external signals. Instead of muting the entire protective device ("Muting", page 79), a suitable (vertical) protective field of the ESPE can be activated during passage.

In addition, field switching may also be required if the hazardous zones of machines change dynamically during machine operation, e.g., adapted exclusion zones for industrial robots with different operating cycles or for transfer trolleys when docking at a station.

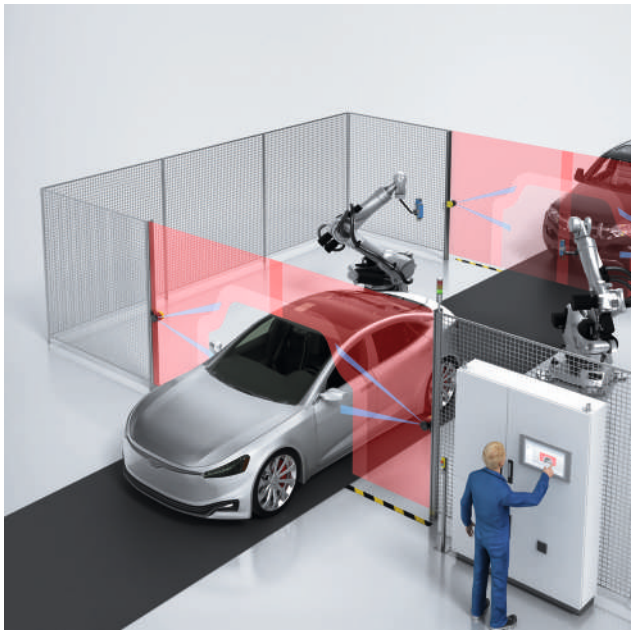


Figure 58: Application example for the passage of materials with a different contour and corresponding automatically adjusted protective fields of safety laser scanners

Muting

The muting function is used to temporarily deactivate the protective function of a protective device. This is necessary when material must be moved through the protective field of the protective device without stopping the work routine (hazardous state of the machine).

It can also be used effectively to optimize the work routine if allowed by certain machine states (e.g., muting the function of a safety light curtain during the non-hazardous upwards movement of a press die, making it easier for the operator to remove workpieces).

Muting shall only be possible if the access to the hazardous point is blocked by the passing material. If it is not possible to stand behind (or pass through) detection areas, muting shall only be possible if the machine functions still taking place are not dangerous (e.g., non-dangerous upward stroke of a press). This status is determined by muting sensors or signals.

For the muting function, great care is necessary when selecting and positioning the muting sensors and controller signals used.

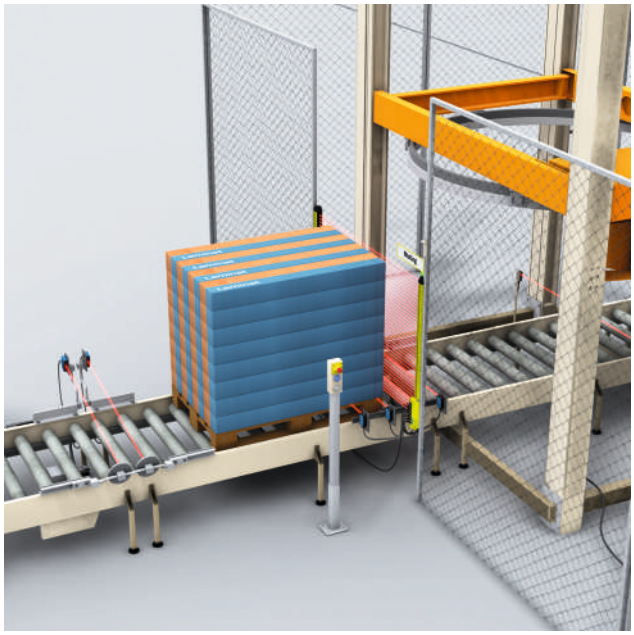


Figure 59: Muting function with safety light curtain and muting sensors on a wrapping machine

The following conditions shall be met to implement a safe, standardized muting function:

- During muting, a safe state must be ensured by other means, therefore it shall not be possible to access the hazardous area.
- Muting shall be automatic, i.e., not manual.
- Muting shall not be dependent on a single electrical signal.
- Muting shall not be entirely dependent on software signals.
- An invalid combination or sequence of muting signals shall not allow any muting state, and it shall be ensured that the protective function is retained.
- The muting status shall end immediately after the material has passed through.

To improve the quality of differentiation, additional limits, interlockings, or signals can be used including:

- Direction of movement of the material (sequence of the muting signals)
- Limiting the muting time
- Material request by the machine control
- Operational status of the material handling elements (e.g., conveyor belt, roller conveyor)
- Material identification by additional properties (e.g., bar code)

NOTE

➜ Practical application of ESPE: IEC 62046

Safety light curtains with entry/exit function

Active differentiation between person and machine (entry/exit function) provides other way of moving material into a safeguarded area.

Horizontally arranged safety light curtains (AOPDs) are used for this application. Each of their light beams can be evaluated to distinguish the interruption pattern of the material or material carrier (e.g., pallet) from that of a person.

By using self-teaching dynamic blanking, as well as other differentiation criteria such as direction of movement, speed, entry and exit in the protective field, etc., a safety-relevant distinction can be made. In this way, undetected entry into the hazardous area by anyone can be reliably prevented (see figure 60).

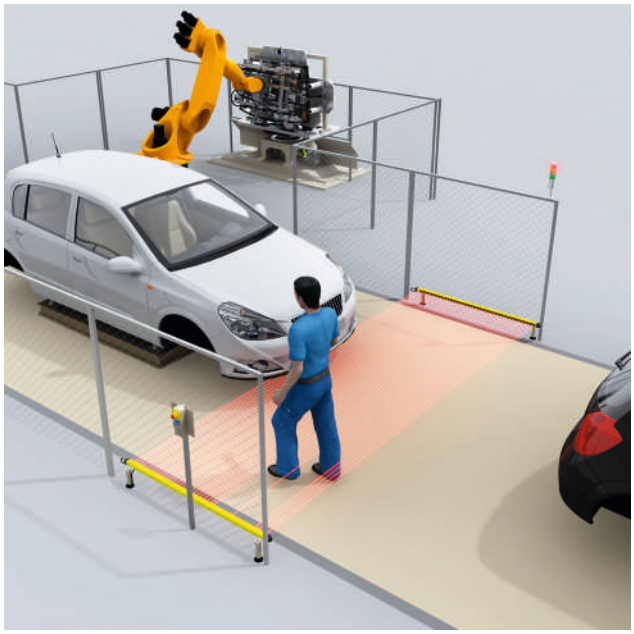


Figure 60: Entry/exit function with horizontally installed safety light curtain in a processing station on an automobile assembly line

Safety laser scanner with protective field switching

Another way of moving material into a protected area is to actively switch protective fields. As an alternative to active protective field switching, it is possible to separately evaluate simultaneous protective fields.

Safety laser scanners with vertical (or slightly tilted) protective fields are generally used for this application.

The appropriate protective field, from a series of preprogrammed protective fields, is activated by corresponding signals from the machine controller and adequately positioned sensors. The contour of the protective field is designed such that passage of the material does not cause the protective device to activate, but unmonitored areas are small enough to prevent undetected entry into the hazardous area by anyone (see figure 61).

Alternatively, protective field switching can be performed independently by the protective device without the need for external sensors or signals (e.g., the Safe Portal system solution from SICK, see figure 58, page 78).

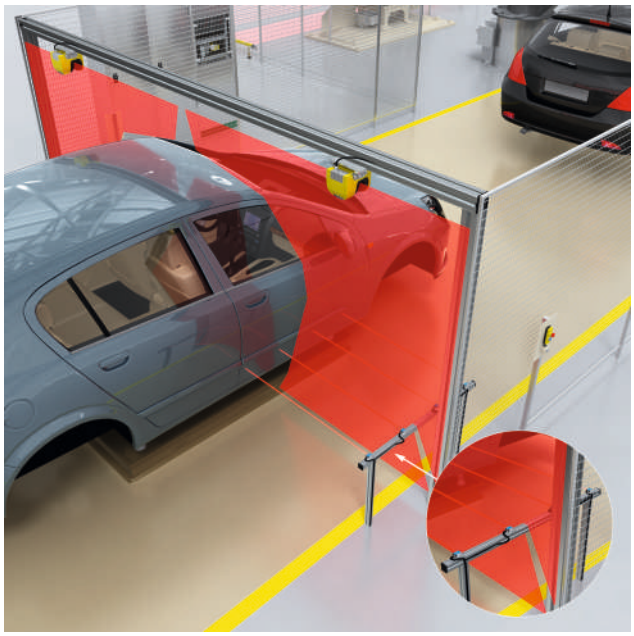


Figure 61: Access protection allowing material passage using safety laser scanners, vertical protective fields, and protective field switching with suitably arranged sensors

Additional functions of ESPE

Blanking

For many AOPDs, configuration of the detection capability and/or protective field can be designed such that the presence of one or more objects within a defined section of the protective field does not trigger the safety function (OFF state). Blanking can be used to allow specific objects through the protective field, e.g., hose for cooling lubricant, slide/carrier for workpieces (see figure 62).

For **fixed blanking**, the blanked area is precisely defined in terms of its size and position. For **floating blanking**, only the size of the blanked area is defined, not its position in the protective field (see table 30).

To prevent gaps in the protective field, the presence (or in some cases, a change in the size or position) of an object can trigger the safety function (OFF state).

If the blanked area is not completely covered by the blanked objects, a gap(s) is created in the protective field. This/these must be closed by additional coverage (see figure 62). Alternatively, the detection capability resulting from the gap must be taken into account in the minimum distance calculation.

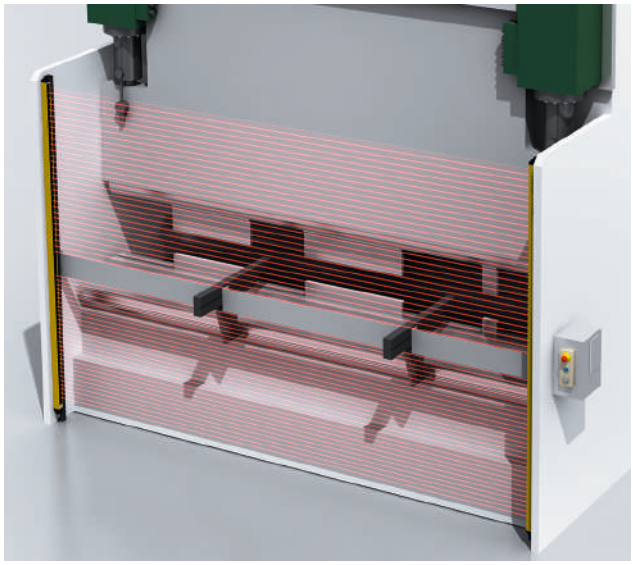
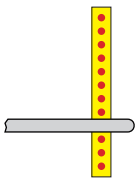
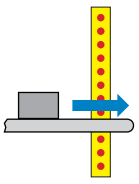
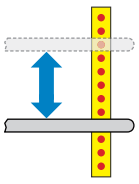
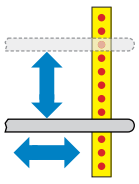


Figure 62: Fixed blanking of light curtain beams on a trimming press

NOTE

In the blanked area, the resolution capability of ESPE is enlarged (deteriorates). Take the corresponding manufacturer's specifications into account when calculating the minimum distance.

Table 30: Criteria for fixed and floating blanking

Fixed blanking		Floating blanking	
Fixed blanking	**Fixed blanking with increased size tolerance**	**Floating blanking with complete object monitoring**	**Floating blanking with partial object monitoring**
An object of fixed size must be at a specific point in the protective field.	From the operator side, an object of limited size is allowed to move through the protective field.	An object of fixed size must be within a specific area of the protective field. The object is allowed to move.	An object of fixed size is allowed in a specific area in the protective field. The object is allowed to move.
			

To prevent gaps in the protective field, the presence (or in some cases, a change in the size or position) of an object can trigger the safety function (OFF state).

Control of a work operation using a protective device - PSDI mode

Using the protective device to trigger the machine function (controlling protective device) is described as PSDI mode (PSDI – Presence Sensing Device Initiation). This operating mode is advantageous if parts must be manually loaded and unloaded cyclically.

Conforming to the standards, PSDI mode can only be executed with type 4 AOPDs and an effective resolution d ≤ 30 mm. In PSDI mode, the machine waits at a defined position for a specified number of interruptions by the operator. The safety light curtain releases the dangerous movement again automatically after a specific number of interruptions.

The ESPE has to be reset under the following conditions:

- When the machine starts
- On restart when the AOPD is interrupted within a dangerous movement
- If no PSDI was triggered within the specified PSDI time

It must be checked that no danger to the operator can arise during the work process. This limits the use of this operating mode on machines in which there is no possibility for whole body access and it is not possible for the operator to remain undetected between the protective field and the machine (presence detection).

Single break PSDI mode means that the AOPD initiates the machine function after the operator has completed one intervention.

Double break PSDI mode means that the AOPD holds the machine function in the locked state after the operator's first intervention (e.g., removal of a machined workpiece). Only after the operator has completed the second intervention (e.g., feeding in of a blank) does the safety light curtain release the machine function again.

PSDI mode is often used on presses and stamps, but can also be used on other machines (e.g., rotating tables, automatic assembly systems). When using PSDI mode, it must not be possible to stand behind the light curtain. For presses, special conditions apply for PSDI mode.

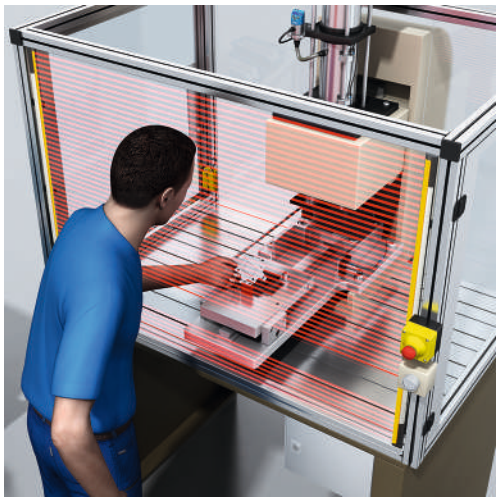


Figure 63: Single break PSDI mode on an automatic assembly system with safety light curtain. During loading, the tool is at the top point. After the operator leaves the protective field, the assembly process gets underway.

NOTE

For PSDI mode, the resolution of the AOPD shall be better than or equivalent to 30 mm (finger or hand detection).

NOTE

➜ PSDI triggering: Type-B standards ISO 13855, IEC 61496-1

➜ PSDI mode on presses: Type-C series of standards ISO 16092

Different protective fields

If protective fields with different shapes and/or dimensions are required, corresponding requirements must be met. These requirements relate to:

- the safety level of the safety-related parts of the control system (SRP/CS)
- the avoidance of inadmissible conditions or inadmissible reconfigurations
- the activation, as well as the conditions for initiating the automatic mode of the machine
- the state to be adopted when a fault is detected
- the necessary conditions for selecting the protective field
- the installation and the organizational measures

When applications with simultaneous field evaluations are implemented, the number of switchovers is reduced. The design is greatly simplified.

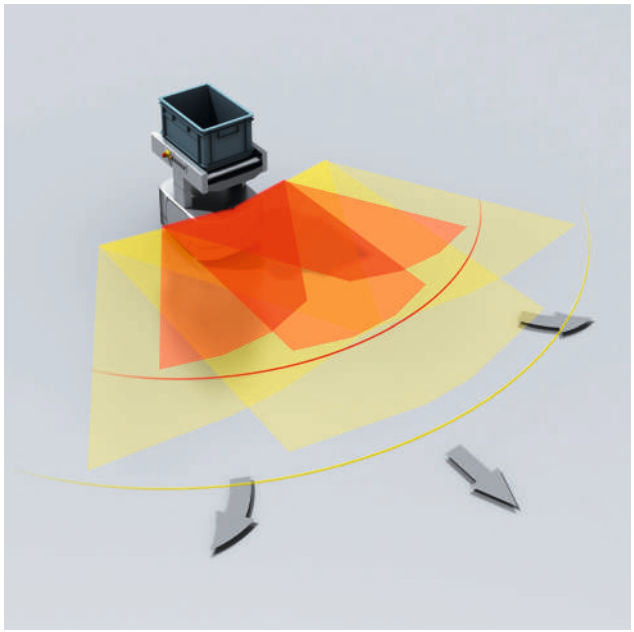


Figure 64: Protective fields of a safety laser scanner with different geometries on an autonomous vehicle

Figure 65: Application example for protective fields on an autonomous vehicle

Additional requirements for automatic selection of active protective fields to allow passage of materials into or out of a hazardous area:

- A “maximum” (largest) active protective field must be configured in such a way as to prevent undetected access to hazardous areas when such access is not blocked by the material.
- At least one of the switching signals must be generated by a sensor that detects the position of the material that is blocking access to the hazardous area.
- Interruption and/or restoration of the power supply to the sensors for material detection must not result in the selection of an active protective field that is not suitable for the machine state.
- The largest protective field is automatically activated immediately after the material passes through the active protective field.
- The automatic selection of the active protective field must not be triggered by a ground fault or an interruption in the signal lines or power supply to the material detection sensor(s).

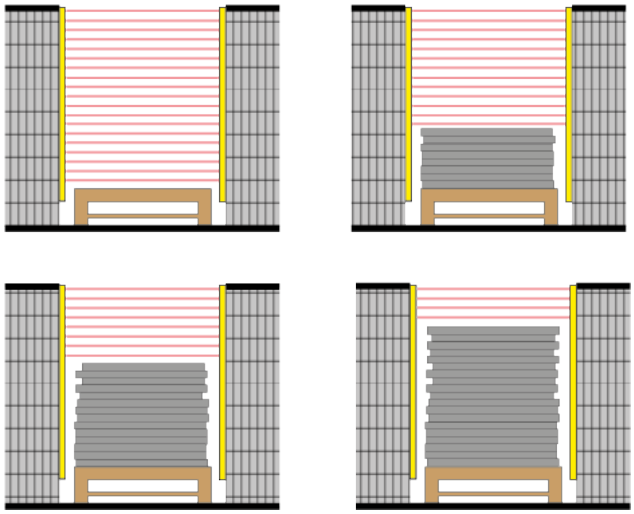


Figure 66: Schematic representation of protective field switching using safety light curtains (AOPD) for the passage of materials

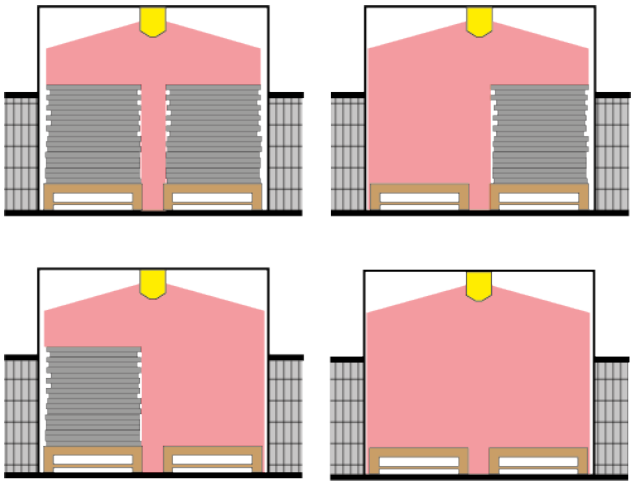


Figure 67: Schematic representation of protective field switching using vertically mounted safety laser scanners (AOPDDR) for the passage of materials

Fixed position protective devices

Fixed position protective devices are non-physical guards that ensure a person is located outside the hazardous area, for example buttons, foot switches or two-hand controls.

NOTE

A comprehensive overview of position fixing protective devices is given in:

➜ Alfred Neudörfer: Konstruieren sicherheitsgerechter Produkte, Springer-Verlag, Berlin u. a., ISBN 978-3-662-62703-7 (8th edition 2020)

Two-hand control device

The hazardous function is only triggered by deliberate actuation of two control switches (e.g., pushbuttons) and ends as soon as one of the control switches is no longer actuated. A two-hand control device can only protect one operator at a time. If several operators operate a machine, a separate two-hand control device must be installed for each operator. There are several types of two-hand control devices. The distinguishing characteristics are listed below.

Figure 68: Example use of a two-hand device. This is designed to be movable (ergonomics). A spacer ring ensures that the safety distance from the hazardous point is maintained.

The following basic principles apply to all types:

- It shall be ensured that both hands are used.
- Releasing one of the two controls stops the dangerous function.
- Accidental actuation must be prevented.
- It is not possible to simply bypass the two-hand control device.
- It must not be possible to take the two-hand control device into the hazardous area.

For type II and type III two-hand control devices, the following also apply:

- A new function may only be initiated after both controls have been released and then actuated.

For type III two-hand control devices, the following also apply:

- A function may only be initiated if both controls have been actuated synchronously within 0.5 seconds.

Sub-types with detailed control-related requirements are defined for type III two-hand control devices. The most important sub-types are:

- Type III A: PLc or SIL 1
- Type III B: PLd or SIL 2 with HFT1
- Type III C: PLe or SIL 3 with HFT1

NOTE

HFT1: see "Hardware fault tolerance (HFT)", page 140

NOTE

➜ Requirements on two-hand control devices: ISO 13851 (Type-B standard)

NOTICE

➜ Calculation of the minimum distance for two-hand control devices see "Approaches to calculating the minimum distance", page 100

Enabling devices

Enabling devices are control switches which the operator can use to purposely enable a machine function.

Generally, pushbuttons or foot switches are used as enabling devices. Having proven their worth in industrial applications, 3-position enabling devices are to be recommended.

- Position 1, not actuated
  Execution of the function is not enabled
- Position 2, actuated in middle position
  Execution of the function is enabled
- Position 3, actuated beyond the middle position
  Execution of the function is not enabled and it must stop immediately. Depending on the application, the triggering of a safety-related stop function or an emergency stop function may also be required.

During machine setup and maintenance, and if it is necessary to observe production processes close up, the functions of the protective devices intended for normal operation can be temporarily disabled using enabling devices. This is only permissible, however, in conjunction with other measures that minimize the risk (reduced force or speed, etc.).

Figure 69: Enabling device for setting up an automatic drilling machine

NOTICE
The machine start shall not be initiated solely by the actuation of an enabling device. Instead, movement is only permitted as long as the enabling device is actuated.

The enabling device function must not be released while changing back from position 3 to position 2.

If enabling devices are equipped with separate contacts in position 3, it is recommended to integrate them into a safety-related stop function or the emergency stop function.

Protection against manipulation shall be considered when using enabling devices.

NOTE
➜ Requirements on enabling devices: IEC 60204-1

Foot switches

Foot switches are used to control work processes.

On certain machines (e.g., on presses, punches, bending and sheet metal working machines), foot switches may only be used in safety functions under the following conditions:

- only for special operating modes
- always in conjunction with other technical protective measures (e.g., slow speed of a dangerous movement)

Foot switches used in this way must be designed as follows:

- A protective cover to protect against unintentional actuation
- A 3-position design similar to the enabling switch principle (see "Enabling devices", page 86)
- With manual reset on actuation of the actuator beyond the pressure point
- In such a way that after the dangerous machine function has stopped, the restart occurs only after the foot switch is released and actuated again

- In such a way that a short circuit in the connection cable between the foot switch and the control system does not trigger an unintentional start (e.g., with at least one normally open contact and one normally closed contact for evaluation)
- In appropriate numbers for all operators, so that a dangerous machine function can only be initiated and maintained if all foot switches are actuated

Sensors for monitoring machine parameters

The risk assessment may show that certain machine parameters shall be monitored and detected during operation (see "Monitoring machine parameters", page 47).

Safe position monitoring

If, for safety reasons, parts of a machine are not allowed to overrun or leave a certain position, position switches or safety-related sensors should be used for this purpose.

Electro-sensitive safety inductive position switches are particularly suitable for this task (see table 21, page 63). They monitor a certain part of a robot's axis or a moving part of a machine for presence without the need for a specific actuator, without wear, and with a high enclosure rating.

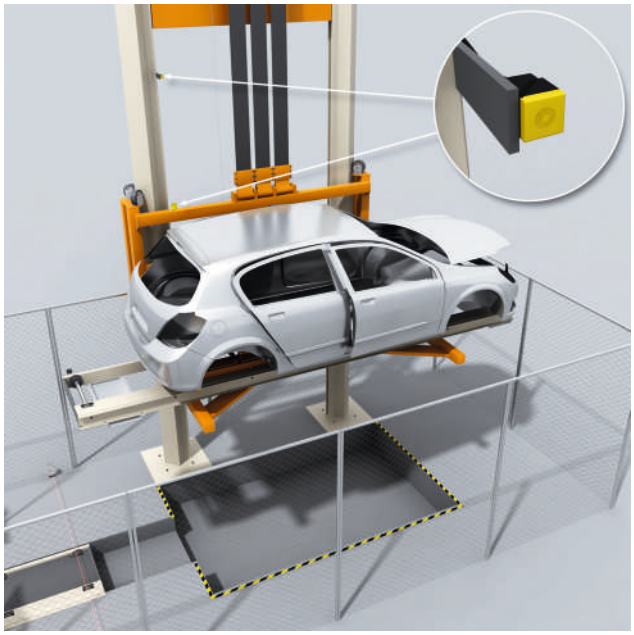


Figure 70: Safe position monitoring for a lift on an automobile production line

Monitoring of rotation, speed, overrun

Encoders or travel measurement systems are used to detect and evaluate rotation, speed, and overrun.

The signals from encoders can be used in automated guided vehicles to adapt the protective field size of safety laser scanners to the speed at which the vehicles are moving.

Safe standstill or rotation evaluation modules monitor the movement of drives using sensors or rotary encoders to generate a safe control signal at standstill or on deviation from preset parameters. If safety-related requirements are more stringent, either safety encoders or redundant encoders shall be used.

Another possibility is to monitor the voltage induced by residual magnetism on a motor that is spinning down.

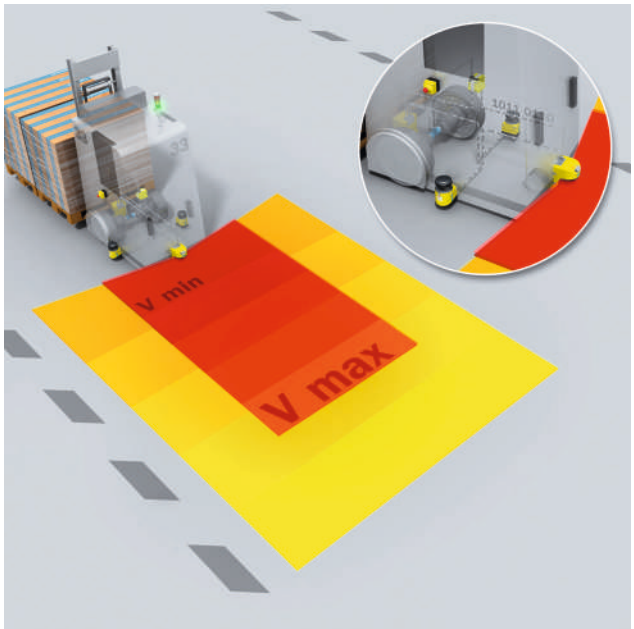


Figure 71: Speed monitoring for protective field switching on an automated guided vehicle

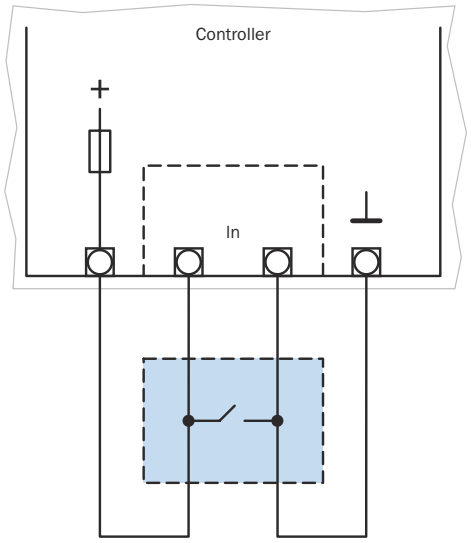
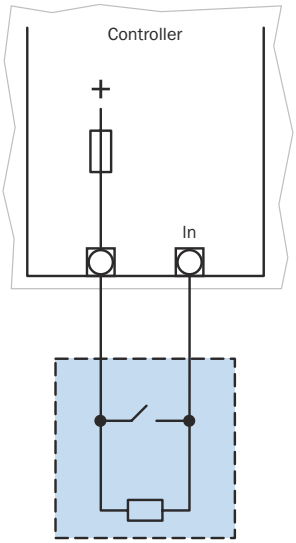
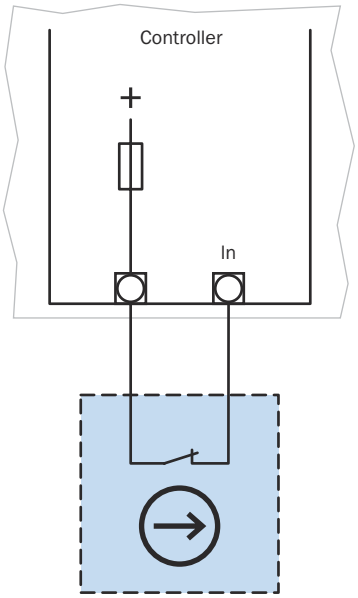
Pressure-sensitive protective devices

In some applications, pressure sensitive protective devices such as pressure sensitive mats, pressure sensitive rails or bumpers may be useful. The principle of operation is based in the majority of cases on the elastic deformation of a hollow body that ensures an internal signal generation (electromechanical or optical) which triggers the safety function.

The standard electromechanical systems are available in various designs.

Correct mechanical layout and integration is imperative in all cases for an effective protective function. The detection of children with body weights less than 20 kg is not considered in the product standards for pressure-sensitive mats and floors.

Table 31: Principles of operation of pressure sensitive mats, pressure sensitive rails, bumpers

Short circuiting designs (power to lock)		Positive opening contact design
4-wire version	Resistance version	(power to release)
		
In both variants, a short-circuit is produced when the protective device is activated. In the case of the 4-wire version, a circuit is short-circuited (a few ohms). In the case of the resistance version, a change from a set resistance (a few kOhms) is detected. These designs require more complex evaluation.		This design is more universal and offers more advantages. As on a safety switch, a switch contact is opened on activation of the protective device. A short-circuit between the cables can be prevented by using a special cable layout.

NOTE
Design of pressure sensitive protective devices: Type-B standard ISO 13856 (series of standards)

Complementary protective measures

If necessary, provision must be made for further protective measures which are neither inherently safe designs or technical precautionary measures.

These might include:

- Emergency stop devices
- Measures to free and rescue persons who have become trapped
- Measures for isolating and dissipating energy
  (see "Power supply connection", page 31 and see "Mains disconnection device", page 33)
- Preventive measures for easy and safe handling of machines and heavy parts
- Measures for safe access to machinery

If these complementary measures are dependent upon the correct function of the corresponding control components, then they are safety functions. The requirements on functional safety must be met for these measures. (see "Application of reset and restart", page 110).

Emergency operation

To prevent impending hazards to persons, damage to machines or production processes, or to minimize existing ones, functions must be provided for such emergencies. These functions, which cause machine functions to stop (emergency stop) or electrical power to be disconnected (emergency switching off) in an emergency, are complementary protective measures for hazards on machines. They do not replace the use of inherently safer design or protective devices.

Figure 72: Emergency stop and reset control switches at a robot station

Emergency stop (ISO 13850)

In the event of an emergency, not only shall all hazardous machine functions be ceased, but the energy from all energy sources which pose a hazard shall be dissipated. This procedure is known as emergency stopping. Every machine must be equipped with at least one emergency stop function, except:

- Machines for which an emergency stop would not reduce the risk
- Hand-held and hand-guided machines

The emergency stop function must be triggered by a single action of a person. The following fundamental requirements apply to the emergency stop function and its devices in accordance with ISO 13850:

- The actuators of emergency stop control switches must be easily accessible.
- The emergency stop function must end the dangerous state in a suitable manner as quickly as possible without creating additional risks.
- The emergency stop function must take priority over all other functions and commands in all operating modes.
- The emergency stop function must not impair the effectiveness of other safety functions.
- Resetting the emergency stop control switches must not initiate a restart.
- The principle of direct mechanical positive actuation with mechanical interlocking function must be applied (referred to as a latching function in IEC 60947-5-1).
- When an emergency stop control switch is actuated, a stop command must be triggered, regardless of the effectiveness of the mechanical interlock function or latching function.
- The emergency stop function must conform to stop category 0 or 1 (see "Stopping", page 35).
- The emergency stop function must be designed in such a way that decisions to trigger it do not require the relevant person to think about the consequences (e.g., economic losses).

Reset

If an emergency stop device is actuated, devices triggered by this action must remain in the off state until the device has been reset. Actuated emergency stop devices must be reset by hand locally. The reset must only prepare the machine to be put back into operation (see "Application of reset and restart", page 110).

The operating instructions of the machine must provide information that after actuation and before resetting the control switch, the machine must be checked to determine the reason for the actuation. If the emergency stop control switch is operated by ropes or wires, the instructions must include checking the entire length of the ropes or wires.

In the case of emergency stop control switches in portable operator panels, resetting the emergency stop command must only be possible after the actuated emergency stop control switch has been unlocked.

If the area of operation of the machine is not fully visible (see figure 73, page 90), an additional reset must be carried out by one or more reset buttons to avoid the risk of an unexpected start-up. This is to ensure that no persons are present in a danger zone or that persons in need of assistance remain undetected.

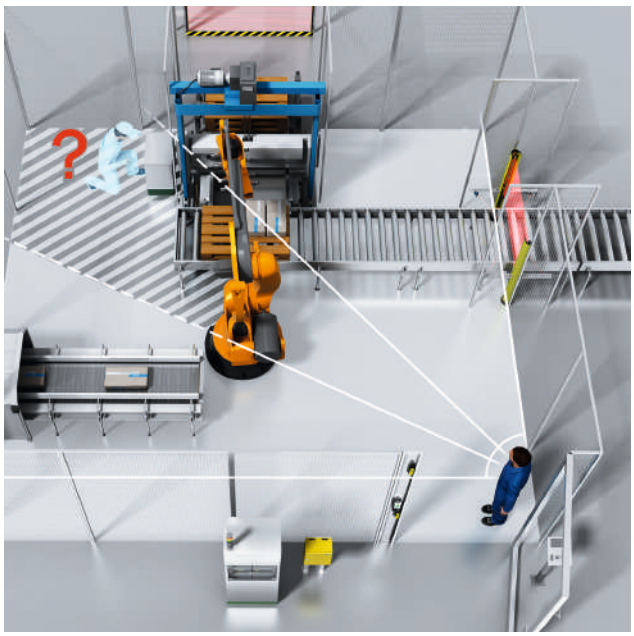


Figure 73: Example of an area of operation that is not fully visible

Emergency stop equipment

The emergency stop function is a “safety function” and therefore the requirements of functional safety must be met (ISO 13849-1 or IEC 62061).

The required reliability of the safety function (PL or SIL) should correspond to the purpose of the emergency stop function. The minimum requirement, however, is PL c according to ISO 13850 or SIL1 according to IEC 62061.

The hydraulic and pneumatic equipment that performs an emergency stop function must comply with the requirements of ISO 4413 or ISO 4414.

The electrical equipment for emergency stop functions must meet the requirements of IEC 60204-1. The contacts on the electrical control switches must be positive opening normally closed contacts.

The actuators must be red. The background must be yellow, if present and technically possible. The following types of control device may be used:

- Switches actuated with mushroom head pushbuttons
- Switches actuated with wires, ropes, or rails
- Foot switches without protective cover (only for emergency stop and only if other solutions cannot be used)
- Mains disconnecting devices operated by handles according to IEC 60204-1

Figure 74: Emergency stop control switches in various designs

If wires and ropes are used as actuators for emergency stop devices, they must be designed and attached so that they are easy to actuate. Reset devices shall be arranged so that the entire length of the wire or rope is visible from the location of the reset device. Measures must be taken to prevent loss of the emergency stop function due to breakage or unhooking of the wires or ropes.

Neither the emergency stop actuator nor the background must be marked with text or symbols. If needed for clarification, only the following symbol (IEC 60417-5638) may be applied:

Figure 75: Symbol IEC 60417-5638: Emergency stop

To avoid confusion between actuation (e.g., pressing an actuator) and release (e.g., turning an actuator), the marking for release must be the same or approximately the same color as the actuator.

Emergency stop control switches must be mounted in such a way that their actuation cannot be prevented by simple means or blocked unintentionally. Actuating surfaces with locks for resetting should be avoided. If such emergency stop control switches are used, the operating instructions for the machine must provide information on their correct usage. In particular, attention should be drawn to the possibility of injury if actuated with a key inserted.

Area of operation of the emergency stop function

The area of operation of the emergency stop function must always include the complete machine. If this creates additional hazards or has an unnecessary impact on production, the machine can be divided into several areas of operation of the emergency stop function. Areas of operation may include parts of a machine, a single machine, or a group of machines. Different areas of operation may overlap.

A division into areas of operation should take into account the following:

a) the visible areas resulting from the machine design
b) the ability to recognize dangerous situations (visibility, audibility, etc.)
c) all safety-relevant consequences for other parts of the machine or other machines
d) the foreseeable hazard exposures
e) all possible hazards in the area of operation

The different areas of operation must be defined and marked so that the emergency stop control switches can be easily associated with the appropriate areas. The actuation of an emergency stop device for one area of operation must not prevent the triggering of an emergency stop function in another area of operation. The

operating instructions of the machine must contain information on the area(s) of operation of the emergency stop control switches. Emergency stop control switches with different areas of operation should, as far as technically possible, not be arranged next to each other or located close to each other.

Position of emergency stop control switches

Emergency stop control switches must be provided at each operator panel unless the risk assessment indicates that it is not required. Emergency stop control switches must also be located in other places if the risk assessment indicates this (e.g., at entry and exit points or loading and unloading points).

Emergency stop control switches that are to be operated by hand must be installed at a height between 0.6 and 1.7 m above the access level (reference level). Foot switches for emergency stop functions must be permanently mounted at the access level.

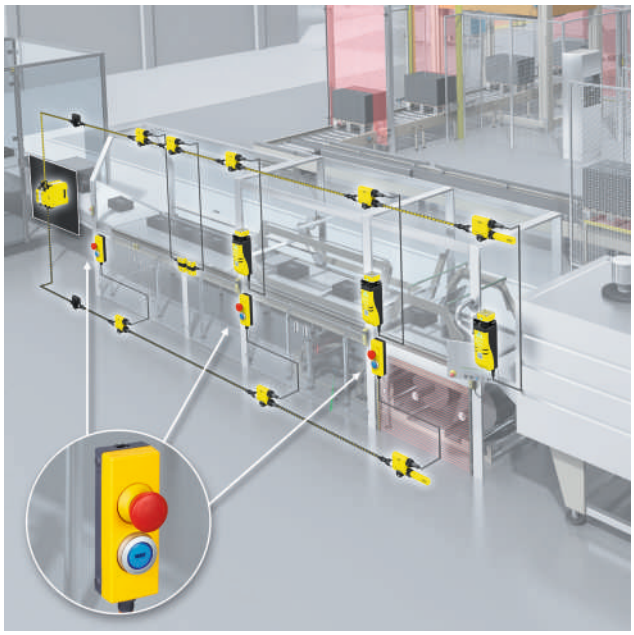


Figure 76: Distributed emergency stop control switches on a packaging system

Avoiding unintentional triggering

Unintentional triggering of emergency stop control switches must be avoided as far as possible without hindering intentional triggering. This is more likely to be achieved by layout than by design measures:

- Locating the emergency stop device away from foreseeably busy areas
- Mounting the emergency stop device in a recessed surface of the enclosing operator panel
- Selecting a suitable type of emergency stop device
- Selecting the appropriate size and shape of the emergency stop device

The use of a protective collar around the emergency stop device should be avoided. An exception exists if unintentional actuation must be prevented and other measures are not practicable.

Protective collars must not have any sharp corners or edges or rough surfaces and must not hinder or prevent operation with the palm of the hand. This applies from any foreseeable position of the machine operator or other persons who must be able to operate it (nearby operator or work stations).

Emergency stop control switches in portable operator panels

When emergency stop control switches are installed in portable operator panels, measures must be used to avoid confusion between active and non-active emergency stop control switches. This also applies to operator panels where the emergency stop commands are transmitted via plug connections on the controller. At least one of the following measures must be used:

- Identification of the active emergency stop control switches through a color change by means of illumination
- Covering the inactive emergency stop control switches, if possible automatically
- Provision of suitable storage for the inactive operator panels

Emergency switching off (switching off in an emergency situation - IEC 60204-1)

Provision should be made for emergency switching off if there is a possibility of hazards or damage caused by electrical energy. The incoming electrical energy supply should be switched off by electromechanical switching devices.

It shall not be possible to switch on the incoming energy supply until all emergency off commands have been reset. The emergency switching off is achieved with stop category 0 ("Stopping", page 35).

NOTE

➜ Design guidelines for emergency stop devices: ISO 13850 (type-B standard)

➜ Emergency shutdown: Machinery Directive 2006/42/EC

Positioning and sizing of protective devices

It must be ensured that the dangerous state can be eliminated in good time before the hazardous point is reached. This requires the protective device to be positioned at the required minimum distance from the hazardous point. The necessary minimum distance also depends on the properties of the protective device. This can also affect the selection of the optimal protective device.

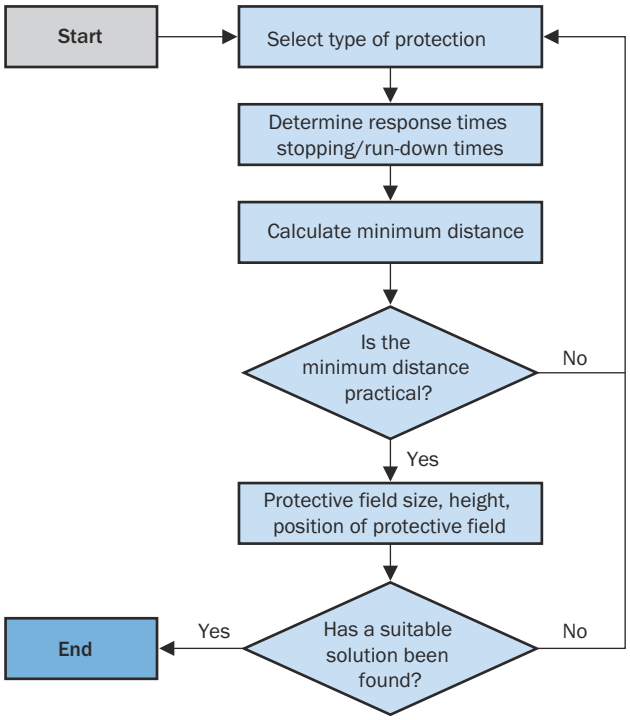
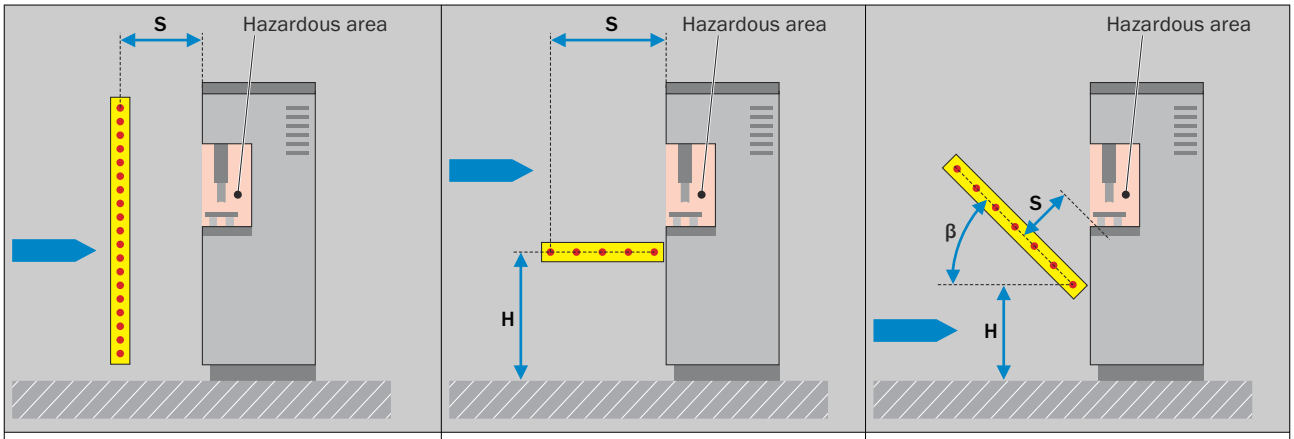


Figure 77: Basic procedure for positioning and sizing a protective device

Minimum distance of the protective field of an ESPE depending on the type of approach

Table 32: Approach types and minimum distance for ESPE



Approach at right angles to the plane of the protective field.	Approach parallel to the plane of the protective field.	Approach at any angle to the plane of the protective field.

The consideration of the minimum safety distance applies to ESPEs with two-dimensional protective fields, e.g., light curtains, single-beam photoelectric safety switches (AOPD), laser scanners (AOPDDR), or two-dimensional camera systems. There are three types of approach.

After the stop initiating ESPE has been selected, the required minimum distance between the ESPE's protective field and the nearest hazardous point is to be calculated.

The following parameters shall be taken into account:

- Stopping time of the machine
- Response time of the safety-related control system
- Response time of the protective device (ESPE)
- Supplements according to the resolution capability of the ESPE, the protective field height, and/or the type of approach as well as the possibility of bypassing the protective field by reaching around, over or under it (see table 40, page 103).

If the minimum distance to the hazardous area is too large and unacceptable from an ergonomic viewpoint, either the overall stopping time of the machine must be reduced or an ESPE with a better detection capability (smaller resolution) chosen. Risks due to a person possibly remaining undetected between the protective field of the ESPE and the hazardous point must be avoided by taking suitable measures against unexpected start-up:

- Restart interlocks that require a manual reset
- Additional device for detecting persons in the hazardous area (see table 40, page 103)

NOTE

The calculation of the minimum distance S for ESPE is described in the ISO 13855 standard (type-B standard).

General calculation formula
$S = (K \times T) + C$

S Minimum distance in millimeters, measured from the nearest hazardous point to the detection zone of the ESPE.

K Parameter in millimeters per second, derived from the data for the approach speeds of the body or parts of the body.

T Stopping/run-down time for the entire system in seconds.

C Additional distance in millimeters that represents the entry into the hazardous area before the protective device is triggered.

Supplement determined by resolution C_{RT}
$8 \times (d-14)$

Depending its detection capability (resolution), the ESPE may trigger (detect a person) when parts of the body have already passed the protective field.

This must be taken into account by adding the supplement determined by the resolution C_{RT} (RT = Reach Through).

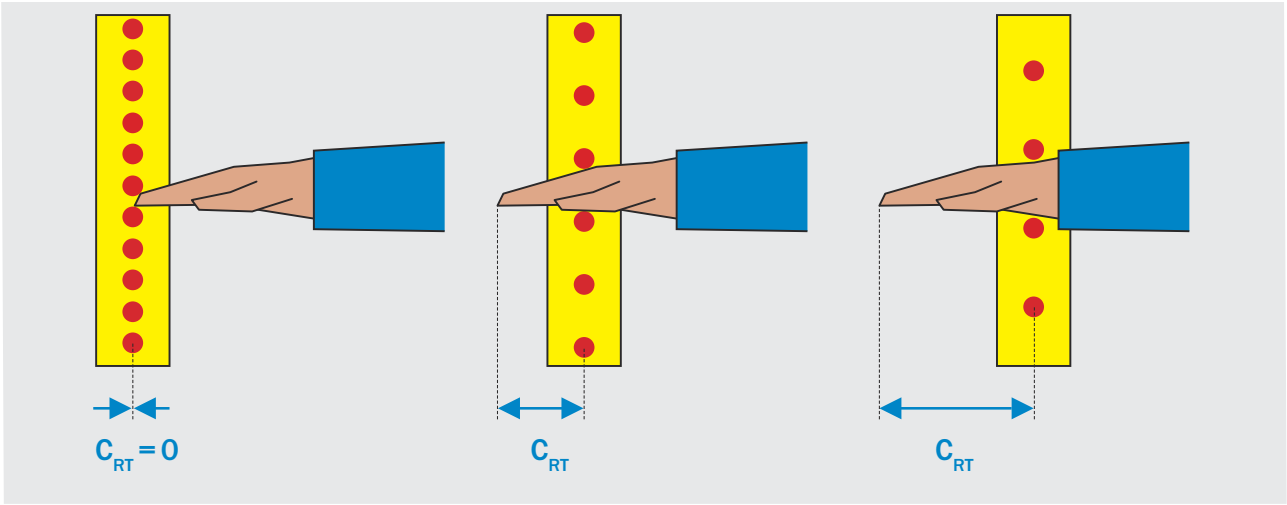
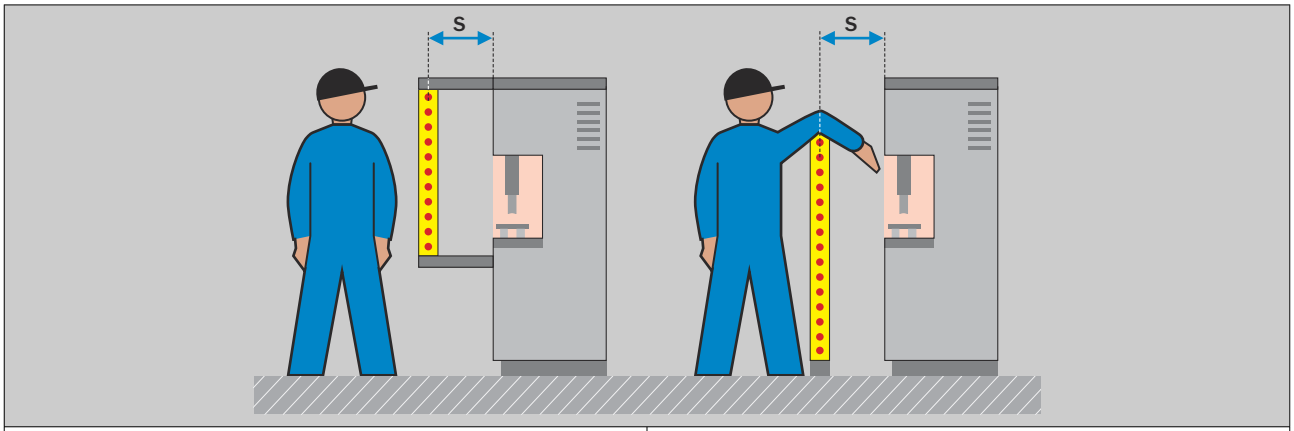


Figure 78: The figure shows an example of undetected intrusion (C_{RT}) for safety light curtains with different detection capabilities.

Protective devices that can be reached over

Depending on the height and position of the protective field of an ESPE, the shape of the machine, and other factors, the protective field of an ESPE can be reached over to gain access to hazardous points before the hazardous machine functions have ceased and the intended protection is thereby not provided. The figure shows an example comparing an ESPE that cannot be reached over and an ESPE that can be reached over.

Table 33: Comparison of an ESPE that cannot be reached over and an ESPE that can

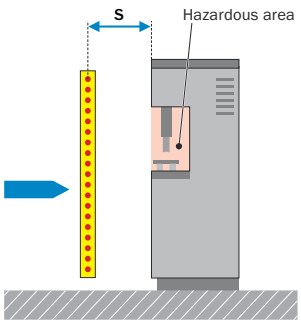


ESPE cannot be reached over	ESPE can be reached over

If access to the hazardous area by reaching over a protective field cannot be prevented, the height of the protective field and minimum distance of the ESPE must be determined. This is done by comparing the calculated values based on the possible detection of limbs or body parts with the values resulting from possibly reaching over the protective field. The higher value of this comparison shall be applied. This comparison is to be carried out according to ISO 13855, Section 6.5.

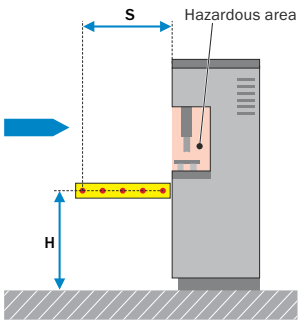
If it is not possible to reach over the protective field of the ESPE, C is determined by the detection capability (resolution) of the ESPE and is referred to as C_{RT} (reach through). If it is possible to reach over the protective field of the ESPE, C is determined by the height of the protective field and is referred to as C_{RO} (reach over).

Table 34: Formula for calculating the minimum distance S for a perpendicular approach

<table>
<tr><th colspan="5">Perpendicular approach: β = 90° (± 5°)</th></tr>
<tr><td rowspan="5"> 
</td><td colspan="4">Step 1: Calculation of the minimum distance S</td></tr>
<tr><td>d ≤ 40 mm</td><td>S = 2 000 × T + 8 × (d – 14)
If S > 500 mm, then use:
S = 1 600 × T + 8 × (d –14). In this case, S must not be < 500 mm.</td><td colspan="2">The minimum distance S cannot be < 100 mm.
C = 8 × (d – 14) is here the additional distance in millimeters that represents the intrusion into the hazardous area before the protective device is triggered.</td></tr>
<tr><td>40 < d ≤ 70 mm</td><td>S = 1 600 × T + 850</td><td colspan="2">Height of the bottom beam ≤ 300 mm Height of the top beam ≥ 900 mm</td></tr>
<tr><td>d > 70 mm</td><td>S = 1 600 × T + 850</td><td>Number of beams
4
3
2</td><td>Recommended heights
300, 600, 900, 1 200 mm
300, 700, 1 100 mm
400, 900 mm
(400 mm can only be used if there is no risk of crawling beneath.)</td></tr>
<tr><td colspan="4">Step 2: Calculation of the required height of the top edge of the protective field (see "Increase minimum distance (height of top edge prescribed)", page 104)</td></tr>
</table>

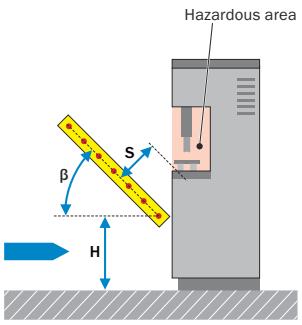
S Minimum distance
H Height of protective field (detection plane)
d Resolution of the ESPE
β Angle between the detection plane and the approach direction
T Stopping/run-down time of the overall system

Table 35: Formula for calculating the minimum distance S for parallel approach

<table>
<tr><th colspan="4">Parallel approach: β = 0° (± 5°)</th></tr>
<tr><td rowspan="4"> 
</td><td colspan="3">Step 1: Calculation of the minimum distance S</td></tr>
<tr><td>S = 1 600 × T + (1 200 – 0.4 × H)
where
C = (1 200 – 0.4 × H) ≥ 850 mm</td><td colspan="2">H ≤ 1 000 mm</td></tr>
<tr><td colspan="3">Step 2: Calculation of the required resolution depending on the protective field height</td></tr>
<tr><td></td><td>$d \leq \frac{H}{15} + 50$ mm</td><td>H ≤ 1 000 mm
d ≤ 117 mm</td></tr>
</table>

S Minimum distance
H Height of protective field (detection plane)
d Resolution of the ESPE
β Angle between the detection plane and the approach direction
T Stopping/run-down time of the overall system

Table 36: Formula for calculating the minimum distance S for approach at an angle

Approach at an angle: 5° < β < 85°			
	β > 30°	See perpendicular approach.	$d \leq \frac{H}{15} + 50$ mm refers to the lowest beam.
	β < 30°	See parallel approach.	
			S then applies to the beam that is furthest away from the hazardous area and is ≤ 1,000 mm in height.

S Minimum distance
H Height of protective field (detection plane)
d Resolution of the ESPE
β Angle between the detection plane and the approach direction
T Stopping/run-down time of the overall system

Special cases

Special case 1: Press application

Unlike general standards, machine-specific type-C standards can contain special requirements. In particular for metal-working presses, the following applies:

Table 37: Supplements for the minimum distances of ESPE on presses according to ISO 16092-1 and ISO 16092-3

Calculation of the supplement for presses		
Resolution d (mm) of the ESPE	**Supplement C (mm)**	**Stroke initiation by ESPE/PSDI mode**
d ≤ 14	0	Allowed
14 < d ≤ 20	80	
20 < d ≤ 30	130	
30 < d ≤ 40	240	Not allowed
> 40	850	

NOTE
➜ Press standards: ISO 16092-1, ISO 16092-3 (type-C standards)

Special case 2: ESPE for presence detection

This type of protection is recommended for large systems that are accessible from the floor. In this special case, starting of the machine (“preventing start” safety function) must be prevented while there is an operator inside. This is a secondary protective device which detects the presence of persons in the hazardous area and simultaneously prevents the machine switching to the dangerous state. In addition to the ESPE for presence detection, there shall be a primary protective measure for the “initiating a stop” safety function, e.g., in the form of another ESPE or a locked, movable physical guard.

The minimum distance shall be calculated in this case for the main protective device (e.g., a vertical light curtain that has the task of stopping the machine).

Figure 79: Safety laser scanner on a machining center as safety function pos. 1, initiating a stop and safety function pos. 2, preventing start (presence detection)

Special case 3: ESPE applications on autonomous vehicles

If the dangerous state is as a result of a collision with an autonomous vehicle, the determination of the minimum distance is generally based only on the speed the vehicle is traveling and not on the approach speed of the person. It is assumed that the person recognizes the approaching vehicle (vehicle with protective device) and stops or moves away.

Figure 80: Hazardous area protection on an autonomous vehicle with safety laser scanners

The minimum distance needs to be set to a length that is sufficient to stop the vehicle safely. The minimum distance corresponds to the braking distance of the vehicle. An exact calculation of the braking distance is not possible, as it depends on several factors, e.g., friction between the tire and ground, total weight incl. load, braking force, etc.

It is therefore recommended to first calculate the minimum distance and validate (confirm) the result by testing.

For the calculation, the braking deceleration of the vehicle (a) at nominal load, maximum operating speed (v_0) and under the intended operating conditions must be known or determined. The braking distance (S_B) is then calculated as follows:

$$S_B = \frac{v_0^2}{2a}$$

Safety supplements may be necessary depending on the application and the technology used. The calculated value must be validated by two tests:

1. For detecting a lying person
   A test body with a diameter of 200 mm and a length of 600 mm must be used. The test body is placed horizontally in a fixed position on the left, in the middle, and on the right of the vehicle path to be protected and orthogonal (perpendicular) to the vehicle path.

Figure 81: Positioning of a test body on an autonomous vehicle for testing the detection of a person lying down

2. For detecting a standing person
   A test body with a diameter of 70 mm and a length of 400 mm must be used. The test body is placed vertically and completely in a fixed position anywhere on the vehicle path to be protected.

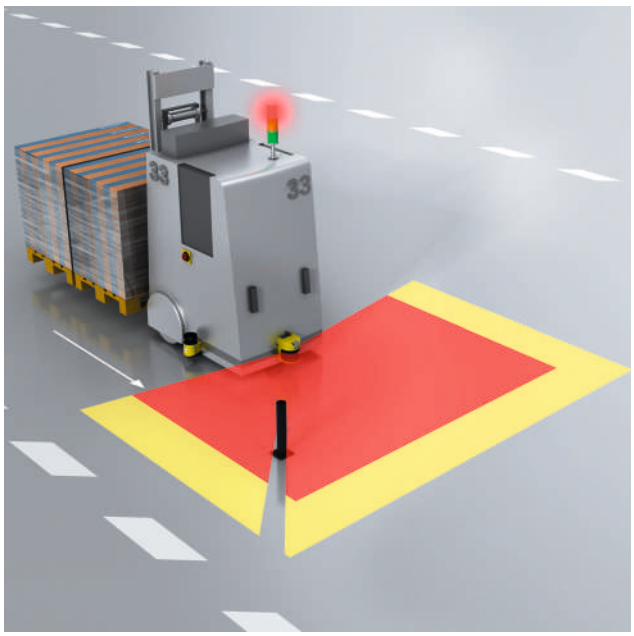


Figure 82: Positioning of a test body on an autonomous vehicle for testing the detection of a standing person

3. Validation
   The vehicle must be loaded with the nominal load and approach the test body at the maximum operating speed. The vehicle must stop in time, therefore either not touch the test body or, if contact occurs, the force applied to the (1) horizontal test body must not exceed 750 N and to the (2) vertical test body must not exceed 250 N.

This is the current standardized method to be used for the protection of autonomous vehicles in the industrial sector (ISO 3691-4).

The method can also be used for the non-industrial sector, but it is important to consider the following:

- It cannot always be assumed that persons will never approach the moving vehicle. Both speeds (person and vehicle) may therefore need to be considered accordingly.
- The maximum permissible forces in the event of contact with children or elderly people are much lower than those specified.
- The bodily dimensions of children cannot be simulated using the specified test bodies. In this case, the dimensions of the test bodies should be taken from the relevant literature.

Special case 4: Stationary application of an onboard ESPE

The way in which some machines function requires that operators are located very close to the hazardous area. On press brakes, small pieces of plate must be held very close to the bending edge. Moving systems that form a protective field around the tool openings have proven to be practical protective devices. Because the hand approach speed of the operator is not taken into account in such applications, the general formula is not applicable.

The requirements to be met by the resolution are very high and reflections on metal surfaces shall be prevented. For this reason, focused laser systems with image-based evaluation are used. This type of protection is defined in the type-C standards in conjunction with other measures (e.g., 3-pedal foot switch, automatic stop time measurement, requirement to wear gloves, etc.).

NOTE
➜ Safety of press brakes: EN 12622 (type-C standard)

NOTE
Specific know-how and equipment are required to measure the stopping/run-down time and the required minimum distance. SICK offers these measurements as a service.

Approaches to calculating the minimum distance

Solution approach 1: Perpendicular approach – hazardous point protection with presence detection

The calculation results in a minimum distance of S = 320 mm (see figure 83). By using a safety light curtain with the best possible resolution (14 mm), this is already the optimal minimum distance.

Two AOPDs are used to ensure that the person is detected everywhere in the hazardous area:

- a vertical AOPD positioned according to the calculated minimum distance (vertical approach) - for the safety function: initiating a stop
- a horizontal AOPD to eliminate the risk of standing behind - for the safety function: preventing an unexpected start-up

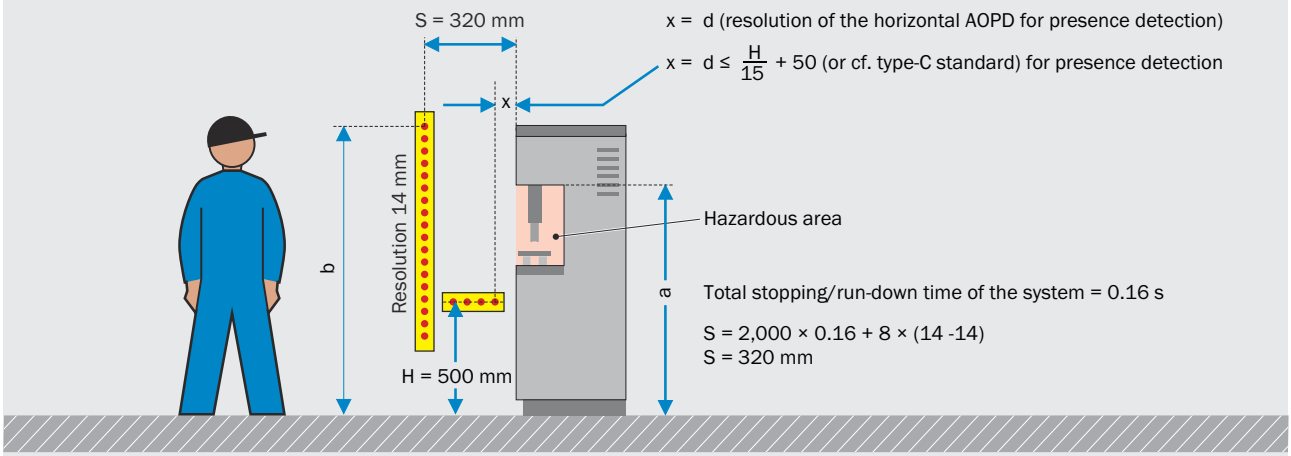


Figure 83: Determining the positioning and sizing of ESPE for hazardous point protection and presence detection using a safety light curtain

Solution approach 2: Parallel approach – hazardous area protection

A horizontal AOPD is used. The following figure shows a horizontally arranged AOPD and the calculation of the minimum distance S. If the installation height of the AOPD is increased to 300 mm, the minimum distance is reduced. For this height, an AOPD with a resolution less than or equal to 80 mm can be used. It must not be possible, however, to access the hazardous area beneath the AOPD (evaluate the risk of crawling beneath). This type of safeguarding is also often implemented using AOPDDR (laser scanners). However, supplements have to be added for these devices for technology-related reasons.

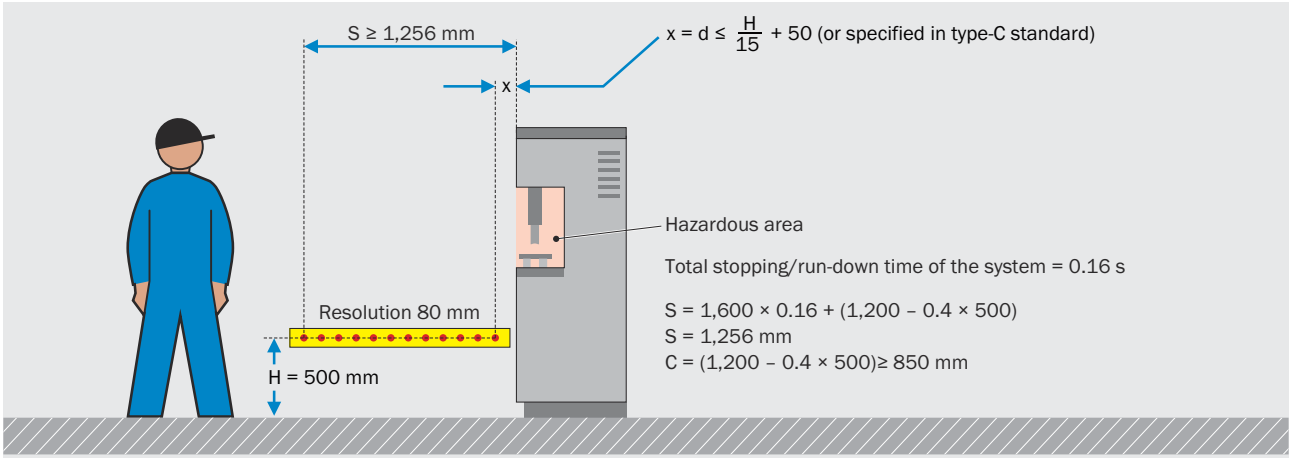


Figure 84: Determining the positioning and sizing of ESPE for hazardous area protection using a safety multibeam sensor and for a perpendicular approach

Solution approach 3: Access protection

Access protection using three beams (at heights of 300 mm, 700 mm and 1,100 mm) allows a perpendicular approach. This solution allows the operator to stand between the hazardous area and the AOPD without being detected. For this reason, additional safety measures shall be applied to reduce this risk. The control device (e.g., a reset button) must be positioned so that the entire hazardous area can be overseen. It must not be accessible from the hazardous area.

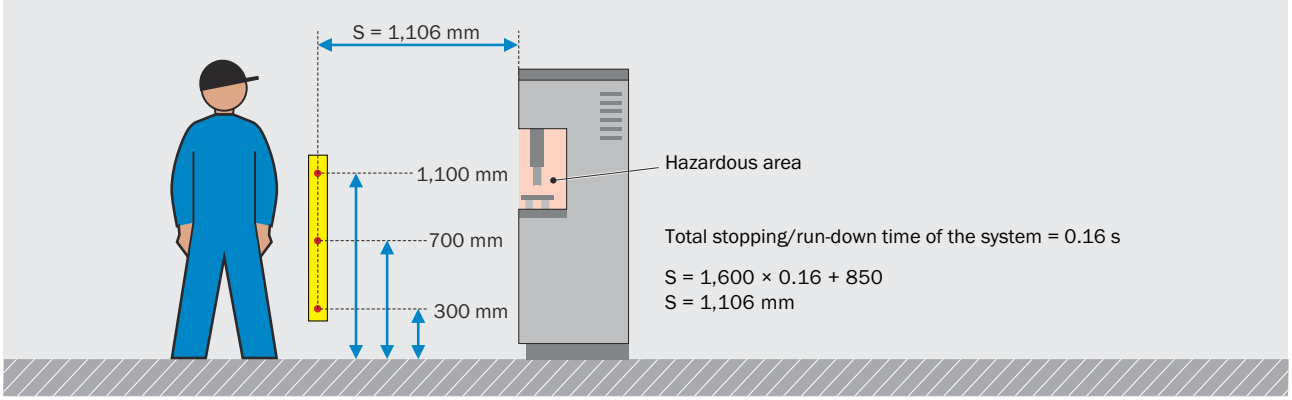


Figure 85: Determining the positioning and sizing of ESPE for access protection using a safety multibeam sensor and for a parallel approach

Comparison of the results

Table 38: Comparison of solution approaches, selection according to operational requirements

Solution approach for stopping/run-down time = 0.16 s		Advantages	Disadvantages
1	**Hazardous point protection** **S = 320 mm**	• Increased productivity, as the operator is closer to the work process (short paths) • Automatic start or PSDI mode possible • Very little space required	• Higher price for the protective device due to good resolution and presence detection
2	**Hazardous area protection** **S = 1,256 mm**	• Automatic start possible • Enables access to be protected independent of the height of the hazardous area	• The operator is much further away (long paths) • More space required • Lower productivity
3	**Access protection** **S = 1,106 mm**	• Cost-effective solution • Enables access to be protected independent of the height of the hazardous area • Protection on several sides possible using deflector mirrors	• The operator is much further away (long distances) • Lowest productivity (always necessary to reset the ESPE) • The risk of standing behind is to be taken into account. Not to be recommended if more than one person is working in the same location.

Required protective field size/height of the ESPE

As a general rule, the following faults must be excluded when assembling protective devices:

- It shall only be possible to reach the hazardous point through the protective field.
- In particular, it shall not be possible to reach hazardous points by reaching over/under/around.
- If it is possible to stand behind protective devices, additional measures to prevent an unexpected startup are required (e.g., restart interlock, secondary protective device).

Once the minimum distance between protective field and the nearest hazardous point has been calculated, the protective field height required must be determined in a further step. This ensures the hazardous point cannot be reached by reaching over.

Table 39: Examples of correct assembly of ESPE

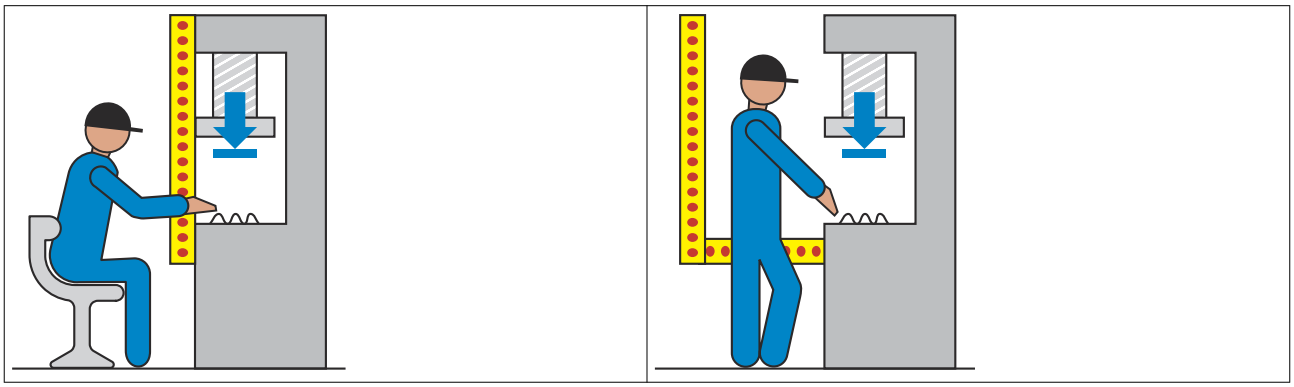
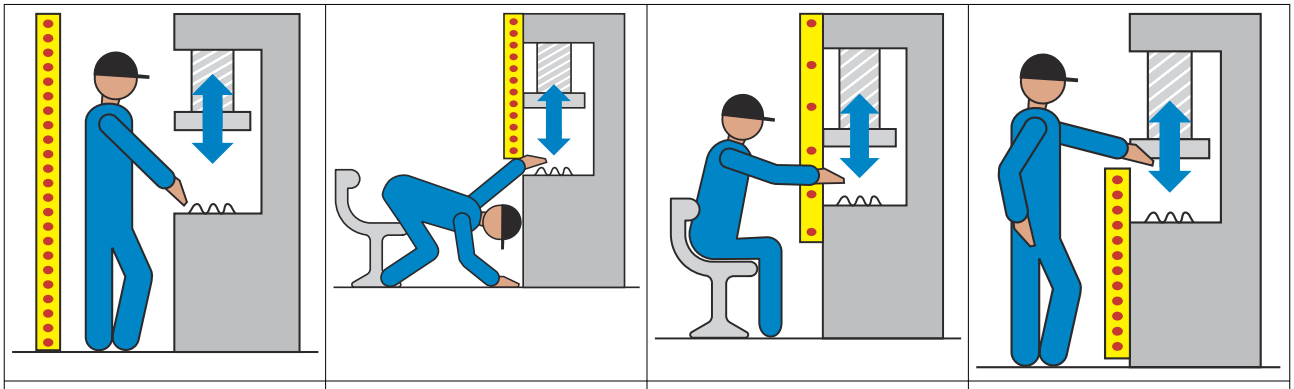


Table 40: Examples of dangerous assembly faults



Take the possibility of reaching over into account

If there is a possibility of reaching over the vertical protective field of an ESPE, the height **b** of the top edge of the protective field shall be increased or the supplement **C** adjusted. The relevant table from the ISO 13855 standard must be used.

Some type-C standards differ from ISO 13855 in the calculation of the minimum distances.

Increase height of top edge

When the height of the top edge of the protective field **b** is increased, in addition to the height of the hazardous area **a**, the supplement determined by the resolution C_{RT} is also used to calculate the required height of the top edge of the protective field when the minimum distance remains unchanged. With the top edge of the protective field calculated at this height, it is not possible to reach over and into the hazard zone and a C_{RO} supplement is not required.

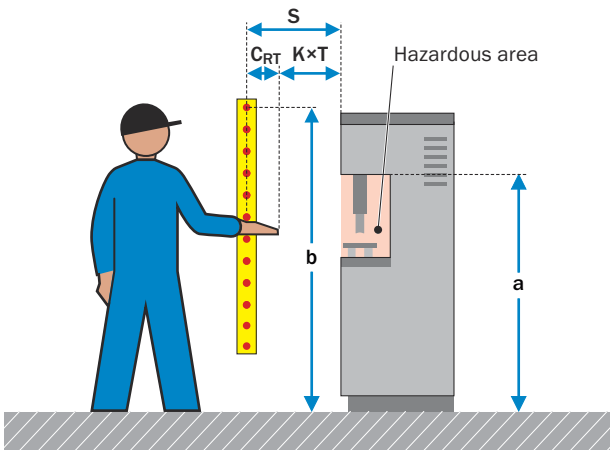


Figure 86: Parameters for determining the required minimum distance for reaching through

To take the possibility of reaching over into account, the ISO 13855 standard includes the following table. This table is used to calculate the increased height of the top edge of the protective field or the increased minimum distance.

Table 41: Consideration of a possible reaching over according to ISO 13855

Height a of the hazardous area (mm)	**Additional horizontal distance C_{RO} to the hazardous area (mm)**											
2 600	0	0	0	0	0	0	0	0	0	0	0	0
2 500	400	400	350	300	300	300	300	300	250	150	100	0
2 400	550	550	550	500	450	450	400	400	300	250	100	0
2 200	800	750	750	700	650	650	600	550	400	250	0	0
2 000	950	950	850	850	800	750	700	550	400	0	0	0
1 800	1 100	1 100	950	950	850	800	750	550	0	0	0	0
1 600	1 150	1 150	1 100	1 000	900	850	750	450	0	0	0	0
1 400	1 200	1 200	1 100	1 000	900	850	650	0	0	0	0	0
1 200	1 200	1 200	1 100	1 000	850	800	0	0	0	0	0	0
1 000	1 200	1 150	1 050	950	750	700	0	0	0	0	0	0
800	1 150	1 050	950	800	500	450	0	0	0	0	0	0
600	1 050	950	750	550	0	0	0	0	0	0	0	0
400	900	700	0	0	0	0	0	0	0	0	0	0
200	600	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0
	Height b of the top edge of the protective field (mm)											
	900	**1 000**	**1 100**	**1 200**	**1 300**	**1 400**	**1 600**	**1 800**	**2 000**	**2 200**	**2 400**	**2 600**

Increase minimum distance (height of top edge prescribed)

If the top edge of the protective field **b** is prescribed for an already existing product, the minimum distance must be increased. This is done by determining the height of the hazardous area **a** and the height of the top edge of the protective field **b**.

The result of the intersection represents the intrusion distance C_{RO}. Once C_{RO} and C_{RT} have been determined, the larger of the two values is used to calculate the minimum distance.

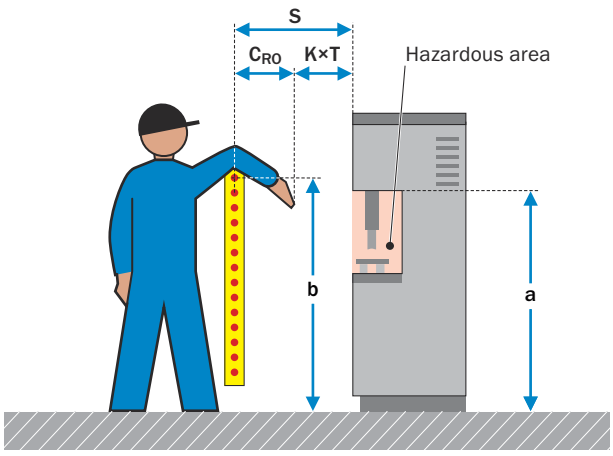


Figure 87: Parameters for determining the required minimum distance with possibility of reaching over

The following applies to the additional distance for reaching over and reaching through:

$C \geq C_{RO}$ (reaching over) and $C \geq C_{RT}$ (reaching through)

On the following pages you will find the table you need for each particular application, as per ISO 13855, and examples of how to use them.

How to determine the required height of the top edge of the protective field:

1. Determine the height of the hazardous point **a** and find the equivalent or next highest value in the left-hand column.
2. Calculate the supplement C_{RT} determined by the resolution using the familiar formulas for perpendicular approach:
   - ESPE, resolution d ≤ 40 mm: $C_{RT} = 8 \times (d - 14)$
   - ESPE, resolution d > 40 mm: $C_{RT} = 850$ mm
3. In the row defined by **a**, find the last column in which the shortest additional horizontal distance **C** is less than or equal to the calculated supplement C_{RT} determined by the resolution.
4. Read the resulting height **b** of the top edge of the protective field from the bottom row of the column determined in Step 2.

Table 42: Determining the required height of the top edge of the protective field according to ISO 13855

Height a of the hazardous area (mm)	**Additional horizontal distance C to the hazardous area (mm)**											
2 600	0	0	0	0	0	0	0	0	0	0	0	0
2 500	400	400	350	300	300	300	300	300	250	150	100	0
2 400	550	550	550	500	450	450	400	400	300	250	100	0
2 200	800	750	750	700	650	650	600	550	400	250	0	0
2 000	950	950	850	850	800	750	700	550	400	0	0	0
1 800	1 100	1 100	950	950	850	800	750	550	0	0	0	0
1 600①	1 150	1 150	1 100	1 000	900	850②	750	450	0	0	0	0
1 400	1 200	1 200	1 100	1 000	900	850	650	0	0	0	0	0
1 200	1 200	1 200	1 100	1 000	850	800	0	0	0	0	0	0
1 000	1 200	1 150	1 050	950	750	700	0	0	0	0	0	0
800	1 150	1 050	950	800	500	450	0	0	0	0	0	0
600	1 050	950	750	550	0	0	0	0	0	0	0	0
400	900	700	0	0	0	0	0	0	0	0	0	0
200	600	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0
	Height b of the top edge of the protective field (mm)											
	900	**1 000**	**1 100**	**1 200**	**1 300**	**1 400** ③	**1 600**	**1 800**	**2 000**	**2 200**	**2 400**	**2 600**
Example	• Resolution of the ESPE: > 40 mm • Height a of the hazardous area: 1 600 mm ① This gives a resolution-dependent supplement (C_{RT}) of 850 mm • The condition C ≥ C_{RO} and C ≥ C_{RT} is satisfied by the value C = 850 mm ② The height b of the top edge of the protective field of the ESPE must not be less than 1 400 mm ③. If this is not technically possible, the horizontal distance to the hazardous area must be increased.											

If the required height for the top of the protective field cannot be achieved, the C_{RO} supplement must be determined as follows:

1 Define the necessary height **b** of the top edge of the protective field (planned or existing ESPE) and find the equivalent or next lowest value in the bottom row.
2 Determine the height of the hazardous point **a** and find the value in the left-hand column. In the case of intermediate values, select the next row (higher or lower) producing the greater distance in Step 3.
3 Read the required horizontal distance **C** at the intersection between the two values.

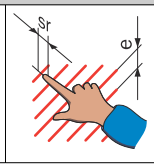
Table 43: Determining the supplement C_{RO} according to ISO 13855, if the required height of the top edge of the protective field cannot be achieved

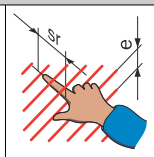
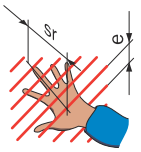
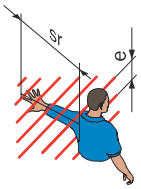
Height a of the hazardous area (mm)	**Additional horizontal distance C_{RO} to the hazardous area (mm)**											
2 600	0	0	0	0	0	0	0	0	0	0	0	0
2 500	400	400	350	300	300	300	300	300	250	150	100	0
2 400	550	550	550	500	450	450	400	400	300	250	100	0
2 200	800	750	750	700	650	650	600	550	400	250	0	0
2 000	950	950	850	850	800	750	700	550	400	0	0	0
1 800	1 100	1 100	950	950	850	800	750	550	0	0	0	0
1 600	1 150	1 150	1 100	1 000	900	850	750	450	0	0	0	0
1 400 ②	1 200	1 200	1 100 ③	1 000	900	850	650	0	0	0	0	0
1 200	1 200	1 200	1 100	1 000	850	800	0	0	0	0	0	0
1 000	1 200	1 150	1 050	950	750	700	0	0	0	0	0	0
800	1 150	1 050	950	800	500	450	0	0	0	0	0	0
600	1 050	950	750	550	0	0	0	0	0	0	0	0
400	900	700	0	0	0	0	0	0	0	0	0	0
200	600	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0
	Height b of the top edge of the protective field (mm)											
	900	**1000**	**1 100** ①	**1 200**	**1 300**	**1 400**	**1 600**	**1 800**	**2 000**	**2 200**	**2 400**	**2 600**
Example	• Three-beam standard ESPE (300/700/1 100 mm) • Height **b** of the top edge of the protective field: 1 100 mm ① • Height **a** of the hazardous area: 1 400 mm ② • C_{RO} supplement due to possible reaching over: 1 100 mm ③											

Safety distance for guards

Physical guards must be at an adequate distance from the hazardous area if they have openings. This requirement also applies to openings between a protective device and a machine frame, jigs, etc.

Table 44: Safety distance s_r depending on openings in physical guards according to ISO 13857

Part of the body		**Opening e (mm)**	**Safety distance s_r (mm)**		
			Slot	**Square**	**Circle**
Fingertip		e ≤ 4	≥ 2	≥ 2	≥ 2
		4 < e ≤ 6	≥ 10	≥ 5	≥ 5

Part of the body		Opening e (mm)	Safety distance s_r (mm)		
			Slot	Square	Circle
Finger up to wrist		6 < e ≤ 8	≥ 20	≥ 15	≥ 5
		8 < e ≤ 10	≥ 80	≥ 25	≥ 20
		10 < e ≤ 12	≥ 100	≥ 80	≥ 80
		12 < e ≤ 20	≥ 120	≥ 120	≥ 120
		20 < e ≤ 30	≥ 850	≥ 120	≥ 120
Arm up to shoulder		30 < e ≤ 40	≥ 850	≥ 200	≥ 120
		40 < e ≤ 120	≥ 850	≥ 850	≥ 850

Minimum distance for interlocked physical guards

For interlocked physical guards that initiate a stop, a minimum distance must also be observed analogous to the procedure for ESPE. Alternatively, locks with interlocking mechanisms may be used to prevent access until the hazard is no longer present.

Description of the parameters:

- **S**: Minimum distance in millimeters, measured from the nearest hazardous point to the nearest door opening point.
- **K**: Parameter in millimeters per second, derived from the data for the approach speeds of the body or parts of the body, usually 1,600 mm/s.
- **T**: Stopping/run-down time for the entire system in seconds.
- **C**: Safety distance (s_r, see table 44). This is necessary if it is possible to insert fingers or hands through the opening and towards the hazard zone before a stop signal is generated.

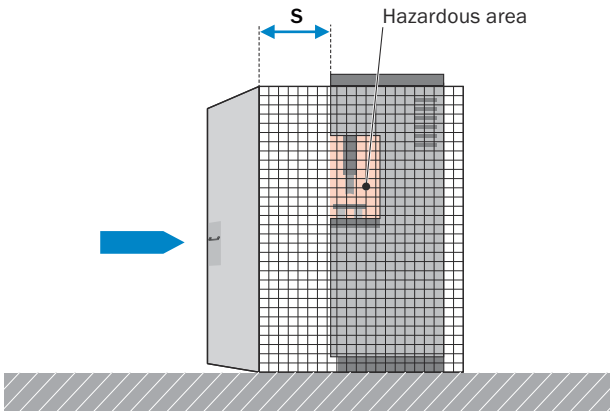


Figure 88: Minimum distance S for interlocked physical guards

General calculation formula
S = (K × T) + C

NOTE

➜ Calculation of the minimum distance for interlocked physical guards: ISO 13855 (type-B standard)

Required height for physical guards

Similar to the procedure for ESPE, the same procedure is also to be used for physical guards. Different calculation tables are to be used depending on the potential hazard.

To prevent crawling beneath physical guards, it is normally sufficient if the guards start at 180 mm above the reference level.

Required height of physical guards in case of low potential hazard according to ISO 13857

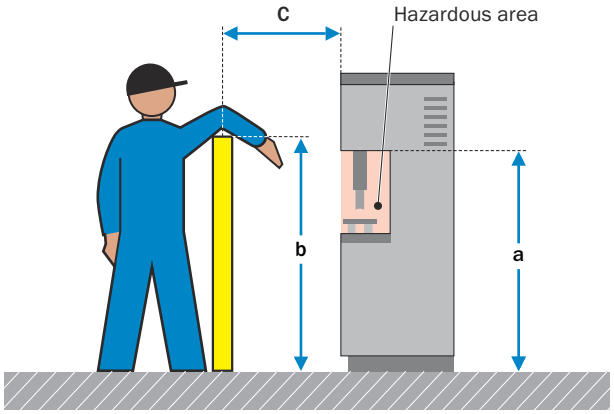


Figure 89: Parameters for determining the height requirements for guards

Table 45: Required height of physical guards in case of low potential hazard according to ISO 13857

Height a of the hazardous area (mm)	Horizontal distance C to the hazardous area (mm)								
2,500	0	0	0	0	0	0	0	0	0
2,400	100	100	100	100	100	100	100	100	0
2,200	600	600	500	500	400	350	250	0	0
2,000	1,100	900	700	600	500	350	0	0	0
1,800	1,100	1,000	900	900	600	0	0	0	0
1,600	1,300	1,000	900	900	500	0	0	0	0
1,400	1,300	1,000	900	800	100	0	0	0	0
1,200	1,400	1,000	900	500	0	0	0	0	0
1,000	1,400	1,000	900	300	0	0	0	0	0
800	1,300	900	600	0	0	0	0	0	0
600	1,200	500	0	0	0	0	0	0	0
400	1,200	300	0	0	0	0	0	0	0
200	1,100	200	0	0	0	0	0	0	0
0	1,100	200	0	0	0	0	0	0	0
	Height b of the physical guard (mm)								
	1,000	**1,200**	**1,400**	**1,600**	**1,800**	**2,000**	**2,200**	**2,400**	**2,500**

Required height of physical guards in case of high potential hazard according to ISO 13857

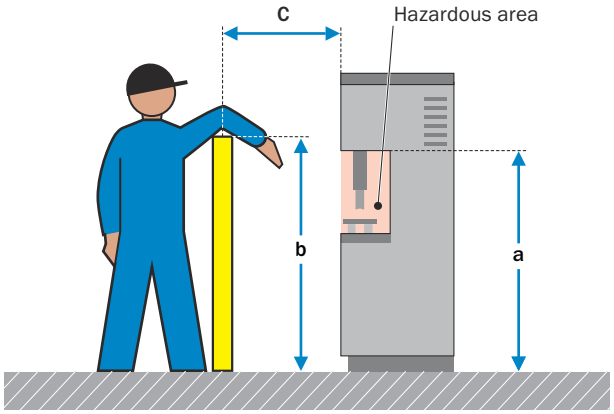


Figure 90: Parameters for determining the height requirements for physical guards

Table 46: Required height of physical guards in case of high potential hazard according to ISO 13857

Height a of the hazardous area (mm)	**Horizontal distance C to the hazardous area (mm)**									
2,700	0	0	0	0	0	0	0	0	0	0
2,600	900	800	700	600	600	500	400	300	100	0
2,400	1,100	1,000	900	800	700	600	400	300	100	0
2,200	1,300	1,200	1,000	900	800	600	400	300	0	0
2,000	1,400	1,300	1,100	900	800	600	400	0	0	0
1,800	1,500	1,400	1,100	900	800	600	0	0	0	0
1,600	1,500	1,400	1,100	900	800	500	0	0	0	0
1,400	1,500	1,400	1,100	900	800	0	0	0	0	0
1,200	1,500	1,400	1,100	900	700	0	0	0	0	0
1,000 ①	1,500	1,400	1,000	800	0 ②	0	0	0	0	0
800	1,500	1,300	900	600	0	0	0	0	0	0
600	1,400	1,300	800	0	0	0	0	0	0	0
400	1,400	1,200	400	0	0	0	0	0	0	0
200	1,200	900	0	0	0	0	0	0	0	0
0	1,100	500	0	0	0	0	0	0	0	0
	Height b of the physical guard (mm)									
	1,000	**1,200**	**1,400**	**1,600**	**1,800** ③	**2,000**	**2,200**	**2,400**	**2,500**	**2,700**
Example	The physical guard must therefore start at 180 mm above the reference level and end at 1,800 mm. If the height of the physical guard is to be 1,600 mm, the safety distance must be increased to at least 800 mm.									

Proceed as follows to determine the required height of the top edge of the physical guard for this safety distance:

1. Determine the height of the hazardous point **a** and find the value in the left-hand column, e.g., 1,000 mm.
2. In this row, find the first column in which the horizontal distance **C** is less than the safety distance calculated, e.g., the first field with the value “0”.
3. Read the resulting height **b** for the physical guard in the bottom row, e.g., 1,800 mm.

NOTE

➜ Safety distances and required protective field height: ISO 13857

Minimum distance for fixed position protective devices

If the two-hand control device is fitted to a portable stand, then the maintenance of the necessary minimum distance must be ensured by a distance ring or limited cable lengths (to prevent the operator impermissibly carrying the control into the hazardous area).

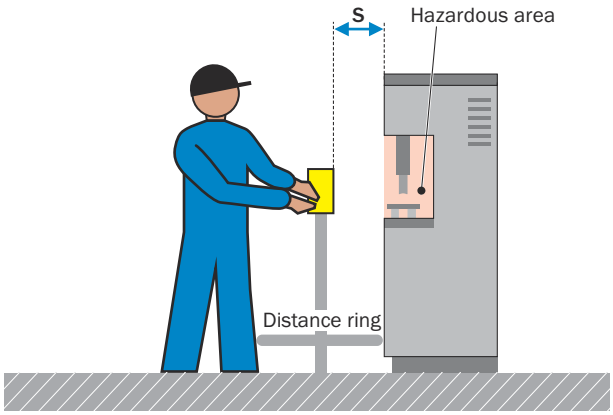


Figure 91: Minimum distance of a two-hand control device

Example: Minimum distance for two-hand control device
S = (K × T) + C

S Minimum distance in millimeters measured from the control to the nearest hazardous point

K Parameter in millimeters per second, derived from the data for the approach speeds of the body or parts of the body, usually 1,600 mm/s

T Stopping/run-down time of the overall system from when the control is released in seconds

C Supplement 250 mm. It might not be required under certain conditions (e.g., covering of the control switch).

NOTE

➜ Calculation of the minimum distance: ISO 13855 (type-B standard)

Application of reset and restart

If a protective device triggers a stop command, the stop status must be maintained until a safe state for a restart exists. The risk assessment may indicate that the stop status must only be ended by means of a manual, separate and intentional reset. The machine can be restarted in a further step.

The reset must be performed using a special operated device. The operated device must be able to withstand the foreseeable stresses and must be used properly to prevent unintentional actuation (touch panels may be unsuitable). Furthermore, the device must be installed in a safe location outside the hazardous area. The hazardous area must be fully visible from this location to ensure that no person is in the hazardous area.

The signal from the operated device must enable the controller to issue a separate start command for restarting. The signal processing must ensure that the restart can only take place if all safety functions and protective devices are functional.

ISO 13849-1 (section 5.2.2) therefore requires that resetting may only occur by releasing the command device from its actuated (ON) position and that the signal processing should detect the falling signal edge of the command device. This means that the acknowledgment must only occur by releasing the actuating element from its actuated (ON) position.

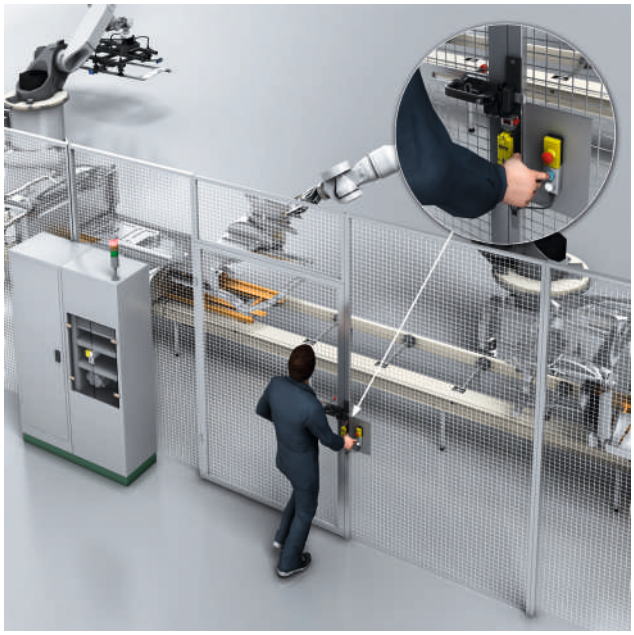


Figure 92: The position of the reset pushbutton allows a full view of the hazardous area when resetting the protective device.

Manual resetting is a safety function and must be implemented accordingly, e.g., by applying the ISO 13849-1 or IEC 62061 standards.

The signal (on actuation) of the reset device is part of the safety function. **One** of the following measures must therefore be implemented:

- The signal must be discretely wired to the safety-related logic unit.
- The signal must be transmitted via a safety-related bus system.

The reset shall not initiate any movement or hazardous situation. Instead, the machine control system shall only accept a separate start command after the reset.

An exception to the application of reset and restart exists if protective devices are used that allow continuous detection of at-risk persons in the hazardous area (e.g., presence detection).

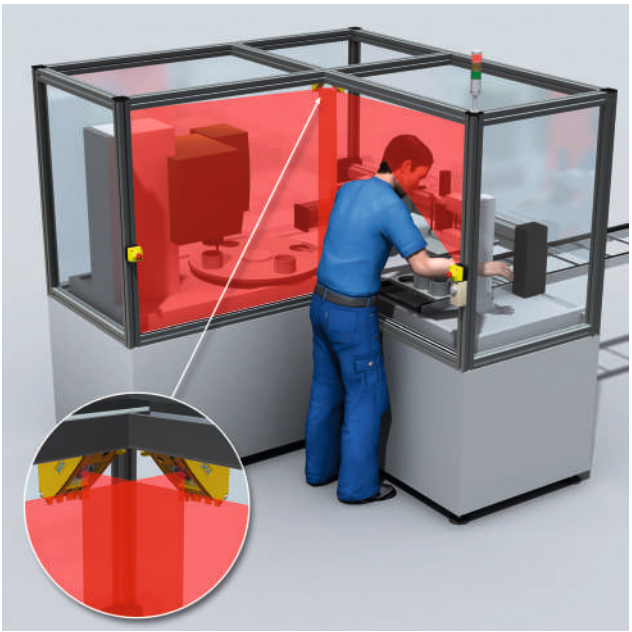


Figure 93: In this arrangement, it is not possible to remain in the hazardous area without being detected by the protective device. Therefore, a separate reset of the protective device is not necessary.

Integration of protective devices in the control system

Along with mechanical aspects, a protective device must also be integrated in the control system.

NOTE

"Control systems are functional assemblies that form part of the information system of a machine and implement logical functions. They coordinate the flows of material and energy to the area of action of the tool and workpiece system in the context of a task. [...] control systems differ in terms of the technology used, i.e., the information carriers, fluid, electrical and electronic control systems."

Translation of text from: Alfred Neudörfer: Konstruieren sicherheitsgerechter Produkte, Springer-Verlag, Berlin u. a., ISBN 978-3-642-33889-2 (5th Edition 2013)

The general term **control system** describes the entire chain of a control system. The control system comprises input elements, logic units, power control elements, and drive/actuator elements.

Safety-related parts of the control system are designed to perform safety functions. For this reason special requirements are placed on their reliability and their resistance to errors. They are based on the principles of preventing and controlling faults.

Table 47: Safety aspects of control systems with different operating principles. Translation of text from: Alfred Neudörfer: Konstruieren sicherheitsgerechter Produkte, Springer-Verlag, Berlin u. a., ISBN 978-3-642-33889-2 (5th Edition 2013)

Controller			**Aspects relating to safety technology**	
Principle of operation of the control system		**Typical devices**	**Interfering factors**	**Explanations**
Fluid	**Pneumatic** 	• Multiway valves • Vent valves • Manual shut-off valves • Filters with water trap • Hoses	• Changes in energy levels • Purity and water content of the compressed air	Mostly designed as electro-pneumatic control systems. Service unit necessary for conditioning compressed air.
	Hydraulic 	• Accumulators • Pressure limiters • Multiway valves • Filter • Level gages • Temperature gages • Hoses and cables • Threaded fittings	• Purity • Viscosity • Temperature of the pressurized fluid	Mostly designed as electrohydraulic control systems. Measures necessary to limit the pressure and temperature in the system and to filter the medium.
Electrical	**Electromechanical** 	• Control switches: o Position switch o Selector switches o Pushbuttons • Switching amplifiers: o Contactors o Relay o Circuit breakers	• Protection class of the devices • Selection, sizing and arrangement of components and devices • Design and routing of the cables	Due to their design and unambiguous switch settings, parts are insensitive to moisture, temperature fluctuations, and electromagnetic disturbances if selected correctly.
	Electronic 	• Individual components, for example: o Transistors o Resistors o Capacitors o Coils • Highly integrated devices, for example integrated circuits (IC)	As listed under “Electromechanical”. In addition: • Temperature fluctuations • Electromagnetic disturbances coupled via cables or fields	Exclusion of faults not possible. Reliable action can only be achieved using control system concepts, not through the selection of components.
	Microprocessor-controlled 	• Microprocessors • Software	• Installation fault in the hardware • Systematic errors including common cause errors • Programming faults • Handling faults • Operating error • Manipulation • Malware	• Measures to prevent faults: o Structured design o Program analysis o Simulation • Measures to control faults: o Redundant hardware and software o RAM/ROM test o CPU test

The safety-related input elements have been described above with the safety sensors (protective devices). For this reason only the logic unit and the power control elements are described below.

Errors and failures in drive/actuator elements are normally excluded.

Fluid control systems are often implemented as electropneumatic or electrohydraulic control systems. In other words, the electrical signals are converted to fluid energy by valves to move cylinders and other power control elements.

Logic units

In a logic unit, different input signals are linked to output signals. Electromechanical, electronic, or programmable electronic components are often used for this purpose.

NOTICE
Depending on the required reliability, the signals from the protective devices shall not be processed only by standard control systems. There must, if necessary, also be parallel cut-off paths.

Logic unit: basic construction with auxiliary contactors

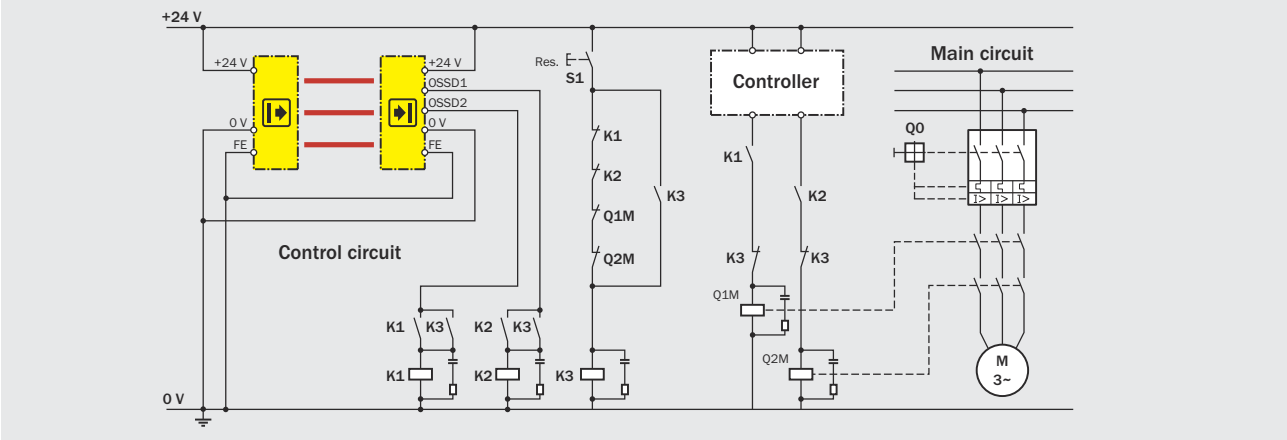


Figure 94: Circuit design for a safety-related logic unit with contactors

Using individual auxiliary contactors with positively guided contacts, it is possible to design control functions with any level of complexity. Redundancy and monitoring by positively guided contacts are features of this safety principle. Wiring provides the logical operators.

Function: If the contactors K1 and K2 are de-energized, on pressing S1 the K3 contactor is energized and remains energized. If no object is detected in the active protective field, the outputs OSSD1 and OSSD2 are conducting voltage. The contactors K1 and K2 are energized by the normally open contacts on K3 and latch. K3 is de-energized by releasing S1. Only then are the output circuits closed. On detection of an object in the active protective field, the K1 and K2 contactors are de-energized by the OSSD1 and OSSD2 outputs.

Logic unit as safety relay (safety/relay combination)

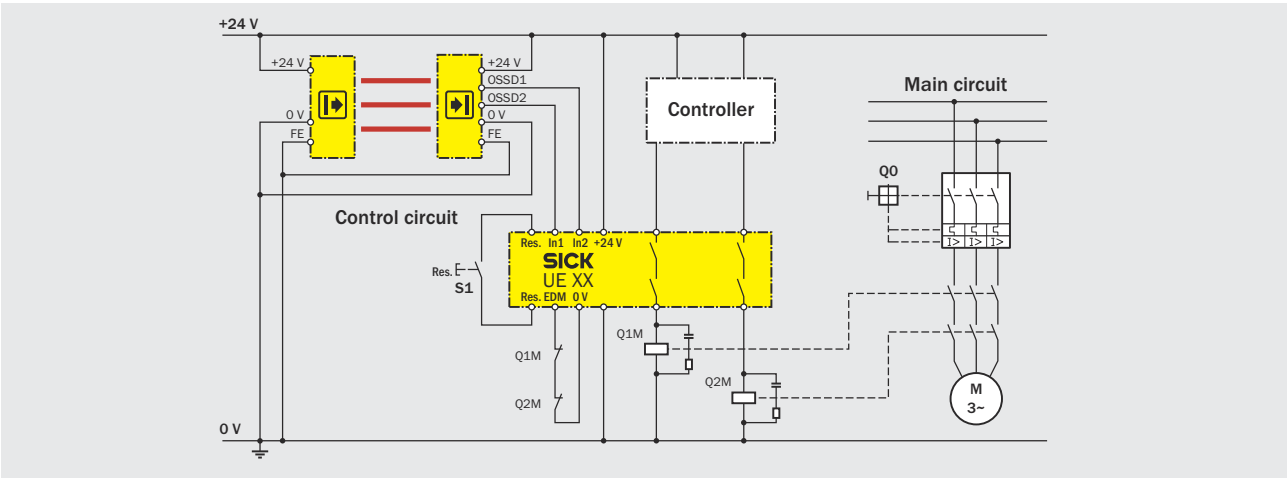


Figure 95: Circuit design for a safety-related logic unit with safety relay

Safety relays combine one or more safety functions in one housing. They generally also have automatic monitoring functions. The cut-off paths can be set up based on contact or using semiconductors. They can also have signaling contacts.

Building more complex safety applications is simplified by integrating multiple functions into one device. The certified safety relay also reduces the time and effort involved in validating the safety functions. In safety relays, semiconductor elements can perform the task of the electromechanical switching elements instead of relays. Using measures to detect faults such as the sampling of dynamic signals or measures to control faults such as multiple channel signal processing, purely electronic control systems can achieve the necessary degree of reliability.

Logic unit with software-based components

Similar to automation technology, safety technology has developed from hard-wired auxiliary contactors through safety relays (some with configurable safety logic for which parameters can be set) to complex fail-safe PLCs. The concept of “proven components” and “proven safety principles” must be transferred to electrical and programmable electronic systems.

The logical operators for the safety function are implemented in the software. Software is to be differentiated from firmware — developed and certified by the manufacturer of the control device — and the actual safety application, which is developed by the machine manufacturer using the functionality supported by the firmware.

The choice and adjustment of the functions of logic units is offered in different levels of flexibility:

- Parameterization
- Configuration
- Programming

Parameterization

Is the selection of properties from a defined pool of functionality by selector switch/software parameters at the time of commissioning.
Features: low logic depth, AND/OR logic

Configuration

Flexible operators for defined function blocks in certified logic with a software-supported configuration interface, parameterization of times and configuration of the inputs/outputs of the control system, for example.
Features: any logic depth, binary logic

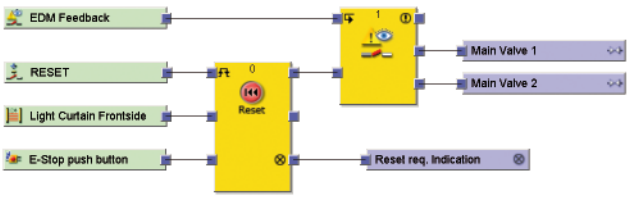


Figure 96: Example of linking the function blocks of a software-supported logic unit

Programming

Defines the logic as required using the functionality defined by the predefined programming language, mostly using certified function blocks.
Features: any logic depth, word level

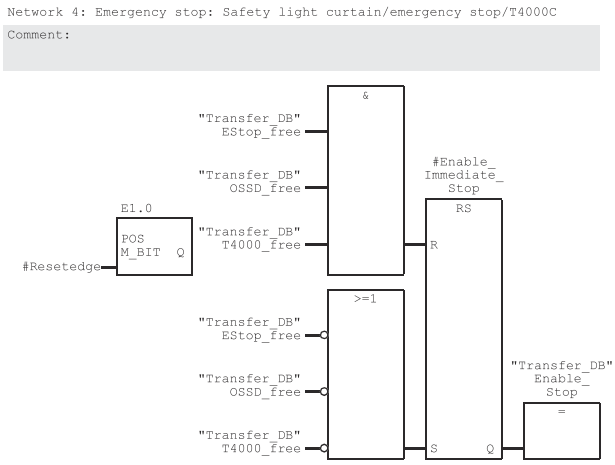


Figure 97: Example of linking logic blocks and function blocks when programming a function

Reliable data transmission

Bus systems are used to transmit signals between the control system and sensors or power-controlling elements on the machine. Bus systems are also responsible for the transmission of states between different parts of control systems. A bus system makes wiring easier and as a result reduces the possible errors. It is reasonable to use bus systems already used in the market for safety-related applications.

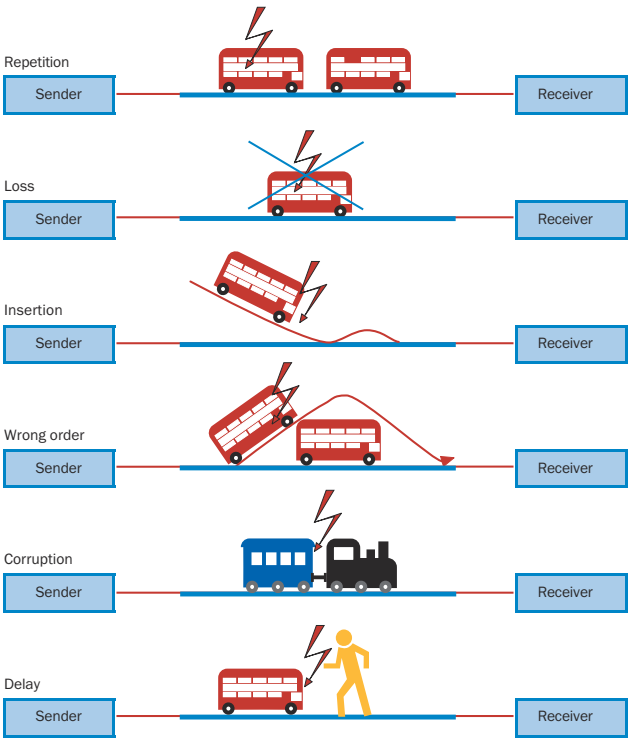
An examination of the hardware and software errors that arise in transmission systems shows that these errors lead to the following transmission errors in bus systems:

- Repetition
- Loss
- Insertion
- Wrong sequence
- Corruption
- Data delay

Transmission errors can be avoided using various measures in the higher-level control system, e.g., by sequential numbering of the safety-related telegrams or a time expectation for incoming telegrams with acknowledgment. Protocol extensions based on the field-bus used include such measures.

In the ISO/OSI layer model, they act over the transport layer and, therefore, use the field-bus with all its components as a “black channel”, without modification. Examples of established safe bus systems are:

- Actuator Sensor Interface Safety at Work
- DeviceNet CIP Safety™
- PROFIsafe



Source: Safety in Construction and Design of Printing and Paper Converting Machines – Electrical Equipment and Control Systems, BG Druck- und Papierverarbeitung (today BG ETEM); Edition 06/2004; page 79

Figure 98: Transmission errors of bus systems.

Selection criteria

The criteria for the selection of a control system model are initially the number of safety functions to be implemented as well as the scope of the logical operators on the input signals.

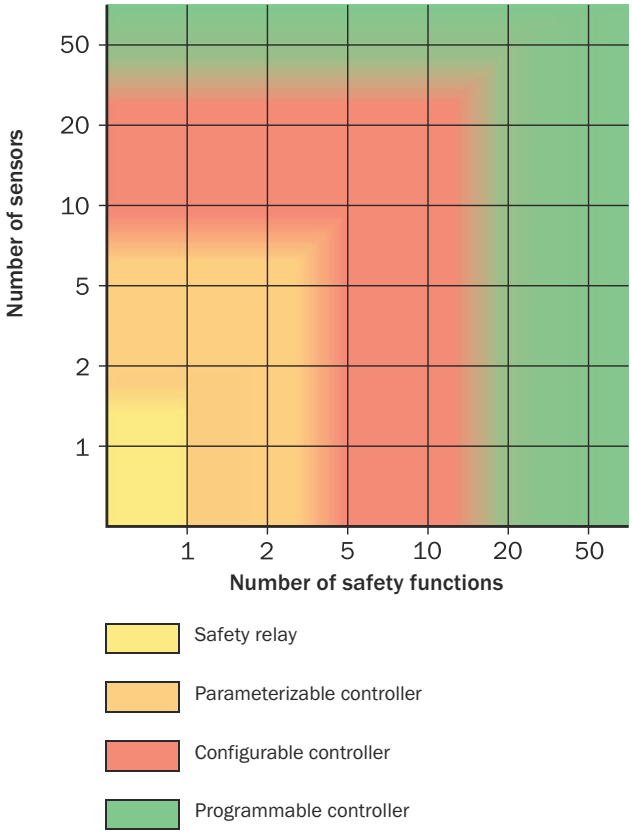


Figure 99: Illustration of the preferred fields of application of safe control technologies depending on the number of sensors and safety functions

The functionality of the logical operators — e.g., simple AND, Flipflop, or special functions such as muting — also affects the selection.

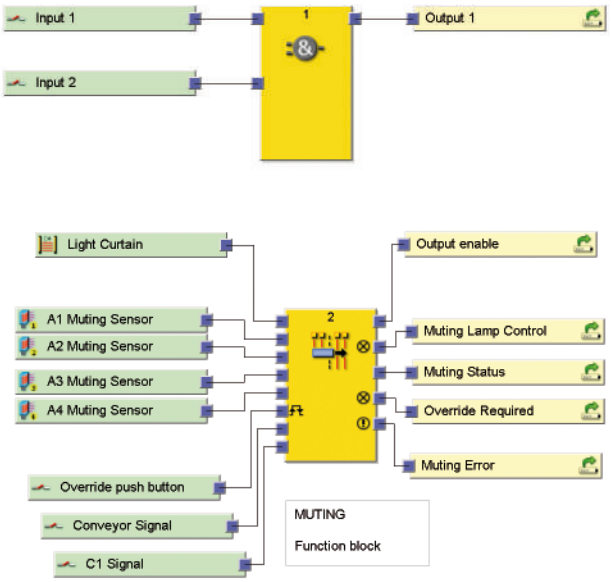


Figure 100: Example of a safe software function block for muting with inputs and outputs

Software specification

To prevent the occurrence of a dangerous state, software-based logic units in particular shall be designed so that they can be relied upon to prevent errors in the logic. To detect systematic errors, a thorough systematic check should be made by someone other than the designer and thus the principle of counter-checking by a second person applied.

A simple way of implementing this specification is the so-called **design matrix**. Here certain combinations of safety-related input signals for specific cases (e.g., “position lost”, or “robot left”) are combined. These cases shall act on the machine functions via the safety-related outputs in accordance with the requirements of the safety function. This simple method is also used by SICK during the design of application software.

It is advisable to have this reviewed by all involved in the project.

In the case of programs that are poorly documented and unstructured, errors occur during subsequent modifications; in particular, there is a risk of unknown dependencies or side effects, as they are often referred to. When the software is developed externally, good specifications and program documentation are very effective in avoiding faults.

Design Matrix

0 = Logical 0 or OFF
S = Enable (restart)
I = Logic 1 or ON
– = any status

	Case \ Effect	Safety outputs: Robot	Table on left	Table on right	...	...
Safety inputs	Position lost	0	–	–		
	Robot left	S	–	–		
	Robot right	S	–	–		
	Robot center	S	–	–		
	Access left	S	I	–		
	Access right	–	–	I		
	Emergency stop	0	0	0		
	...					

Figure 101: Example of a design matrix as an aid in the development of safety functions

Power control elements

The safety function initiated by the protective devices and the logic unit shall stop dangerous machine functions. For this purpose, the drive/actuator elements are switched off by power control elements.

NOTE

➜ Principle of switch off/power shutdown: ISO 13849-2 (type-B standard)

Contactors

Electromechanical contactors are the most commonly used type of power control element. One or more contactors can form a safety function subsystem by combining special selection criteria, wiring, and technical measures. By protecting the contacts against overcurrent and short-circuits, over-sizing (normally by a factor of 2) and other measures, a contactor is considered a proven component. To be able to perform diagnostics on contactors for safety functions, unambiguous feedback of the output state is necessary (EDM = external device monitoring). This requirement can be met using a contactor with positively guided contacts. The contacts are positively guided when the contacts in a set of contacts are mechanically linked in such a way that normally open contacts and normally closed contacts can never be closed simultaneously during at any point during the intended mission time.

The term “positively guided contacts” refers primarily to auxiliary contactors and auxiliary contacts. A defined distance between the contacts of at least 0.5 mm at the normally closed contact must be ensured even in the event of a fault (welded N/O contact). Since on contactors with low switching capacity (< 4 kW) there is essentially no difference between the main contact elements and the auxiliary contact elements, it is also possible to use the term “positively guided contacts” to refer to those small contactors.

On larger contactors, what are known as “mirror contacts” are used: While a main contact on a contactor is closed, no mirror contact (auxiliary normally closed contact) is allowed to be closed. A typical application for mirror contacts is the highly reliable monitoring of the output state of a contactor in control circuits on machines.

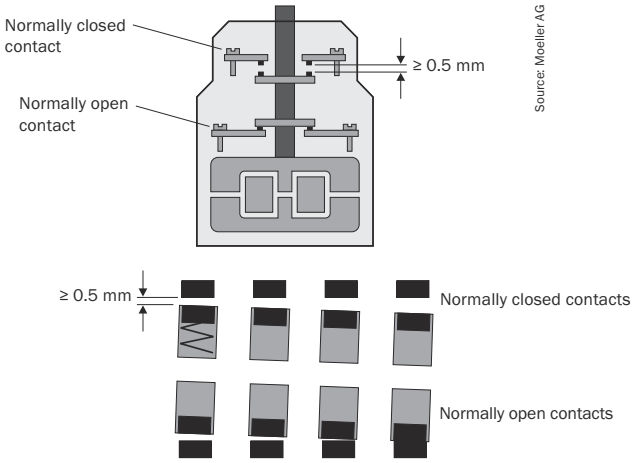


Figure 102: Contact system of a contactor with positively guided contacts. A normally-open contact is welded.

Suppressor elements

Inductances such as coils on valves or contactors must be equipped with a suppressor to limit transient voltage spikes on shutdown. In this way the switching element is protected against overload (in particular against overvoltage on particularly sensitive semiconductors). As a rule, such circuits have an effect on the release delay and, therefore, on the required minimum distance of the protective device (see "Approaches to calculating the minimum distance", page 100). A simple diode for arc suppression can result in a release (switch to OFF) time up to 14 times longer.

Table 48: Example diode suppressors for limiting transient overvoltages

Suppressor elements (via inductance)	Diode	Diode combination	Varistor	RC element
				
Protection against overvoltage	Very high	High	Limited	High [1]
Release delay (delay in switching OFF)	Very long (relevant to safety)	Short (but must be taken into account)	Very short (not relevant to safety)	Very short [1] (not relevant to safety)

1) The element must be exactly matched to the inductance!

Drive technology

When considering safety functions, drives represent a central sub-function, as they pose a risk of unintentional movement, for example.

The safety function extends from the sensor to the power-controlling element.

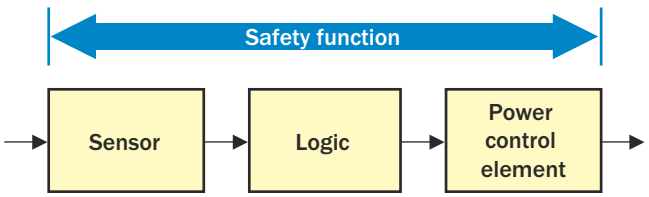


Figure 103: Elements of a safety function

The power control element can comprise several components (contactor, drives, feedback), depending on the technical design and safety function. Braking systems and holding systems are also to be taken into account on axes subject to gravity.

The actual motor is not part of the assessment.

Servo amplifiers and frequency inverters

In drive technology, three-phase motors with frequency inverters have largely replaced DC drives. The inverter generates an output voltage of variable frequency and amplitude from the fixed three-phase mains. Depending on design, regulated rectifiers can feed the energy absorbed by the intermediate circuit during braking back to the mains.

The rectifier converts the electrical power supplied from the mains and feeds it to the DC intermediate circuit. To perform the required control function, the inverter forms a suitable revolving field for the motor using pulse-width modulation and semiconductor switches. The usual switching frequencies are between 4 kHz and 12 kHz.

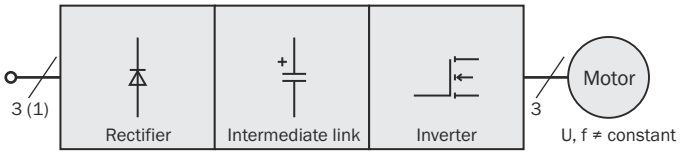


Figure 104: Design of circuits with servo and frequency converters

To limit transient overvoltages caused by switching loads in DC and AC circuits, interference suppression components are to be used, in particular if sensitive electronic assemblies are being used in the same control cabinet.

Checklist

- Mains filter fitted to the frequency inverter?
- Sinusoidal filter fitted to the output circuit on the inverter?
- Connection cables as short as possible and shielded?
- Components and screens connected to earth/equipment earthing conductor using large area connections?
- Commutation choke connected in series for peak current limiting?

Safety functions on servo amplifiers and frequency inverters

Different cut-off paths are possible when implementing the safety function:

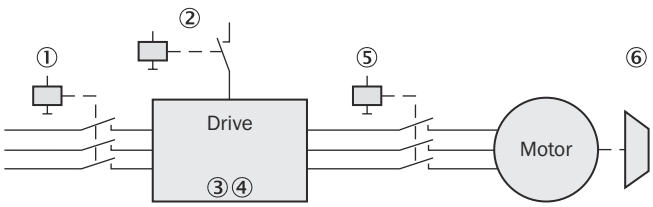


Figure 105: Safety-relevant elements and functions for circuits with servo and frequency inverters

① Mains contactor – poor due to long re-energization time, high wear due to the current on the switch
② Controller enable – not safety-related
③ Pulse inhibit “safe restart interlock (stop)”
④ Setpoint – not safety-related
⑤ Motor contactor – not allowed on all inverters
⑥ Retaining brake – normally not a functional brake

The contribution of the drive to the safety function can be implemented in various ways:

- By disconnecting the supply of power, e.g., using a mains contactor ① or a motor contactor ⑤
- By external monitoring circuits, e.g., by monitoring an encoder
- By safety sub-functions integrated directly in the drive ("Safety sub-functions integrated in the drive", page 121)

Disconnection of the supply of power

When using inverters, the energy stored in the intermediate circuit's capacitors and the energy produced by a regenerative braking process must be taken into account in the risk assessment.

During the consideration of the residual travel, it is to be assumed that the motion control system does not initiate a brake ramp. After shutdown, the drive continues running at more or less the same speed, depending on the friction (stop category 0). The use of a brake ramp by changing the setpoint and/or controller enable and subsequent shutdown of the contactor or the pulse inhibit (stop category 1) can reduce the braking distance.

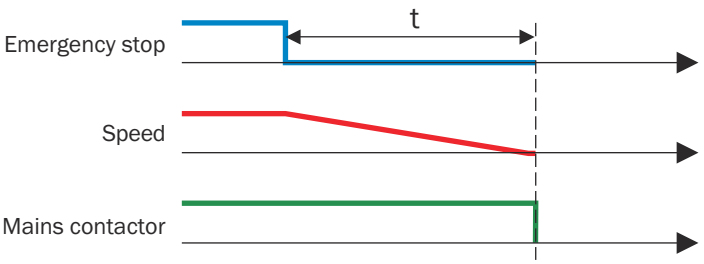


Figure 106: Disconnection of the supply of power by the mains contactor after emergency stop and initiation of a braking ramp

Speed detection with external monitoring units

To monitor the drive, external monitoring units require various signals providing information about the current movement parameters. In this case the signal sources are sensors and encoders. These must either be designed as safe sensors or with redundancy, depending on the required safety level PL or SIL.

Alternatively, standstill monitoring can also be implemented by reading back the voltage induced by the motor coasting down. This technique also functions with speed-controlled drives.

Safety sub-functions integrated in the drive

Safety functions are implemented by safety-related parts of control systems (SRP/CS). They include the sub-functions of measuring (sensor), processing (logic unit), and switching or actuation (power control element). In this context, safety-related functions integrated in the drive are to be considered safety sub-functions.

They are generally divided into two groups:

- Safety-related stopping and braking functions: These functions are used to stop the drive safely (e.g., safe stop).
- Safe monitoring functions: These functions are used for the safe monitoring of the drive during operation (e.g., safely reduced speed).

In general, the drive monitoring functions necessary depend on the application. Boundary conditions include parameters such as the necessary braking distance, the presence of kinetic energy, etc.

The shutdown response varies depending on the selected safety sub-function. For example, on a stop request, safe torque off (STO) results in uncontrolled coasting down of the movement. During a safe stop (SS1 or SS2), controlled retardation is initiated. A combination of element functions may also need to be implemented as a suitable measure.

Possible interfaces for the implementation of safety sub-functions integrated directly in the drive are:

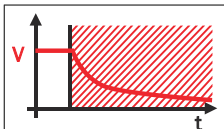
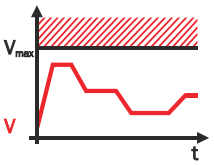
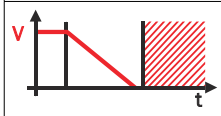
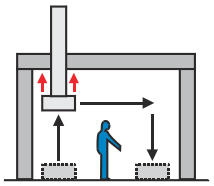
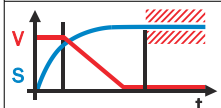
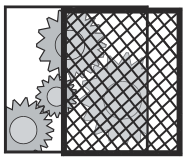
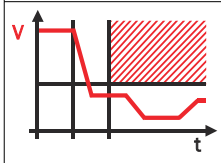
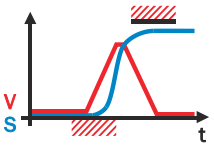
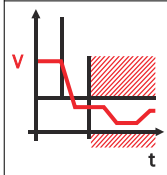
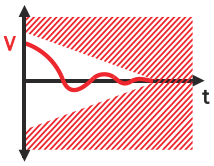
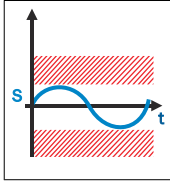
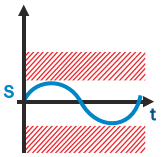
- Discrete 24-V signals
- Control communication (channel 1)/24 V discrete (channel 2)
- Safe communication systems (field-bus systems/network interface)

In control communication, a setpoint for speed or position is transmitted from the standard controller to the drive; via a non-safety fieldbus or a network.

The majority of safety sub-functions for variable speed drives available today are specified in the harmonized standard IEC 61800-5-2 “Adjustable speed electrical power drive systems”, Part 5-2 “Safety requirements – Functional safety”. Drives that meet this standard can be used as safety-related parts of a control system in accordance with ISO 13849-1 or IEC 62061.

Safety functions of servo drives according to IEC 61800-5-2

Table 49: Safety functions of servo drives according to IEC 61800-5-2. Source: Bosch Rexroth AG

	Safe torque Off (STO) • Corresponds to stop category 0 according to IEC 60204-1 • Uncontrolled stopping by means of immediate interruption of the supply of power to the actuators • Safe restart interlock: prevents unexpected starting of the motor		Safe maximum speed (SMS) [1] • Safe monitoring of the maximum speed independent of the operating mode
	Safe stop 1 (SS1) [2] • Corresponds to stop category 1 according to IEC 60204-1 • Controlled stopping while maintaining the supply of power to the actuators • After stopping or below a speed limit: Activation of the STO function • Optional: Monitoring of a brake ramp		Safe braking and holding system (SBS) [1] • The safe braking and holding system controls and monitors two independent brakes.
	Safe stop 2 / safe operating stop (SS2, SOS) [2] • Corresponds to stop category 2 according to IEC 60204-1 • Controlled stopping while maintaining the supply of power to the actuators • After standstill: Safe monitoring of the drive shaft position in defined range		Safe door locking (SDL) [1] • The door lock is only unlocked if all drives in a protected area are in the safe state.
	Safely-limited speed (SLS) • If an enable signal is given, a safely reduced speed is monitored in a special operating mode. • If the speed is exceeded, a safe stop function is triggered.		Safely limited increment (SLI) • If an enable signal is given, a safely limited increment is monitored in a special operating mode. • Then the drive is stopped and remains in this position.
	Safe direction (SDI) • In addition to the safe movement, a safe direction (clockwise/counterclockwise) is monitored.		Safely monitored deceleration (SMD) [1] • Safe monitoring of deceleration on stopping with predetermining behavior
	Safely monitored position (SLP) [1] • In addition to the safe movement, a safe absolute position range is monitored. • If the limits are infringed, the drive is shut down via one of the stop functions (pay attention to overrun).		Safely limited position (SLP) • Monitoring of safe software switches

1 Not defined in IEC 61800-5-2.
2 Unsafe braking: If a brake ramp has not been defined, then motor acceleration during the delay will not be detected

NOTE
➜ Functional safety of power drives IEC 61800-5-2 (type-B standard)

Fluid control systems

Valves

All valves contain moving switching elements (piston slide, plunger, seat, etc.) which, due to their function, are subject to wear.

The most frequent causes of the safety-related failure of valves are:

- Failure of functional elements of the valve (reset function, switching function, sealing function)
- Contamination of the fluid

Contamination constitutes unintended use and generally leads to malfunctions. A general rule for all valves is that contamination leads to premature wear, thus negating the essential prerequisites used for design and dimensioning based on a defined probability of failure.

The mechanical springs for the reset function used in monostable valves are generally designed for high endurance and can be considered proven in accordance with ISO 13849-2. However, exclusion of failure in the event of the springs breaking is not possible.

An important differentiating factor between the valves is the design of the moving switching element inside the valve.

The failure mode for each valve is essentially determined by its design. Poppet valves might leak, but in piston valves, the piston slide might jam.

With a poppet valve, the switching function is effected by the moving switching element (valve plate), which changes position relative to a seat inside the housing. This design enables large cross-sections to be released with short strokes. The risk of leaks can be excluded with an appropriate design.

In the case of piston valves, the valve body closes or opens the flow path by moving over a bore or circumferential groove. The changes in the cross-section of the piston slide relative to the changes in cross-section inside the housing affect volume flow and are known as control edges. An essential feature of this valve design worthy of note is what is known as the lap. The lap is the longitudinal distance between the stationary and moving control edges of the slide valve. Due to the gap between the piston and the housing bore required for hard-sealing valves, a leak will occur in the event of a pressure differential.

Safety-related design principles

For the safety-related use of valves, feedback of the valve position may be necessary.

Here various techniques are used:

- Reed switches that are actuated by a magnet fixed into the moving valve body
- Inductive proximity switches that are actuated directly by the moving switching element of the valve
- Analog position detection of the moving switching element of the valve
- Pressure measurement downstream of the valve

In the case of electromagnetically actuated valves, like a contactor, the solenoid requires a suppressor. In terms of safety as defined in ISO 13849, valves are defined as power control elements. The failure of drives/work elements must also be considered according to the possible repercussions.

Figure 107: Valve with position monitoring

Filter concept

The vast majority of failures of fluid control systems are due to disturbances related to contamination of the related fluid. The two main causes are:

- Contamination that occurs during assembly = assembly contamination (e.g., chips, mold sand, fibers from cloths, basic contamination)
- Contamination that occurs during operation = operating contamination (e.g., ambient contamination, component abrasion)

These contaminations must be reduced to an acceptable degree with the aid of filters.

For this purpose, a filter concept must be developed that defines the filter principle and its installation location. The filter concept must be designed so that it is able to retain in the filter the contamination added to the entire system in such a way that the required purity is maintained throughout the operating time.

NOTE

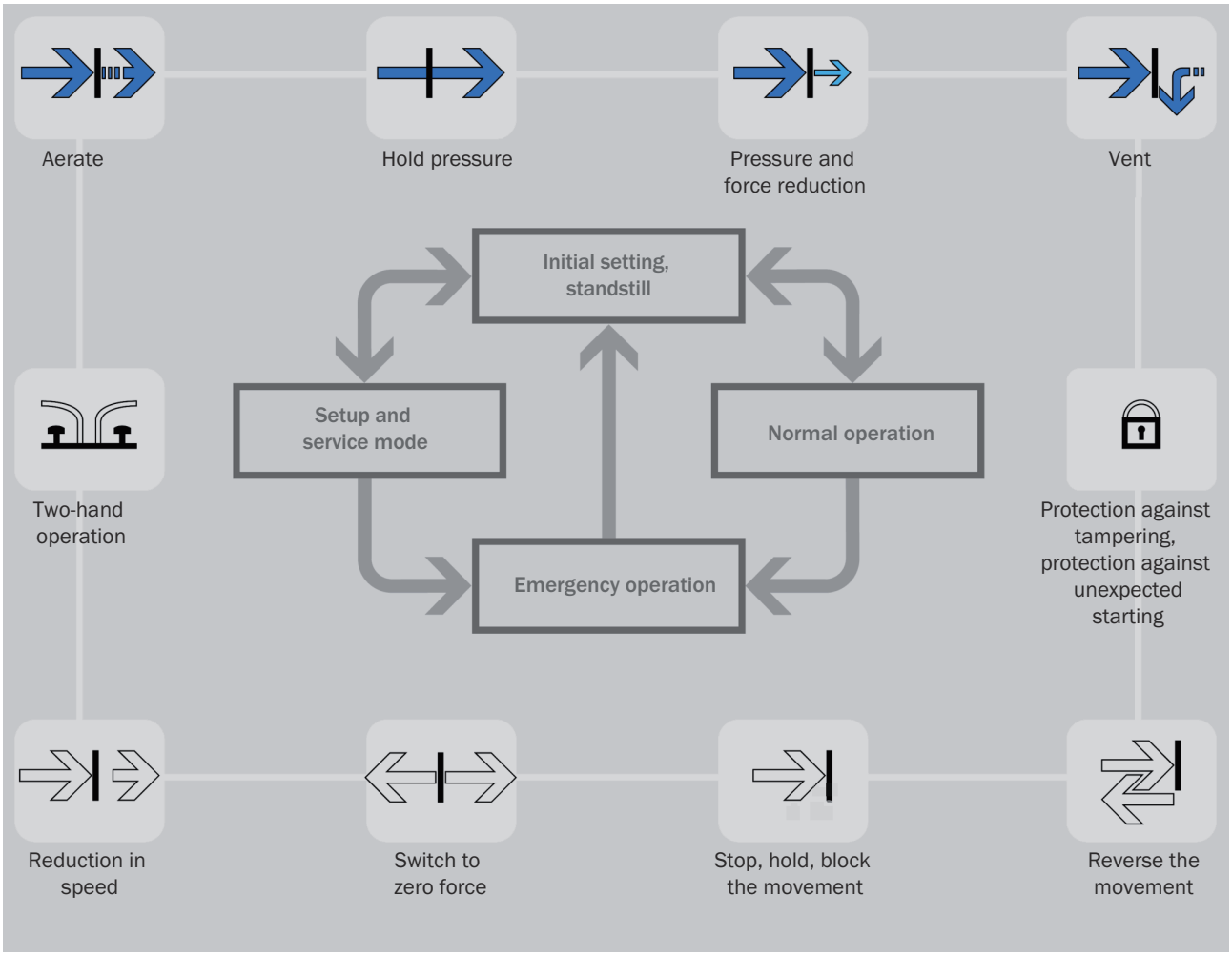
➜ Proven safety principles: ISO 13849-2 (type-B standard)

➜ Safety-related requirements on hydraulic/pneumatic systems: ISO 4413, ISO 4414

➜ Aging process on hydraulic valves: BIA Report 6/2004 ISBN 3-88383-672-9

Safety-related pneumatics

Electropneumatic control systems use a logic unit to implement safety functions. The logic unit provides electrical signals that act on the drive/actuators via a combination of a number of valves; these valves act as power control elements. Typical safety-related functions can be allocated to a machine's operating modes as safety sub-functions. Purely pneumatic control systems exist alongside electropneumatic control systems. The advantage of these solutions is that the deterministic nature of the pneumatics makes it relatively easy to set up safety sub-functions that are purely pneumatic.



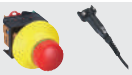
Direct pneumatic effect on movement
Indirect pneumatic effect on movement

Source: Festo SE & Co. KG – Safety Technology Guidelines

Figure 108: Control circuit with pneumatic safety sub-functions

Overview of safety technology products

Table 50: Products for functional safety from SICK

Sensors	Logic	Power control elements
Electro-sensitive protective equipment Safety light curtains  Safety camera systems  Multiple light beam safety devices  Single-beam safety devices  Safety laser scanners  Safety multibeam scanner 	 Safety relays	 Electrical drives with element safety sub-functions [1]  Safety pneumatic valves [2]
Interlocking devices With seperate actuator  With actuator for locking devices  For switching cam, turning lever  Magnetically coded  RFID coded  Inductive 	 Safety controllers and Motion Control	 Contactors [3]  Frequency Inverters [4]  Brakes [2]  Pneumatic Valves [1]  Hydraulic Valves [1]
Emergency stop pushbutton enabling switch 	 Safe sensor cascade	
Motor feedback system, encoder 		
Photoelectric switches, magnetic and inductive sensors 		

Service solutions from SICK

With the approval of: 1) Bosch Rexroth AG, 2) FESTO SE & Co. KG, 3) Eaton Industries GmbH, 4) SEW-EURODRIVE GmbH & Co. KG.

NOTE

➜ All SICK products and service solutions are listed in our online product finder at www.sick.com.

Summary: Designing the safety function

General

- Develop a concept for the required safety functions. In this concept, consider the characteristics of the machine, design, surroundings, protective device, and also take into account human characteristics.
- Design appropriate safety functions for the required safety level. Safety functions comprise sensor, logic, and power control element subsystems.
- Determine the safety level of each subsystem based on safety aspects (structure, reliability, diagnostics, resistance, process conditions).

Properties and application of protective devices

- Determine the necessary properties for your protective device. Do you need, for example, one or more electro-sensitive protective devices (ESPE), physical guards, movable physical guards or position fixing protective devices?
- Determine the correct positioning and dimensions for each protective device, in particular the safety distance (minimum distance) and the necessary protective field size/height for the protective device concerned.
- Integrate the protective devices as stated in the instruction handbook and as necessary for the level of safety.

Logic units

- Choose a suitable logic unit based on the number of safety functions and the logic depth.
- Use certified function blocks and keep your design clear.
- Have the design and the documentation thoroughly checked (principle of counter checking by a second person).

3d – Verifying the safety function

During verification, analyses and/or checks are carried out to demonstrate that the safety function meets the objectives and requirements of the specification in all aspects.

Verification essentially involves the following:

- Verification of physical guards
- Verification of functional safety
- Verification of the design of non-physical guards

Verification of physical guards

In the case of physical guards, the design must be checked to ascertain whether the devices meet requirements with regard to separation or distancing from hazardous points and/or requirements with regard to the restraining of ejected parts, hazardous substances or radiation. Particular attention should be paid to compliance with ergonomic requirements.

This is to ensure that the protective device provides the protection that meets the requirements.

Separating and/or distancing effect

- Sufficient safety distance and dimensioning (reaching over, reaching under, etc.)
- Suitable mesh size or grid spacing for fence elements
- Sufficient rigidity and suitable mounting
- Selection of suitable materials
- Safe setup
- Resistance to aging
- Design of the guard prevents climbing on the guard

Restraining of ejected parts, hazardous substances or radiation

- Sufficient rigidity, impact resistance, fracture strength (retention)
- Sufficient retention for the prevailing type of radiation, in particular where thermal hazards are concerned (heat, cold)
- Suitable mesh size or grid spacing for fence elements
- Sufficient rigidity and suitable mounting
- Selection of suitable materials
- Safe setup
- Resistance to aging

Ergonomic requirements

- Suitable transparency (so that machine operation can be observed)
- Setup, color, aesthetics
- Handling (weight, actuation, etc.)

Verification of non-physical guards

Depending on the type of non-physical guard (safety light curtains, pressure sensitive mats, ...), different systematic properties must be verified.

The effectiveness of a non-physical guard can be tested with the help of a checklist.

Table 51: Example checklist for the manufacturer or equipment supplier when installing non-physical guards (e.g., an ESPE)

Checklist			
1	Have adequate measures been taken to prevent access to hazardous areas or hazardous points or can they only be accessed via safeguarded areas (ESPE, protective doors with interlocking device)?	Yes ☐	No ☐
2	Have appropriate measures been taken to prevent the undetected presence of persons in the hazardous area (mechanical protection) or to detect the presence of persons (protective devices), and have these devices been secured or locked to prevent their removal?	Yes ☐	No ☐
3	Do the protective devices conform to the required reliability level (PL or SIL) for the relevant safety functions?	Yes ☐	No ☐
4	Has the maximum overrun (stopping time) of the respective dangerous machine functions been measured and are these times specified and documented (either on the machine or in the operating instructions)?	Yes ☐	No ☐
5	Have the required safety or minimum distances of protective devices to the nearest hazardous points been maintained?	Yes ☐	No ☐
6	Have effective measures been taken to prevent reaching under, reaching over, climbing under, climbing over, or reaching around the protective devices?	Yes ☐	No ☐
7	Have the protective devices or switches been properly mounted and secured against manipulation after adjustment?	Yes ☐	No ☐
8	Are the required protective measures against electric shock in effect (protection class)?	Yes ☐	No ☐
9	Are the control switches for resetting protective devices present and located in such a way that they cannot be actuated from inside the hazardous areas?	Yes ☐	No ☐
10	Are the components used for the protective devices integrated in accordance with the manufacturer's instructions?	Yes ☐	No ☐
11	Are the given safety functions effective at every setting of the operating mode selector switch?	Yes ☐	No ☐
12	Are the protective devices effective during the entire time in which the machine functions to be safeguarded are taking place?	Yes ☐	No ☐
13	Once initiated, will the dangerous machine functions be ceased when switching the protective devices off or when changing the operating mode, or when switching to another protective device?	Yes ☐	No ☐
14	Are the instructions for the operator, that are supplied with the protective device, attached in a clearly visible manner?	Yes ☐	No ☐

Verification of functional safety

Machine-specific type-C standards and some type-B standards require a target level for safety functions. There are two different methods for determining the level of safety achieved:

- Determining the performance level (PL) achieved as per ISO 13849-1
- Determining the safety integrity level achieved (SIL) according to IEC 62061

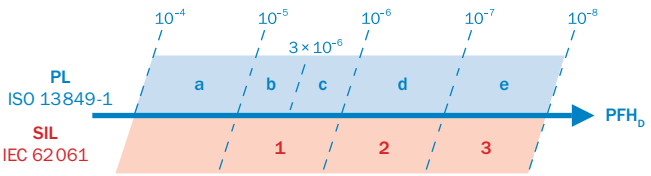


Figure 109: Illustration of the relationship between performance level and safety integrity level

Both methods can be used to check whether the required level of safety has been achieved. The PFH_D value is determined as a quantitative measure for this purpose.

In both examples (see figure 110), sensor and logic data is available but power control element data is not.

NOTE

- Performance level (PL): Capability of safety-related components to perform a safety function under foreseeable conditions in order to achieve the expected reduction in risk
- PFH_D: Probability of a dangerous failure per hour
- SIL: Discrete level for defining the integrity of the safety function.

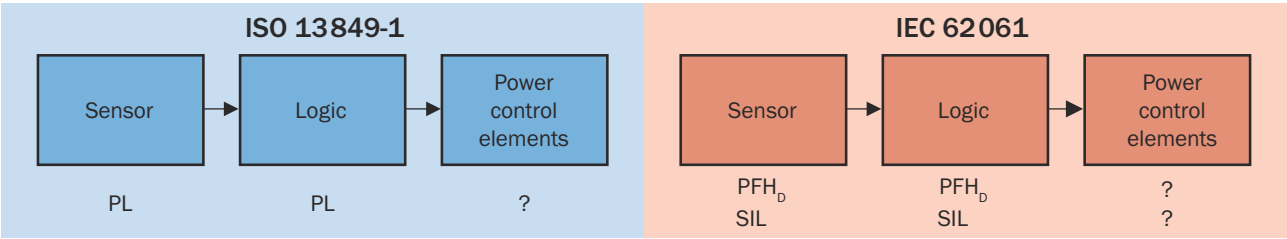


Figure 110: Subsystems of a safety function and parameters for determining the safety level according to ISO 13849-1 and IEC 62061

Determining the achieved Performance Level (PL)

Subsystems

A safety function that is implemented using control measures generally comprises sensor, logic unit, and power control elements. Such a chain can include discrete elements such as guard interlocking devices or valves, but also complex safety controllers. Safety functions are therefore often divided into subsystems to reduce complexity.

In practice, pre-certified subsystems are often used for safety functions. PL or PFH_D values are provided by the manufacturer for these subsystems, e.g., for a safety light curtain or a safety controller.

These values apply only for the mission time to be specified by the manufacturer. In addition to the quantifiable aspects, it is also necessary to verify the measures against systematic failures.

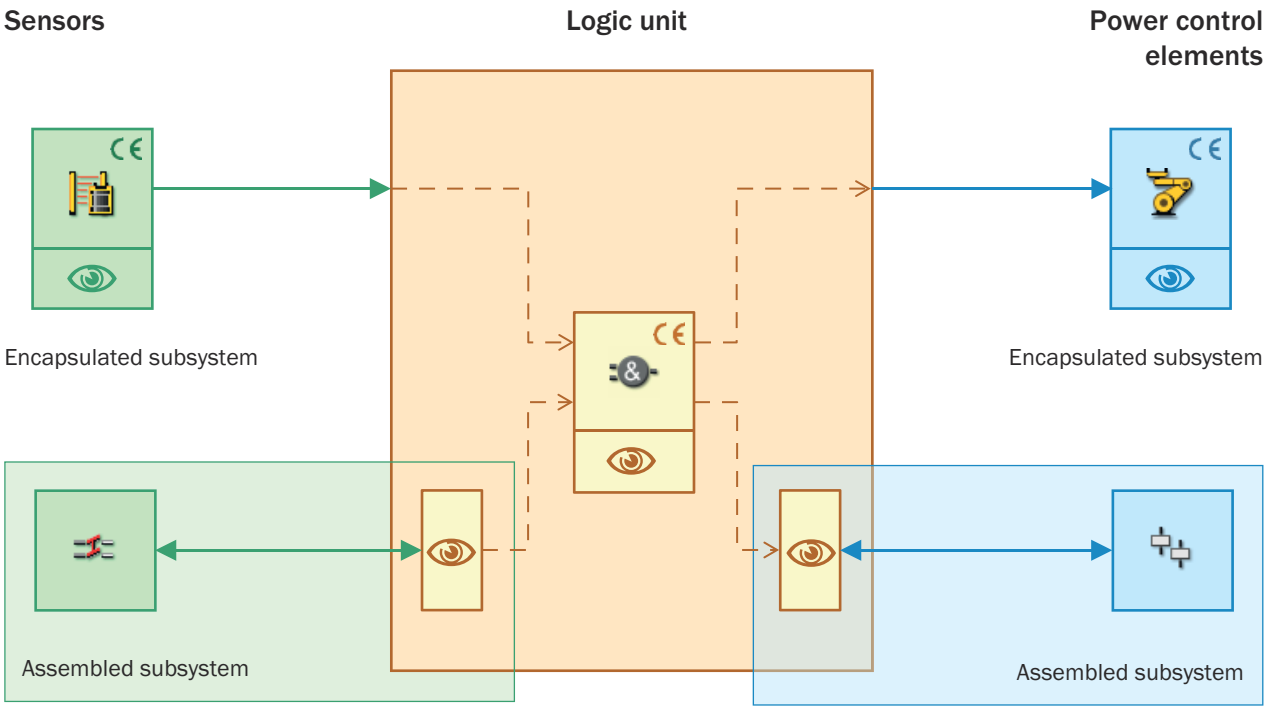


Figure 111: Encapsulated and assembled subsystems of a safety function

ESPE Electro-sensitive protective equipment
PDS(SR) Adjustable speed electrical power drive system (PDS) providing safety sub-functions

Diagnostic measures

ISO 13849-1 sets out two methods for determining performance level:

- **Simplified method** (see "Simplified procedure according to ISO 13849-1", page 131): Tabular determination of performance level based on the performance level of each subsystem
- **Detailed method** (see "Detailed procedure according to ISO 13849-1", page 132): Calculation of the performance level based on the PFH_D values of the subsystems. (This method is only described indirectly in the standard).

More realistic performance levels than those using the simplified method can be determined by applying the detailed method. For both methods, structural and systematic aspects relating to the achievement of the performance level must also be taken into account in addition to the quantitative assessments.

NOTE

➜ More information about validation: ISO 13849-2

➜ You will find a large amount of information on verification using ISO 13849-1 at **www.dguv.de/ifa/13849**

Simplified procedure according to ISO 13849-1

This method also allows the overall PL for many applications to be estimated with sufficient accuracy without knowing individual PFH_D values. If the PL of all subsystems is known, the overall PL achieved by a safety function can be determined using the following table.

This method is based on mean values within the PFH_D value ranges for the different PLs. Therefore, using the detailed method (see next section) may deliver more accurate results.

Table 52: Table from ISO 13849-1 for determining the total PL based on the simplified method

PL (low)	n (low)		PL
(lowest PL of a subsystem)	(number of subsystems with this PL)		(Maximum achievable PL)
a	> 3	→	–
	≤ 3	→	a
b	> 2	→	a
	≤ 2	→	b
c	> 2	→	b
	≤ 2	→	c
d	> 3	→	c
	≤ 3	→	d
e	> 3	→	d
	≤ 3	→	e

Procedure

- Determine the PL of the subsystem(s) with the lowest PL in a safety function: **PL (low)**
- Determine the number of subsystems with this PL (low): **n (low)**

Example 1:

- All subsystems achieve PL “e”, so the lowest PL (low) is “e”.
- The number of subsystems with this PL is 3 (i.e., ≤ 3). Therefore, the overall PL achieved is “e”.
- According to this method, adding another subsystem with a PL of “e” would reduce the overall PL to “d”.

Example 2:

- One subsystem achieves PL “d”, two subsystems achieve PL “c”. The lowest PL (low) is, therefore, “c”.
- The number of subsystems with this PL is 2 (i.e. ≤ 2). Therefore, the overall PL achieved is “c”.

This method is based on mean values within the PFH_D value ranges for the different PLs. Therefore, using the detailed method (see next section) may deliver more accurate results.

NOTE

➜ If the PL is not known for all subsystems, their safety level can be determined (see "Determining the safety level of a subsystem", page 132).

Detailed procedure according to ISO 13849-1

An essential – but not exclusive – criterion for determining the PL is the “probability of a dangerous failure per hour (PFH_D)” of the safety components. The resulting PFH_D value is the sum of the individual PFH_D values.

Determining the safety level of a subsystem

If the PFH_D value is not known for all subsystems, then their safety level can be determined. Subsystems can consist of several components, even from different manufacturers. Examples of components in subsystems:

- Input side: 2 safety switches on a physical guard
- Output side: 1 contactor and 1 frequency inverter to stop a dangerous movement

For these subsystems with multiple components, the PL must be determined separately.

The performance level achieved for a subsystem is made up of the following parameters:

- Structure and behavior of the safety function under fault conditions ("Structure and category of safety-related parts of controllers", page 132)
- $MTTF_D$ values of individual components ("Mean time to dangerous failure ($MTTF_D$)", page 133)
- Diagnostic coverage ("Diagnostic coverage (DC)", page 134)
- Common cause failure ("Common cause failure (CCF)", page 135)
- Software aspects that are relevant to safety
- Systematic failures

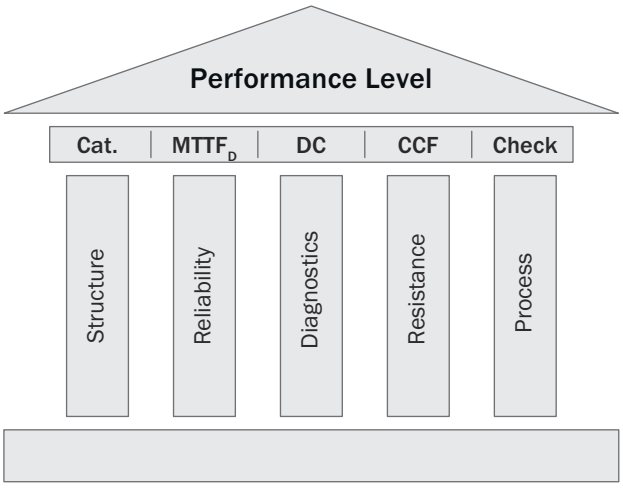


Figure 112: Aspects for determining the performance level of a subsystem

Structure and category of safety-related parts of controllers

Subsystems are usually single-channel or dual-channel. Unless additional measures are in place, single-channel systems respond to errors with a dangerous failure. Errors can be detected by introducing additional testing components or dual-channel systems supporting reciprocal testing. ISO 13849-1 defines categories for classifying the structure of subsystems:

Table 53: Description of the categories according to ISO 13849-1

Category	Brief summary of requirements	System behavior	Principles for achieving safety
B	**The safety-related parts of control systems and/or their protective devices, as well as their components, must be set up, built, selected, assembled, and combined in compliance with applicable standards so that they are able to tolerate anticipated influencing factors.**	• The occurrence of an error can result in the loss of the safety function.	Primarily characterized by component selection
1	**The requirements of category B must be met. Well-tried components and well-tried safety principles shall be used.**	• The occurrence of an error can result in the loss of the safety function, but the probability of occurrence is lower than in category B.	
2	**The requirements of category B shall be met and well-tried safety principles used. The safety function must be tested by the machine controller at appropriate intervals (test rate 100 times higher than demand rate).**	• The occurrence of an error can result in the loss of the safety function between checks. • The loss of the safety function is detected by the test.	Predominantly characterized by the structure
3	**The requirements of category B shall be met and well-tried safety principles used. Safety-related parts shall be designed so that:** • **A single error in any of these parts will not lead to the loss of the safety function, and** • **Wherever it is reasonably possible, the single error is detected.**	• When the single error occurs, the safety function is always retained. • Some, but not all errors are detected. • Accumulation of undetected errors may lead to loss of the safety function.	
4	**The requirements of category B shall be met and well-tried safety principles used. Safety-related parts shall be designed so that:** **An single error in any of these parts will not lead to the loss of the safety function** **The single error is detected on or before the next request for the safety function or** **If this is not possible, an accumulation of errors will not lead to the loss of the safety function.**	• The safety function is always retained when errors occur. • The errors are detected in a timely manner to prevent the loss of the safety function.	

Mean time to dangerous failure ($MTTF_D$)

MTTF stands for Mean Time To Failure. From the point of view of ISO 13849-1, only dangerous failures need to be considered (hence the “D” for “dangerous” in $MTTF_D$).

This value represents a theoretical parameter expressing the probability of a dangerous failure of a component (not the entire subsystem) within the lifetime of that component. The actual lifetime of the subsystem is always shorter.

The MTTF value can be derived from the failure rates. Where:

- The B_{10} values apply to electromechanical or pneumatic components. Their maximum lifetime depends on the wear and the switching frequency. B_{10} therefore indicates the number of switching cycles until 10% of the components fail.
- The B_{10D} value is concerned with the dangerous failure of components (the “D” in B_{10D} stands for “dangerous”). The value indicates the number of switching cycles until 10% of the components fail dangerously. If the B_{10D} value is not specified, it may generally be assumed that: $B_{10D} = 2 \times B_{10}$
- The failure rate λ applies to electronic components. Often the failure rate is given in FIT (Failures In Time). FIT=1 means one failure per 10^9 hours.

ISO 13849-1 combines the $MTTF_D$ values into ranges:

Table 54: Ranges of the $MTTF_D$ value according to ISO 13849-1

Designation	Range
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	30 years ≤ $MTTF_D$ < 100 years

The mean time to a dangerous failure in years ($MTTF_D$) can be calculated for the overall system from the component values.

To avoid overrating the impact of reliability, the useful maximum value for the $MTTF_D$ has been limited to 100 years.

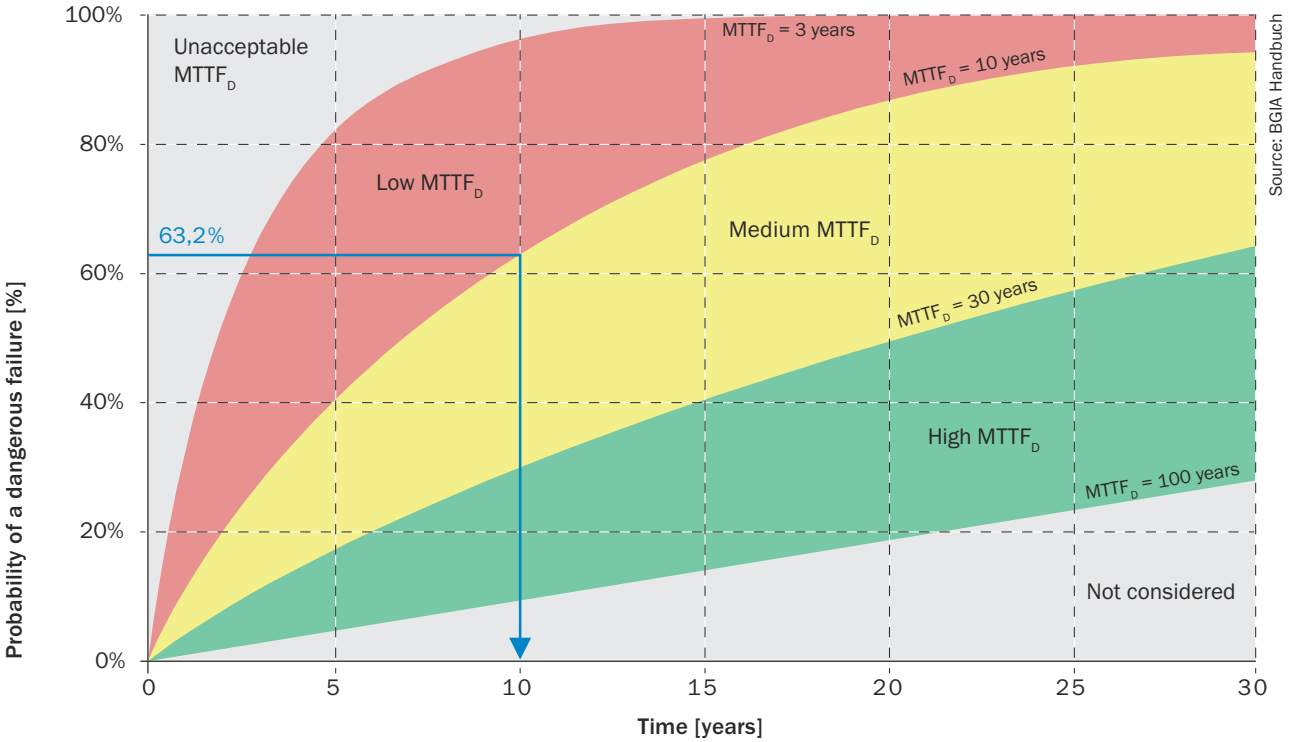


Figure 113: Probability of dangerous failure as a function of the operating time

Diagnostic coverage (DC)

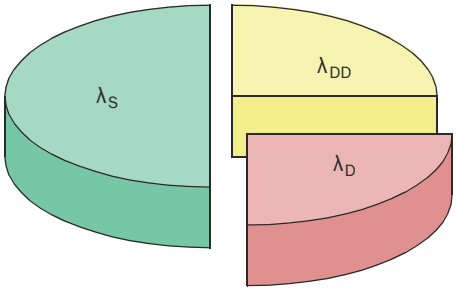
The level of safety can be increased if fault detection is implemented in the subsystem. The diagnostic coverage (DC) is a measure of the capability to detect dangerous errors. Poor diagnostics only detect a few errors, good diagnostics detect a large number of or even all failures.

Instead of a detailed analysis (FMEA), the ISO 13849-1 standard contains various quantified measures. The DC is divided into various ranges:

Table 55: CCF measures with the maximum achievable values according to ISO 13849-1

Designation	Range
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

DC = 50%
SFF = 75%



Common cause failure (CCF)

External influences (e.g., voltage level, overtemperature) can cause several identical components to become unusable at the same time, regardless of how infrequently they would otherwise fail or how well they have been tested. To illustrate this: When the light goes out, you can neither read the newspaper with one eye or with both eyes because it is dark. Such common cause failures must be prevented.

Annex F of ISO 13849-1 provides a simplified method to evaluate measures taken against CCF. A maximum number of points is defined for each measure. Suitable points are awarded for each measure that has been applied. A total score of 65 or higher indicates that adequate CCF measures are in place.

Requirement		Points	Minimum requirement
Separation	Separation of signal circuits, separate routing, isolation, air paths, etc.	**15**	**Total score ≥ 65**
Diversity	Different technologies, components, principles of operation, designs	**20**	
Design, application, experience	Protection against overload, overvoltage, overpressure, etc. (depending on technology)	**15**	
	Use of components and methods proven over many years	**5**	
Analysis, evaluation	Use of a failure analysis to avoid common cause failures	**5**	
Competence, training	Training for designers so that they understand and can avoid the causes and consequences of CCF	**5**	
Environmental impact	For electrical/electronic systems, prevention of contamination and electromagnetic interference (EMI) to protect against common cause failures in accordance with relevant standards (e.g., IEC 61326-3-1) Fluidic systems: Filtration of the pressure medium, prevention of dirt ingress, dehumidification of compressed air, e.g., in accordance with the manufacturer's requirements on the purity of the pressure medium. ℹ **NOTE** | Both aspects should be taken into consideration when there is a combination of fluidic and electrical systems.	**25**	
	Consideration of the requirements regarding insensitivity to all relevant ambient conditions, e.g. temperature, shock, vibration, humidity (e.g., as defined in the applicable standards)	**10**	

Process

The standard provides various sources of help to ensure that the preceding aspects are implemented correctly in the hardware and software, that they are tested thoroughly (four-eyes principle), and that version and change history information is readily available in comprehensive documentation. This includes the measures for fault prevention and fault control:

- Organization and expertise (responsibilities, qualification of employees, procedures, system of quality management processes)
- Design rules (e.g., specifications templates, coding guidelines)
- Test concepts and test criteria
- Documentation and configuration management

The process for the correct implementation of safety-relevant topics is part of the remit of managers and includes appropriate quality management.

Determination of the PL of a subsystem

The following figure shows the relationship between the $MTTF_D$ value (per channel), the DC, and the category of safety-related parts of controllers.

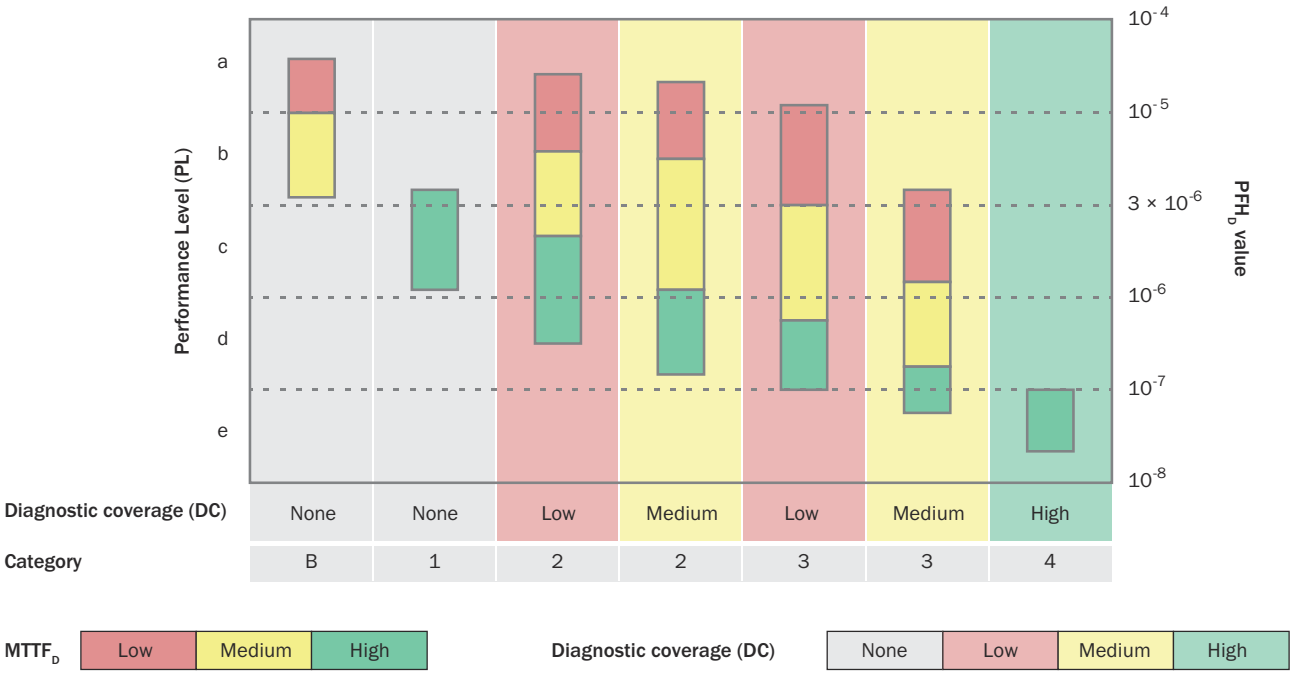


Figure 114: Relationship between the categories DC, $MTTF_D$ of each channel, and PL according to ISO 13849-1

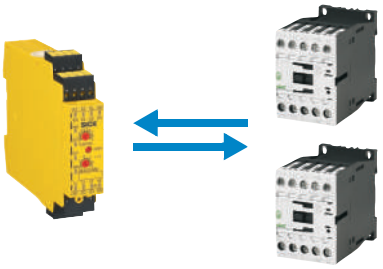
A performance level of “d” can be achieved, for example, using a dual-channel control system (category 3). This can be achieved either with components of good quality ($MTTF_D$ = medium) if almost all errors are detected (DC = medium) or with components of very good quality ($MTTF_D$ = high) if many errors are detected (DC = low).

A complex mathematical model underlies this procedure. To ensure a pragmatic approach, the parameters category, $MTTF_D$ and DC are predefined.

Example: Determining the PL of the "power control elements" subsystem

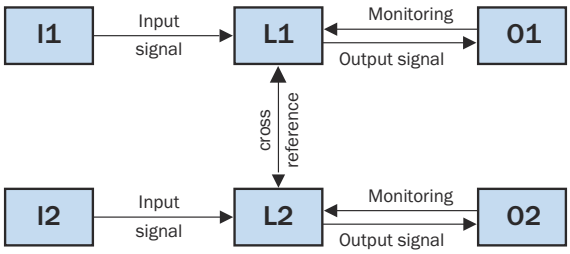
1) Definition of the "power control element" subsystem

The "power control element" subsystem comprises two contactors with "feedback". As the contactor contacts are positively guided, a safety-relevant failure of the contactors can be detected (EDM).
The UE410 logic unit is not itself part of the "power control element" subsystem, but it is used for diagnostics purposes.



2) Determination of the category

Single-error safety (with error detection) makes the equipment **suitability for category 3 or 4**.
Note: The category is not defined definitively until the DC value has been specified.



3) Determination of the $MTTF_D$ per channel

As contactors are subject to wear, the B_{10D} value and the estimated switching frequency (n_{op}) must be used to calculate the $MTTF_D$. The following formula applies:
The figure for the switching frequency comprises operating hours/day [h_{op}], working days/year [d_{op}] as well as the switching frequency per hour [C]:
General conditions according to the manufacturer:

- B_{10D} = 2,600.000
- C = 1 / h (assumed)
- d_{op} = 220 d/a
- h_{op} = 16 h/d

These boundary conditions result in an **$MTTF_D$ of 7,386 years** per channel, which is interpreted as "high".

$$MTTF_D = \frac{B_{10D}}{0,1 \times n_{op}}$$

$$MTTF_D = \frac{B_{10D}}{0,1 \times d_{op} \times h_{op} \times C}$$

$MTTF_D$	Range
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	**30 years ≤ $MTTF_D$ < 100 years**

4) Determination of DC

As the contacts are positively guided, a **high DC (99%)** can be derived from ISO 13849-1 according to the table.

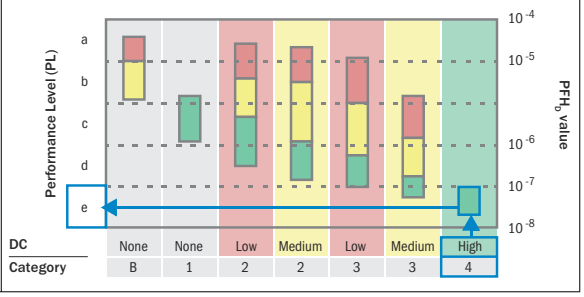
DC	Range
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	**99% ≤ DC**

Example: Determining the PL of the "power control elements" subsystem

5) Evaluation of the measures to prevent common cause failures

Measures to avoid the common cause effect are implemented in multi-channel systems. The evaluation of the measures results in a score of 75. This meets the minimum requirement.

Requirement	Points	Minimum requirement
Separation	15	**Total points 75 ≥ 65**
Diversity	20	
Design, application, experience	20	
Analysis, evaluation	5	
Competence/training	5	
Effect of the environment	35	
Total	**75**	

Example: Determining the PL of the “power control elements” subsystem	
6) Evaluation of process measures Similarly, systematic aspects for the avoidance and management of faults must be taken into account. For example: • Organization and competence • Rules governing design (e.g., specifications templates, coding guidelines) • Test concept and test criteria • Documentation and configuration management	**Fulfilled**
7) Result The PL of the subsystem can be determined from the figure for determining the PL of the subsystem (see "Determining the achieved Performance Level (PL)", page 130). In this case, the PL “e” has been achieved. The resulting **PFH_D value of 2.47 × 10^{-8}** for this subsystem can be obtained from a detailed table in ISO 13849-1. The high DC means that the dual-channel structure meets the requirements of **category 4**.	

NOTE

With the resulting data for the subsystem, it is now possible to determine the performance level of the entire safety function achieved (see "Determining the achieved Performance Level (PL)", page 130).

Alternative: Determining the achieved safety integrity level (SIL)

The achieved safety integrity level (SIL) according to IEC 62061 is determined based on the following criteria:

- The safety integrity of the hardware
  - Structural restrictions (SIL claim limit)
  - Probability of dangerous hardware failures (PFH_D)
- The requirements for systematic safety integrity
  - Avoidance of failures
  - Management of systematic errors

Here – similar to ISO 13849-1 – to determine the PL the safety function is first broken down into function blocks and then transferred to subsystems.

Figure 115: Subsystems in the safety chain: safety light curtain. Logic unit, contactor

Safety integrity of the hardware

When considering the overall safety function, the safety integrity of the hardware is determined by the following factors ...

- The lowest SIL of a subsystem restricts the maximum SIL that can be achieved by the overall system.
- The PFH_D of the overall control system from the sum of the individual PFH_D does not exceed the values in Figure see figure 109 “Verification of functional safety”.

Example
In the figure above, all subsystems achieve SIL3. The addition of the PFH_D values does not exceed 1×10^{-7}. The relevant measures for systematic safety integrity are in place. Therefore, the safety function achieves SIL3.

Systematic safety integrity

When different subsystems are interconnected to create a control system, additional measures for systematic safety integrity must be taken to avoid systematic errors.

Measures for avoiding systematic hardware errors include, amongst other things, the following:

- Design in accordance with the functional safety plan
- Correct selection, combination, arrangement, assembly, and installation of subsystems, including cabling, wiring, and other connections
- Use within the manufacturer's specifications
- Compliance with application instructions provided by the manufacturer (catalog data, installation instructions, and application of proven practical experience, for example)
- Observance of requirements with regard to electrical equipment in accordance with IEC 60204-1

Furthermore, consideration must be given to the control of systematic errors, for example through the following measures:

- Cutting off the power supply to induce a safe status
- Measures to manage the effects of errors and other effects arising out of a shared data communication process, including transmission errors, repeats, loss, insertion, incorrect sequence, corruption, delay, etc.

Determining the level of safety for a subsystem as per IEC 62061

IEC 62061 also supports the determination of the safety level of subsystems created by interconnecting individual components.

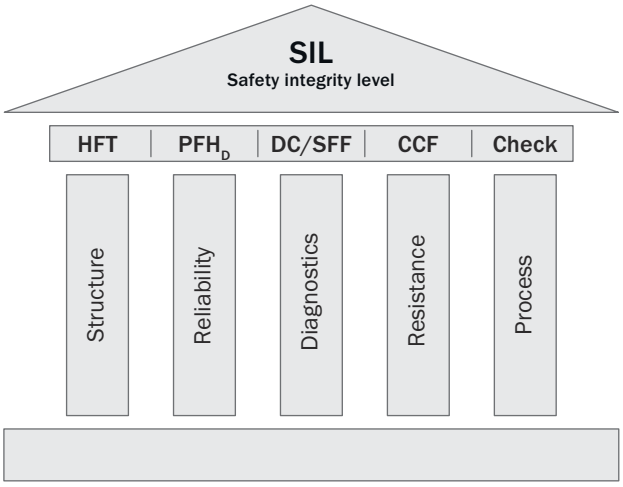


Figure 116: Aspects for determining the safety integrity level of a subsystem

The safety integrity level (SIL) achieved for a subsystem is made up of the following parameters:

- Hardware fault tolerance (HFT)
- PFH_D value
- Safe failure fraction (SFF)
- Common cause failures (CCF)
- Software aspects that are relevant to safety
- Systematic failures

Hardware fault tolerance (HFT)

IEC 62061 defines the structure based on subsystem types and hardware fault tolerance (HFT).

HFT 0 means that a single failure in the hardware can result in the loss of the safety function (single-channel systems). HFT 1 means that despite a single failure in the hardware, protection is maintained (dual-channel systems).

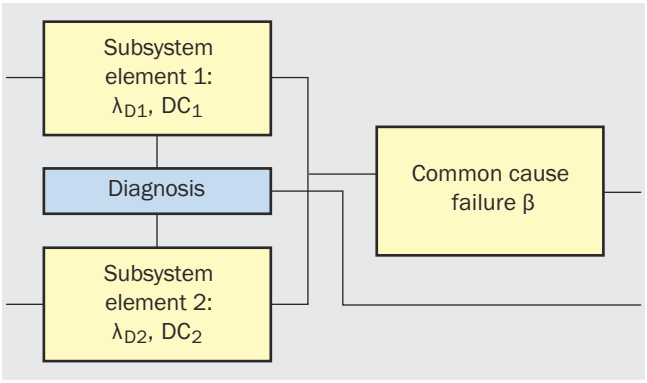


Figure 117: Logical representation of a subsystem

Probability of dangerous hardware failures (PFH_D)

Alongside structural restrictions, the “probability of dangerous hardware failures” must also be taken into account for each subsystem. For each subsystem, a formula exists to describe the mathematical model to calculate the PFH_D value. The following parameters are included in the calculation:

- Diagnostic coverage
- Mission time
- Diagnostic test interval
- Failure rate of the components (λ_D)
- Common cause failure (common cause factor β)

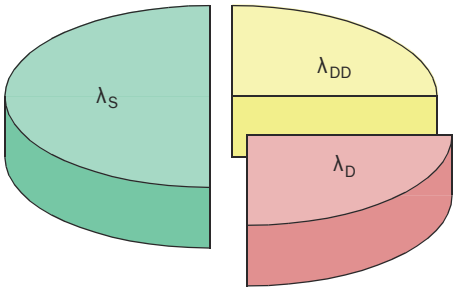
HFT = 1
Diagnosis with DC_1 and DC_2

$$PFH_D = (1 - \beta)^2 \times \left\{ \frac{\lambda_{D1} \times \lambda_{D2} \times (DC_1 + DC_2) \times T_D}{2} + \frac{\lambda_{D1} \times \lambda_{D2} \times (2 - DC_1 - DC_2) \times T_P}{2} + \beta \times \frac{\lambda_{D1} + \lambda_{D2}}{2} \right\}$$

$$PFH_D \approx \beta \times \frac{\lambda_{D1} + \lambda_{D2}}{2}$$

Safe failure fraction (DC/SFF)

DC = 50%
SFF = 75%



λ_S Safe failure rate
λ_{DD} Rate of detected dangerous failures
λ_D Rate of undetected dangerous failures

In addition to the diagnostic coverage DC ("Diagnostic coverage (DC)", page 134), the “safe failure fraction” (SFF) indicates the proportion of the total failure rate that does not lead to a dangerous failure.

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D}$$

Resistance to common cause failure (CCF)

IEC 62061 also requires a range of considerations with regard to resistance to common cause failures. A common cause factor (β) is calculated based on the number of positive permutations.

Table 56: Criteria with points for determining the CCF according to IEC 62061

Requirement		Points
Separation	Separation of signal circuits, separate routing, isolation, air paths, etc.	**15**
Diversity	Different technologies, components, principles of operation, designs	**20**
Design, application, experience	Protection against overload, overvoltage, overpressure etc. (depending on technology)	**15**
	Use of components and methods proven over many years	**5**
Analysis, evaluation	Use of a failure analysis to avoid common cause failures	**5**
Competence, training	Training for designers so that they understand and can avoid the causes and consequences of CCF	**5**
Environmental impact	Testing the system for susceptibility to EMC	**25**
	Testing the system for susceptibility to temperature, shock, vibration, etc.	**10**

Table 57: Estimation of the CCF factor (beta) according to IEC 62061

Points	CCF factor (β)
≤ 35	10%
36 to 65	5%
66 to 85	2%
86 to 100	1%

Process

Given that IEC 62061 is strongly aligned with programmable electrical systems, in addition to the aspects described above (V model, quality management, etc.), it also includes numerous detailed notes and requirements about the correct approach when developing software for safety-related systems.

Result - Determining the SIL for the subsystem

First, the safety integrity of the hardware is determined separately for each subsystem:

If the subsystems are already developed (as is the case with safety light curtains, for example), the manufacturer of the subsystem will supply the corresponding parameters in the context of the technical specification. A subsystem of this type is usually described in sufficient detail by the specification of SIL, PFH_D, and mission time.

For subsystems consisting of subsystem elements (interlocking devices for protective doors or contactors, for example), on the other hand, safety integrity must be determined.

SIL claim limit

Once the hardware tolerance (architecture) has been specified, the maximum achievable SIL (SIL claim limit) can be determined for the subsystem.

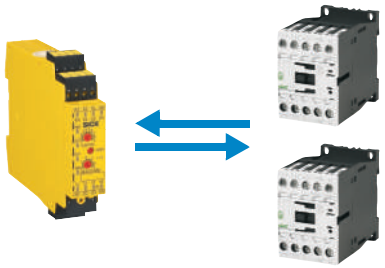
Safe failure fraction (SFF)	Hardware fault tolerance	
	0	1
< 60%	-	SIL 1
60 to < 90%	SIL 1	SIL 2
90 to < 99%	SIL 2	SIL 3
≥ 99%	SIL 3	SIL 3

A dual-channel system with HFT 1 and an SFF of 90% can achieve SIL3.

Example: Determining the SIL and PFH_D of the "power control elements" subsystem

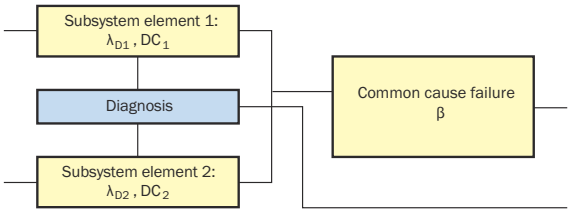
1) Definition of the "power control elements" subsystem

The "power control elements" subsystem comprises two contactors with "feedback". As the contactors are positively guided, a safety-relevant failure of the contactors can be detected (EDM).
The UE410 logic unit is not itself part of the "power control elements" subsystem, but it is used for diagnostics purposes.



2) Definition of hardware fault tolerance (HFT)

Single-error safety with error detection results in an HFT of 1.



3) Determination of the PFH_D

a) Based on the fault rate λ_D

Since contactors are subject to wear, the B_{10D} value and the estimated switching frequency must be used to calculate the switching frequency per hour [C].
IEC 62061 contains no statements about the behavior of mechanical components. The fault rate λ_D is therefore determined based on ISO 13849-1. It is assumed that the fault rate remains constant during application.
General conditions according to the manufacturer:

- B_{10D} = 2,600.000
- C = 1 / h (assumed)

These boundary conditions result in a λ_D of 3.8×10^{-8} 1 / h.

b) Based on the CCF factor (β)

Measures to avoid the common cause effect are required in multichannel systems. The effect is determined based on measures as per the requirements of IEC 62061. In the example, the factor is 5% (see: "5) Evaluation of the measures to avoid common cause errors" in this table)
$PFH_D \approx 1.9 \times 10^{-9}$.

$$\lambda_D = \frac{1}{MTTF_D} = \frac{0,1 \times C}{B_{10D}}$$

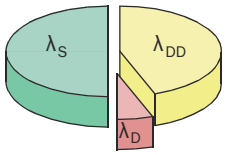
Value	CCF factor (β)
≤ 35	10%
36 to 65	5%
66 to 85	2%
86 to 100	1%

$$PFH_D \approx \beta \times (\lambda_{D1} + \lambda_{D2}) \times ½$$

$$\approx \beta \times \lambda_D$$

$$\approx 0,05 \times 0,1 \times \frac{C}{B_{10D}}$$

$$PFH_D \approx 1,9 \times 10^{-9}$$

<table>
<tr><th colspan="2">Example: Determining the SIL and PFH_D of the “power control elements” subsystem</th></tr>
<tr><td>4) Determination of the SFF via DC
As the contacts are positively guided, a “high” DC (99%) is derived. In other words, 99% of 70% of dangerous errors λ_D for contactors are detected. Accordingly, the SFF = 30% + 69.3% = 99.3%.</td><td>DC = 99%
SFF = 99.3%
 
</td></tr>
<tr><td>5) Evaluation of the measures to prevent common cause failures
Measures to avoid the common cause effect are required in multi-channel systems. The evaluation of the measures as per IEC 62061 yields in this example a CCF factor (β) of 5%.</td><td><table>
<tr><th>Value</th><th>CCF factor (β)</th></tr>
<tr><td>≤ 35</td><td>10%</td></tr>
<tr><td>36 to 65</td><td>5%</td></tr>
<tr><td>66 to 85</td><td>2%</td></tr>
<tr><td>86 to 100</td><td>1%</td></tr>
</table></td></tr>
<tr><td>6) Evaluation of process measures
Similarly, systematic aspects for the avoidance and management of faults must be taken into account. For example:
Organization and competence
Rules governing design (e.g., specifications templates, coding guidelines)
Test concept and test criteria
Documentation and configuration management</td><td>Fulfilled</td></tr>
<tr><td>Result
In the final step, the structural restrictions must be considered. Based on the available redundancy (hardware fault tolerance 1) and the SSF of > 99%, the SIL claim limit for this subsystem is SIL 3.</td><td><table>
<tr><th rowspan="2">Safe failure fraction (SFF)</th><th colspan="2">Hardware fault tolerance</th></tr>
<tr><th>0</th><th>1</th></tr>
<tr><td>< 60%</td><td>-</td><td>SIL 1</td></tr>
<tr><td>60 to < 90%</td><td>SIL 1</td><td>SIL 2</td></tr>
<tr><td>90 to < 99%</td><td>SIL 2</td><td>SIL 3</td></tr>
<tr><td>≥ 99%</td><td>SIL 3</td><td>SIL 3</td></tr>
</table>
$PFH_D \approx 1.9 \times 10^{-9}$</td></tr>
</table>

Useful support

The verification methods described require knowledge and experience of the concepts of performance level (PL) and safety integrity level (SIL). This knowledge and practical experience is available to you in SICK's service and training portfolio (see "How SICK supports you", page 161).

The SISTEMA software assistant, which was developed by IFA in Germany and is available free of charge, supports an effective method for calculating performance level. SICK offers a library of certified safety products for this purpose.

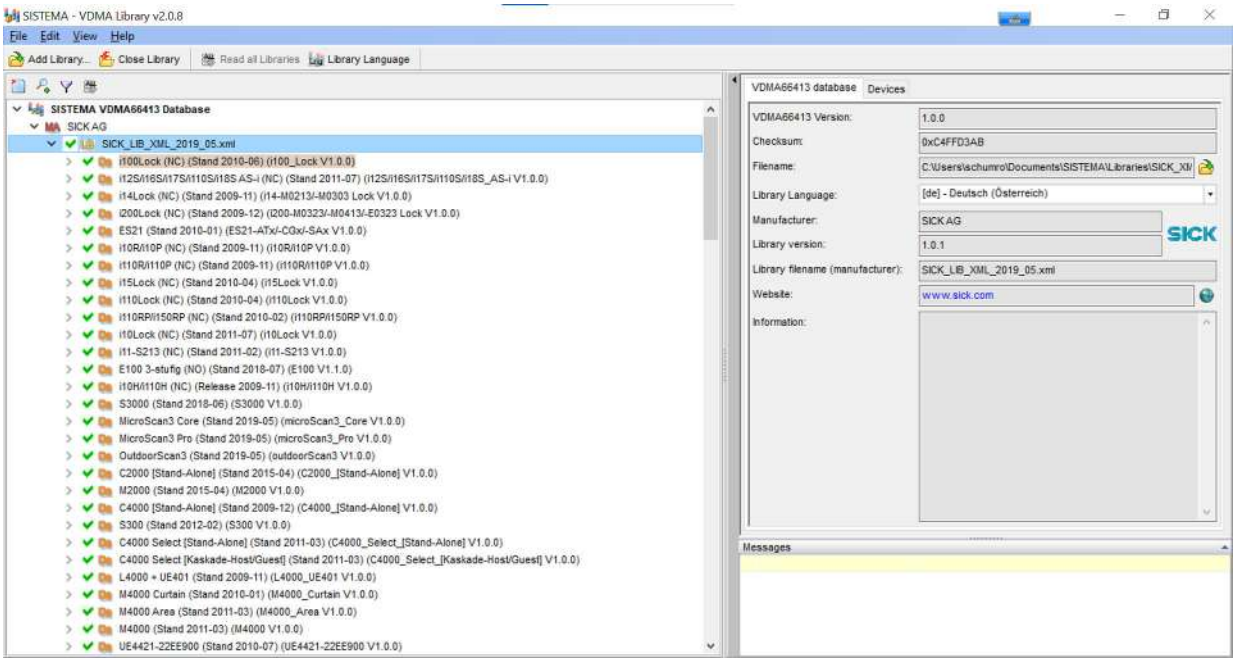


Figure 118: Library of certified safety products from SICK in the SISTEMA software tool for determining the performance level

NOTE

The SICK component library for SISTEMA can be found online under Project Planning Software **Library for functional safety**.

Summary: Verifying the safety function

General

- Verify that the intended safety functions conform to the required safety level. To do this, verify mechanical and functional safety.

Methods

- Determine the resulting level of safety as per ISO 13849-1 (PL). Available methods:
  - Simplified method (based on PL)
  - Detailed method (based on PFH_D values)
- If neither the PL nor the PFH_D value of the subsystem (e.g., the power control element) is known, determine the safety level of the subsystem from the following aspects: “structure, reliability, diagnostics, resistance, and process”.
- Alternatively, determine the resulting level of safety as per IEC 62061 (SIL). Here too it is possible to determine even the safety level of a subsystem that is not certified.

Help

Use the recommended tools and take advice.

3e – Validating all safety functions

Validation is the checking of a theory, a plan, or a proposed solution in relation to a problem that needs to be solved. Unlike verification, where only the correct implementation of a solution in accordance with specification is assessed, validation is about the ultimate assessment of a solution in general terms with regard to its suitability to reduce risk as required.

Figure 119: Service employee inspecting a protective device

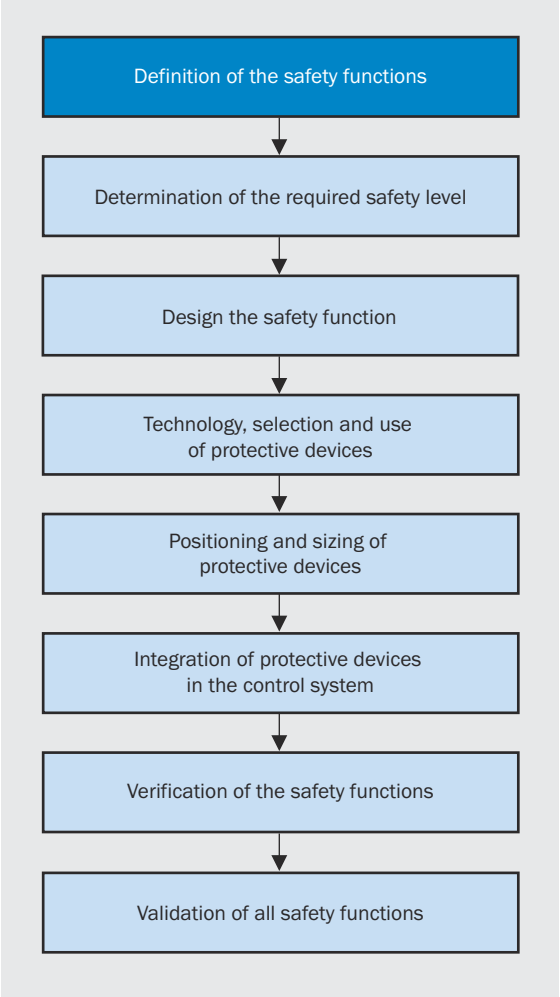


Figure 120: From definition to validation of the safety functions

The purpose of the validation procedure is to check the specification and the conformity of how the components involved in the safety function have been integrated on the machine. Validation shall show that safety-related parts of the control function meet the requirements of ISO 13849-2, in particular the requirements for the level of safety defined.

Insofar as is reasonable, validation should be carried out by persons who were not involved in the design of the safety-related parts of the control systems. In the validation process, it is important to check errors and in particular omissions in the formulated specification. The critical part of how a safety-related control function has been designed is usually the specification.

For example, access to a robot cell is to be safeguarded by a light curtain. The safety function is thus specified as follows:

“If the protective field of a light curtain is interrupted, all hazardous machine functions shall cease as quickly as possible.”

However, the designer shall also have considered restarting when the protective field becomes clear again, in particular if access can be gained to it by standing behind this field. The validation process shall uncover such aspects. As a rule, a validation process involves the application of a number of procedures that complement each other.

These include the following procedures:

- Technical inspection of the positioning and effectiveness of protective devices
- Practical inspection of response to failure with regard to the expected results by means of simulations

- Validation of environmental requirements by means of functional tests:
  - Sufficient protection against influencing factors from the environment (temperature, moisture, shock, vibration behavior, etc.)
  - Sufficient resistance to interference from electromagnetic sources

3f – Functional safety and cybersecurity

The increasing requirements for linking plants and machines of production facilities, and the data exchange via open interfaces required for this, opens up the possibility of intentional or an unintentional access to safety parameters and production-related data. This creates new challenges for information security and must be taken into account to prevent injury to persons or damage to machines and systems or the environment.

Consequently, this necessitates an overall assessment of machine safety and information security aspects by component manufacturers, machine manufacturers, system integrators and plant operators. The overall assessment always starts with defining the limits of the machine (usage limits and spatial limits). The limits also include communication interfaces relevant to cybersecurity, both between humans and machines, between machines and the control system, and between machines. A risk assessment or hazard assessment is performed based on these limits. Based on the risk analysis, all sources of danger are analyzed and appropriate measures taken. Cybersecurity attacks do not create new hazards in terms of machine safety, but the effectiveness of protective measures can be negatively impacted or interrupted. For example, the system components associated with a safety requirement might not stop or speeds might not be reduced to the necessary level, creating hazards.

Cybersecurity considerations are relevant to the following machines:

- Machines with programmable controllers with electronic interfaces
- Machines with programmable controllers with a network connection

Machines with contact-based controls or machines with electronic but non-programmable controllers are not directly relevant to cybersecurity considerations. If electronically parameterizable components are integrated, hazards can in turn arise via the interface to the parameterization device.

What measures are necessary to address the cybersecurity aspects of machine safety?

Protective measures familiar from office communications or in the private sphere (firewall, virus scanner) are not sufficient for the industrial environment. A systematic approach is necessary. In general, the following applies to all participants operating in the value chain

- the corporate culture and thus awareness within the company of the issue of cybersecurity must be sufficiently developed.
- an appropriate safety management system must be installed.
- the relevant knowledge must be up to date.
- the necessary technologies with an appropriate level of IT security must be available.

Figure 121: Review of the safety management in a production plant

The following table summarizes the machine security related aspects that machine manufacturers, equipment manufacturers, system integrators, service providers, equipment and machine operators need to consider to prevent cybersecurity attacks:

Table 58: Machine security related aspects that machine manufacturers, equipment manufacturers, system integrators, service providers, equipment/machine operators need to consider to prevent cybersecurity attacks

Machine manufacturer	Equipment manufacturer, system integrator, service provider	Plant/machine operator
Security risk assessment E.g., according to IEC TR63074. Identification of components and information requiring protection and assessment of relevance	**Security risk assessment** E.g., according to IEC TR63074. Identification of components, system parts and information requiring protection and assessment of relevance	**Security threat assessment** for reasonably foreseeable unauthorized actions
Zone division Determine the protection requirements of the machine. Grouping of components and information with similar protection requirements into zones	**Zone division** Grouping of components, machines and information with similar protection requirements into zones	**Zone division** Grouping of machines and information with similar protection requirements into zones
Authentication and authorization Structuring and assigning of rights, definition of access and transmission mechanisms	**Authentication and authorization** Structuring of rights, definition of access and transmission mechanisms	**Authentication and authorization** Assignment of rights
Implement the monitoring Archive security-relevant information (log file) in read-only mode or integrate into higher-level systems	**Implement the monitoring** Archive security-relevant information (log file) in read-only mode or integrate into higher-level systems	**Use monitoring** Evaluation of logs to detect attacks or unauthenticated access attempts
Provide backup mechanisms	**Provide backup mechanisms**	**Perform backup** Recovery of data and information

Machine manufacturer	Equipment manufacturer, system integrator, service provider	Plant/machine operator
Organization Security concept, definition of responsibilities, ensuring state of the art, consideration of the dynamic developments in cyberattacks	**Organization** Security concept, definition of responsibilities, ensuring state of the art, consideration of the dynamic developments in cyberattacks	**Organization** Security concept, definition of responsibilities, guidelines, implementation of vulnerability management, consideration of the dynamic developments in cyberattacks
Operating instructions Consideration of the cybersecurity information of the component manufacturers and formulation of the cybersecurity instructions for the user	**Operating instructions** Consideration of the cybersecurity instructions of the component and machine manufacturers and formulation of the cybersecurity instructions for the user	**Operating instructions** Consideration of the cybersecurity instructions of the machine and plant manufacturers
Component selection Support of the security concept	**Component and machine selection** Support of the security concept	**Machine and plant selection** Support of the security concept
Emergency mode Putting the machine in a safe operating state in the event that critical safety functions are restricted or rendered ineffective by a cybersecurity attack	**Emergency mode** Putting the system in a safe operating state in the event that critical safety functions are restricted or rendered ineffective by a cybersecurity attack	**Emergency mode** Integration of the machines and systems into the asset management in the event of cybersecurity attacks

Cybersecurity assistance and information resources:

- For a checklist for operators of company networks and an example assessment of existing systems, see specialist area AKTUELL FBHM-102 “Safety and Security in networked production” from the DGUV, specialist area Wood and Metal dated October 1, 2018
- ISO/TR 22100-4 “Safety of machinery - Relationship with ISO 12100 - Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cybersecurity)”
- IEC 62443 series of standards “Industrial communication networks - Network and system security”
- IEC 61508 series of standards “Functional safety of electrical/electronic/programmable electronic systems”
- IEC 61511 series of standards “Functional safety - Safety instrumented systems for the process industry sector”

4 – Information for use

If the application of safe design measures and technical protective measures does not provide the required risk reduction, the user shall receive additional warning with regard to prevailing residual risks and be informed of the necessity to take further protective measures (in particular to use personal protective equipment).

Information for use includes, for example:

- Acoustic and optical warning devices
- Information and warnings on the machinery
- Operating instructions including their warning and safety instructions
- Operating procedures, training requirements, or briefing of users
- Instructions about the use of personal protective equipment

NOTE

Information for use shall not be a replacement for other measures!

NOTE

➜ Safe design, risk assessment and risk reduction type-A standard: ISO 12100

➜ Design principles for information for use: EN ISO 20607, EN IEC/IEEE 82079-1

Acoustic and visual warning devices

If the operation of a machine is not monitored, warning devices must be provided on the machine to alert the operator to hazards caused by malfunctions. Warning devices must be clearly and readily understandable. It shall be possible for the operating personnel to check that they are constantly ready for operation. Where residual risks remain, the manufacturer must warn of these.

Figure 122: Autonomous vehicle with a safety laser scanner as a protective device and acoustic and optical warning device

Information and warnings on the machinery

Information and warnings on the machine should take the form of symbols or pictograms whenever possible. They shall be drawn up in the official language of the country in which the machine is being put to market. Additional warnings in other languages may be used. Information that is relevant to safety must be formulated in a way that is clear, easy to understand, succinct, and precise. Interactive means of communication must be easy to understand and support intuitive operation.

Figure 123: Examples of information and warnings on machines

Safety-relevant information in the operating instructions

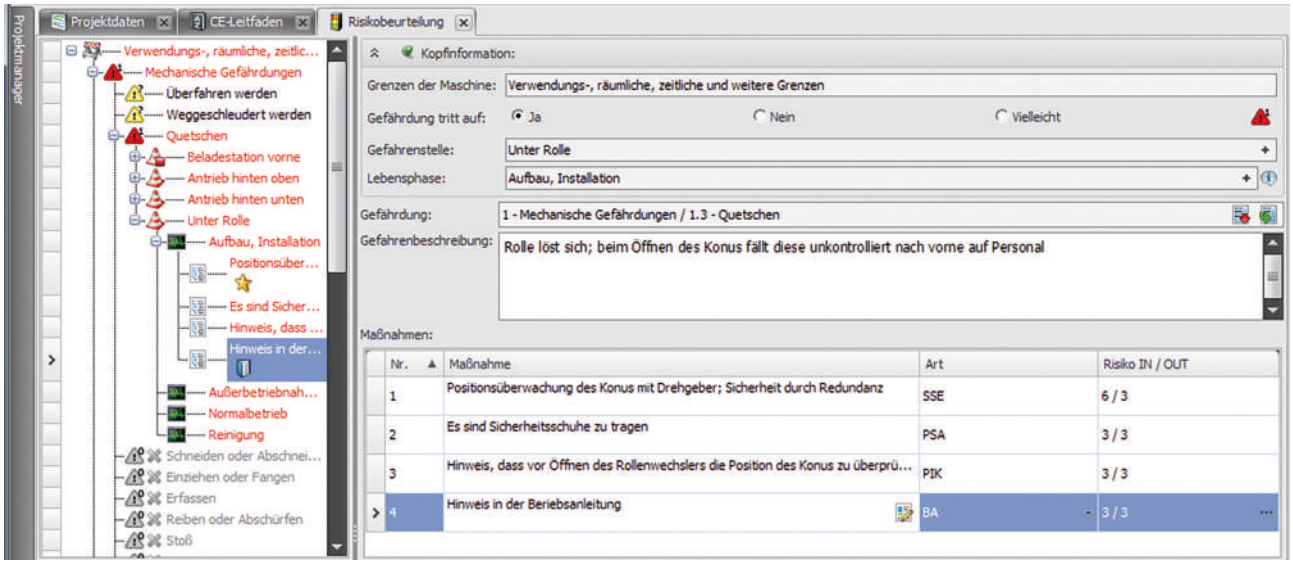
The operating instructions must include all safety-relevant information for the machine. The following information, in particular, must be provided:

- Safety instructions advising how to safely use the machine, as well as any warnings relevant to a specific action
- Description of the intended use, and warnings relating to reasonably foreseeable misuse of the machine
- Notes about commissioning and operation of the machine as well as about required training and/or briefing of operating personnel
- Information on residual risks, including warnings, that remain despite the measures taken to incorporate safety into the design and application of protective devices and complementary protective measures
- Instructions for protective measures to be taken by the user and personal protective equipment requirements
- Conditions under which requirements with regard to stability are met in the various phases of the machine's life cycle
- Safety notes on transport, handling, and storage
- Instructions on the procedures to be followed in the event of accidents or incidents and for safe troubleshooting
- Instructions on safe setup and maintenance and the required protective measures associated with these
- Specification of the spare parts to be used which may affect the health and safety of operating personnel

Documentation

NOTE

The Safexpert® software from the company ibf ("Risk assessment using Safexpert®", page 27) makes it easy to meet the requirements on the technical documentation. For instance the user can integrate information from the risk assessment directly in the instruction handbook.



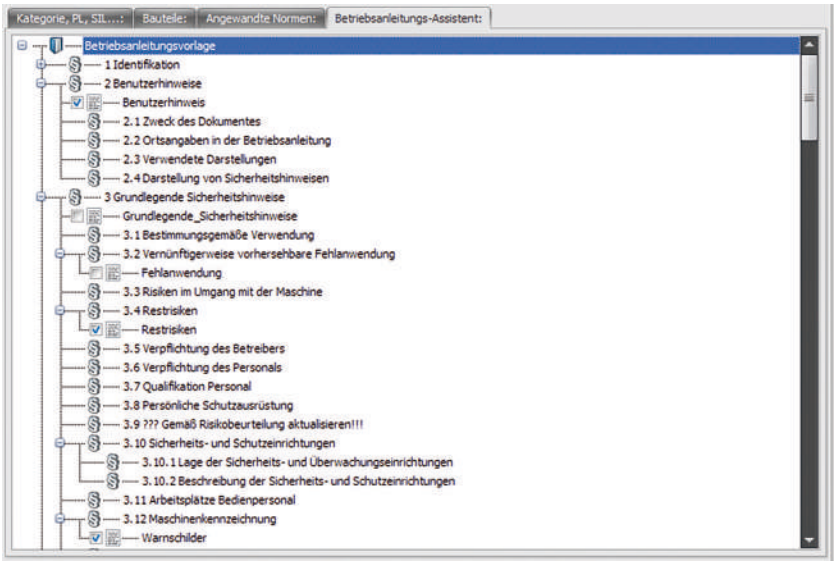


Figure 124: Safexpert® operating instructions wizard

Summary of steps 2, 3 and 4 for risk reduction

General

To reduce the risks posed by the analyzed hazard, proceed in accordance with the 3-step method:

1 Design the machine so that the risk is eliminated as far as possible.
2 Define, apply, and check the required protective measures.
3 Define how any remaining residual risks can be reduced and provide this information to the user.

Technical protective measure

- Either of the ISO 13849-1 (PL) or IEC 62061 (SIL) standards can provide assistance with regard to functional safety.
- Define the safety functions and determine the required safety level for each.
- Draft the safety concept. Select the most effective protective devices and how they will be assembled and integrated into the control system.
- Make sure that the protective measures are implemented effectively and that the required safety level is achieved.

5 – Overall validation

As functional safety is only one component of risk reduction, all measures (design and build, technological, and organizational) shall be assessed for their overall effect as part of an overall validation process.

Figure 125: Service employee from SICK performing an overall validation of a machine

In practice, therefore, it may be the case that an individual technical measure does not reduce risk however a satisfactory result is achieved in the overall context. Sufficient risk reduction can be considered to have been achieved if all of the following questions can be answered with “yes”:

- Have all operating conditions in all phases of the machine's life cycle been taken into account?
- Was the 3-step method used?
- Have the hazards been dealt with or the risks posed by the hazards minimized to the fullest possible practical extent?
- Is there an assurance that the measures taken will not result in new hazards?
- Have users been given sufficient information about and warning of the residual risks?
- Is there an assurance that the protective measures that have been taken will not impair the working conditions of operating personnel?
- Are the protective measures that have been taken compatible with one another?
- Has sufficient consideration been given to the possible consequences of using the machine in a non-commercial or non-industrial environment?
- Is there an assurance that the measures taken will not unduly impair the function of the machine as intended?
- Has the risk been reasonably reduced?

NOTE

SICK offers to check the entire machine with regard to significant hazards as part of a safety inspection. This service is performed by the safety specialists at SICK.

6 – Placing on the market

Once conformity has been ascertained in the context of overall validation (if applicable by involving a notified Body), during the course of the preparation of technical documentation, the declaration of conformity can be issued and the CE marking added to the machine. The declaration of conformity shall take into account all European directives applicable to the machine.

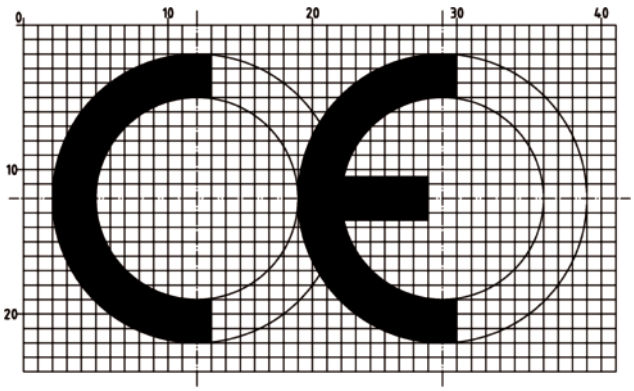


Figure 126: Form of the CE marking according to the Machinery Directive 2006/42 / EC

Technical documentation

The scope of the technical documentation is described in Annex VII, Section A of the Machinery Directive. For incomplete machines, the particular requirements of Annex VII, Section B of the Machinery Directive apply.

Based on the technical documentation, it shall be possible to assess the extent to which the machine meets the requirements of the Machinery Directive. Insofar as is necessary for the purpose of this assessment, the technical documentation shall contain the design, build, and function of the machine.

These documents must be drafted in one or more official European Community languages. This does not apply to the operating instructions of the machine, for which the special provisions of Annex I, Number 1.7.4.1 apply.

Retention period and deadlines

The technical documentation must be held ready for the responsible authorities of the member states as follows:

- From the day of construction of the machine
- For at least 10 years following completion of the last unit
- The technical documentation does not necessarily have to be physically located in the European Community and also does not need to be in material form (e.g., digital storage is permitted). However, the person designated in the EU declaration of conformity shall be able to make the technical documentation available by a reasonable deadline.

NOTE

Note: If the technical documentation is not submitted to the competent national authorities upon justified request, this may give rise to doubts! The question may arise: Does the machine in question actually comply with the essential health and safety requirements?

NOTE

➜See also section "Issuing the declaration of conformity", page 14.

➜See also section "EU conformity assessment procedure for machinery and safety components", page 16.

Scope of the technical documentation

- General description of the machine:
  - Overview drawing of the machine, circuit diagrams of the control circuits along with descriptions and explanations necessary to understand how the machine operates
  - Complete detailed drawings (possibly including calculations), test results, certificates, etc., necessary to examine the extent to which the machine meets essential health and safety requirements
- List of applicable standards and other technical specifications citing the essential health and safety requirements taken from these standards

- Risk assessment documentation ("1 – Risk assessment", page 22) showing which procedure was used:
  - List of the essential health and safety requirements applicable to the machine
  - Description of the protective measures taken to avoid the hazards identified or reduce risk and, if applicable, list of the residual risks posed by the machine
- All technical reports with the results of tests carried out by the manufacturer or a body selected by the manufacturer or the manufacturer's agent
- Instruction handbook for the machine
- Copy of the EU declaration of conformity
- If applicable, copy of the EU declarations of conformity for the other machines or products incorporated into the machine
- If applicable, declaration of incorporation and mounting instructions for incomplete machines

Operating instructions

The person placing the machine on the market (manufacturer or his authorized representative) must supply with the machine an instruction handbook in one of the official EU languages of the Member State in which the machine is placed on the market. These operating instructions supplied with the machine must either be the “original operating instructions” or a “translation of the original operating instructions”. In the latter case, the original operating instructions must also be supplied (all operating instructions for which the manufacturer assumes responsibility are deemed to be “original operating instructions”). For additional information, see "4 – Information for use", page 151.

Responsibility of the user

Employers are responsible for the safety of their employees. Machines shall be ergonomic and be capable of being operated safely according to the qualifications of the machine operators.

As well as acceptance testing to verify safety and inspections on delivery, the correct and proper specification of safety requirements is something that ought to be taken into account as early as when purchasing a machine.

How should machinery be purchased?

The procurement process is crucial to the success of a project to build or modernize a production facility. The following points, for example, should be considered:

- For complex assemblies of machines, designate a “site manager” in accordance with the Machinery Directive.
- Clarify the procedure for the machinery or machine components provided in advance.
- Draw up a contract specifying how additional documentation is to be provided (e.g., risk assessment, etc.) so that it will be easier to make changes downstream.
- Define, as far as possible, the usage of important standards (harmonized standards in the EU) as the basis.
- Agree on a procedure in the event of deviations from harmonized standards.

Safety inspections

Experience shows that in practice, machine safety is not perfect. Protective devices are often manipulated by the machine operator in order to work without hindrance. Other problems are the incorrect positioning of protective devices and improper integration into control systems.

The safety state of work equipment and systems in operation is regulated by EU Directive 2009/104 / EC (“Work Equipment Directive”); it shall be inspected to ensure conformance with applicable national legislation. In particular, Article 4a of the Directive defines the inspection of work equipment. Technical rules, standards or certain regulations can serve as a guide as to how the inspection should be carried out. The user of the respective equipment must perform a risk assessment and is responsible for ensuring that the inspection is carried out and that occupational safety is ensured.

In so doing, the user shall ensure that work equipment is inspected in accordance with the national transposition of the Work Equipment Directive to the country of use.

The following requirements must be met:

1 Type of inspection
2 Scope of the inspection
3 Level of detail of the inspection
4 Inspection intervals
5 Level of competence of the inspector

A safety inspection by SICK provides you with a fast overview of the safety status of your machines.

Parts of SICK's sales organization have already been accredited as an inspection body.

Accreditation by an independent body verifies that SICK is capable of carrying out the activities specified in the accreditation scope with a high level of reliability and quality.

We discuss potential for improvement with you and work in partnership to realize them.

NOTE
Work Equipment Directive, Article 4a Inspection of work equipment

1 The employer shall ensure that where the safety of work equipment depends on the assembly conditions, it shall be subject to an initial inspection (after assembly and before first being put into service) and an inspection after assembly at a new site or in a new location by competent persons within the meaning of national laws and/or practices, to ensure that the work equipment has been assembled correctly and is operating properly.
2 The employer shall ensure that work equipment exposed to conditions causing such deterioration is subject to:
   - Periodic inspections and, where appropriate, testing by competent persons within the meaning of national laws and/or practices; and
   - Special inspections by competent persons within the meaning of national laws and/or practices each time that exceptional circumstances which are liable to jeopardize the safety of the work equipment have occurred, such as modification work, accidents, natural phenomena or prolonged periods of inactivity, in order to ensure compliance with health and safety regulations and the timely detection and rectification of resulting damage.
3 The results of inspections shall be recorded and kept at the disposal of the authorities concerned. They must be retained for a suitable period of time. When work equipment is used outside the undertaking it shall be accompanied by physical evidence that the last inspection has been carried out.
4 Member States shall determine the conditions under which such inspections are made.

Significant modification of machinery

Machines usually have a service life of several decades. The further development of technologies and the requirements of the market lead to a continuous improvement of machines and production systems. In many cases, machines are also modified to fit existing production lines and systems. Such modifications may include features and functions that can have a significant impact on the safety of the machine or production line.

National regulations may impose specific requirements on the modification of existing machinery, while others are limited to general mandatory clauses for the user (employer). The European Machinery Directive also requires that significantly modified machinery comply with the essential health and safety requirements. The Machinery Directive does not clarify, however, what is to be considered a significant modification. The national European occupational health and safety authorities are given the freedom to define the criteria for a significant modification.

The following methodology was developed jointly by industry and occupational health and safety authorities in Germany and has been in use since 2010.

General requirements

When a machine is modified, the procedure described in the Methodology section must be performed to determine if the modification(s) is (are) significant.

Legal note: Limiting the risk assessment and reduction to the modified parts and/or zones of the machine may not be sufficient to comply with national legal requirements.

Methodology

The following steps must be carried out in the specified order (see figure 127, page 160):

Table 59: Steps of the methodology for evaluating significant modifications in machinery

Step	Description
Step 1	Determine if the modifications will result in the occurrence of new hazards. If newly identified hazards result in significant risks, follow Step 3; otherwise, the modifications are considered to be non-substantial.
Step 2	If no new hazards have been identified and the modifications do not increase any of the existing risks, the changes are considered non-substantial. If pre-existing risks are increased by the modifications, follow Step 3.

Step	Description
Step 3	The modifications are considered not to be significant if the existing risk reduction measures adequately reduce the risks arising from the new hazards (Step 1) or from the increased risks (Step 2). Otherwise, follow Step 4.
Step 4	If the new hazards are eliminated by simple protective devices or by simple integration of additional protective devices, or if the increased risk is adequately reduced, the modifications are considered not to be significant. Otherwise, the modification is considered to be significant.

If a modification is considered significant, a risk assessment and risk reduction must be performed in accordance with ISO 12100:2010, but may be limited to those parts and/or zones affected by the modification.

Simple protective devices are:

- Fixed physical guards or
- Movable physical guards, or non-physical guards that do not significantly interfere with the existing safety-related control of the machine.

The **simple integration of additional protective devices** is limited to those that also do not significantly interfere with the existing safety-related parts of control systems (SRP/CS) of the machine:

- The signals of the new protective devices are processed in the existing design of the SRP/CS.
- Independent of the existing safety controller, only the safe stop of the dangerous machine function is affected.

A **non-significant modification** is considered to be:

- Replacement of components of a machine by identical components or components with an identical function and identical safety level.
- Installation of safety devices that result in an increase in the safety level of the machine and do not allow for advanced features or functions.

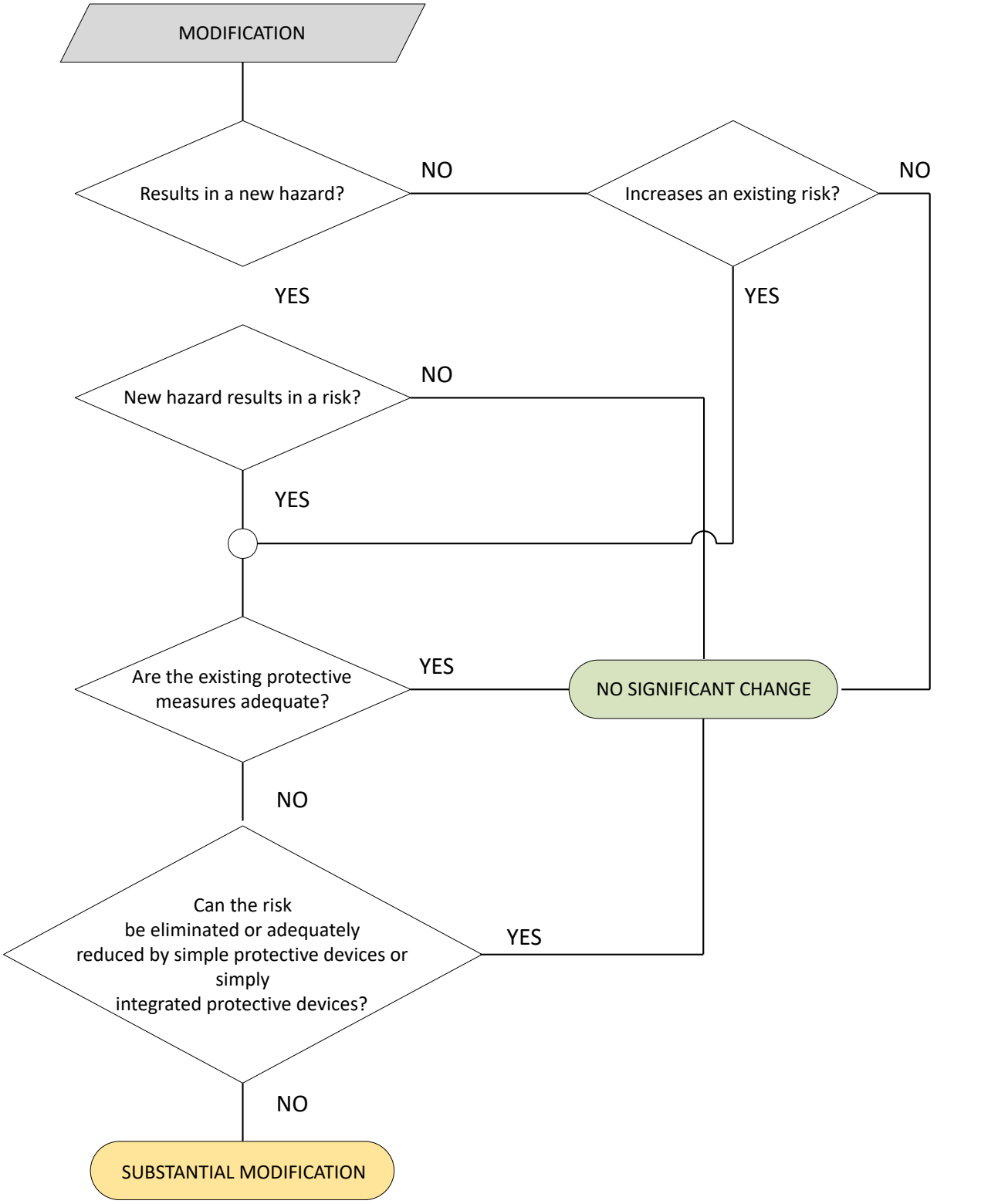


Figure 127: Decision steps for determining a significant modification (Source: Interpretation paper on the subject of "Significant Modification of Machinery", BMAS Germany 2015)

Annex

How SICK supports you

Integrating a safety function into a machine or machine concept requires a high level of safety engineering expertise. Achieving this level of expertise requires not only practical experience and current and extensive safety-related knowledge, but also expertise in the application of appropriate processes.

With more than 70 years of experience in machine safety, SICK is your safety partner with safety expertise.

Our tailored services provide you with the expertise you need to implement your machine safety in a manner that is compliant with the directives.

In doing so, SICK is contributing to the ongoing development of the safety culture in your organization with the following goals:

- Improving the safety of existing machines and systems
- Ensuring integral safety when new machines and systems are purchased
- Supporting designers in the application of the CE procedure and adjusting the design of machines and systems in order to reduce risk

As your partner for machine safety, SICK offers:

- Experience spanning many decades
- Innovative solution ideas at the cutting edge of technology
- International team of experts

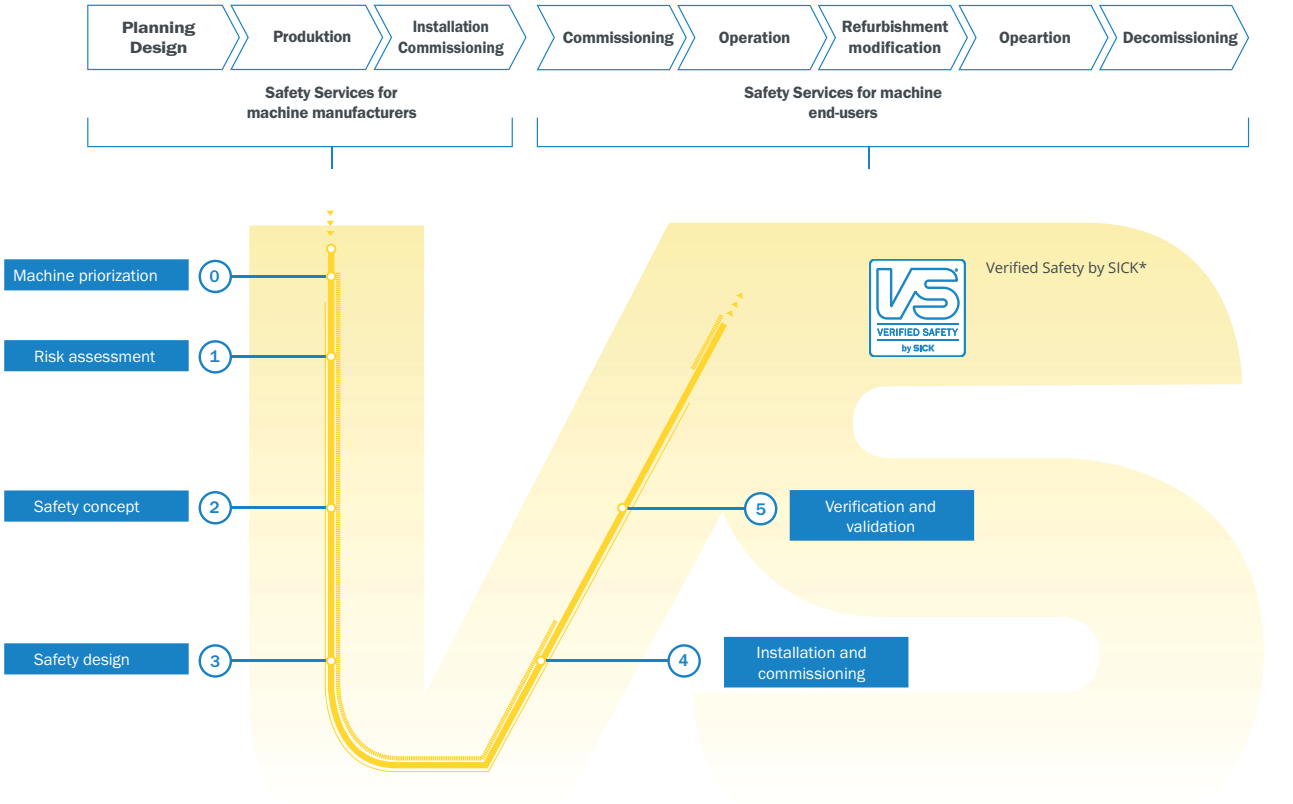
By involving SICK experts at an early stage, the following is achieved:

- Safety will be planned as an integral part of your project.
- Potential weaknesses will be identified early in the process.
- Overdimensioning will be avoided.
- Effectiveness and competitiveness will be ensured.

Services from SICK increase safety and add value.

SICK services for conformity and design of safe machines and systems

As a manufacturer or end user of machines, you are responsible for the safety of the machines you develop or supply. The safety aspects can also change during the life cycle of the machine. Each phase of the machine life cycle poses specific challenges. SICK provides services to support you in these phases.



* When creating and processing customer projects related to functional safety, the “VERIFIED SAFETY by SICK” quality seal ensures compliance with defined processes. As part of quality assurance and defined measures for fault prevention, the work results are subjected to checks by a second person. VERIFIED SAFETY from SICK means functional safety with verifiable quality.

Safety services for machine manufacturers and users

For a safe machine, you have the choice: Take advantage of the experience and expertise of SICK in all phases or get targeted support for individual steps. The closer the cooperation, the better the safety solution can be integrated into your machine.

Certified safety experts accompany you step by step to a safe machine with professional project management. Depending on requirements, the scope of the project can be extended in phases and individually adapted to your needs.

You can find our SICK Consulting Assistant for Safety Services and all our safety services at www.sick.com.

Training and workshops

Figure 128: In-person training at SICK

Practical knowledge for all users

It is generally accepted that the more experience you have, the safer your applications will be. Sharing experience and thereby optimizing applications is an important and integral component of the training seminars and workshops provided by SICK. These therefore focus very much on practical applications.

Tailored training

Based on the needs of our delegates and the training content to be delivered, we will select the best way of sharing knowledge and safeguarding its transfer:

- Safety training
- Standards and directives training
- Workshops
- Online tutorial
- Modular training concepts
- Update training
- Web-based training

NOTE
On request, we can also conduct our training sessions and workshops at your site. Contact us!

Standards and directives training

Legal provisions and standards change over time. Technological change requires that we adapt to innovations. In our modular training seminars for basic safety we share the latest knowledge in the following key areas:

- How to select the right protective device in compliance with standards
- How to integrate a protective device into the overall control system
- How to correctly assess protective measures based on applicable directives, standards, and ordinances

Product, system, and software training

In these training sessions you will get to know our products even better in order to integrate them efficiently, reliably and safely into the planned application.

The general design of our training sessions covers the different phases in the process for selecting and integrating a product:

- Selection
  - Safety aspects
  - Product features and possible applications
- Integration
  - Adding to the application (assembly) and wiring
  - Programming
  - Commissioning
- Safe operation
  - Error analysis and troubleshooting

On request SICK will draw up a customized qualification concept for your application. This service helps to optimize the quality of your work and accelerate knowledge transfer where safety is concerned.

Staying up to date

So that you are always up to date and have your finger on the pulse, we can offer you special options for ongoing and advanced training customized in line with existing levels of knowledge within your organization.

Become a certified functional safety expert or technician.
SICK in conjunction with SGS-TÜV Saar offers a special multi-day training course on functional safety. After passing the examinations at the end, you are permitted to use the title “Certified Functional Safety Application Expert (CFSAE)” or “Certified Functional Safety Application Technician (CFSAT)”, for example on your business card.

CFSAE by SGS-TÜV Saar

CFSAT by SGS-TÜV Saar

NOTE
For the very latest detailed information, visit us on the Internet at www.sick.com/training or take a look at our seminar program.

For training in your country, please contact your SICK representative or visit us at www.sick.com.

SICK – At your side throughout your system's product life cycle

With certified safety products, systems and services customized to meet your needs, SICK is able to support you throughout the life cycle of your machine, from planning, commissioning right through to maintenance and upgrades.

Components and systems

Using certified products and systems makes it easier for machine manufacturers to prove conformity with the requirements of the Machinery Directive and various standards. SICK offers machine manufacturers a wide range of products from simple single-beam safety light-beam sensors, safety light curtains, safety laser scanners, safety camera sensors, and safety switches right through to modular and network-capable safety controllers and software solutions for the conformity of machinery. Solutions for human-material differentiation in automatic loading and unloading points or for robot cell protection are examples of certified safety systems that significantly minimize the development effort for machine manufacturers.

Consultancy: Our knowledge to the advantage of your applications

SICK is a global company with subsidiaries or agencies in approx. 100 industrial countries worldwide where you can receive the specialist consultancy and advisory services you need from our competent employees. They will support you not only by providing technical knowledge about our products but also with their knowledge of the market as well as national legislation and standards.

NOTE

➜ Overview of safety technology products, page 126

➜ All products are listed in our online product finder at **www.sick.com**

➜ To find out more about the services available in your country, contact your national SICK representative or visit us at **SICK LifeTime Services**

An overview of the relevant standards

Table 60: Relevant type-A, B and C safety standards as referenced in this guide

Type	International standard ISO/IEC	European standard EN	Title/Reference
A	ISO 12100	EN ISO 12100	Safety of machinery – General principles for design – Risk assessment and risk reduction
B	ISO 4413	EN ISO 4413	Hydraulic fluid power - General rules and safety requirements for systems and their components
	ISO 4414	EN ISO 4414	Pneumatic fluid power - General rules and safety requirements for systems and their components
	ISO 11161	EN ISO 11161	Safety of machinery - Integrated manufacturing systems - Basic requirements
	ISO 13849-1	EN ISO 13849-1	Safety-related parts of control systems Part 1: General principles for design
	ISO 13849-2	EN ISO 13849-2	Part 2: Validation
	ISO 13850	EN ISO 13850	Emergency stop - Principles for design
	ISO 13851	EN ISO 13851	Two-hand control devices - Functional aspects and design principles
	ISO 13854	EN ISO 13854	Minimum distance to avoid crushing of parts of the human body
	ISO 13855	EN ISO 13855	Positioning of protective devices with respect to the approach speeds of parts of the human body
	ISO 13856-1	EN ISO 13856	Pressure-sensitive protective devices – General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors
	ISO 13856-2	EN ISO 13856-2	Pressure-sensitive protective devices – General principles for design and testing of pressure-sensitive edges and pressure-sensitive bars
	ISO 13856-3	EN ISO 13856-3	Pressure-sensitive protective devices – General principles for design and testing of pressure-sensitive bumpers, plates, wires and similar devices
	ISO 13857	EN ISO 13857	Safety distances to prevent hazard zones being reached by upper and lower limbs
	ISO 14118	EN ISO 14118	Prevention of unexpected startup
	ISO 14119	EN ISO 14119	Interlocking devices associated with physical guards - Principles for design and selection
	ISO 14120	EN ISO 14120	Physical guards – General requirements for the design and construction of fixed and movable guards (currently being revised for future publication as EN ISO 14120)
	ISO 14122-1	EN ISO 14122-1	Safety of machinery - Permanent means of access to machinery - Part 1: Choice of fixed means and general requirements of access
	ISO 14122-2	EN ISO 14122-2	Safety of machinery - Permanent means of access to machinery - Part 2: Working platforms and walkways
	ISO 14122-3	EN ISO 14122-3	Safety of machinery - Permanent means of access to machinery - Part 3: Stairs, stepladders and guard-rails
	ISO 14122-4	EN ISO 14122-4	Safety of machinery - Permanent means of access to machinery - Part 4: Fixed ladders
	ISO 14123-1	EN ISO 14123-1	Safety of machinery - Reduction of risks to health resulting from hazardous substances emitted by machinery - Part 1: Principles and specifications for machinery manufacturers
	ISO 14123-2	EN ISO 14123-2	Safety of machinery - Reduction of risks to health resulting from hazardous substances emitted by machinery - Part 2: Methodology leading to verification procedures
	ISO 14159	EN ISO 14159	Safety of machinery - Hygiene requirements for the design of machinery
	ISO 19353	EN ISO 19353	Safety of machinery - Fire prevention and fire protection
	ISO 20607	EN ISO 20607	Safety of machinery – Instruction handbooks – General principles for design

Type	International standard ISO/IEC	European standard EN	Title/Reference
	IEC 60204	EN 60204-1	Electrical equipment of machines Part 1: General requirements
	IEC 61496-1	EN 61496-1	Electro-sensitive protective devices Part 1: General requirements and tests
	IEC 61496-2	EN IEC 61496-2	Part 2: Particular requirements for equipment using active optoelectronic protective devices (AOPDs)
	IEC 61496-3	EN IEC 61496-3	Part 3: Particular requirements for active optoelectronic protective devices responsive to diffuse reflection (AOPDDR)
	IEC 61496-3	EN IEC 61496-3	Part 3: Particular requirements for active optoelectronic protective devices responsive to diffuse reflection (AOPDDR)
	IEC 62061	EN 62061	Functional safety of safety-related electrical, electronic and programmable electronic control systems
	IEC 62046	EN IEC 62046	Application of protective equipment to detect the presence of persons
C	–	EN 201	Plastics and rubber machines; Injection molding machines – Safety requirements
	–	EN 289	Plastics and rubber machines; Presses and injection molding machines; Safety requirements for the design
	–	EN 415-X	Packaging machines (*: Only Parts -1, -3, and -5 to -9 of this standard are harmonized)
	–	EN 422	Rubber and plastics machines. Safety – blow molding machines intended for the production of hollow articles – requirements for the design and construction
	–	EN 528	Automated storage and retrieval systems – Safety requirements
	–	EN 710	Safety requirements for foundry molding and coremaking machinery and plant and associated equipment
	–	EN 869	Safety requirements for pressure metal diecasting units
	ISO 1010-X	EN ISO 1010-X	Printing and paper converting machines
	–	EN 1114-1	Plastics and rubber machines – Extruders and extrusion lines Part 1: Safety requirements for extruders
	–	EN 1459	Safety of machinery – Variable-reach trucks
	–	EN 1526	Safety of industrial trucks – Additional requirements for automatic functions on trucks
	–	EN 1612	Plastics and rubber machines – Reaction molding machines Part 1: Safety requirements for metering and mixing units
	–	EN 1672-1	Food processing machinery – Safety and hygiene requirements – General principles for design
	ISO 3691-4	EN ISO 3691-4	Safety of industrial trucks – Driverless trucks and their systems
	ISO 10218-1	EN ISO 10218-1	Industrial robots – Safety requirements Part 1: Robots
	ISO 10218-2	EN ISO 10218-2	Part 2: Robot systems and integration
	ISO 11111-1	EN ISO 11111-1	Textile machinery – Safety requirements Part 1: General requirements
	ISO 12622	EN 12622	Hydraulic press brakes
	–	EN ISO 16092-1 in conjunction with EN ISO 16092-2 (replaces EN 692)	Machine tools - Safety - Presses - Part 1: General safety requirements Machine tools - Safety - Presses - Part 2: Mechanical presses

Type	International standard ISO/IEC	European standard EN	Title/Reference
	–	EN ISO 16092-1 in conjunction with EN ISO 16092-3 (replaces EN 693)	Machine tools - Safety - Presses - Part 1: General safety requirements Machine tools - Safety - Presses - Part 3: Safety requirements for hydraulic presses
	–	EN ISO 16092-1 in conjunction with EN ISO 16092-4 (replaces EN 13736)	Machine tools - Safety - Presses - Part 1: General safety requirements Machine tools - Safety - Presses - Part 4: Pneumatic presses
	ISO 20430	EN ISO 20430	Plastics and rubber machines - Injection molding machines - Safety requirements

Useful links

Table 61: List of relevant links

Where can I find ...?	
Text of directives (EU)	Complete texts of the directives among others in the EUR-Lex legal information system of the European Union: eur-lex.europa.eu
Lists of standards	Europäische Komission, harmonised standards www.baua.de www.vdma.org Europäische Kommission: www.ec.europa.eu/growth/index_en.htm Beuth Verlag GmbH: www.beuth.de
Publishers of standards, international	CEN: www.cen.eu/cenorm/homepage.htm CENELEC: www.cenelec.eu ISO: www.iso.org/iso/home.htm IEC: www.iec.ch
Publishers of standards, in German	Germany (DIN): www.din.de Austria (ON): www.as-institute.at Switzerland (SVN): www.snv.ch

Where can I find ...?	
Publishers of standards, European	Belgium (NBN): www.nbn.be Bulgaria (BDS): www.bds-bg.org Denmark (DS): www.ds.dk Estonia (EVS): www.evs.ee Finland (SFS): www.sfs.fi France (AFNOR): www.afnor.org Greece (ELOT): www.elot.gr United Kingdom (BSI): www.bsigroup.com Ireland (NSAI): www.nsai.ie Iceland (IST): www.stadlar.is Italy (UNI): www.uni.com/it Latvia (LVS): www.lvs.lv Lithuania (LST): www.lsd.lt Luxembourg (SEE): www.see.lu Malta (MSA): www.msa.org.mt Netherlands (NEN): www2.nen.nl Norway (SN): www.standard.no Poland (PKN): www.pkn.pl Portugal (IPQ): www.ipq.pt Romania (ASRO): www.asro.ro Sweden (SIS): www.sis.se Slovenia (SIST): www.sist.si Slovakia (SUTN): www.sutn.sk Spain (AENOR): www.aenor.es Czech Republic (CNI): www.unmz.cz/urad/unmz Hungary (MSZT): www.mszt.hu Cyprus (CYS): www.cys.org.cy
Notified certification bodies Germany	European Commission, Notified Bodies Germany
Notified certification bodies Austria	European Commission, Notified Bodies Austria
Notified certification bodies Switzerland	European Commission, Notified Bodies Switzerland
List of expert committees within Employers' Liability Insurance Associations (Germany)	Specialist areas of the DGUV
Accident insurers	Germany: Employer's Liability Insurance Associations/Accident Insurance Funds Austria: General accident insurance: www.auva.at Switzerland: Swiss Accident Insurance Fund: www.suva.ch

Co-authors and acknowledgments

SICK AG and the editorial team would like to express our sincere thanks to all co-authors who have contributed to this guide by annotating the text with necessary corrections, providing photographs, or submitting text. Numerous readers of the previous edition of this guide have also played their part in the success of this update by sharing their expert specialist knowledge with us and providing feedback from practical applications. Thank you for your support!

In particular we would like to thank (in alphabetical order):

- Dr. Tilmann Bork, Festo SE & Co. KG
- Pablo Ruiz, Festo SE & Co. KG
- SEW-EURODRIVE GmbH & Co KG

8007988/2024-03-13/en

SICK AT A GLANCE

SICK is a leading manufacturer of intelligent sensors and sensor solutions for industrial applications. With almost 7,000 employees and over 50 subsidiaries and equity investments as well as numerous representative offices worldwide, we are always close to our customers. A unique range of products and services creates the perfect basis for controlling processes securely and efficiently, protecting individuals from accidents and preventing damage to the environment.

We have extensive experience in various industries and understand their processes and requirements. With intelligent sensors, we can deliver exactly what our customers need. In application centers in Europe, Asia and North America, system solutions are tested and optimized in accordance with customer specifications. All this makes us a reliable supplier and development partner.

Comprehensive services round out our offering: SICK LifeTime Services provide support throughout the machine life cycle and ensure safety and productivity.

For us, that is “Sensor Intelligence.”

Worldwide presence:

Australia, Austria, Belgium, Brazil, Canada, Chile, China, Czech Republic, Denmark, Finland, France, Germany, Great Britain, Hungary, India, Israel, Italy, Japan, Malaysia, Mexico, Netherlands, New Zealand, Norway, Poland, Romania, Russia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Arab Emirates, USA, Vietnam.

Detailed addresses and additional representatives → www.sick.com