Guide for Safe Machinery

SIX STEPS TO A SAFE MACHINE

SICK
Sensor Intelligence.

Six steps to a safe machine

8007988/2015-07-07
Subject to change without notice

Safe machinery provides legal protection for both manufacturer and user. Machine users 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. These regulations are subject to regional variations. 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 (formerly also called a hazard analysis).
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 cannot be tolerated, 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.

We can guide you to safe machinery in 6 steps. The procedure is outlined on the left.

About this guide

What does the guide contain?
In front of you is an extensive guide on the legal background relating to machinery 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.
This guide describes the legal requirements relating to machinery in the European Community 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 only 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.

Who is this guide for?
This guide is aimed at manufacturers, operating organizations, designers, system engineers, and all individuals who are responsible for machine safety. (For reasons of legibility we will use mostly male terms in this guide.)

Your editorial team

Left to right: Max Dietrich, Rolf Schumacher, Doris Lilienthal, Harald Schmidt, Hans-Jörg Stubenrauch, Otto Görnemann, Matthias Kurrus (no fig.)

→ In this guide, references to further standards and aids are marked with a blue arrow.

Safeguarding 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 work process were something of a nuisance; for this reason, they were often not used at all.
Innovative technology has enabled protective devices to be integrated into the work process. As a result, they are no longer a hindrance for the operator; in fact, they often even help productivity.

For this reason, reliable protective devices integrated into the workplace are essential these days.

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.
The following objective can be derived from this situation:
Operators and maintenance personnel shall be able to rely on the safety of a machine!

It is often said 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.

Safety is a management task

Decision-makers 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 organization. And not without reason: after all, nine out of ten accidents are due to human error.

Involvement of the employees results in acceptance

It is very important that the needs of operators and maintenance personnel are included in the planning at concept level. Only an intelligent safety concept matched to the work process and the personnel will result in the necessary acceptance.

Expert knowledge is required

The safety of machinery depends to a large extent on the correct application of directives and standards. In Europe, national legal requirements are harmonized through European directives such as the Machinery Directive.

These directives describe general requirements that are specified in more detail by standards. European standards are also often accepted outside Europe.
Implementing all these requirements in a practical manner requires extensive expert knowledge, application knowledge, and many years of experience.

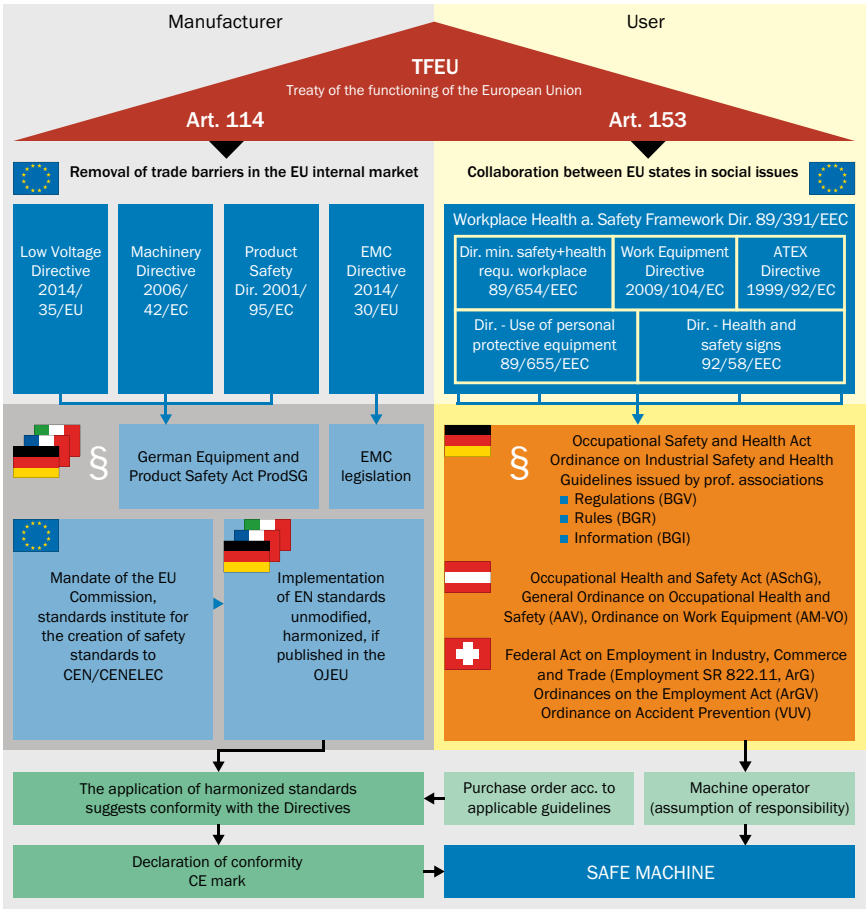
8007988/2015-07-07
Subject to change without notice

European directives

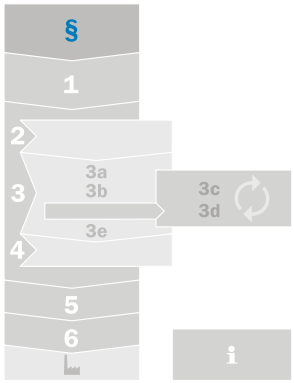
One of the fundamental principles of the European Community is the protection of the health of its citizens both in the private and in the professional sphere. A further fundamental principle is the creation of a single market with free movement of goods.
In accordance with the Treaty on the Functioning of the European Union, the European Commission and the Council of the European Union have passed various directives with the aim of achieving free movement of goods and protecting its citizens.

The Member States shall implement these directives in their national law. The directives define basic objectives and requirements and, as far as possible, they are kept technologically neutral. 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



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



In this chapter ...

§

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

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, a "new Machinery Directive" (2006/42/EC) was passed which replaces the previous version. All EC Member States were obliged to implement the new directive by 2009/12/29.

As of 2009/12/29, only Machinery Directive 2006/42/EC is to be implemented!

The Machinery Directive was implemented in the German-speaking countries as follows:
- Germany: Ninth ordinance (Machinery Ordinance/9. ProdV) to the Product Safety Act (ProdSG) dated 2011/11/08
- Switzerland: Federal law on product safety (PrSG) dated 2009/06/12 and Ordinance on the safety of machinery (Machinery Ordinance) dated 2008/04/02
- Austria: Federal act on protection against dangerous products (Product Safety Act 2004 [PSG 2004]) and Machine safety ordinance 2010

The member states shall not prohibit, restrict, or prevent the distribution and commissioning of machinery and safety components which comply with the Machinery Directive. It is also forbidden for them to apply national laws, ordinances, or standards to impose more stringent requirements on machinery quality!

8007988/2015-07-07
Subject to change without notice

§

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 aims to ensure that the use of work equipment is compliant with minimum regulations in order to improve occupational health and safety. Each member state is allowed to add its own national requirements: for example on the inspection of work equipment, service or maintenance intervals, use of personal protective equipment, design of the workplace, etc. The requirements of the Work Equipment Directive as well as national requirements and regulations are in turn implemented in national laws.

- 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

What are the obligations for machinery manufacturers?

Safe design of machinery

The manufacturers are obliged to construct their machines compliant with the essential safety and health requirements of the Machinery Directive. The manufacturers shall take account of the safety integration during the design process. In practice, this means that the designer shall perform risk assessment as early as during the development phase of the machine. The resulting measures can flow directly into the design. Steps 1 to 5 of this Guide describe in detail how to proceed here.

Preparation of operating instructions

The machine manufacturer shall prepare operating instructions, known as “original operating instructions”. A set of operating instructions in the official language of the country of use shall be supplied with every machine. These operating instructions supplied with the machine shall either be the original operating instructions or a translation of the original operating instructions. In the latter case, the original operating instructions are also to be supplied. Original operating instructions are all operating instructions published by the machine manufacturer, independent of language.

Preparation of technical documentation

The machine manufacturer shall prepare technical documentation according to Annex VII of the Machinery Directive. This technical documentation ...

- 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
- 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

If the machine manufacturer has built the machine appropriately, 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 complete process for the conformity assessment. A differentiation is made between two procedures for machinery (➜ "The EC conformity assessment process for machinery and safety components" ➜ §-6).

- Standard procedure: Machines that are not listed explicitly in Annex IV of the Machinery Directive are subject to the standard process. The requirements described in the "Essential health and safety requirements" section of Annex I shall be met. It is the responsibility of the manufacturer to apply the CE marking, without involving a test body or the authorities ("self-certification"). However, the manufacturer shall first compile the technical file so that the documentation can be submitted to the national authorities on request.
- 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 safety components; this list includes electro-sensitive protective equipment such as photoelectric safety switches and safety laser scanners. The requirements described in the "Essential health and safety requirements" section in Annex I of the Machinery Directive shall be met first. If harmonized standards exist for the machine or safety components and these standards cover the entire range of essential health and safety requirements, the declaration of conformity can be reached in one of three ways:
- Self-certification
- EC type examination by a notified body
- Use of a full quality management system that has been assessed

8007988/2015-07-07
Subject to change without notice

If no harmonized standards exist for the machine or if the machine or parts of the machine cannot be built according to harmonized standards, the declaration of conformity can only be reached as follows:

- EC type examination by a notified body: In the case of a test by a notified body, the manufacturer shall make his machine and the related technical documentation available so that it can be determined by means of an "EC type examination" whether the machine meets the essential health and safety requirements. The notified body tests for compliance with the directive and issues an EC type examination certificate that contains 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 always responsible for the effective and appropriate use of the QMS. See also Annex X to the Machinery Directive.

Marking of the machine as CE-compliant

Once all the requirements have been met, the CE marking shall be applied to the machine.

Warning! The CE marking can only be applied if the machine meets all applicable European directives. (Only then is a product 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" a collection 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.

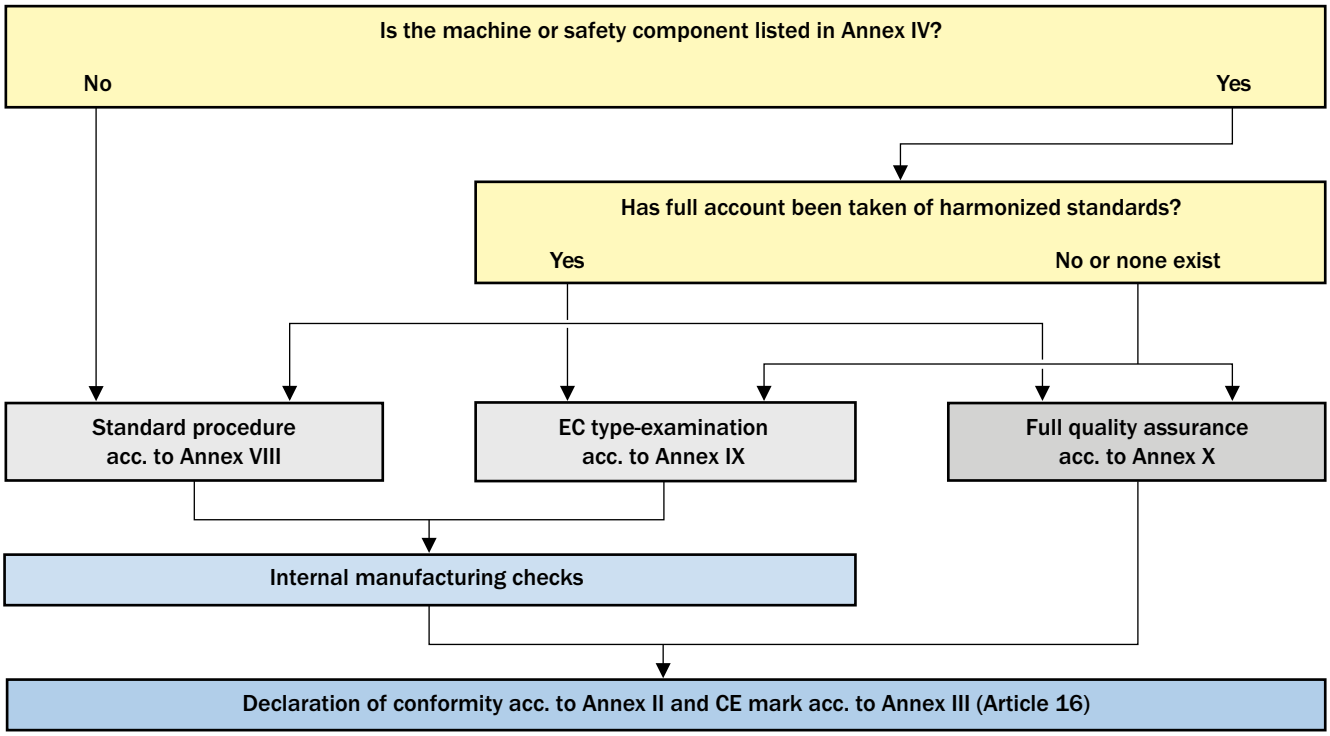
Partly completed machinery cannot meet all requirements of the Machinery Directive. Therefore, the Machinery Directive regulates their free trade using a special procedure:

- 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).

→ See also section "Test bodies, insurance providers, and authorities" → §-12

§

EC conformity assessment procedure for machinery and safety components



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 the official language of the country of use. The original version is also to be supplied with the product.
- You shall complete a declaration of conformity and mark the machine or the safety component with the CE mark.

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

- You shall comply with the requirements of the Work Equipment Directive
- You shall find out whether further national requirements (e.g., testing of work equipment, service or maintenance intervals, etc.) exist and comply with them

8007988/2015-07-07
Subject to change without notice

Standards

This Guide essentially references international standards (ISO-IEC). A list of relevant standards is provided in the annex. The list also contains their regional equivalents (e.g. EN) or equivalent national standards to the referenced International Standards (ISO, IEC) based on the regional validity of this Guide.

Relevant international and local standards are listed in Annex i starting i-6.

Standards are 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 of the standards to be applied is an aid for the machine manufacturer for compliance with the legal requirements.

Global standardization organizations and structures

ISO (International Standardization Organization)
ISO is a worldwide network of standardization organizations from 157 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.

Different types of standard

There are three different types of standard:

A-type standards
(Basic safety standards) contain basic terminology, principles of design and general aspects that can be applied to all machinery.

B-type standards
(Group safety standards) address a safety aspect or protective device that can be used for a wide range of machinery. B-type standards are in turn divided into:

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

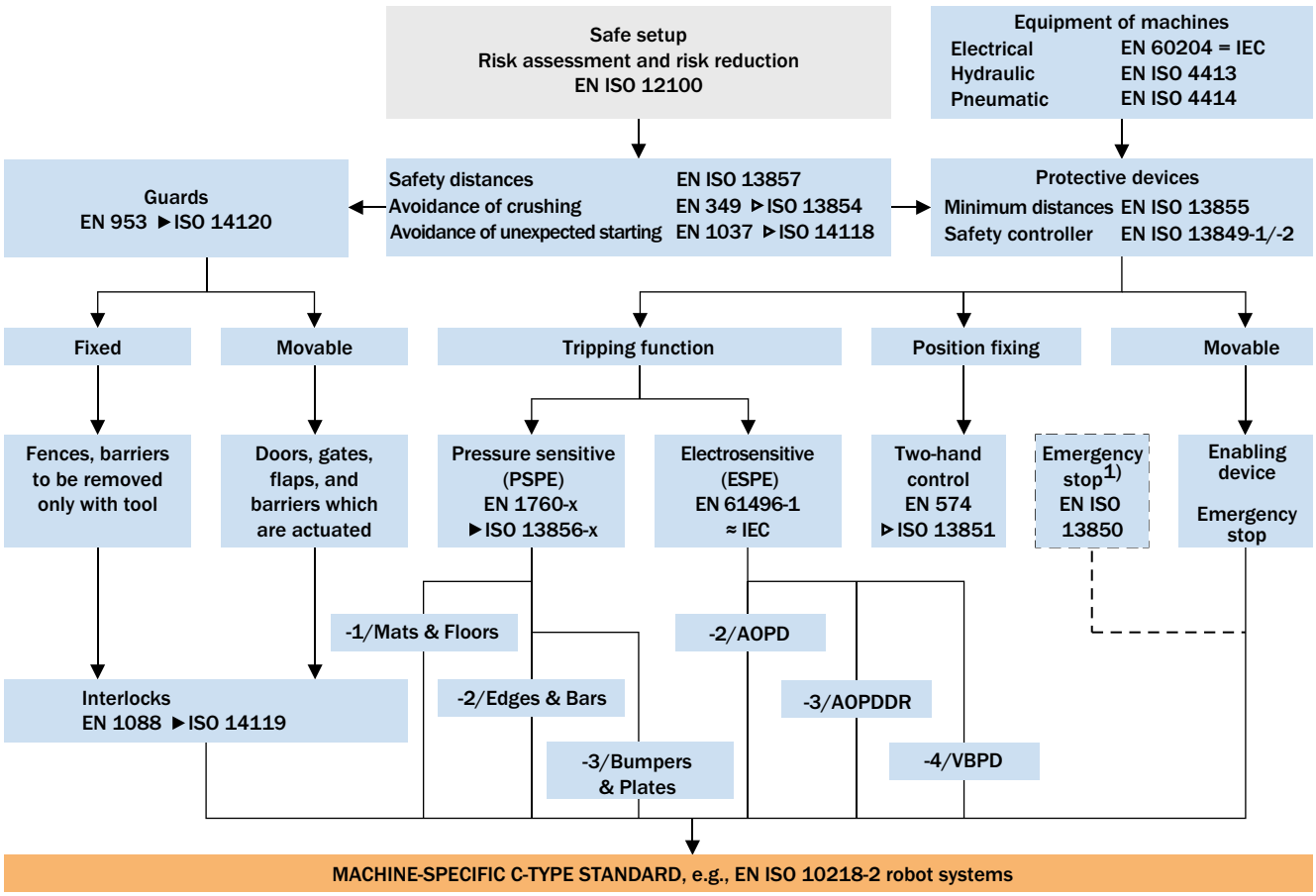
C-type standards
C-type standards contain all safety requirements for a specific machine or a type of machine. If this standard exists, it has priority over the A-type or B-type standard. Nevertheless, a C-type standard can refer to a B-type standard or an A-type standard. In all circumstances the requirements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

Many A-type and B-type standards are currently being revised, along with a number of important C-type standards. This will result in a new numbering system for the EN-ISO series of standards. However, as a rule there are transition periods. For this reason, a standard under revision may apply in 5 or even 6 years.

→ You will find a list of important standards in the “Overview of the relevant standards” section of the Annex → i-6

§

Overview of protective devices and related standards



1) Emergency stop is a safety measure but it is not a protective device!
▶ EN standard is currently being revised and will be published as an EN ISO standard.
▷ EN standard is to be revised in the future and will be published as an EN ISO standard.
AOPD active opto-electronic protective device
AOPDDR active opto-electronic protective device responsive to diffuse reflection
VBPD vision based protective device

Type A standards
Type B standards
Type C standards

8007988/2015-07-07
Subject to change without notice

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 EU members. 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. Similar to the situation between CEN and ISO, 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 standardization organizations prepare and publish national standards as per the legal requirements of the member state concerned. 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 European 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 prepare 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

To be able to implement the objectives and requirements defined in the European directives in practice, technical standards shall describe and specify these requirements in detail. Standards which describe the requirements of European directives in concrete detail in such a way that conformity with the standards provides presumption of conformity with the directives are classed 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 produced as follows:

1. The EU Commission, as the executive organ of the EU, issues a mandate to CEN or CENELEC to prepare a European standard to specify in detail the requirements of a directive.
2. The preparatory work is undertaken in international forums in which the technical specifications to meet the essential safety requirements in the directive(s) are defined.
3. As soon as the standard is accepted by a balloting, it is published in the Official Journal of the EU. The standard shall also be published in a member state (e.g., as DIN EN). It is then a harmonized European standard.

- A harmonized European standard is used as a reference and replaces all national standards on the same subject.
- The conformity 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.

➜ Overview of standardization: www.normapme.com
➜ A list of the standards with presumption of conformity with the directives is available at ec.europa.eu

- The application of standards, independent of whether they are harmonized or not, is not a requirement of the Machinery Directive. However, the application of harmonized standards justifies what is referred to as the “presumption of conformity” that the machine meets the requirements of the Machinery Directive.
- If a C-type standard exists for a type of machine, then this standard has priority over all other A-type and B-type standards and any information in this guide. In this case, only the C-type standard applied justifies the presumption of conformity for meeting the requirements of the Machinery Directive.

8007988/2015-07-07
Subject to change without notice

Summary: Standards

- Technical standard specify in more detail the objectives defined in the European directives.
- The application of harmonized standards justifies 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 A-type standards (basic safety standards), B-type standards (group safety standards), and C-type standards (standards on the safety of machinery). If a C-type standard exists, it has priority over the A-type or B-type standard.

§

Test bodies, insurances, and authorities

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 in the UK from the HSE and DTI, for example.

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 normally employ highly competent specialists.

Notified bodies
Each EC 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 EC type examinations and to issue EC 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.

Insurances

Berufsgenossenschaften (professional associations)/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 – Authorities

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.

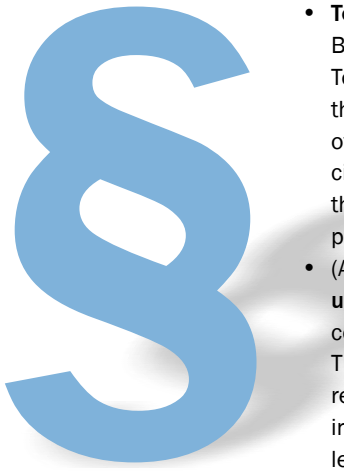
➜ You will find a list of important addresses in the “Useful links” section of the Annex ➜ i-8.

8007988/2015-07-07
Subject to change without notice

Basics of product liability

The term **product liability** is often used as a generic term for any form of liability related to a product on the part of a manufacturer or seller (including liability for product defects or for damage caused by them). However, in legal terms there are considerable differences depending on the nature of the damage or its cause. First, a differentiation is to be made between liability for defects and product liability in the broader sense.

Liability for defects (warranty) is the liability for defects on the product itself. Claims resulting from defect liability can only be made between the parties to a contract, not by any other third party.



Product liability in the broader sense can be further broken down:

- **Tortious liability** (under German law defined in § 823 of BGB).
  Tortious product liability applies if someone intentionally or through negligence harms another (in this context by means of a product he has manufactured). Any injured party can cite this precept if the prerequisites below exist, including those who are not parties to a contract (referred to as third parties).
- (Actual) **product liability in accordance with the law on product liability** (German ProdHaftG) can be cited by parties to a contract and also third parties.
  The German law on product liability is based on an EU directive. There is, therefore, a comparable legal arrangement in all European countries. In addition, there are equivalent legal arrangements in many non-European countries. A brief overview of the arrangements that apply under German law appears below. However, it deliberately lists only the key points and not all prerequisites and exclusions.

Prerequisites

The liability of the manufacturer is defined in § 1 of the German ProdHaftG as follows:

> "If due to a defect in a product an individual is killed, injured, or his health harmed, or property damaged, the manufacturer of the product has the obligation to pay the resulting damages." (Literal translation of the German law)

This clause results in the following requirements:

Manufacturer (§ 4 of German ProdHaftG)
The manufacturer shall have placed the product on the market. This term includes those who import a product into the European economic area or market the product produced by another manufacturer as a private-label product using their own label (known as "quasi-manufacturers").

Defective product (§ 3 of German ProdHaftG)
If a product does not provide the safety that can be expected taking into account all circumstances.

Damage caused by the defective product: injury or harm to health, or damage to property (but not to the product itself and only to items that are normally intended for private use or consumption and that were used primarily by the injured party). Purely financial losses are not compensated via the German ProdHaftG; the only exception is if the financial losses are a direct consequence of an injury or harm to health or damage covered by the German ProdHaftG (e.g., costs of medical treatment, regular payment due to a reduction in ability to earn a living, etc.).
Unlike claims for damages under statutory rights or due to tortious liability, for liability in accordance with the German ProdHaftG no blame is necessary; liability can, therefore, arise even if the necessary due care has been taken in placing the product on the market (and, therefore, without negligence). This is a case of what is known as strict liability in which for the substantiation of the liability it is sufficient if a hazard, which materializes later, arises in the context of a permitted activity.

§

Manufacturer obligations

A differentiation is made between several types of defect that can substantiate liability in accordance with the German ProdHaftG:

Design defects
These defects are caused by the design of the product, e.g., by the technical design or by the selection of the materials; they materialize across all products manufactured.

Manufacturing defects
Manufacturing defects are defects in individual products or batches that occur during production; in accordance with the ProdHaftG, the manufacturer is also liable for what are referred to as outliers.

Instruction defects
Instruction defects occur if risks are caused by defective instructions for the product (e.g., operating instructions); these defects also include the lack of warnings or hidden warnings. This is a case of what is known as strict liability in which for the substantiation of the liability it is sufficient if a hazard, which materializes later, arises in the context of a permitted activity. The German ProdHaftG therefore places the obligation on the manufacturer to ensure the product is safe during development, production, and in the instructions.

Here above all attention is to be paid to compliance with mandatory statutory provision – if a defect is (only) due to compliance with these provisions, the manufacturer is not liable. In this context technical standards (European standards – EN – or national standards such as in Germany DIN, VDE, etc.) shall be taken into consideration as a minimum standard for the necessary safety. The obligations on the manufacturer can also go beyond compliance with laws or technical standards, if measures to ensure product safety could legitimately have been expected. According to high court decisions, compliance with EN standards is no longer sufficient to meet the manufacturer's legal duty to ensure safety if the development has gone beyond the EN standards or if the use of a device produces a hazard that is not taken into account in EN standards.

Extent of loss

In principle the manufacturer shall pay in full the damages the injured party has suffered. The German ProdHaftG (law on product liability) only includes a limit for personal injury. Here a maximum liability limit of 85 million euros applies. Further limiting of liability in relation to injured parties such as users or other third parties is not possible as there is no contract. It is also not permitted to limit liability in relation to customers by means of general terms and conditions or specific contracts.

The manufacturer can obtain protection by concluding a product liability insurance policy with appropriate cover.

Summary: Product liability

- Avoid liability in accordance with the ProdHaftG (German law on product liability):
  - Follow the applicable standards
  - Check whether further measures are necessary to ensure the safety of a product
- Avoid defects by means of rigorous quality assurance and quality control
- Minimize the remaining risk for the manufacturer with adequate insurance

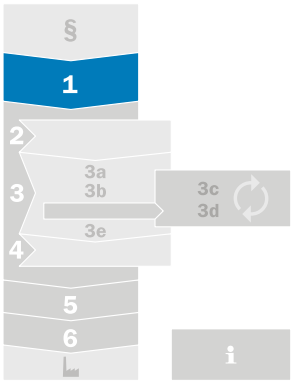
It remains to be stated that – provided the case does not involve a shift in the burden of proof – in the event of a claim the injured party always bears the burden of proof that a defective product has led to injury or damage and was the cause of the claim. This task is not always straightforward, particularly if there are several possible causes.

8007988/2015-07-07

Step 1; Risk assessment

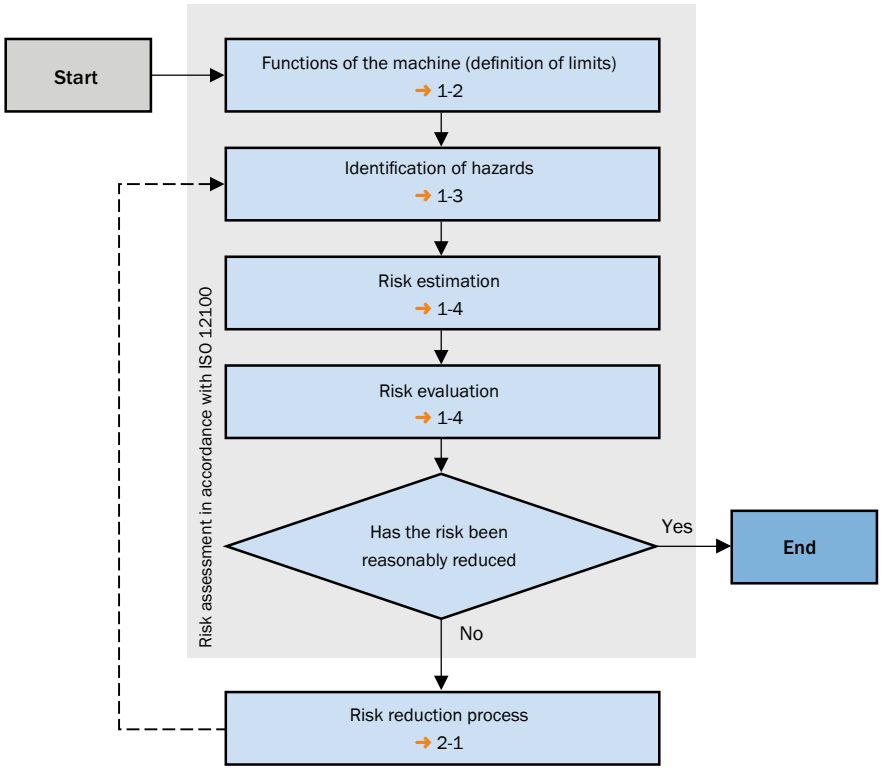
When designing a machine, the possible risks must be analyzed and, where necessary, additional protective measures must be taken to protect the operator from any hazards that may exist.
To aid the machine manufacturer with this task, the standards define and describe the process of risk assessment. A risk assessment is a sequence of logical steps that facilitate the systematic analysis and evaluation of risks. The machine must be designed and built taking into account the results of the risk assessment.

Where necessary, a risk assessment is followed by risk reduction, which is achieved by applying suitable protective measures. A new risk should not result from the application of protective measures. The repetition of the entire process (risk assessment and risk reduction) may be necessary to eliminate hazards as far as possible and to sufficiently reduce the risks identified or newly emerged. In many C-type standards the risk assessment is defined to suit the specific machine and application. If no C-type standards are applicable or they are insufficient, the requirements in the A-type and B-type standards can be used.



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

The risk assessment process



In this chapter ...

- The process must 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 are to 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 place of use
- Planned life limit
- 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

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)

Malfunctions and disturbances to be expected

There is significant potential for hazards due to malfunctions and disturbances in the components relevant to functionality (in particular components of the control system). Examples:

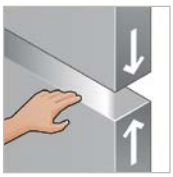
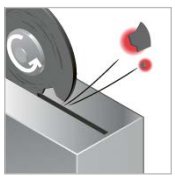
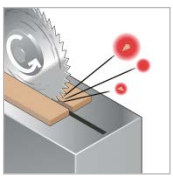
- Reversing of roller movement (with the result that hands are drawn in)
- Movement of a robot outside its programmed working area

8007988/2015-07-07

Identification of hazards

After the definition of 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.

In particular the machine manufacturer should take into account the dangers listed below ...	**... in all phases of the service life of the machine.**
• Mechanical hazards • Electrical hazards • Thermal hazards • Hazards generated by noise • Hazards generated vibrations • Hazards generated by radiation • Hazards generated by materials and substances • Hazards generated by neglecting ergonomic principles during the design of machinery • Slipping, tripping, and falling hazards • Hazards related to 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

Examples of mechanical hazards at machines/systems			
	Cutting		Crushing
	Shearing		Stabbing
	Drawing in or trapping		Drawing in or trapping
	Entanglement		Impact
	Impact from broken parts		Impact from ejected chips

Risk estimation and risk evaluation

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

Risk	=	Extent of damage	×	Probability of occurrence

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

- 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 defined 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

Various tools are available for the estimation of risks; these include tables, risk graphs, numeric methods, etc.
Based on the results of the risk estimation, the **risk evaluation** defines whether the application of protective measures is necessary and when the necessary risk reduction has been achieved.

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

Documentation

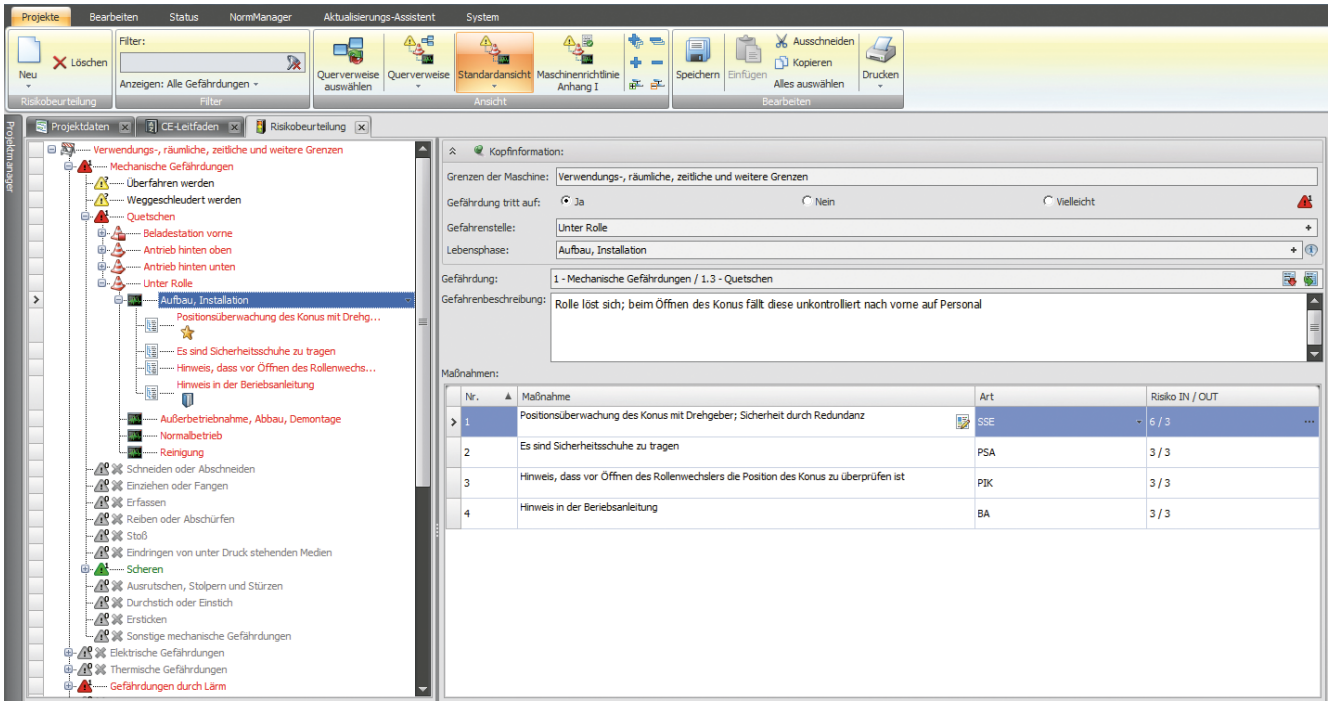
The risk assessment documentation shall include the procedure applied and the results obtained, as well as the following information:

- 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 prepared during the risk assessment

The Machinery Directive does not require the risk assessment documentation to be handed over with the machine!

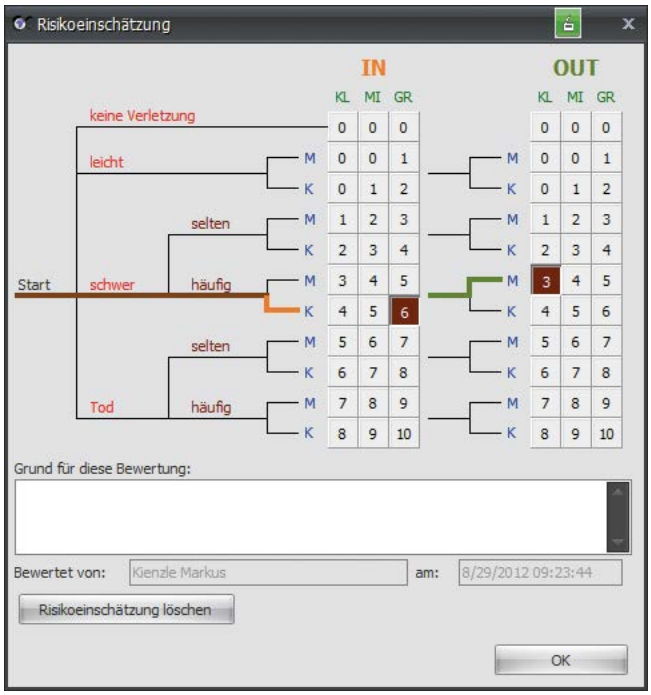
8007988/2015-07-07

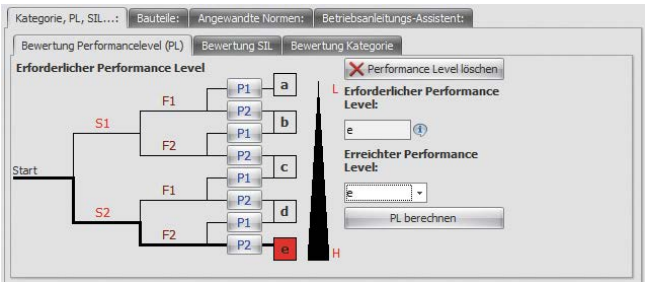
Risk assessment with Safexpert®



The risk assessment process is set up in Safexpert®, a software package for safety engineering. The user is guided through the legal requirements and the requirements in the standards. The task is simplified by the hazard list provided in the software, CE management 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 dangers are evaluated separately at hazardous points and in the appropriate life phases of the machine. Evaluating dangers individually enables the ideal measures for risk reduction to be selected in each case. A combination of risk graph and matrix (table) is used in Safexpert®. The estimation is made before (IN) and after (OUT) the protective measure (e.g., safeguard) has been selected. The risk is categorized on a scale from 0 (no risk) to 10 (highest risk).

Safexpert® has many more uses above and beyond risk assessment. With 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 dangers and risks until there are no residual risks or only acceptable residual risks remain.

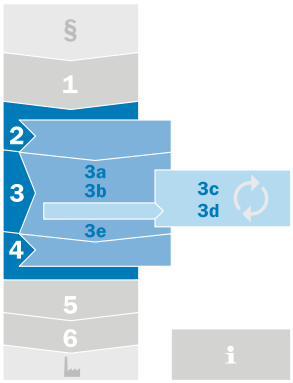
The risk assessment process

- Start the risk assessment with the definition of the functions of the machine.
- During the risk assessment take into account in particular foreseeable misuse and disturbances.
- Then identify the hazards (mechanical, electrical, thermal,etc.) posed by the machine. Take into account these hazards in all phases of the service life of the machine.
- Then estimate the risks posed by the hazards. These depend on the extent of harm and the probability of occurrence of the harm.
- Document the results in your risk assessment.

8007988/2015-07-07

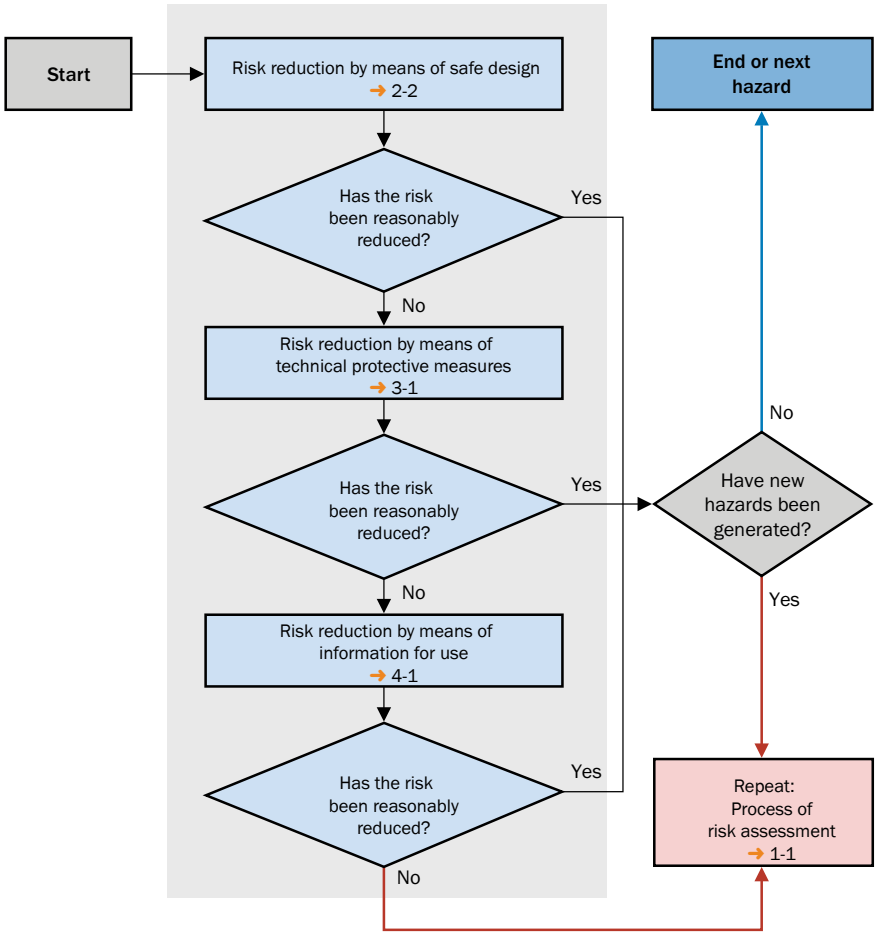
Steps 2 to 4: Risk reduction

If the risk evaluation showed that measures are necessary to reduce the risk, the 3-step method must be used.

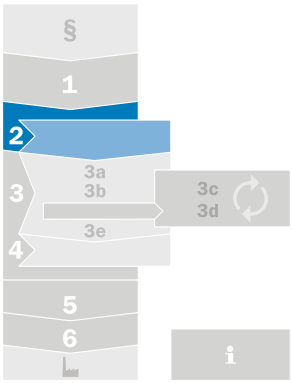


The 3-step method

1. The machine manufacturer shall apply the following principles during the selection of the measures, and in the order given:
2. Safe design: elimination or minimization of residual risks as far as possible (integration of safety in the design and construction of the machine)
3. Technical protective measures: Take the necessary protective measures against risks that cannot be eliminated by design
   Information for use on residual risks



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



2

In this chapter ...

Step 2: Safe design (inherently safe design)

Safe design is the first and most important step in the risk reduction process. During this process, possible dangers are excluded by design. For this reason safe design is 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)
- Concepts for stopping in an emergency situation
- Equipment involving fluids
- Materials and resources used
- Machine function and production process

In all cases, all components shall be selected, used, and adapted in such a way that in the event of a fault on the machine, the safety of people is paramount. The prevention of harm to the machine and the environment is also to be taken into consideration. All elements of the machine design are to be specified so that they function within specified limits. The design should also always be as simple as possible. Safety-related functions are to be separated from other functions as far as possible.

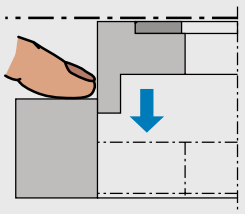
Mechanical design

The first objective of every design shall be to prevent the occurrence of hazards in the first place. This objective can be achieved, for example, by:

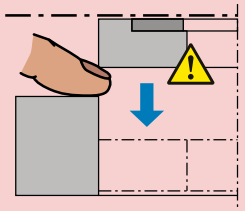
- Avoiding sharp edges, corners, and protruding parts
- Avoiding crushing points, shearing points, and entanglement points
- Limiting kinetic energy (mass and speed)
- Considering ergonomic principles

Example: Avoiding shearing points

Right

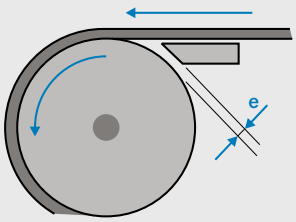


Wrong

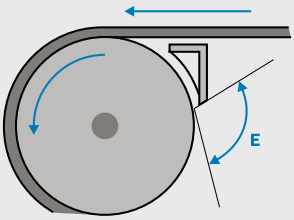


Source: Neudörfer

Examples: Avoiding entanglement points



The distance **e** should be ≤ 6 mm!



The angle **E** should be ≥ 90 °!

Source: Neudörfer

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

8007988/2015-07-07
Subject to change without notice

Operating and maintenance concept

The need for exposure to the hazard should be kept as low as possible. This objective can be achieved by means of:

- 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, e.g., clear marking of controls

Color marking

Controls on pushbuttons as well as indicators or information displayed on monitors are to be marked in color. The various colors have different meanings.

➜ Electrical equipment of machines: IEC 60204-1

General meaning of the colors for controls

Color	Meaning	Explanation
White Gray Black	Unspecific	Initiation of functions
Green	Safe	Actuate during safe operation or to establish normal situation
Red	Emergency situation	Actuate in dangerous state or emergency situation
Blue	Instruction	Actuate in situation that requires mandatory action
Yellow	Abnormal	Actuate in abnormal situation

General meaning of the colors for indicators

Color	Meaning	Explanation
White	Neutral	Use in case of doubt on the use of green, red, blue, or yellow
Green	Normal situation	
Red	Emergency situation	Dangerous state, react with immediate action
Blue	Mandatory	Indicate a situation that requires mandatory action on the part of the operator
Yellow	Abnormal	Abnormal situation, critical situation imminent

Electrical equipment

Measures are necessary to exclude electrical hazards on machines. There are two different types of hazard:

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

➜ In the following sections you will find important information on the design of the electrical equipment.
➜ Electrical equipment of machines: IEC 60204-1

Electrical power supply connection

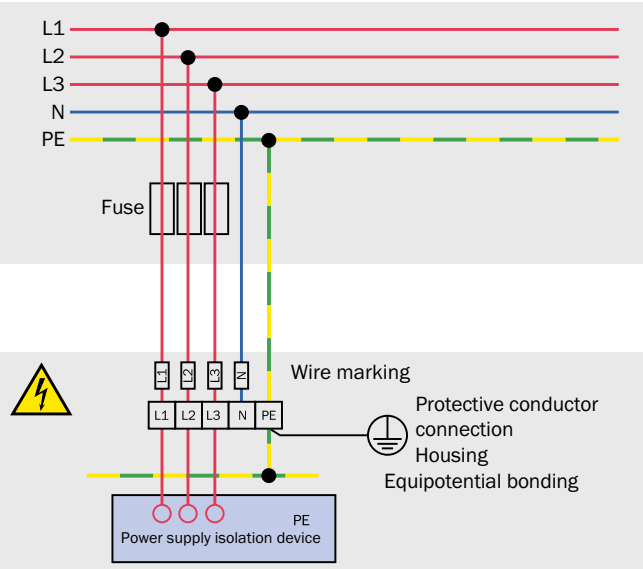
The electrical power supply connection is the interface between the electrical equipment in the machine and the supply grid. The stipulations from the utility concerned are to be followed for the connection.

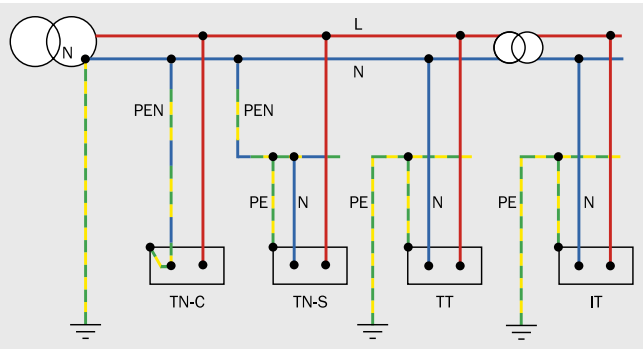
A stable power supply is particularly important in safety-related applications. For this reason the voltage supplies should be able to withstand brief power failures.

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 chassis of electrical equipment on the power supply must be connected to the protective conductor system. Equipotential bonding is a basic means of protection in the event of a fault.





8007988/2015-07-07
Subject to change without notice

TN system
The TN system is the most common form of network in low voltage systems. In the TN system the transformer's star point 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 cables are laid as a common cable (TN-C system) or as two independent cables (TN-S system).

TT system
In a TT system the supply transformer's star point is earthed as in a TN system. The protective conductor connected to the electrically conductive equipment housing is not laid 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 equipment housings are earthed in an IT system as in a TT system, but the supply transformers star point is not earthed in the same way. Systems on which shutdown involves a certain degree of danger which, therefore, are not to be shut down on the occurrence of only a fault to chassis or earth are designed as IT systems.
IT systems are stipulated in the low voltage area (to supply power to operating theaters and intensive care stations in hospitals, for example).

➜ Protective measures: IEC 60364-4-41, with varying national amendments

Power supply isolation devices

A power supply isolation 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:
- Power circuit breaker for usage 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 interlocks 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

During maintenance work, a machine start or the restoration of power shall not produce a hazard for maintenance personnel. For this reason means shall be provided to prevent unintentional and/or mistaken switching of the power supply isolation device.

This can be achieved, for example, by fitting a padlock in the handle of a main switch with the switch in the Off position.

This shutdown device is not suitable for use as a protective measure for brief interventions into the hazard zone for operational purposes.

Protection against electric shock

Protection classes

Categorization in different protection classes indicates the means by which single-fault safety is achieved. This categorization does not provide an indication of the level of protection.

	**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 Vrms and DC voltages up to 120 V are allowed as safety extra-low voltages. Above a limit of 75 V DC, the requirements of the Low Voltage Directive shall also be met. 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. Freedom from harmonics is obtained by superimposing a sinusoidal AC portion of at least 10% rms on the DC voltage.
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.).
A differentiation is made between:

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

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

8007988/2015-07-07
Subject to change without notice

		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	
Relation to earth or a protective 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 casings 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 casings in accordance with standards or • Body and active parts connected to main earthing rail

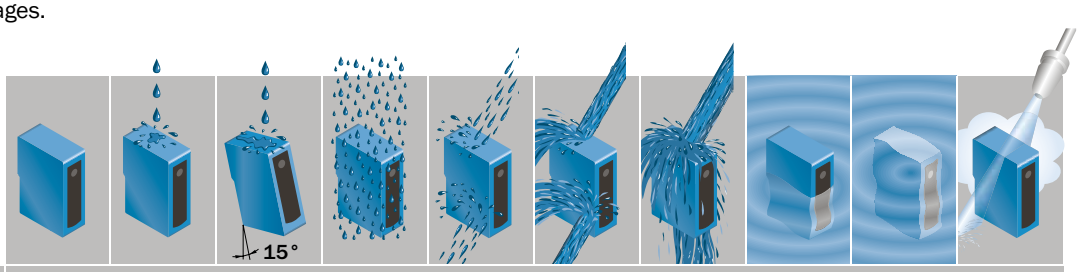
2

→ Protection classes: EN 50178
→ Safety of transformers: EN-61558 series

Protective measures/Enclosure ratings

The enclosure ratings describe the protection of an item of equipment against the ingress of water (not water vapor) 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 must be designed to at least enclosure rating IP 2x; control cabinets must be designed to at least enclosure rating IP 54.



1st indicator Protection against the ingress of solid foreign objects		**2nd indicator** Protection against the ingress of water (no water vapor, no other fluids!)									
		IP ...0	**IP ...1**	**IP ...2**	**IP ...3**	**IP ...4**	**IP ...5**	**IP ...6**	**IP ...7**	**IP ...8**	**IP ...9K**
		Non-protected	Dripping water vertical	Dripping water at an angle	Spraying water	Splashing water	Jetting water	Powerful jetting water	Immersion temporary	Immersion continuous	100 bar, 16 l/min., 80 °C
IP 0... Nonprotected		IP 00									
IP 1... Size of foreign object ≥ 50 mm Ø		IP 10	IP 11	IP 12							
IP 2... Size of foreign object ≥ 12 mm Ø		IP 20	IP 21	IP 22	IP 23						
IP 3... Size of foreign object ≥ 2,5 mm Ø		IP 30	IP 31	IP 32	IP 33	IP 34					
IP 4... Size of foreign object ≥ 1 mm Ø		IP 40	IP 41	IP 42	IP 43	IP 44					
IP 5... Dustprotected		IP 50			IP 53	IP 54	IP 55	IP 56			
IP 6... Dusttight		IP 60					IP 65	IP 66	IP 67		IP 69K

→ Enclosure ratings due to housing: EN 60529

8007988/2015-07-07
Subject to change without notice

Stopping

Along with the stopping of a machine during normal operation, it shall also be possible to stop a machine in an emergency situation for safety reasons.

Requirements

- Every machine shall be equipped with a control for stopping the machine in normal operation.
- A category 0 stop function shall be available as a minimum. 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. If the machine or its dangerous parts has/have been shut down, the supply of power to the drive shall be interrupted.

Stop categories

Safety-related and function-related aspects in machines result in stop functions in various categories. Stop categories are not to be mistaken for the categories defined in ISO 13849-1.

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 isolated

➜ See also section "Stopping in an emergency situation" ➜ 3-7

➜ Stop categories, see "Electrical equipment of machines: IEC 60204-1"

Electromagnetic compatibility (EMC)

The European EMC Directive defines electromagnetic compatibility as “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 are immune to the expected disturbances. Increased requirements apply to safety components.
Electromagnetic disturbances can be caused by:

- 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)

There are interference limits for the industrial sector and for residential areas. In the industrial sector the requirements for susceptibility are higher, but higher interference emissions are also allowed. For this reason components that meet RF interference requirements for the industrial sector may cause RF interference in residential areas. The following table gives example minimum interference field strengths in various application areas.
Typical minimum interference field strengths in the frequency range from 900 to 2000 MHz

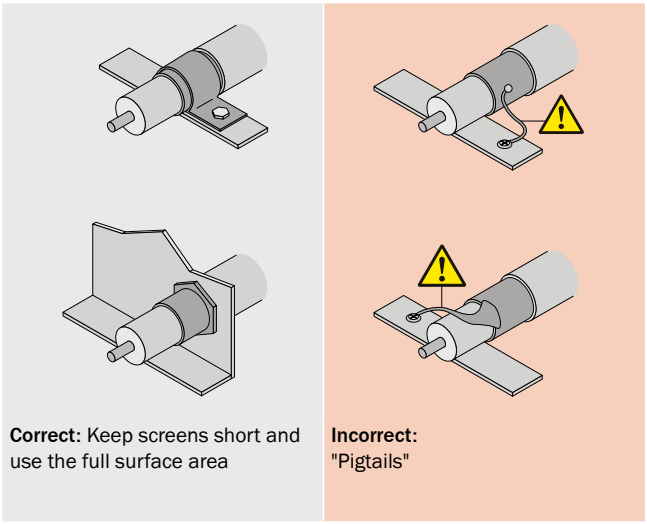
Area of application	Minimum interference field strength for immunity
Entertainment electronics	3 V/m
Household electrical appliances	3 V/m
Information technology equipment	3 V/m
Medical equipment	3 ... 30 V/m
Industrial electronics	10 V/m
Safety components	10 ... 30 V/m
Vehicle electronics	Up to 100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

Example: 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

The following design rules will help to prevent EMC problems:

- Continuous equipotential bonding by means of conductive connections between parts of machinery and systems
- Physical separation from the supply unit (power supply/actuator systems/inverters)
- Do not use the screen to carry equipotential bonding currents
- Keep screens short and use the full surface area
- Connect any functional earth (FE) provided
- Connect any available communication cables carefully. Twisted cables are often required to transmit data (fieldbus)

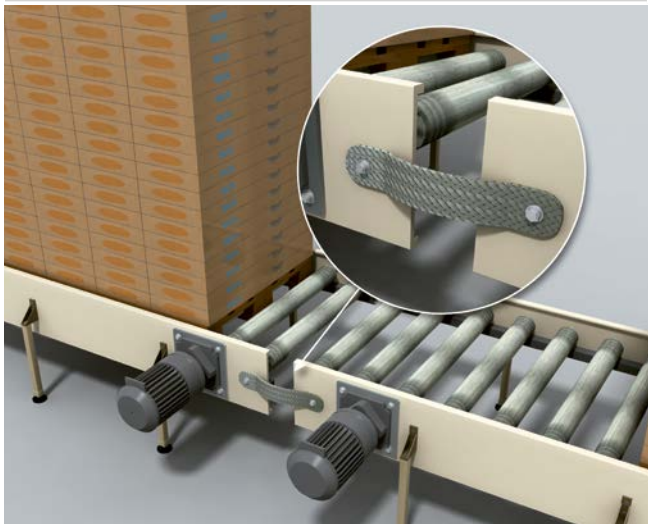
Example: Connecting shield correctly



Correct: Keep screens short and use the full surface area

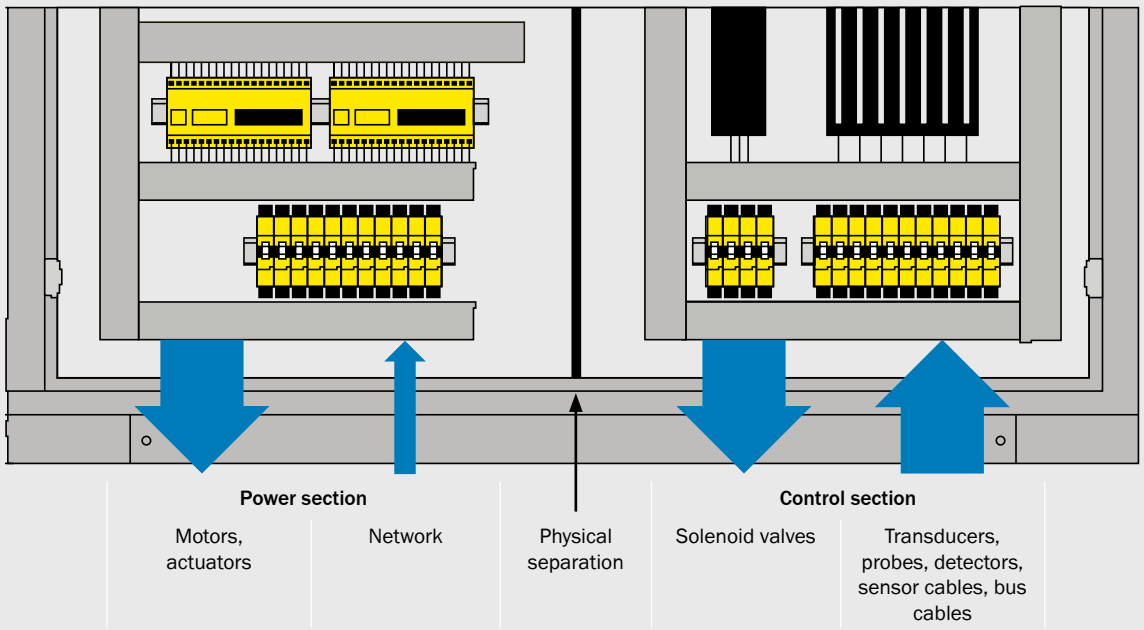
Incorrect: "Pigtails"

Example: Providing equipotential bonding



8007988/2015-07-07
Subject to change without notice

Example: Physical separation



→ EMC standards: EN 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 by means of which energy is transmitted using gases or liquids. A generic term is used because liquids and gases behave similarly. Fluid technology describes processes and systems for the transmission of power using fluids in sealed 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.

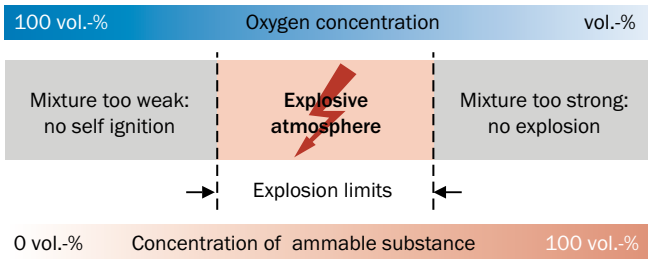
Fluid technology is applied in engineering in hydraulics (energy transmission using hydraulic oils) and in pneumatics (transmission using compressed air). Oil-based hydraulics required a circuit for the fluid (feed and return), while in pneumatics the waste air is discharged to the environment using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

Design principles

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 damaging 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. However, their consequences are spectacular and often result in serious loss of life and extensive economic damage.
Where dust, inflammable 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.



2

Assessing the scope of the protective measures necessary
For an assessment of the protective measures necessary, potentially explosive atmospheres are categorized in zones based on the probability of the occurrence of a hazardous potentially explosive atmosphere, see Directive 1992/92/EC, Annex I.

The information in the following table does not apply in the field of mining (open-cast, underground).

Zone definition				
For gases	**G**	Zone 2	Zone 1	Zone 0
For dust	**D**	Zone 22	Zone 21	Zone 20
Potentially 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		

8007988/2015-07-07
Subject to change without notice

Marking

Equipment must be designed, tested, and marked accordingly for use in these zones.

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

→ ATEX Directive: 1994/9/EG (valid until 19.04.2016), 2014/34/EU (valid from 20.04.2016)
→ Standards: EN 1127-1, EN 60079-0

Summary: Safe design

Mechanics, electronics, operation

- Keep to the principle of not allowing hazards to occur in the first place.
- Design so that the operators are exposed to the hazard zone 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.

Emergency operation, stopping

- Plan a control for stopping the machine in normal operation.
- Use an emergency stop to shut down a dangerous process or a dangerous movement.
- Use emergency switching off if power supplies that produce a hazard need to be safely isolated.

EMC

- Design machines that meet applicable EMC requirements. The components used shall be selected and verified so that ...
  - They do not cause electromagnetic disturbances that affect other devices or systems
  - They are themselves immune to the disturbances to be expected

8007988/2015-07-07

Step 3: Technical protective measures

Technical protective measures are implemented with:

- Protective devices that are part of a safety function, e.g., covers, doors, light curtains, two-hand controls
- Monitoring units (monitoring position, speed, etc.) or
- Measures to reduce emissions.

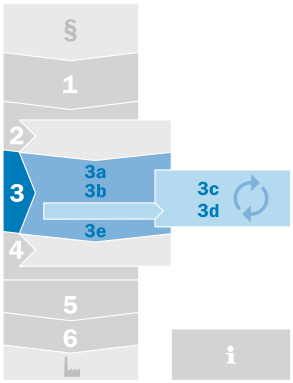
Not all protective devices are integrated into the machine's control system. An example of this situation is a fixed guard (barrier, cover). The main task is complete with the correct design of this protective device.

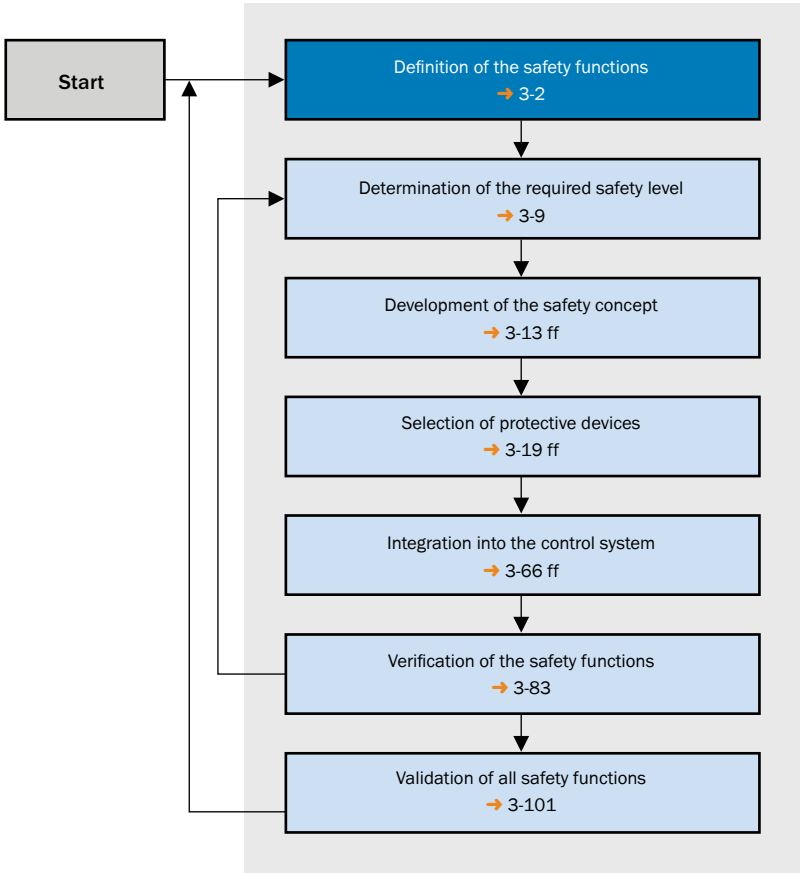
Functional safety

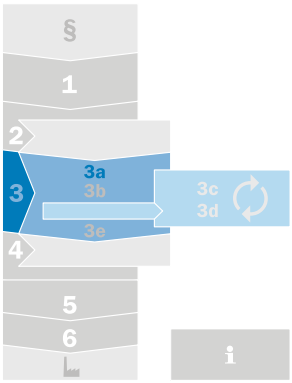
Where the effect of a protective measure is dependent on the correct function of a control system, the term functional safety is used. To implement functional safety, safety functions shall be defined. After this, the required safety level shall be determined and then implemented with the correct components and subsequently verified.

Validation

The validation of all technical protective measures ensures the correct safety functions have a reliable effect.
The design of 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).







3 a

In this chapter ...

Step 3a: Defining the safety functions

The safety functions define how risks are reduced by protective measures. A safety function shall be defined for each hazard that has not been eliminated by the design. It is necessary to provide a precise description of the safety function 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.

➜ Examples for the definition of safety functions: BGIA-Report 2/2008, "Funktionale Sicherheit von Maschinensteuerungen" ("Functional safety of machine controls")

Permanently preventing access

Access to a hazardous point is prevented by means of mechanical covers, barriers, or obstacles (referred to as 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 hazard zones by using guards

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.

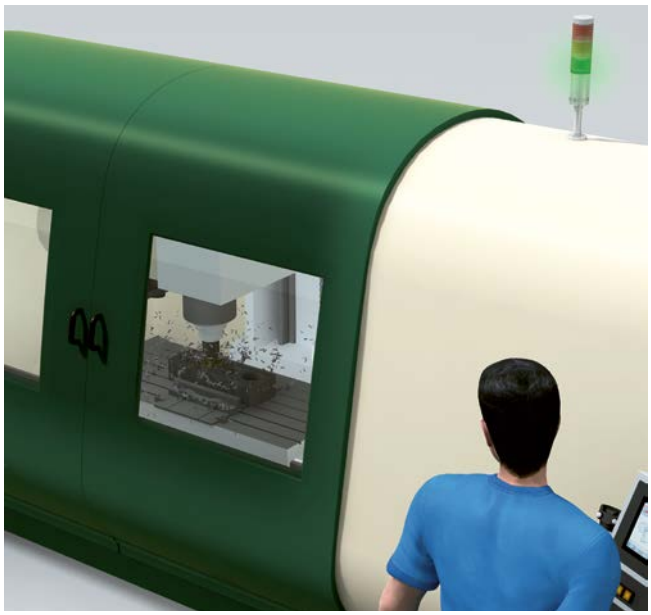
8007988/2015-07-07
Subject to change without notice

Retaining parts/substances/radiation

If parts can be ejected of machines or radiation may occur, mechanical protective devices (guards) must be used to prevent the hazards that occur in these situations.

Examples:

- Safety cover with special observation window on a milling machine for protection from flying chips and parts of workpieces (see figure)
- Fence that can retain a robot arm

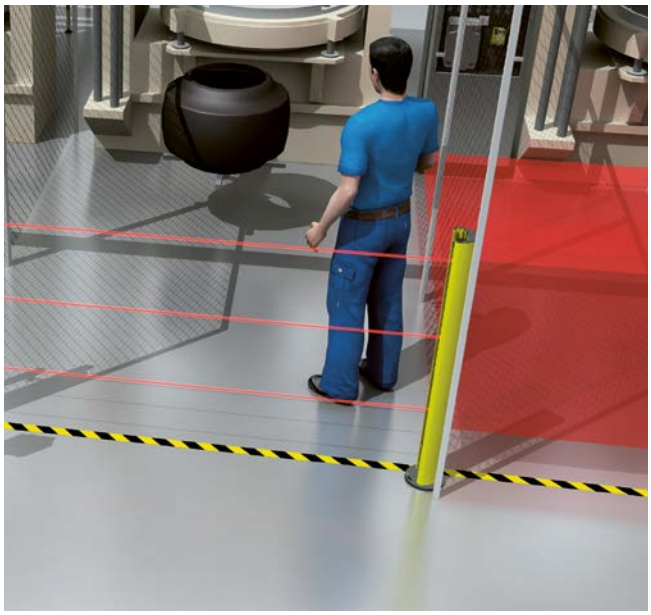


Initiating a stop

A safety-related stop function places the machine in a safe state on demand (e.g., approach of a person). To reduce the required stopping time a stop function which complies with stop category 1 (EN 60204-1 ➜ 2-9) may be applied. Additional safety functions may be necessary to prevent unexpected start-up.

Examples:

- Opening a protective door with an interlock that has no locking device
- Interrupting the light beams on a multiple light beam safety device providing access protection (see figure)



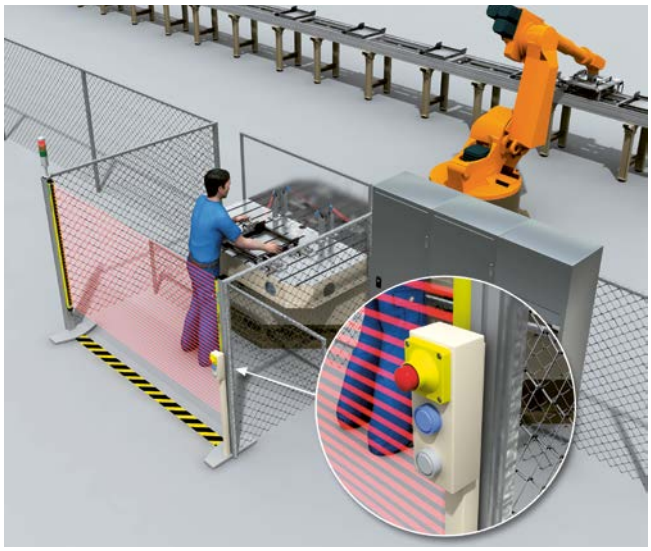
3 a

Avoiding unexpected startup

After initiating the “initiating a stop” function or switching the machine on, specific actions are required 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” ➜ 3-65).

Examples:

- Resetting an optoelectronic protective device (see figure: Blue “Reset” button)
- Resetting the emergency stop device
- Restarting the machine once all the necessary protective devices are effective

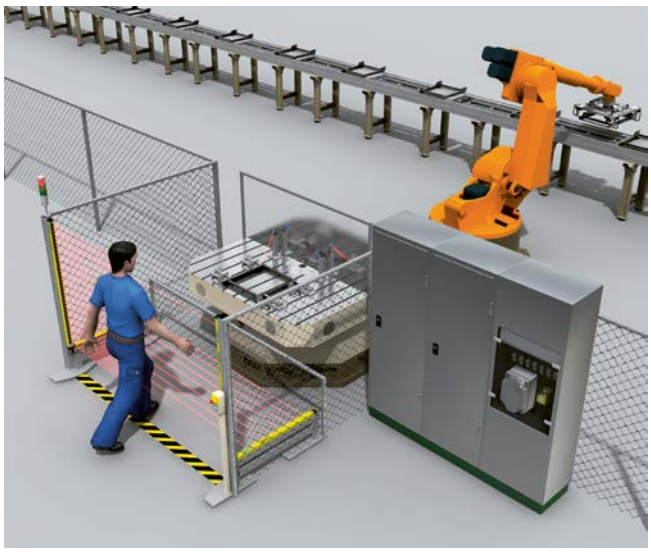


Preventing start

After the “initiating a stop” function, technical measures prevent the machine from starting or being put back into operation as long as there are persons in the hazard zone.

Examples:

- Trapped key systems
- Detection in the active protective field of a horizontal safety light curtain (see figure). The “initiating a stop” function is implemented by the vertical protective field of the 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 hazard zone.

Examples:

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

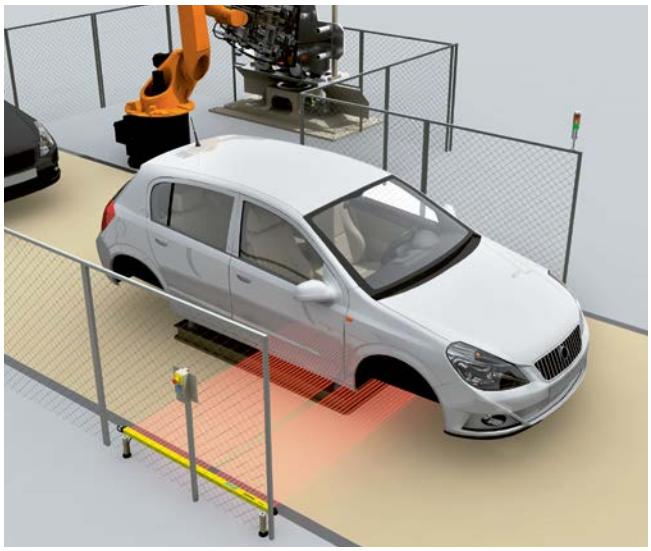
8007988/2015-07-07
Subject to change without notice

Enabling material throughput

To move materials in or out of the hazard zone, 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 allows the material to be detected and the safety function is suspended for a limited time while the material passes through (**muting**)
- Horizontal light curtains with integrated algorithm for **person/material differentiation** (see figure)
- Protective field switching on a safety laser scanner



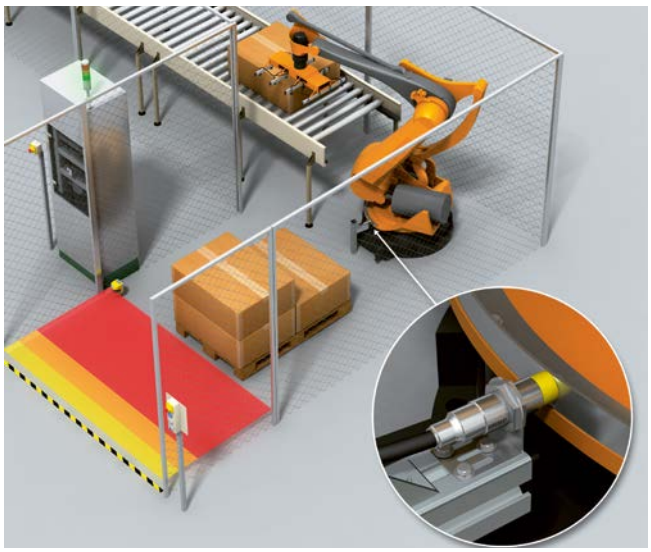
➜ For detailed information, see section “Safety functions that can be integrated in ESPE” ➜ 3-38.

Monitoring machine parameters

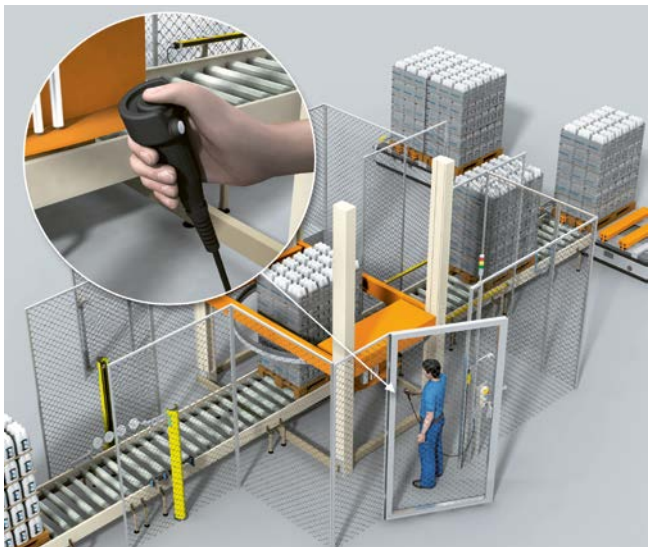
In some applications it is necessary to monitor various machine parameters for safety-related limits. If a limit is exceeded, suitable measures are initiated (e.g., stop, warning signal).

Examples:

- Monitoring of speed, temperature, or pressure
- Position monitoring (see figure)



Disabling safety functions manually and for a limited time



If, for certain operations like set-up or process monitoring, the machine must be able to operate with a guard displaced or removed and/or a protective device disabled, this is only allowed if the following conditions are met:

- An operating mode selector switch with a corresponding operating position shall be used
- Automatic control shall be disabled, there shall be no movement of the machine due to direct or indirect activation of sensors
- No linked sequences shall be possible
- Hazardous machine functions shall only be possible with control devices requiring sustained action (e.g., enabling devices)
- Hazardous machine functions are only permitted under reduced risk conditions (e.g., limitation of speed, movement path, duration of function)

Examples:

- Movement only with enabling button actuated and at reduced speed

3 a

Combining or switching safety functions

A machine can adopt various states or work in various operating modes. During this process different safety measures may be effective or different safety functions coupled together. By means of control functions, it should be ensured that the required level of safety is always achieved. Switching between operating modes or the selection and adjustment of different safety measures shall not lead to a dangerous state.

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 laser scanner to the speed of the vehicle (see figure)

8007988/2015-07-07
Subject to change without notice

Emergency stop

Emergency stop is a complementary protective measure; it is not a primary means of reducing risk. 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” ➜ 3-46).

➜ See IEC 60204-1 and ISO 13850

Safety-relevant 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.

- 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

Other functions

Other functions can also be executed by safety-related devices, even if they are not used to provide personal protection. This does not impair the safety functions themselves.

Examples:

- Tool and machine protection
- PSDI mode (cycle initiation ➜ 3-40 ff)
- Status of the protective device is also used for automation tasks (e.g., navigation)

Summary: Definition of the safety functions

Define which safety functions are necessary for risk reduction:

- Permanently preventing access
- Temporarily preventing access
- Retaining parts/substances/radiation
- Initiating a stop
- Preventing start
- Avoiding unexpected startup
- Combination of initiating a stop/preventing start
- Differentiating man/machine
- Monitoring machine parameters
- Disabling safety functions manually and for a limited time
- Combining or switching safety functions

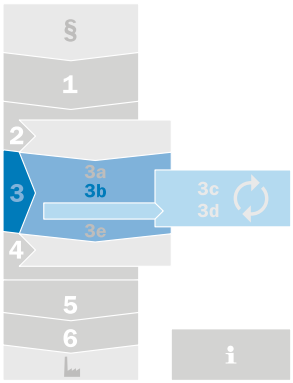
8007988/2015-07-07
Subject to change without notice

Step 3b: Determination of the required safety level

As a rule, C-type standards (machine-specific standards) 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 actuator(s)

If no C-type standard is available for the particular machine, or no particular specifications have been made in the C-type standard, the required safety level can also be determined using one of the following standards:



→ ISO 13849-1
→ IEC 62061

The application of the standards ensures that the effort for implementation is reasonable for the risk defined.
The protection of an operator who manually inserts and removes parts at a metal press requires different consideration compared to the protection of an operator who works on a machine on which the maximum risk is the trapping of a finger.
In addition, there can be different risks on one and the same machine in different phases of the life of the machine at different hazardous points. Here safety functions are to be defined individually for each phase of life and hazard.

The basis for all standards are the following parameters from the risk evaluation: severity of the possible injury, frequency and/or duration of exposure, and possibility of avoidance. These parameters combined determine the required level of safety.
During the application of the procedures described in these standards for the determination of the level of safety, the machine is considered without protective devices.

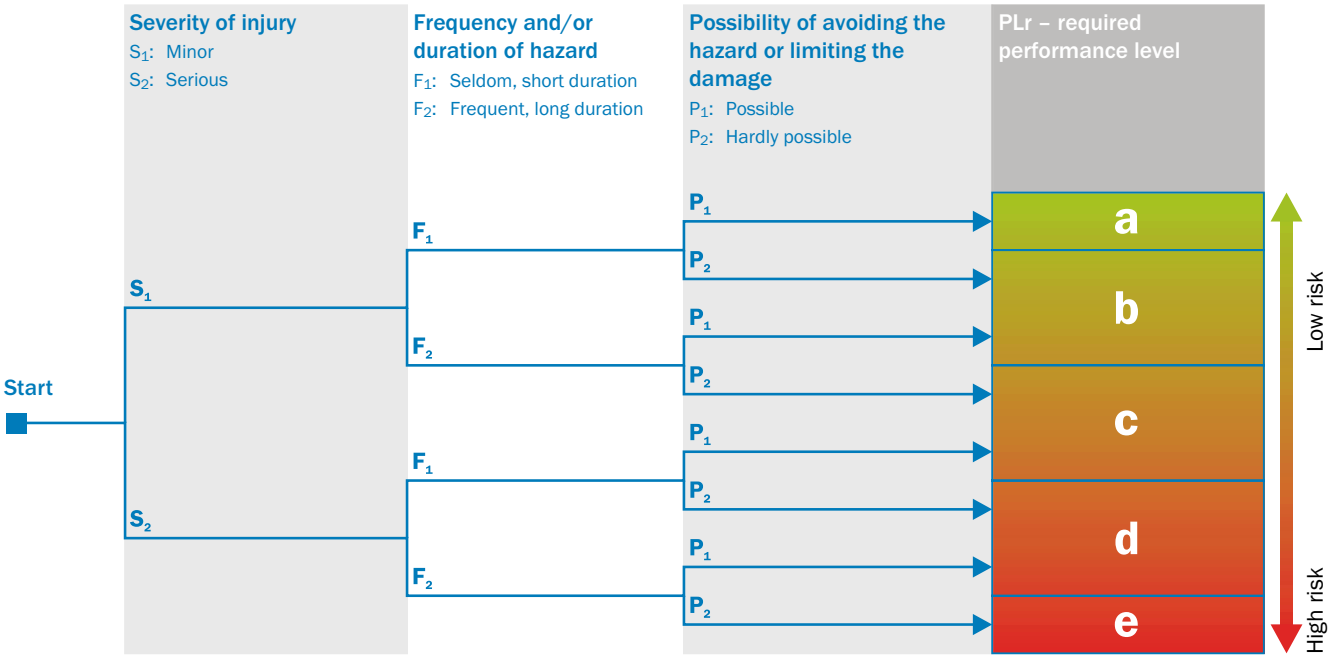
3 b

In this chapter ...

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

This standard also uses a risk graph to determine the required safety 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).



Risk graph according to ISO 13849-1

The performance level is defined in five discrete steps. It 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 (see section “Safety-related parameters for subsystems” ➜ 3-16). In addition, further measures to avoid design faults are required.

8007988/2015-07-07
Subject to change without notice

Safety integrity level (SIL) according to IEC 62061

The procedure used here is a numerical procedure. The extent of harm, the frequency/amount of time in the hazard zone, and the possibility of avoidance 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).

Effects	Extent of harm S	Class K = F + W + P				
		4	5-7	8-10	11-13	14-15
Fatality, loss of eye or arm	4	SIL2	SIL2	SIL2	SIL3	SIL3
Permanent, loss of fingers	3			SIL1	SIL2	SIL3
Reversible, medical treatment	2				SIL1	SIL2
Reversible, first aid	1					SIL1

Frequency [1] of the hazardous event F	
F ≥ 1 × per hour	5
1× per hour > F ≥ 1× per day	5
1× per day > F ≥ 1× in 2 weeks	4
1× in 2 weeks > F ≥ 1× per year	3
1× per year > F	2

Probability of occurrence of the hazardous event W	
Frequent	5
Probable	4
Possible	3
Seldom	2
Negligible	1

Possibility of avoiding the hazardous event P	
Impossible	5
Possible	3
Probable	1

1) Applies for durations > 10 min

The SIL is determined as follows:

1. Define extent of harm S.
2. Determine points for frequency F, probability W, and avoiding P.
3. Calculate class K from the sum of F + W + P.
4. SIL required is the intersection between the row “Extent of harm S” and the column “Class K”.

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 section “Safety-related parameters for subsystems” ➜ 3-16).

Area of application of ISO 13849-1 and IEC 62061

Both ISO 13849-1 and IEC 62061 define requirements for the design and implementation of safety-related parts of control systems. The user can select the relevant standard for the technology used in accordance with the information in the table on the right.

Technology	ISO 13849-1	IEC 62061
Hydraulic	Applicable	Not applicable
Pneumatic	Applicable	Not applicable
Mechanical	Applicable	Not applicable
Electrical	Applicable	Applicable
Electronics	Applicable	Applicable
Programmable electronics	Applicable	Applicable

Summary: Determination of the required safety level

General

- Define the necessary level of safety for each safety function.
- The parameters “severity of the possible injury”, “frequency and duration of exposure”, and “possibility of avoidance” determine the required level of safety.

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 procedure. The result is a required safety integrity level (SIL).

8007988/2015-07-07

Step 3c: Designing the safety function

Steps 3c and 3d describe the design and verification of the safety functions by selecting the correct technology, with suitable protective devices and components. In some circumstances these steps are performed several times in an iterative process.

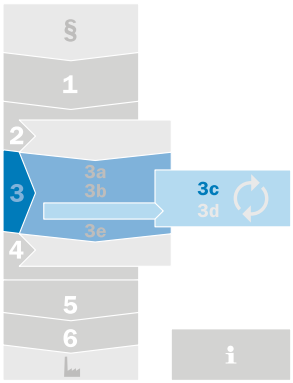
During this process it is necessary to repeatedly check whether the selection of the technology promises sufficient safety and is also technically feasible, or whether other risks or additional risks are produced by the use of a specific technology.

Development of the safety concept

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.

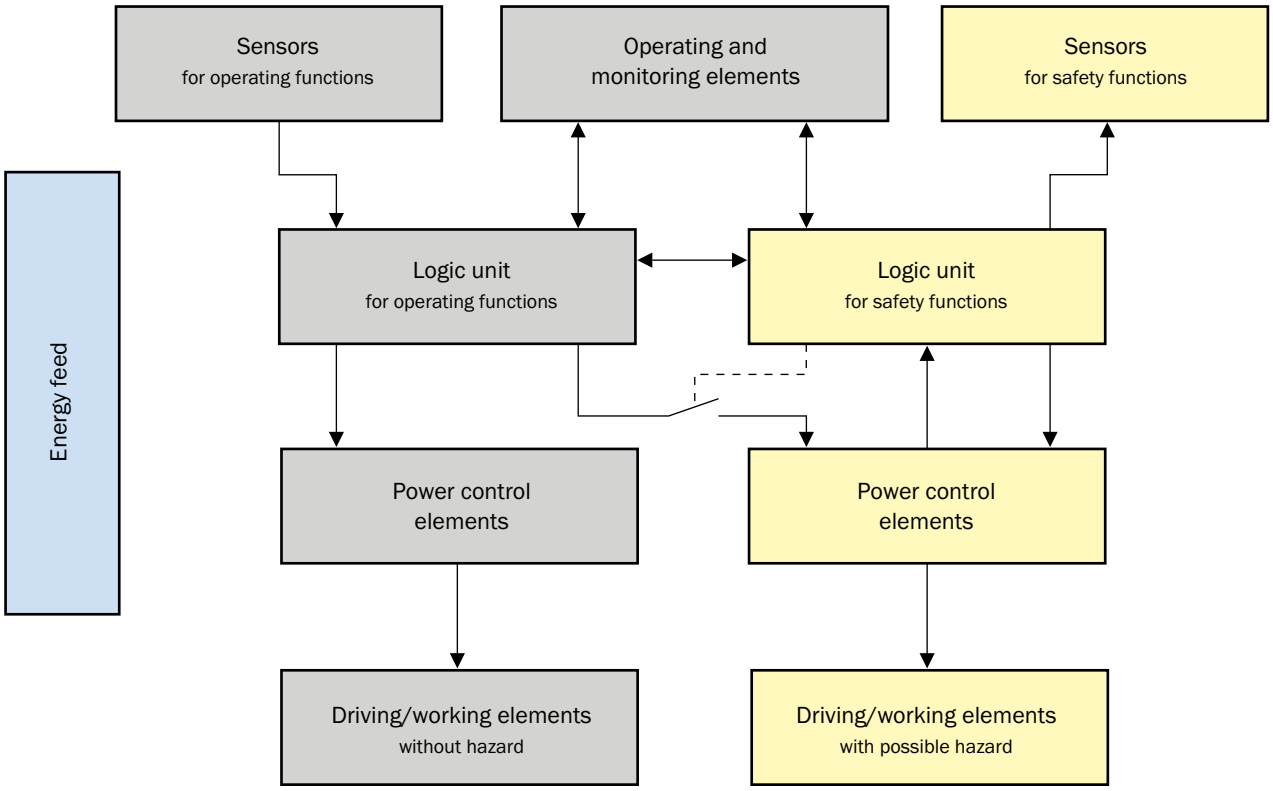
➜ Details on the safety concept: BGIA report 2/2008, "Funktionale Sicherheit von Maschinensteuerungen" ("Functional safety of machine controls") at www.dguv.de/ifa/de/pub



3 c

In this chapter ...

Functional layout of a machine control



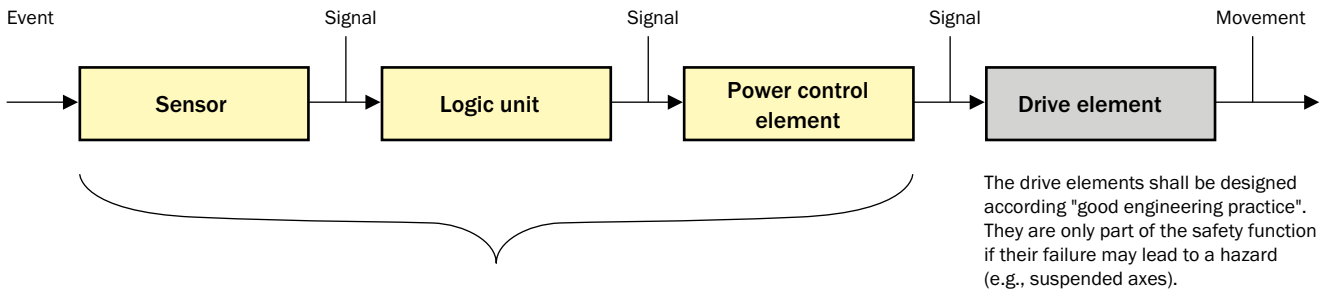
The safety-related parts of control systems are to be selected to suit the safety functions and the necessary level of safety. These parts include sensors, logic units, power control elements, for example, as well as drive and work elements. This selection is generally made in the form of a safety concept.

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. A machine shall only be put into operation by the intentional actuation of a control device provided for this 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



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

Decisive factors

The following features are to be taken into account during the preparation of the safety concept:

- Features of the machine
- Features of the surroundings
- Human aspects
- Features of the design
- Characteristics of safeguarding (➜ 3-19)

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 should be taken into account:

- 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 guards)
- Stopping times (knowledge of stopping times is necessary to ensure the protective device is effective)
- Possibility of monitoring stop time/overrun (this is necessary if changes could occur due to aging/wear)

Features of the surroundings

The following features of the surroundings should be taken into account:

- 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 should be taken into account:

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

Features of the design

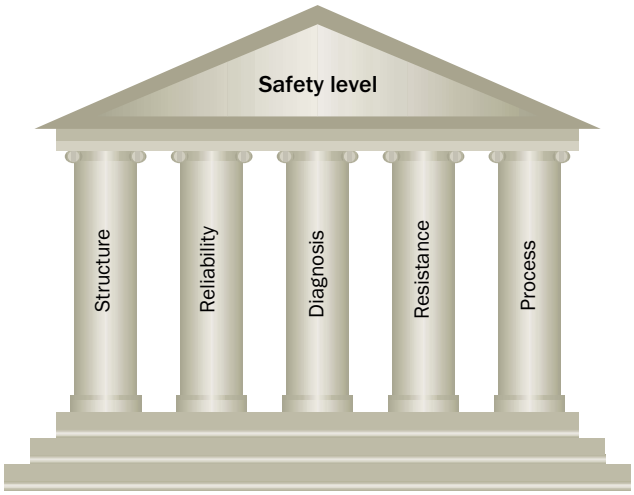
It is always advisable to implement safety functions with certified safety components. Certified safety components will simplify the design process and subsequent verification. A safety function is performed by several subsystems.

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 such cases, the level of safety is dependent on various parameters.

Safety-related parameters for subsystems

The safety level of a subsystem is dependent on various safety-related parameters. These include:

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

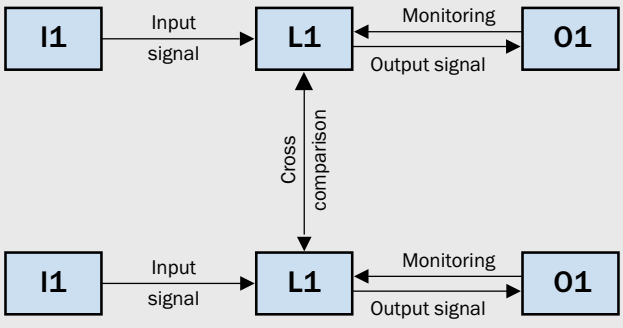


Structure

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 components 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.

Single-channel safety components

Dual-channel safety components

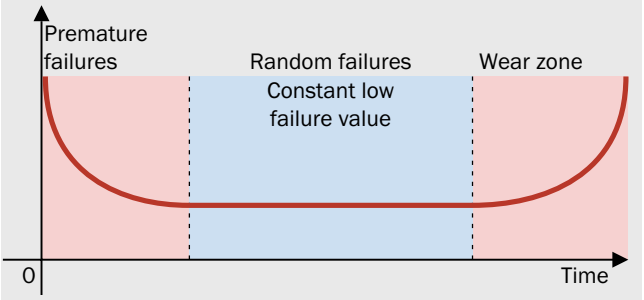


Reliability of the components/devices

Any failure of a safety component will result in an disturbance to the production process. For this reason it is important to use reliable components. The more reliable a component is, the lower the probability of a dangerous failure. Reliability is a measure of random failures within the life limit; it is normally provided in the following formats:

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

Failure rate λ (bathtub curve)



8007988/2015-07-07
Subject to change without notice

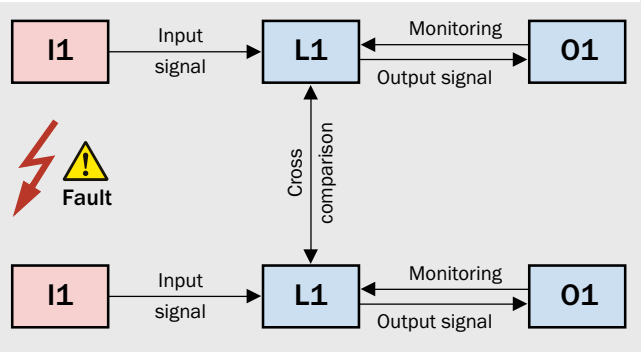
Diagnostics for detecting faults

Certain faults can be detected by diagnostics measures. These include plausibility monitoring, current and voltage monitoring, watchdog functionality, brief function test, etc.

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 shall be taken, e.g., isolated cable routing, suppressors, diversity of components, etc.

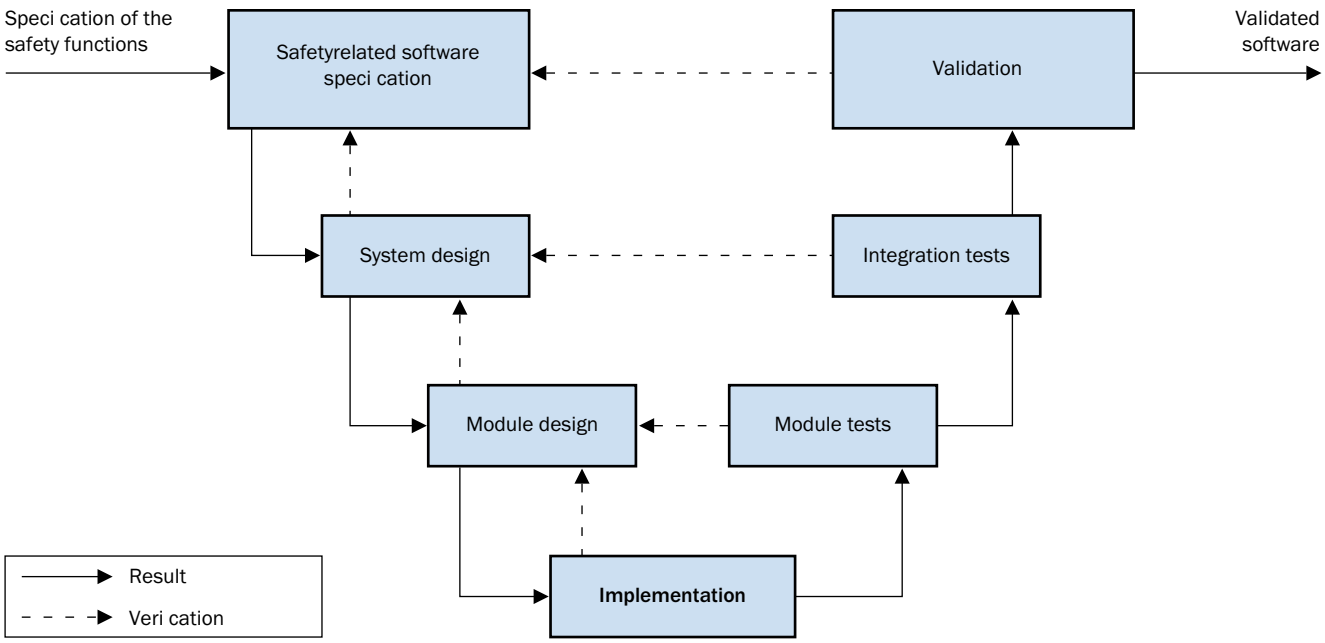


Process

The process combines the following elements that can have an effect:

- Organization and competence
- Rules governing design (e.g., specifications templates, coding guidelines)
- Test concept and test criteria
- Documentation and configuration management

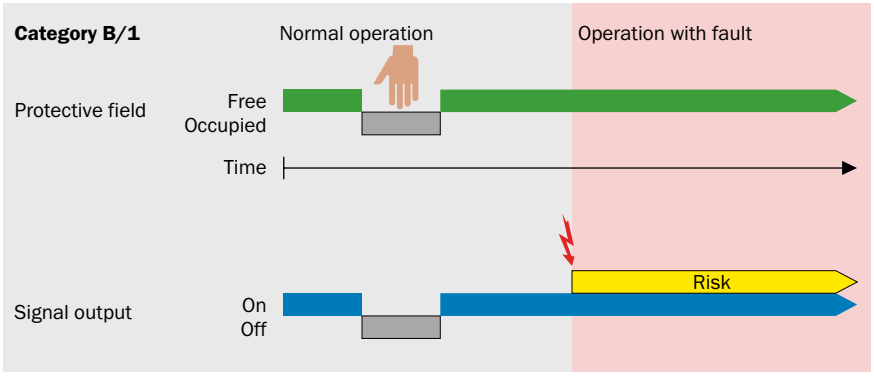
In the safety technology sector a process based on the V-model has proven particularly effective in practice for software design (see figure).



Assessment in accordance with ISO 13849-1*

The ISO 13849-1 standard uses the following categories to describe the structure.

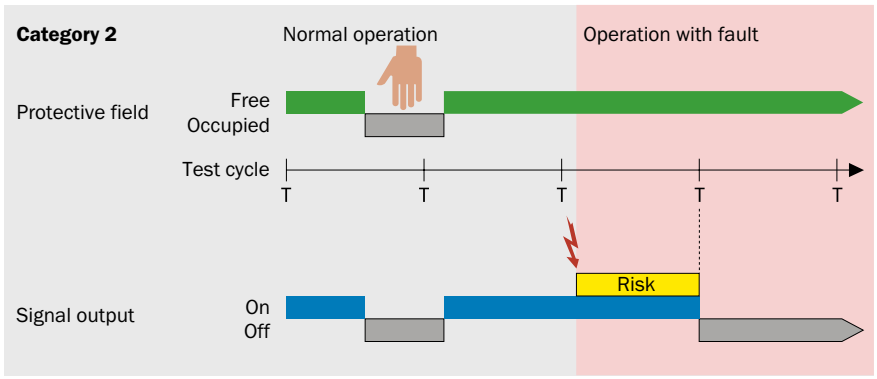
* Note: A safety function is defined as the function whose failure increases the risk. Therefore, the loss of the safety function shall be considered as risk appearance or increasing.



Category B/Category 1

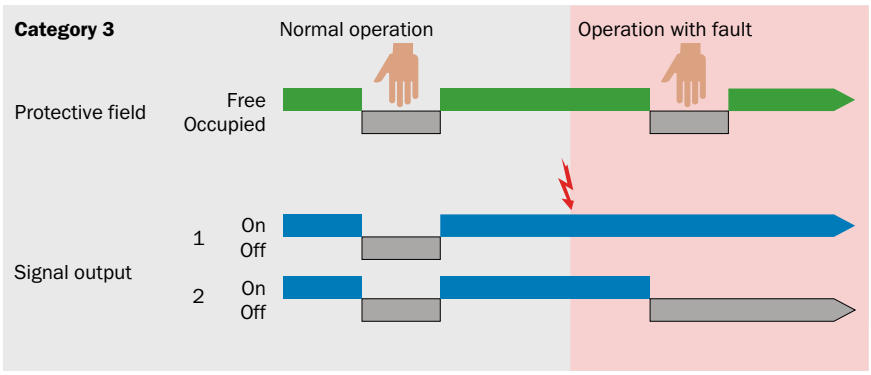
No fault detection. The occurrence of a fault will result in a risk.

The risk can be minimized with reliable and proven components (Category 1).



Category 2

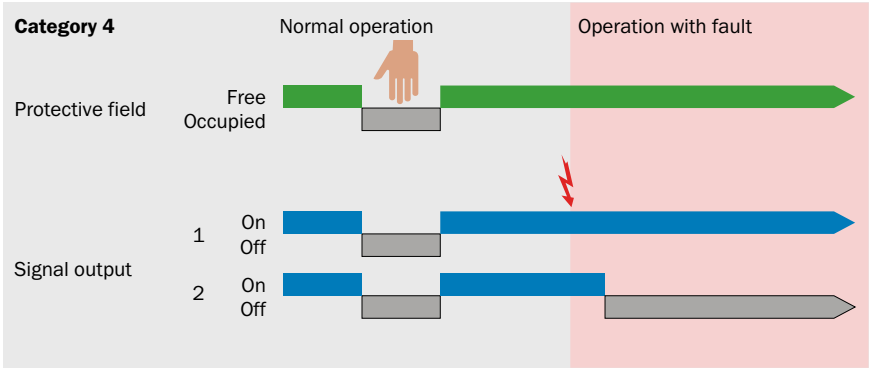
Faults are detected by carrying out a test. A risk prevails during the time between the occurrence of the fault and the next test. The test rate according to ISO 13849-1 shall be considered.



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.



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).

8007988/2015-07-07
Subject to change without notice

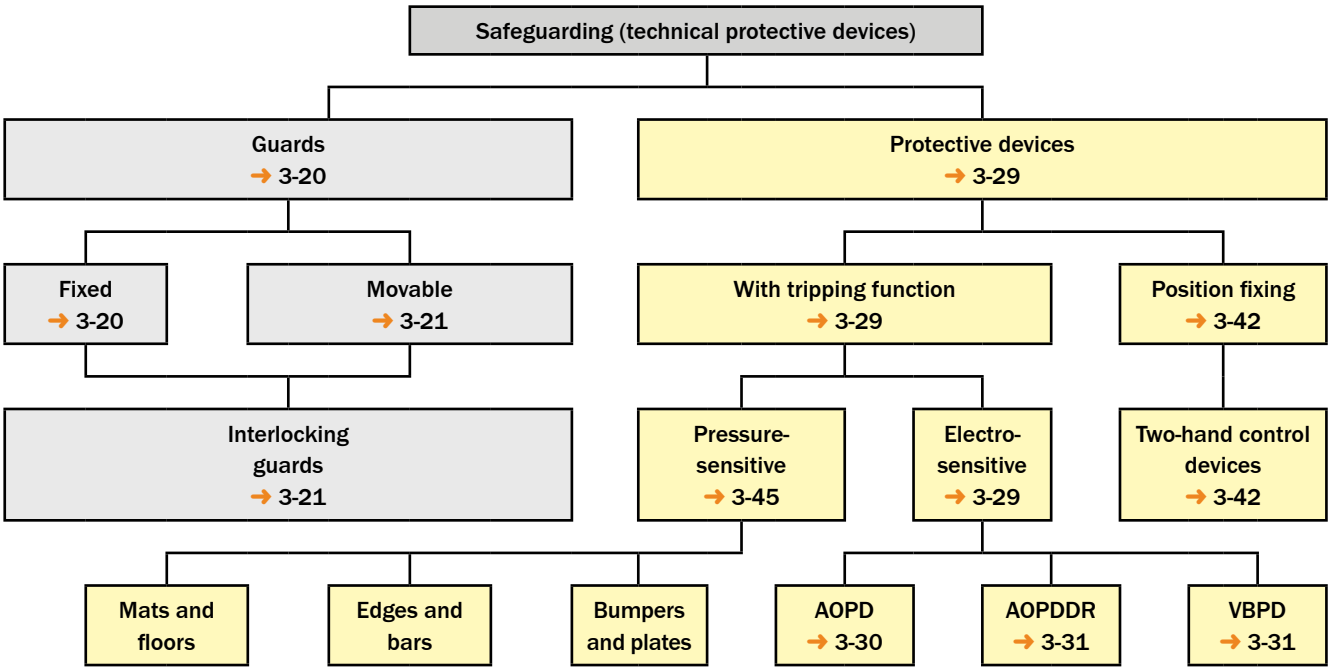
Characteristics of safeguarding

Characteristics of safeguarding to be considered are:

- Properties and applications of guards and protective devices (electro-sensitive, separating, etc. (➜ 3-19ff)
- Position/dimension of guards and protective devices (➜ 3-47)
- Integration in the control system (➜ 3-66)

The following sections describe these points in detail.

Technology, selection, and use of safeguarding



3 c

Guards

Guards are physical barriers, designed as part of the machine, that prevent or avoid the operator reaching the hazardous point directly. They can be fixed or movable. Covers, fences, barriers, flaps, doors, etc. are guards. Covers and lids prevent access from all sides. Fences are generally used to prevent full body access while barriers can only prevent unintentional or inadvertent access to the hazardous points.
The safety function is essential for the design of guards. Is the guard, e.g., only to prevent access, and/or also to retain parts/materials, and radiation?

Examples of ejected materials or parts:

- Fracturing/bursting tools (grinding wheels, drills)
- Materials produced (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 emitted radiation:

- 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 devices
- High voltages from test systems or systems for discharging electrostatic charges (paper and plastic webs)

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

3 c

General requirements of guards

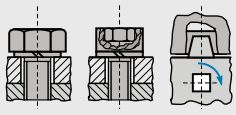
- Protective devices (guards) shall be designed to be adequately robust and durable to ensure they withstand the environmental conditions to be expected during operation. The properties of guards shall be maintained during the entire period of use of the machines.
- They shall not cause any additional 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 hazardous machine function.
- As far as possible, they should not remain in the protective position if unfastened.

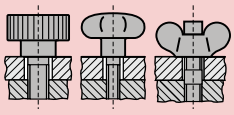
➜ Guards: ISO 14120
➜ Principles for safe machine design: ISO 12100 (A-Norm)

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.

Example: Types of fastening for guards


Allowed


Not permitted

8007988/2015-07-07
Subject to change without notice

Movable guards

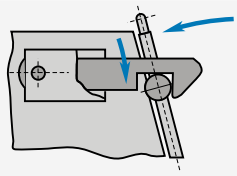
Movable guards that need to be opened frequently or regularly without tools (e.g., for setup work), shall be functionally linked to the hazardous machine function (interlocking, locking device). The term frequent opening is used, e.g., if the guard is opened at least once during a shift.
If hazards are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

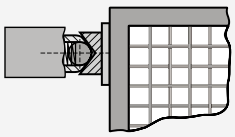
- Easy (e.g., one-handed) opening and closing, lifting, or moving
- Handle to suit function
- Opened guards should allow convenient access

Mechanical locking of movable guards
As far as feasible, movable 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 joints) are not recommended due to their diminishing effectiveness (wear).

Example: Locking guards



Good



Acceptable

Interlocking of guards

Guards must be interlocked if they:

- 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 hazardous machine function. Guards are normally interlocked using position switches.

The interlocking of a guard should fulfill the following functions:

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

Standard ISO 14119, which describes the requirements to be met by interlocking devices associated with guards, is currently being revised.
The following section explains the content of the revision.

There are four types of interlocking device:

Designation	Actuation		Actuator		SICK product	
	Principle	Example	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	Electro-sensitive	Inductive	Not coded	Suitable ferromagnetic materials	IN4000	
		Magnetic		Magnets, electromagnets	MM12 [1]	
		Capacitive		All suitable materials	CM18 [1]	
		Ultrasonic		All suitable materials	UM12 [1]	
		Optical		All suitable materials	WT 12 [1]	
Type 4		Magnetic	Coded	Coded magnet	RE11	
		RFID		Coded RFID transponder	TR4 Direct	
		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.

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 actuating element 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 guard.

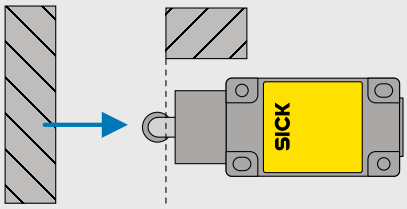
8007988/2015-07-07
Subject to change without notice

Mechanical attachment

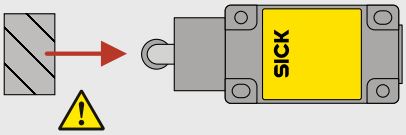
Reliable mechanical attachment of the position switches and actuators is crucial for their effectiveness. The elements of interlocking devices:

- Shall be fitted such that they are protected against damage due to foreseeable external effects.
- Shall not be used as a mechanical stop.
- Their placement and design shall protect them against inadvertent operation, and damage.
- Must be arranged, executed, and mounted so that they are protected against unintentional changes to their position (location). The switch and the actuator can be secured by shape (not force), e.g., using round holes, pins, stops.
- They shall be protected by their actuation method, or their integration in the control shall be such that they cannot be easily bypassed.
- It shall be possible to check the switches for correct operation and, if possible, they shall be easily accessible for inspection.

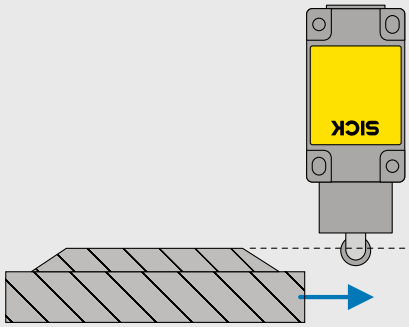
Example: Mechanical attachment of position switches



Correct assembly: The position switch is protected by a mechanical stop.



Incorrect assembly: The position switch is used as a stop.

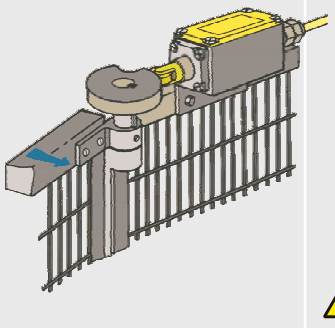


Correct assembly: The height of the cam has been matched to the position switch.

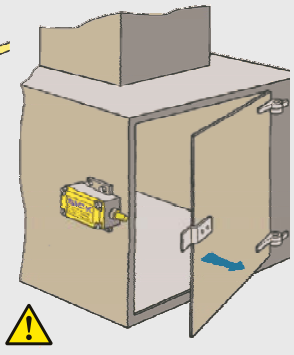
Method of actuation/Positive mechanical actuation

An important requirement to be met by mechanical interlocking devices is that of positive mechanical actuation. Positive mechanical actuation is the forced movement of the mechanical components of the interlocking device (safety switch) forced by the mechanical components of the guard (e.g., fence door) either by means of direct contact or by rigid parts. 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.

Example: Positive mechanical actuation



Safe: The opening of the protective door positively actuates the mechanical plunger of the position switch. This opens the safety circuit.



Flawed: The position switch will 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

Marking of contacts that are positive opening as per IEC 60947-5-1, Annex K

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 guard, it must meet the requirements of IEC 60947-5-3.

Prevention of manipulation

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, and similar.

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

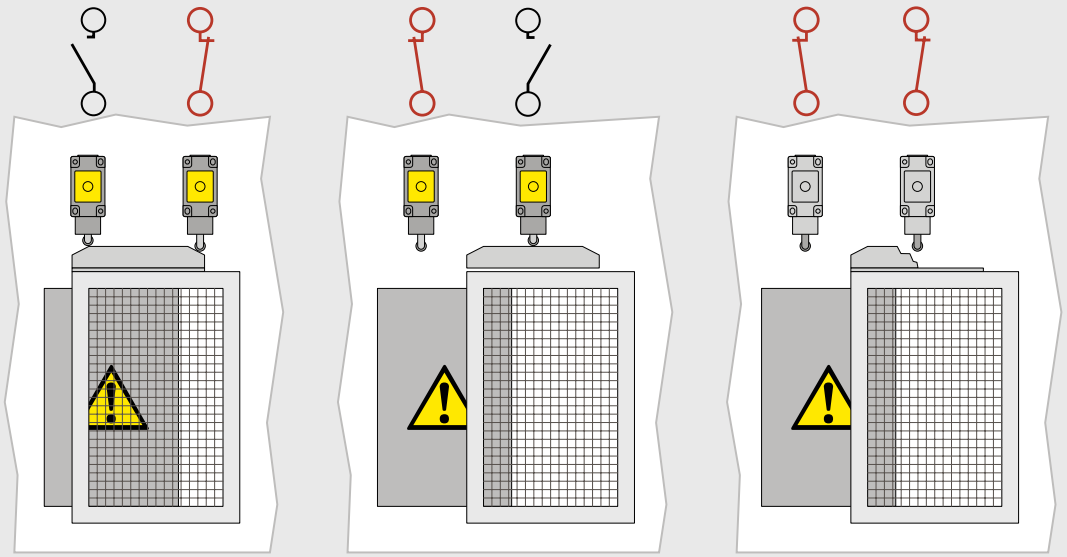
- Making interlocking devices difficult to access by using concealed assembly or assembly out of reach
- Using position switches with coded actuators
- Mounting the elements of the interlocking switches with "one-way" fasteners (e.g., safety screws, rivets)
- Manipulation monitoring in the control system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

Redundant design

The critical failure of an individual safety switch can be caused by manipulation, a mechanical fault on the actuator or position switch (e.g., aging), or the effects of extreme ambient conditions (e.g., roller plunger jammed by dust deposits). 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 operated movable guard. This application requires two mechanical switches.

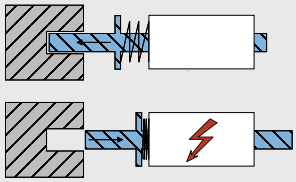
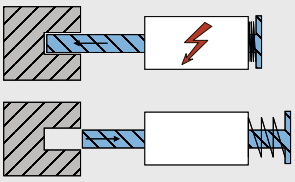
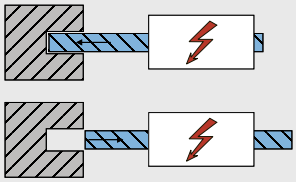
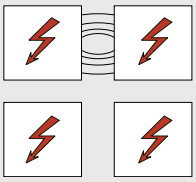
Example: Detection of mechanical faults by means of a diverse redundant arrangement



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 hazard zone (safety function "prevent access by time"). Locking devices shall prevent access to hazard zones 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.

	By shape			By force
Principle				
Principle of operation	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
Term	Mechanical locking device (preferred for safeguarding)	Electrical locking device (preferred for process protection)	Pneumatic/hydraulic locking device	Magnetic 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 state prevailing (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.

Escape release and emergency release

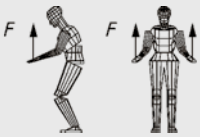
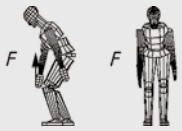
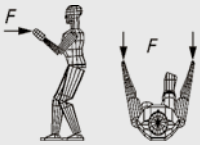
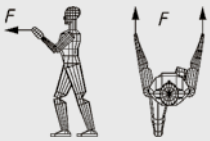
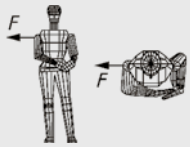
The risk assessment may show that in the case of a fault or in an emergency situation, measures are required for freeing personnel trapped in the hazard zone. A differentiation is to be made between the concepts of mechanical release (using tools) and emergency or escape release (without tools).

Locking force required

An essential criterion when selecting a locking device is the force required to hold the guard. Annex I of standard ISO 14119 (2013) specifies maximum static forces that can be applied to the most commonly used movable guards.

8007988/2015-07-07
Subject to change without notice

Required holding force for guards according to Annex I of standard ISO 14119 (2013)

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, Pull	Standing upright, feet parallel, or in step posture	Bi-manual, vertical grips	1100
	Horizontal, parallel to body symmetry plane forward, Push	Standing, 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 metal plate on the side	1300
	Horizontal, normal to body symmetry plane	Standing, feet parallel	Single-handed, vertical grip	700

3 c

Trapped key systems

Guards have the disadvantage that after entering the hazard zone and the subsequent closing of the protective device, restarting cannot be effectively prevented. Additional measures are necessary, such as a reset device or the insertion of a U-lock in a Type 2 interlocking device actuator. These organizational measures are dependent, however, on the willingness or awareness of the user.

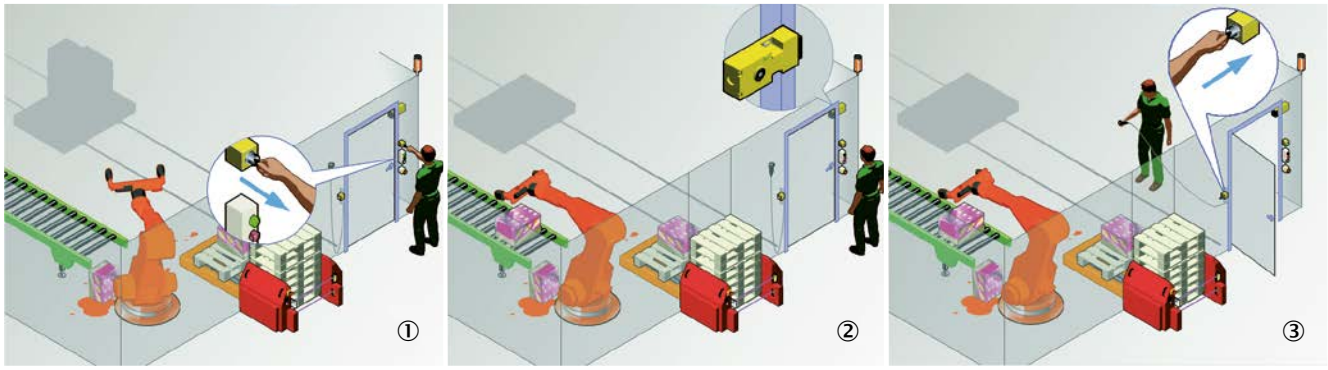
One way of forcibly preventing unintentional starting is to use trapped key systems. Keys which become trapped in the key switches when turned to certain positions have to be used to activate specific functions and operating modes.

When a key is removed (Figure ①), a stop signal is generated and the hazardous machine function is stopped.

In the safe state (at standstill) the door can be opened (Fig. ②).

When a key is inserted in the safeguarded area, "setup" operating mode can be enabled (Figure ③) and "dangerous machine movements" (turn robots to side) can be initiated by actuating an enabling device. Automatic operation is disabled in this situation.

Example: Trapped key system



8007988/2015-07-07
Subject to change without notice

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 hazard zone in a timely manner and depending on the application, the presence of the person in the hazard zone.

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) 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 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, guards must be used.

ESPE technologies

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

In practice, optical protective devices have been proven effective over many years and in large numbers.

Optoelectronic protective devices

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

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

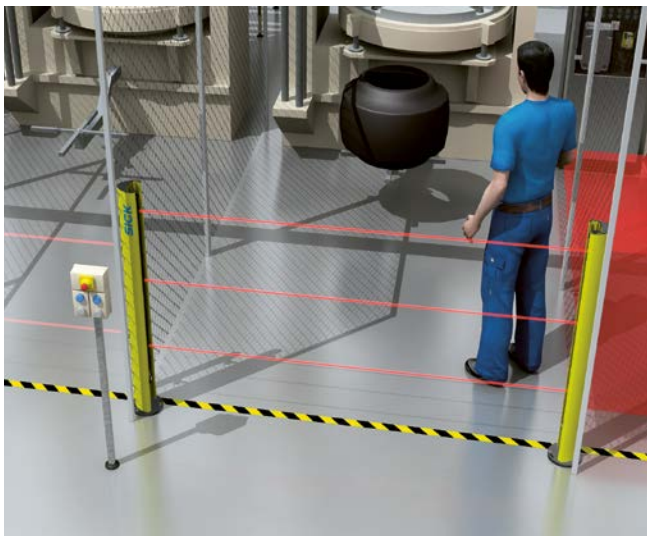
Examples of optoelectronic protective devices

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).

3 c

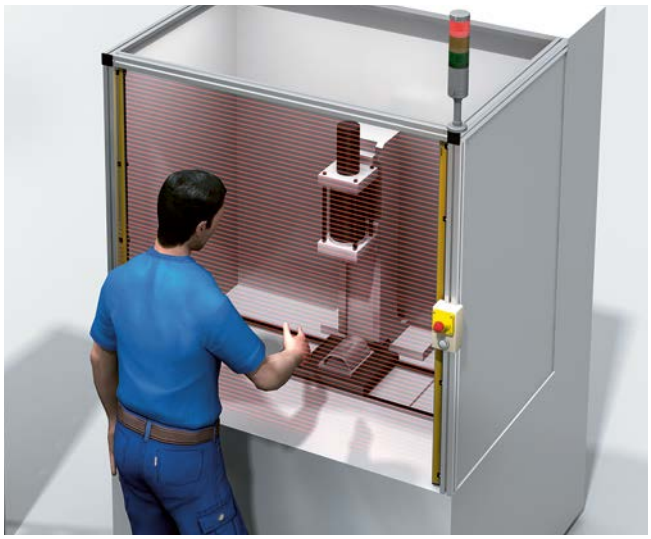
Safety light curtains and photoelectric switches (AOPDs)

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 hazard zone. 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).
This 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 single-beam and multiple light beam safety devices and safety light curtains. AOPDs with a detection capability of more than 40 mm are called multiple light beam safety devices. They are used to protect access to hazard zones (see figure).



Access protection with a multiple light beam safety device

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).



Hazardous point protection using a safety light curtain

With both multiple light beam safety devices 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 optical 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 (➜ 3-40).

8007988/2015-07-07
Subject to change without notice

Safety laser scanners (AOPDDR)

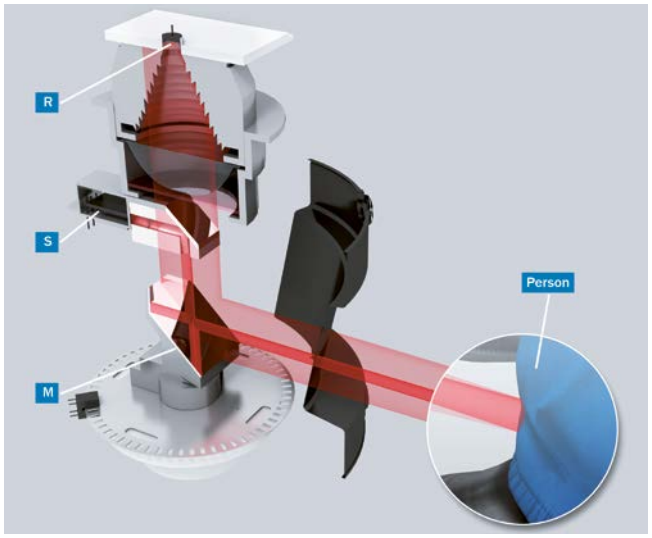
AOPDDRs are protective devices that use optoelectronic sender and receiver elements to detect the reflection of optical radiation generated by the protective device. This reflection is generated by an object in a predefined two-dimensional area. Detection is signaled by a signal change (OFF state) to its output signal switching devices (OSSDs).

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

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

It works on the basis of the principle of time-of-flight measurement (see the figure on the next page). 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.



Basic structure of a laser scanner

The user can program the area in which object detection trips the protective field. State-of-the-art devices allow multiple areas to be monitored simultaneously and switching between these areas during operation. 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) between 30 mm and 150 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.

Vision-based protective devices (VBPD)

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

Special light senders are currently used as light sources. VBPDs that use ambient light are also possible.

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

Camera-based protective device

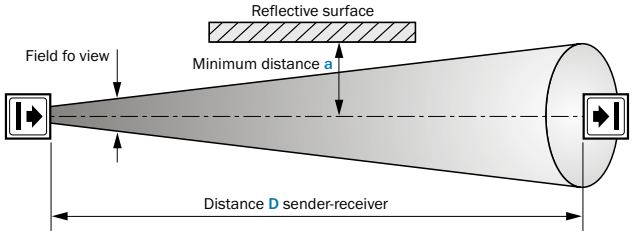
The future international standard series IEC 61496-4 will state safety requirements for VBPDs.

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 independent 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.
Type 3 is defined for AOPDDR. Types 2 and 4 are defined for AOPD (requirements are listed in the table).
Requirements for optical sources of interference (sunlight, different lamp types, devices of the same design, etc.), reflective surfaces, misalignment during normal operation, and the diffuse reflection of safety laser scanners play an important role.

	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 at a distance **D** of < 3 m	262 mm	131 mm
Minimum distance **a** to reflective surfaces at a distance **D** of > 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

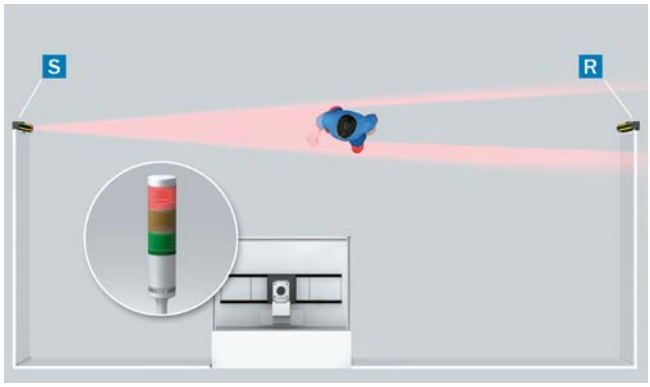


Main differences of type 2 and type 4 AOPDs according to IEC 61496

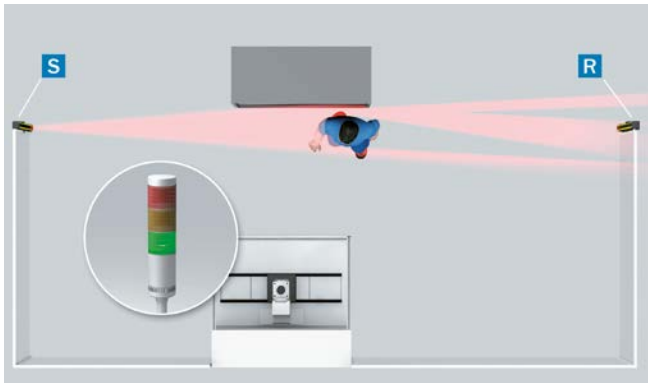
8007988/2015-07-07
Subject to change without notice

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 figures).



The person is detected reliably and the dangerous movement is stopped.



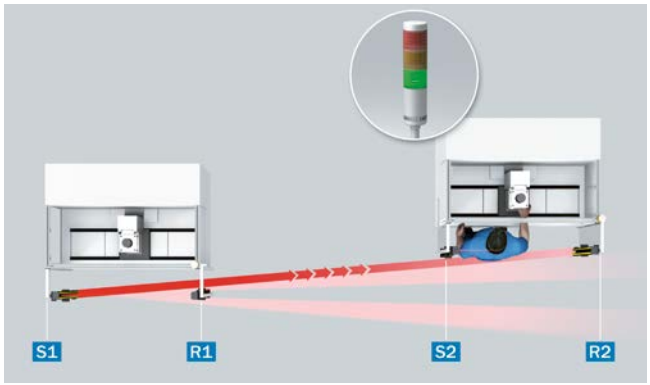
Reflection impedes detection by the ESPE and the hazardous movement is not stopped.

Accordingly, a minimum distance a must be maintained between all reflective surfaces and objects (e.g., containers, reflective floors) and the protective field of the system (see table “Main differences of type 2 and type 4 AOPDs according to IEC 61496” ➜ 3-32).

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

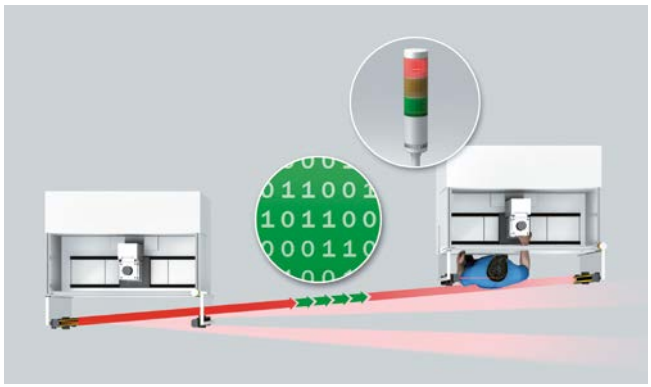
Preventing mutual interference from AOPDs

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).

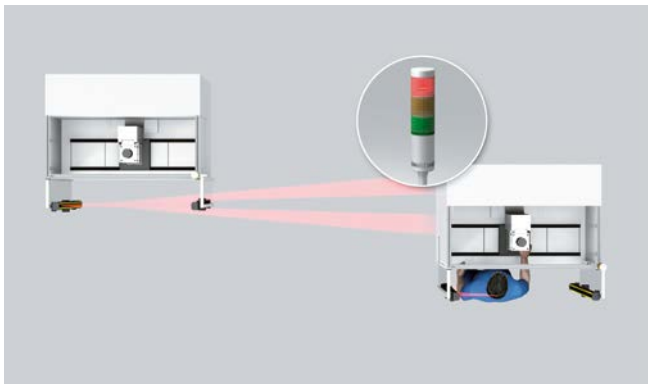


Mutual interference impedes detection by the ESPE and the hazardous movement is not stopped.

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 sender (coded the same, see figures).



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



No mutual interference of protective devices due to suitable arrangement

Selection of a suitable ESPE

Criteria can include:

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

What safety function is the ESPE expected to perform?

- Initiating a stop (➜ 3-3)
- Preventing unexpected start-up (➜ 3-4)
- Preventing start (➜ 3-4)
- Combination: Initiating a stop and preventing start (➜ 3-4)
- Enabling material throughput (➜ 3-5)
- Monitoring machine parameters (➜ 3-5)
- Safety-relevant indications and alarms (➜ 3-7)
- Other functions, e.g., PSDI mode, blanking, protective field switching, etc. (➜ 3-40)

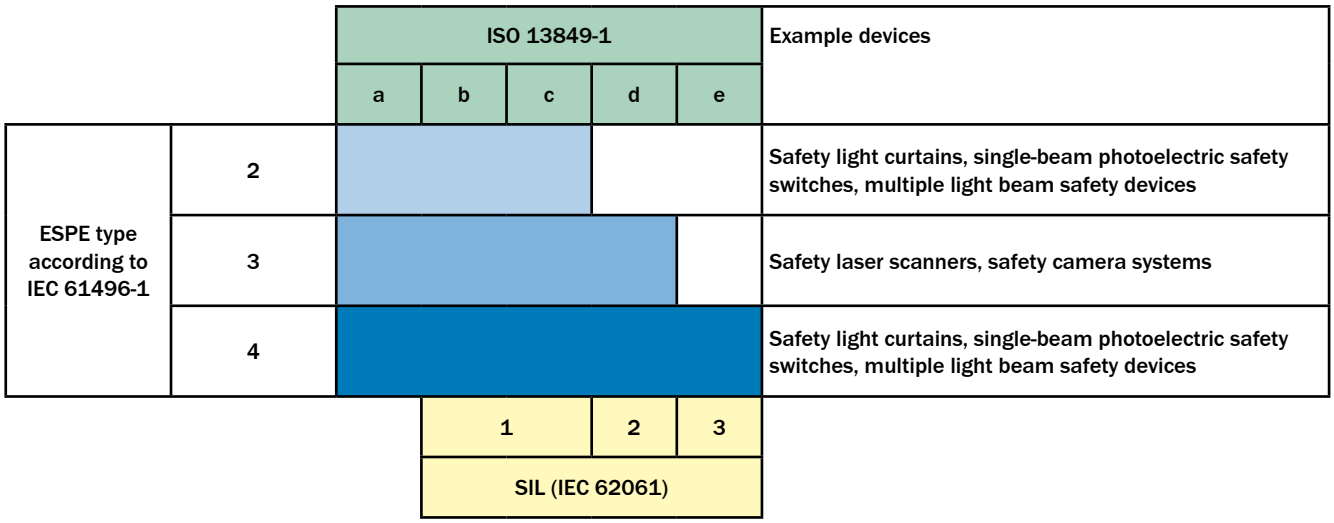
Safety level

For ESPE, the safety-related parameters have been implemented in a type classification (Type 2, Type 3, Type 4).
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 behaviour in presence of interferences (sun, lamps, similar types of device, etc.) but also the opening angle of optics in safety light curtains or safety photoelectric switches (the requirements to be met by a type 4 AOPD are more stringent than those for a type 2 AOPD).

The aperture angle is decisive in determining the minimum distance in relation to reflective surfaces (table ➜ 3-32).

➜ ESPE requirements: IEC 61496-1, IEC 61496-2, IEC 61496-3

Achievable reliability of safety functions with optoelectronic protective devices



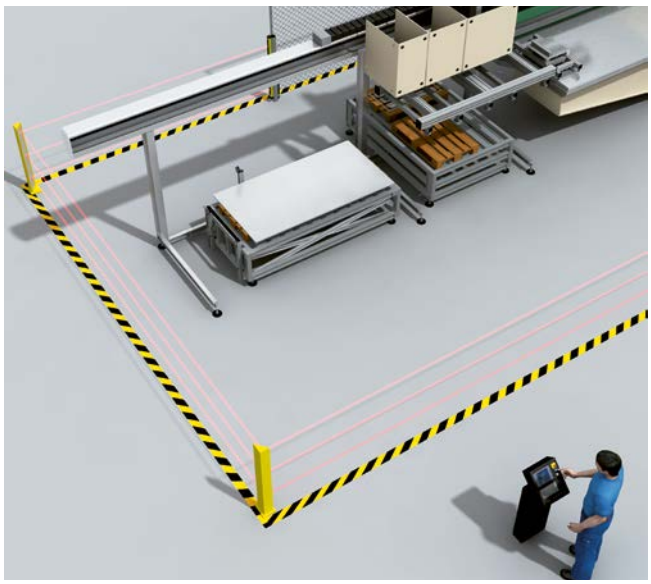
Always follow the additional application notes, information, and instructions in the instruction handbook for the optoelectronic protective devices!

3 c

What should ESPE detect?

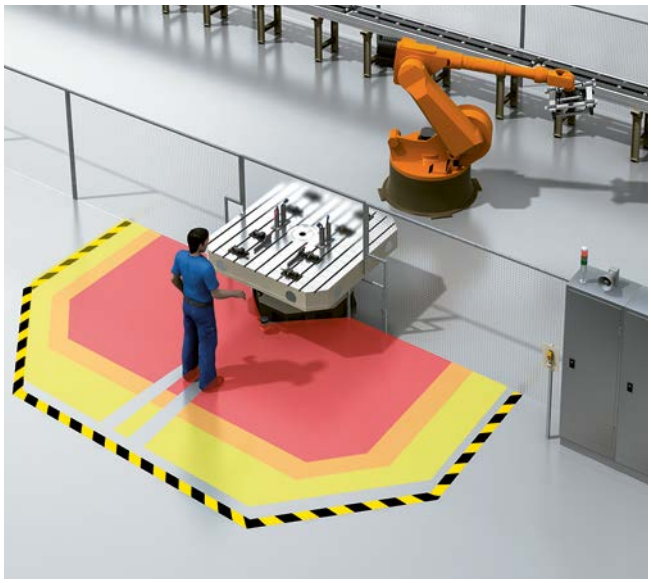
Hazardous point protection with finger or hand detection
In the case of hazardous point protection, approach is detected very close to the hazardous point.
The advantage of this type of protective device is that it allows a short minimum distance and the operator can work more ergonomically (e.g., during loading work on a press).

Access protection: Detection of a person on access to the hazardous area
In the case of access protection, the approach of a person is detected by detecting the body.
This type of protective device is used for protection of access to hazard zones. A stop signal is initiated if the hazard zone is entered. A person who is standing behind the protective device will not be detected by the ESPE!



8007988/2015-07-07
Subject to change without notice

Hazardous area protection: Detection of the presence of a person in the hazardous area
In the case of hazardous area protection, the approach of the person is detected by detecting the person's presence in an area.
This type of protective device is suitable for machines on which, for example, a hazardous area cannot be overseen completely from the position of the reset device. If the hazardous area is entered, a stop signal is initiated and starting prevented.



Mobile hazardous area protection: Detection of a person approaching the hazardous area
Hazardous area protection is suitable for AGV (automated guided vehicle), cranes and stackers, to protect persons during movement of the vehicles or while these vehicles dock to a fixed station.

Safety functions that can be integrated in ESPE

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

Muting

The muting function is used to deactivate the protective function of a protective device temporarily. 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. On the other hand, where protective devices preventing access (protective devices that cannot be tresspassed) are concerned, muting shall only be possible if no dangerous machine functions are present (see figure).

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.

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 hazard zone.
- 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 of the muting duration
- 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)

→ Practical application of ESPE: IEC / TS 62046

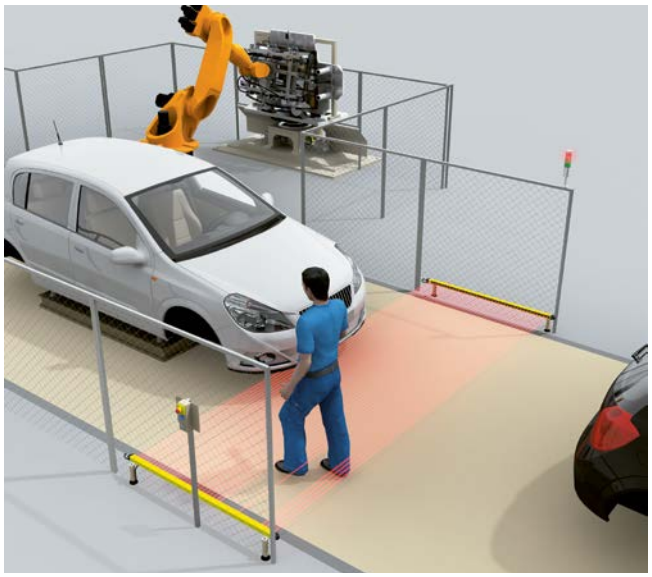
8007988/2015-07-07
Subject to change without notice

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.

For this application, horizontally arranged safety light curtains (AOPDs) are applied. The possibility of evaluating each light beam individually is used to differentiate the interruption pattern of the material or material carrier (e.g., pallet) from 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 hazard zone can be reliably prevented (see figure).



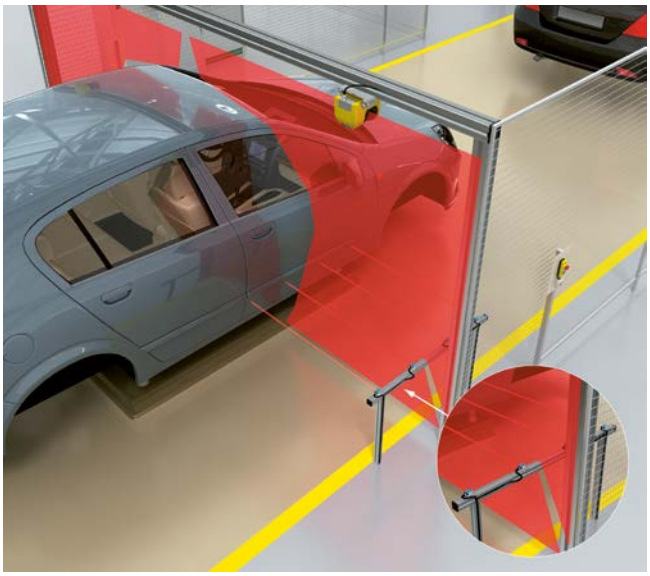
Entry/exit function with horizontally installed safety light curtain in a processing station on an automobile assembly line.

Safety laser scanners with protective field switching

Active switching of protective fields provides other way of moving material into a safeguarded area.

For this application, safety laser scanners are normally used with vertical (or slightly tilted) protective fields.

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 so that passage of the material does not cause the protective device to activate, but unmonitored areas are small enough to prevent undetected access to the hazard zone (see figure).

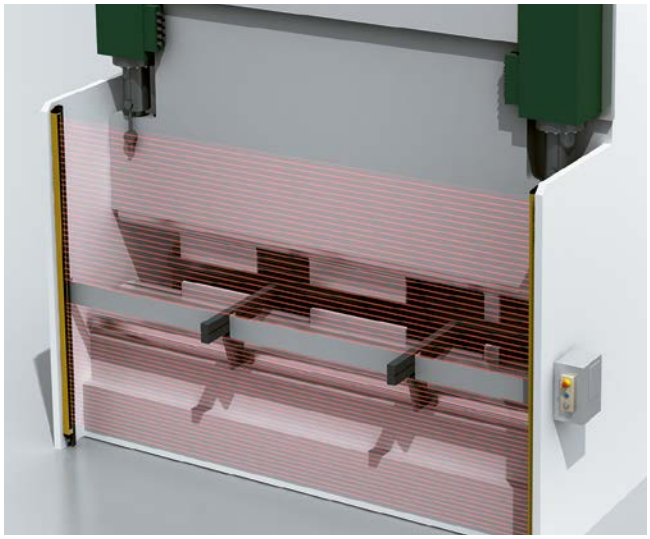


Material throughput with safety laser scanners, vertical protective fields, and protective field switching with suitably arranged sensors

Additional functions of ESPE

Blanking

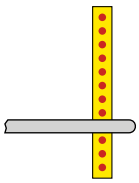
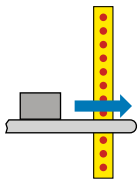
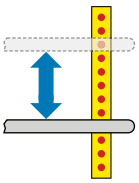
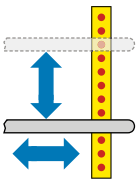
For many AOPDs, configuration of the detection capability and/or protective field can be designed such that the presence of one or more objects within a defined section of the protective field does not trigger the safety function (OFF state). Blanking can be used to allow specific objects through the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



Fixed blanking of light curtain beams on a trimming press.

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

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

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.
			

Criteria for fixed and floating blanking

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).

8007988/2015-07-07
Subject to change without notice

PSDI mode

Use of the protective device to trigger the machine function (controlling protective device) is described as PSDI mode. 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 AOPD s 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 is necessary to check that no hazard 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 (prevention against trespassing e.g., using a presence sensing ESPE).

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., rotary tables, automatic assembly systems). When using PSDI mode, the light curtain must not be tresspassable. For presses, special conditions apply for PSDI mode.

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.

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

→ PSDI mode: B-type standards ISO 13855, IEC 61496-1
→ PSDI mode on presses: C-type standards EN 692, EN 693

3 c

Position fixing protective devices

Position fixing protective devices provide risk reduction by ensuring the position of a person or parts of the body outside the hazard zone.

A comprehensive overview of position fixing protective devices is given in:
➜ Alfred Neudörfer: Konstruieren sicherheitsgerechter Produkte, Springer-Verlag, Berlin u. a., ISBN 978-3-642-33889-2 (5th Edition 2013)

Two-hand controls

A two-hand control only protects one person! If there are several operators, each person must actuate a two-hand control. A hazardous machine function shall only be initiated by intended actuation of the two-hand control and shall stop as soon as a hand releases the control device.

There are various types of two-hand control. The features that vary are the design of the control actuating devices (pushbuttons) as well as the requirements in relation to the control system.

The following basic principles apply to all types:

- It shall be ensured that both hands are used
- Releasing one of the two control actuating devices (pushbuttons) shall stop the dangerous movement
- Inadvertent actuation shall be prevented
- It shall not be possible to easily defeat the device
- It shall not be possible to take the two-hand control into the hazard zone

The following provisions also apply in the case of type II and type III two-hand controls:

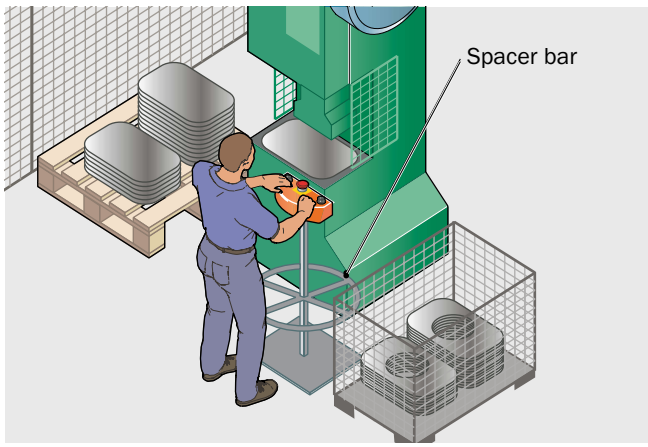
- Hazardous machine functions may only resume after both control actuating devices (pushbuttons) have been released and then activated again

The following provisions also apply in the case of type III two-hand controls:

- Hazardous machine functions may only resume once both control actuating devices (pushbuttons) have been operated synchronously within 0.5 seconds

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

- Type III A: evaluation of one normally open contact per control actuating device (pushbutton) (2 inputs)
- Type III C: evaluation of one normally open contact and one normally closed contact per control actuating device (pushbutton) (4 inputs)



➜ Requirements to be met by two-hand controls: ISO 13851 (B-type standard)

➜ Calculating the minimum distance for two-hand controls ➜ 3-52

8007988/2015-07-07
Subject to change without notice

Enabling devices

During machine setup and maintenance, and if it is necessary to observe production processes close up, functions of the protective devices may need to be disabled in certain circumstances. In addition to other measures that minimize risk (reduced force/speed, etc.), control devices are required that shall be actuated for the entire time the protective devices are disabled. Enabling devices are an option in such cases.
Enabling devices are physically actuated control switches with which the operator's agreement to machine functions is obtained. Generally, pushbuttons or foot switches are used as enabling devices.
Joysticks or inching buttons can be used as additional start controls for the enabling device. Having proven their worth in industrial applications, 3-position enabling devices are to be recommended.

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.

Principle of operation of the 3-position enabling device:

Position	Actuator	Function
1	Not operated	Off
2	In middle position (pressure point)	Enable
3	Beyond middle position	Emergency stop (off)

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, these contacts should be integrated into the emergency stop circuit.

Protection against manipulation shall be considered when using enabling devices.

➜ Requirements for enabling devices: IEC 60204-1 (B-type standard)

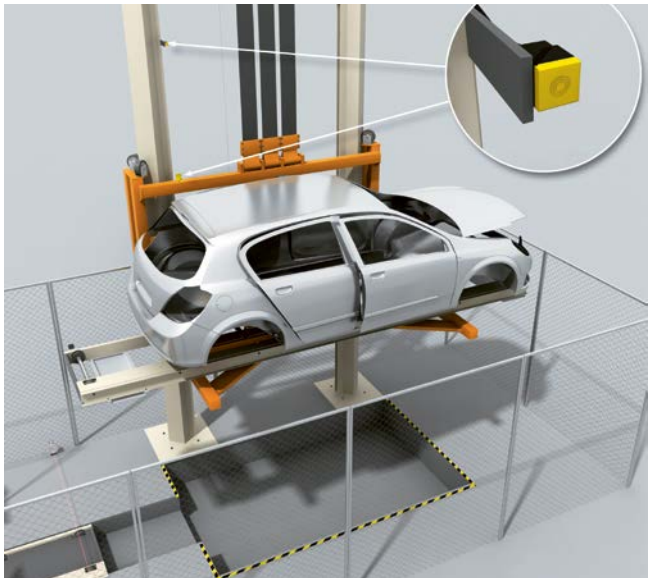
Sensors for monitoring machine parameters

The risk assessment may show that certain machine parameters shall be monitored and detected during operation.

Safe position monitoring

Safety-related sensors or position switches can be used to prevent a machine overrunning or leaving a specific position (➜ 3-19).

Electro-sensitive safety inductive position switches are particularly suitable for this task. 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 mating element, without wear, and with a high enclosure rating.



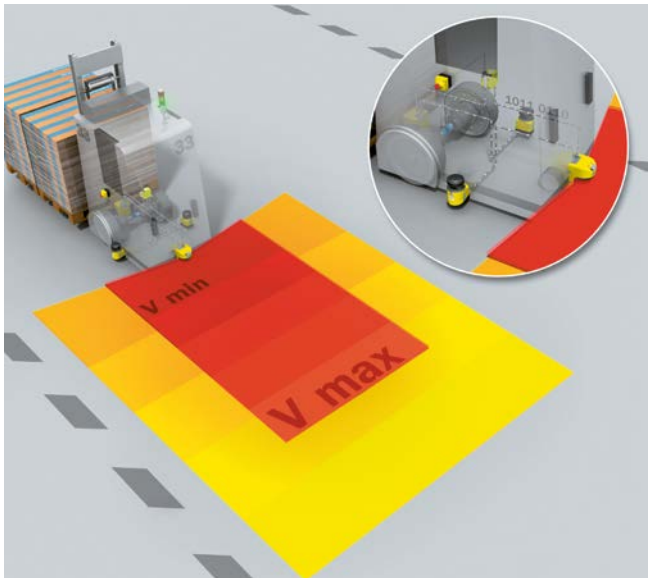
Safe position monitoring for a lift on an automobile production line

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.



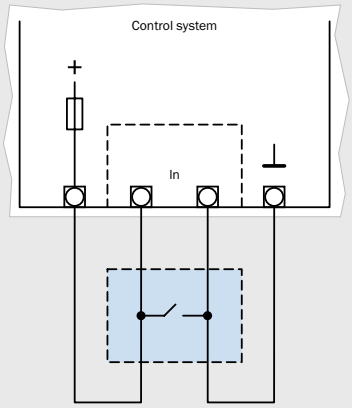
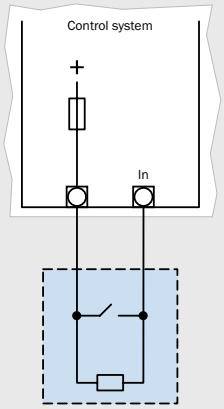
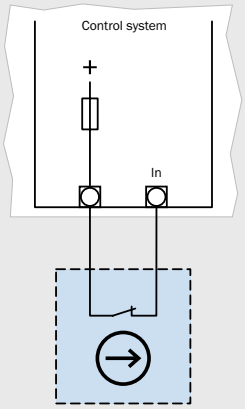
Speed monitoring for protective field switching on an automated guided vehicle

8007988/2015-07-07
Subject to change without notice

Pressure-sensitive mats and floors, pressure-sensitive edges and bars, bumpers and plates

In some applications, pressure sensitive protective devices can 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 initiates the safety function.

The usual 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 addressed in the product standards for pressure-sensitive mats and floors.

Short circuiting designs (energize to trip principle)		Positive opening contact design (de-energize to trip principle)
4-wire version	Resistance version	
		
Here, the activation of the protective device triggers a short-circuit. 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 can be excluded by proper cabling or shielding.

➜ Design of pressure sensitive protective devices: B-type standard ISO 13856 (standard series)

Foot switches

Foot switches are used to control work processes. On some machines (e.g., presses, punches, bending and metal working machines) the use of foot switches for safety functions is only permitted in separate operating modes and only in conjunction with other technical protective measures (e.g., slow speed).

However, in these cases, specific design requirements must be met:

- A protective cover to protect against unintentional actuation
- A 3-position design similar to the enabling switch principle (see “Principle of operation of the 3-position enabling device” ➜ 3-43).
- A means of manual reset on actuation of the actuator beyond the pressure point
- After the hazardous machine function has been stopped, restarting via the foot switch foot is only permitted after releasing and actuating the foot switch again
- Evaluation of at least one normally open contact and one normally closed contact
- If there are several operators, each shall actuate a separate switch

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 (➜ 2-4 and 2-5)
- 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, the "safety functions" and the requirements with regard to functional safety shall be met (see chapter "Application of reset and restart" ➜ 3-65).

Emergency operation

Emergency stop (stopping in an emergency situation)
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. Other than the exceptions described in the related standard (ISO 13850), every machine must be fitted with at least one emergency stop device.

- Emergency stop devices shall be easily accessible.
- An emergency stop shall bring the dangerous state to an end as quickly as possibly without creating additional risks.
- The emergency stop command shall take priority over all other functions and commands in all operating modes.
- Resetting the emergency stop device shall not trigger a restart.
- The principle of direct actuation with mechanical locking function shall be applied.
- The emergency stop must conform to stop category 0 or 1 (➜ 2-9).

Emergency off (switching off in an emergency situation)
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 shall 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.
- Emergency switching off shall only be achieved with stop category 0 (➜ 2-9).

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.

Emergency stop and emergency switching off are complementary protective measures and are not a means for the reduction of risks related to hazards on machinery.

Requirements and forms of implementation
The contacts on the emergency stop devices shall have positive opening normally closed contacts. The actuator shall be red, any background shall be yellow. 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 covers (for emergency stop)
- Mains isolation devices

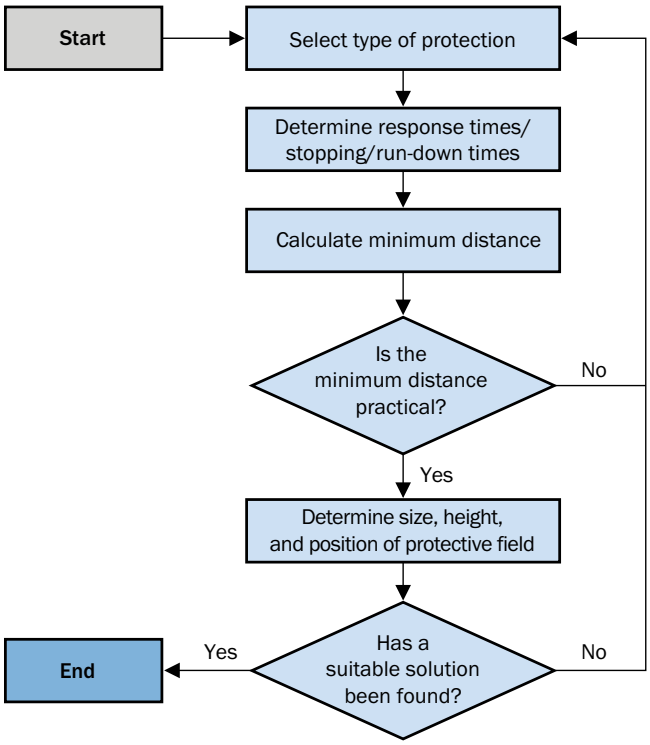
If wires ropes ropes are used as actuators for emergency stop devices, they shall be designed and attached so that they are easy to actuate and trigger the function. Reset devices shall be arranged so that the entire length of the wire or rope is visible from the location of the reset device.

➜ Design principles for emergency stop devices: ISO 13850
➜ Emergency stop: Machinery Directive 2006/42/EC

8007988/2015-07-07
Subject to change without notice

Positioning and dimensioning of protective devices

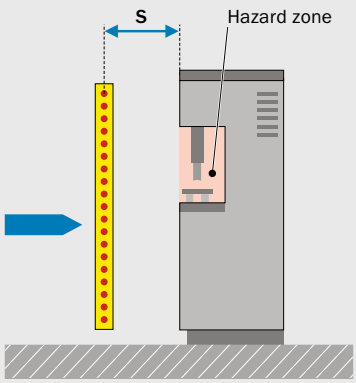
One essential aspect for the selection of an optimal protective device is the space available. It must be ensured that the dangerous state can be eliminated in good time before the hazardous point is reached.
The necessary minimum distance is dependent on, among other aspects, the size and type of the protective device.



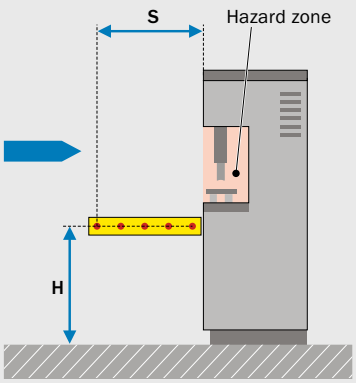
3 c

Minimum distance for ESPE dependent upon approach

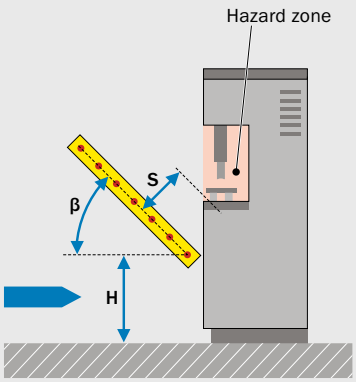
The consideration of the minimum distance applies to ESPE with two-dimensional protective field (e.g., light curtains, photoelectric switches (AOPD), laser scanners (AOPDDR), or two-dimensional camera systems). In general, a differentiation is made between three different approach types.



Perpendicular approach/perpendicular entry to protective field plane



Parallel approach or entry parallel to protective field plane



Angular approach to the protective field plane

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, and/or the type of approach

If the minimum distance to the hazard zone is too large and unacceptable from an ergonomic viewpoint, either the overall stopping time of the machine must be reduced or an ESPE with better resolution chosen. The possibility of someone standing behind shall be prevented.

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

General calculation formula

$$S = (K \times T) + C$$

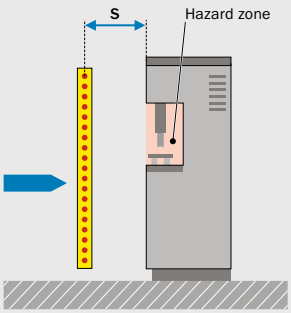
Where ...

- **S** is the minimum distance in millimeters, measured from the nearest hazardous point to the detection point or to the detection line or detection plane of the ESPE.
- **K** is a parameter in millimeters per second, derived from the data for the approach speeds of the body or parts of the body.
- **T** is the stopping/run-down time of the overall system in seconds.
- **C** is the additional distance in millimeters that represents the intrusion into the hazard zone before the protective device is triggered. If it is not possible to reach through 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).

8007988/2015-07-07
Subject to change without notice

The table contains the formulas for calculating the minimum distance S as a function of the approach to the protective field.

Perpendicular approach: β = 90° (± 5°)

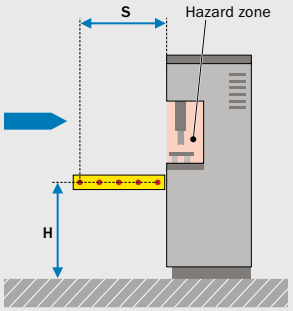


Step 1: Calculation of the minimum distance S

d ≤ 40 mm	S = 2000 × T + 8 × (d – 14) If S > 500 mm, then use: S = 1600 × T + 8 × (d –14). In this case S cannot be < 500 mm.	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 hazard zone **before** the protective device is triggered.
40 < d ≤ 70 mm	S = 1600 × T + 850	Height of the bottom beam ≤ 300 mm Height of the top beam ≥ 900 mm
d > 70 mm	S = 1600 × T + 850	**Number of beams** / **Recommended heights** 4 / 300, 600, 900, 1200 mm 3 / 300, 700, 1100 mm 2 / 400, 900 mm (400 mm can only be used if there is no risk of crawling beneath.)

Step 2: Calculation of the necessary height for the top edge of the protective field (➜ 3-57)

Parallel approach: β = 0° (± 5°)



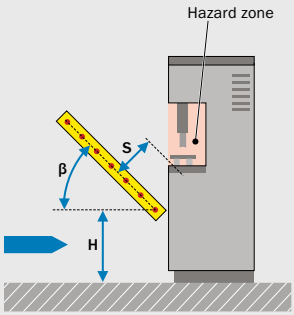
Step 1: Calculation of the minimum distance S

S = 1600 × T + (1200 – 0.4 × H) where C = (1200 – 0,4 × H) ≥ 850 mm	H ≤ 1000 mm

Step 2: Calculation of the necessary resolution depending on the protective field height

$d \leq \frac{H}{15} + 50$ mm	H ≤ 1000 mm d ≤ 117 mm

Angular approach: 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 hazard zone and is ≤ 1000 mm in height.

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

Special cases

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

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	

→ Press standards: EN 692/693 (C-type standards)

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 starting" 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 hazard zone 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 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).

Safety laser scanner on a machining center as safety function pos. 1, initiating a stop and safety function pos. 2, preventing unexpected start

8007988/2015-07-07
Subject to change without notice

ESPE applications on vehicles

When the hazard is originated by a vehicle, the vehicle's traveling speed is generally used to determine the minimum distance and not the approach speed of persons. When the vehicle (and, therefore, the protective device) and a person are approaching each other, under normal circumstances it is assumed the person will recognize the danger and stop or move away. Therefore, the minimum distance only needs to be set to a length that is sufficient to stop the vehicle safely.
Safety supplements may be necessary dependent on the application and the technology used.

Stationary application with an ESPE that moves with the tool

The way in which some machines function requires that operators are located very close to the hazard zone. 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. The hand approach speed is not taken into account here, so the general formula cannot be applied.

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 camera-based evaluation are used. This type of protection is defined in the C-type standards in conjunction with other measures (e.g., 3-position foot switch, automatic stoptime measurement, requirement to wear gloves, etc.).

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

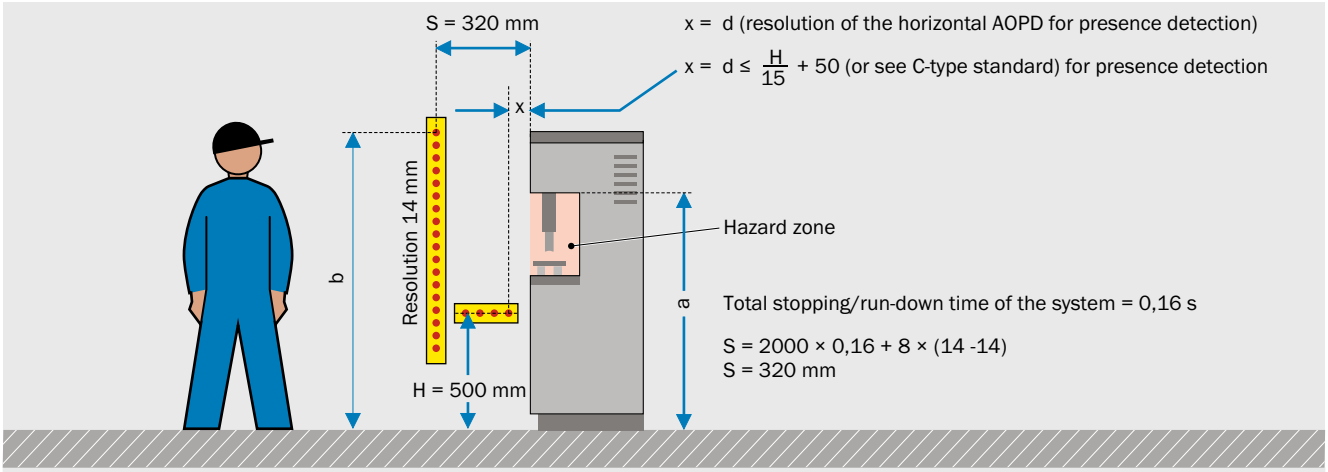
Specific know-how and equipment are required to measure the stopping/run-down time and the necessary minimum distance. SICK offers these measurements as a service.

Examples for calculating the minimum distance

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

The calculation, as shown in the figure, yields a minimum distance of S = 320 mm. By using a safety light curtain with the best possible resolution, this is already the optimal minimum distance.

To ensure that the person is detected anywhere in the hazard zone, two AOPDs are used: a vertical AOPD positioned at the calculated minimum distance (perpendicular approach), and a horizontal AOPD to eliminate the danger of standing behind the vertical AOPD.



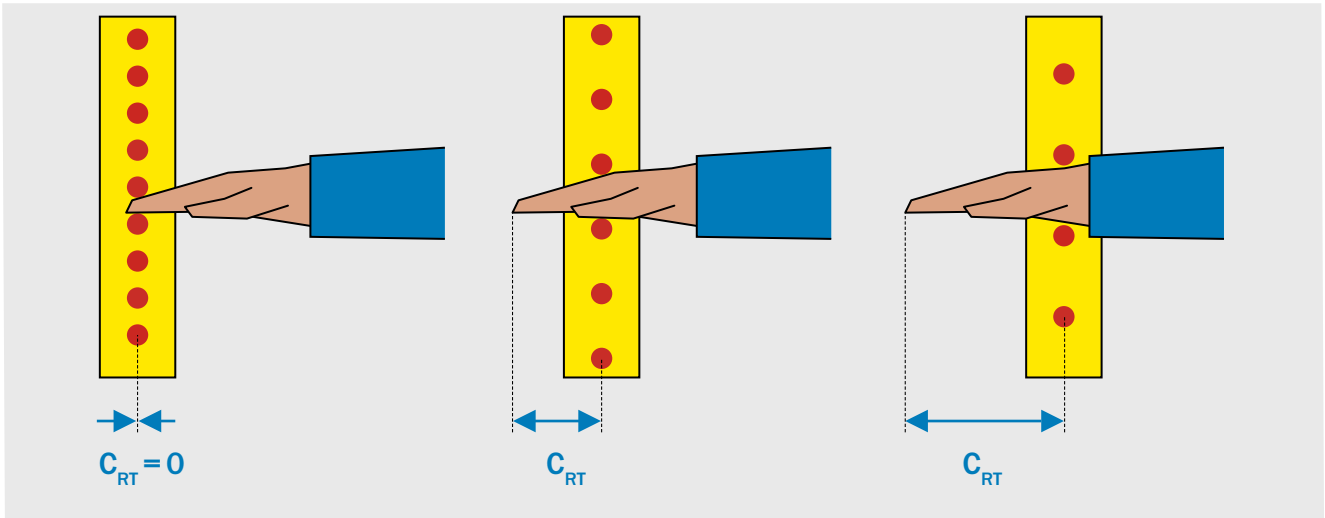
a = height of the hazard zone
d = detection capability (resolution of the AOPD)
H = installation height
S = minimum distance

x = distance from the end of the protective field to the machine
b = height of the uppermost beam, determination see "Necessary protective field size/height for the ESPE" ➜ 3-55

Supplement determined by resolution C_{RT}

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}.



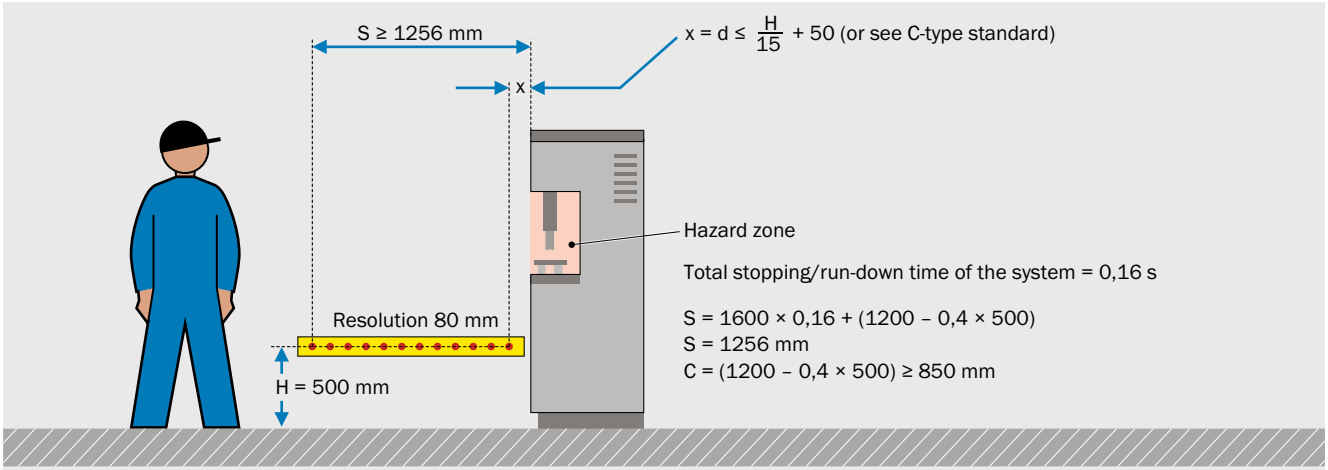
The figure shows an example of undetected depth penetration factor at safety light curtains with different detection capabilities.

8007988/2015-07-07
Subject to change without notice

Solution 2: Perpendicular approach — hazardous area protection

A horizontal AOPD is used. The figure below shows the calculation of the minimum distance S and the positioning of the AOPD. If the installation height of the AOPD is increased to 500 mm, the minimum distance is reduced. For this height an AOPD with a resolution less or equal to 80 mm shall be used.

It must not be possible to access the hazard zone beneath the AOPD. 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.



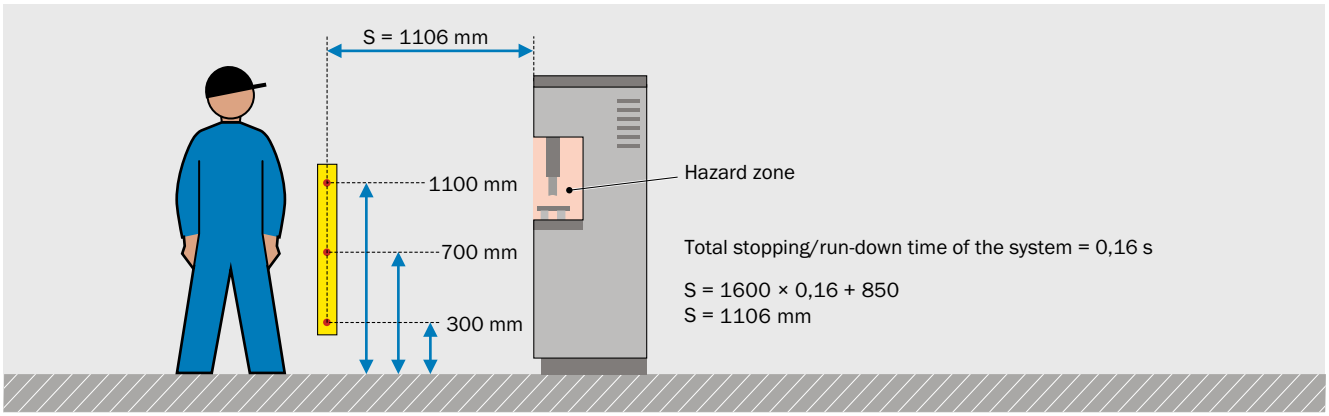
C = additional distance in millimeters that represents entry into the hazard zone before the protective device is triggered
d = detection capability (resolution of the AOPD

H = installation height
S = minimum distance
x = distance from the end of the protective field to the machine

Solution 3: Access protection

Access protection with 3 beams (at heights of 300 mm, 700 mm, and 1100 mm) allows perpendicular approach. This solution also allows the operator to stand between the hazard zone 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) shall be positioned so that the entire hazard zone can be overseen. It shall not be possible to reach the button from inside the hazard zone.



3 c

Comparison of the results

The table below shows the results of these solutions. Operational requirements may determine which of the solutions is selected:

Solution 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 = 1256 mm**	• Automatic start possible • Enables access to be protected independent of the height of the hazard zone	• The operator is much further away (long paths) • More space required • Lower productivity
3	**Access protection** **S = 1106 mm**	• Cost-effective solution • Enables access to be protected independent of the height of the hazard zone • Protection on several sides possible using deflector mirrors	• The operator is much further away (long paths) • 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.

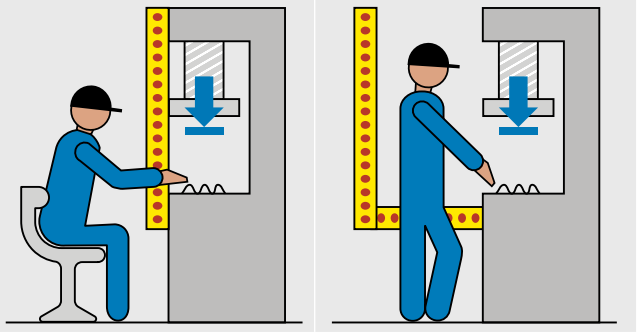
8007988/2015-07-07

Necessary protective field size/height of the ESPE

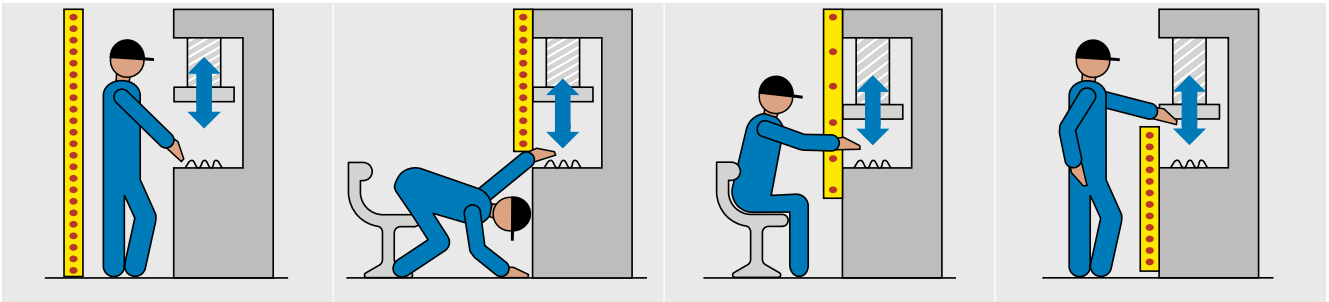
As a general rule, the following faults must be excluded when assembling protective devices:

- 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 are required (e.g., restart interlock, secondary protective device).

Examples of correct assembly



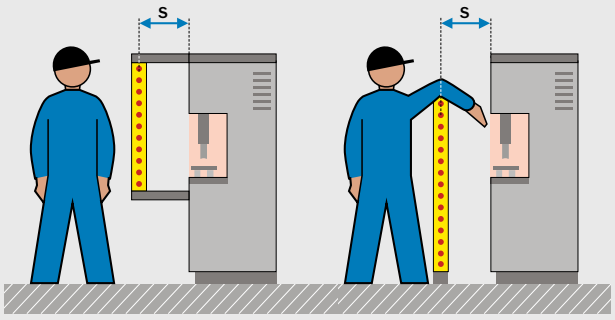
Examples of dangerous assembly faults



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 before the hazardous machine function has ceased.

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 not provided. The figure shows an example comparing an ESPE that cannot be reached over and an ESPE that can be reached over.



ESPE cannot be reached over ESPE can be reached over

If access to the hazard zone 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.

Take the possibility of reaching over into account

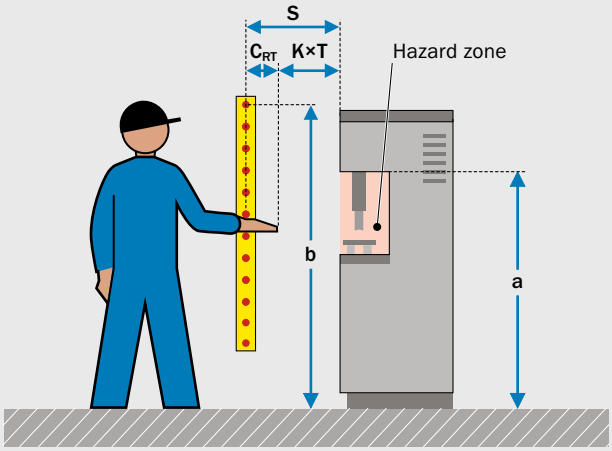
If there is a possibility of reaching over the vertical protective field of an ESPE, the height **b** of the top edge of the protective field shall be increased or the supplement **C** adjusted. The corresponding table from standard ISO 13855 shall be used for both methods.

Consequences

In some applications, in which ESPE is used with d > 40 mm (multiple beam systems), the minimum distance could increase or ESPE with d ≤ 40 (light curtains) shall be used. This situation applies for the application of ISO 13855. Some C-type standards differ from ISO 13855 in the calculation of the minimum distances.

Increase height of top edge

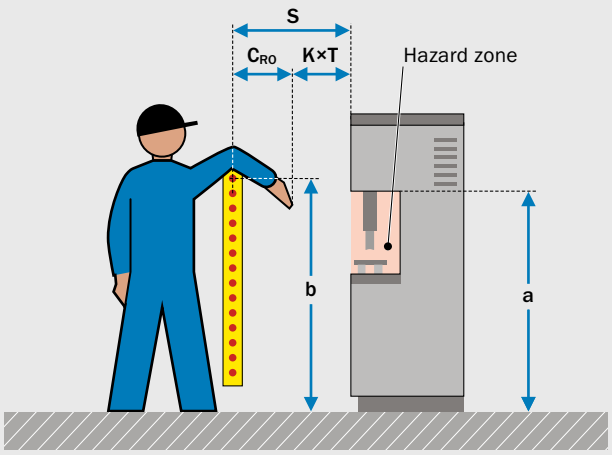
When the height of the top edge of the protective field **b** is increased, in addition to the height of the hazard zone **a**, the supplement determined by the resolution C_{RT} is also used to calculate the required height of the top edge of the protective field when the minimum distance remains unchanged. 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 necessary.



Parameters for determining the required minimum distance for reaching through

Increase minimum distance (height of top edge prescribed)

If the top edge of the protective field **b** is prescribed by a pre-existing product, the minimum distance must be increased. This is achieved with the determination of the height of the hazard zone **a** and the height of the top edge of the protective field **b**. The result of the intersection produced in the table represents the intrusion distance C_{RO}. If $C_{RO} \geq C_{RT}$, the C_{RO} value replaces the C_{RT} value in the calculation of the minimum distance. If $C_{RO} < C_{RT}$, the C_{RT} value continues to be used to calculate the minimum distance.



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

The rule of thumb is:

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

The table from ISO 13855 and practical examples can be found on the following pages.

3 c

How to determine the necessary height for 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:

   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.
3. Read the resulting height **b** for the top edge of the protective field from the bottom row of the column defined by step 2.

- ESPE, resolution d ≤ 40 mm: $C_{RT} = 8 \times (d - 14)$
- ESPE, resolution d > 40 mm: $C_{RT} = 850$ mm

Height **a** of the hazard zone (mm)	Additional horizontal distance **C** to the hazard zone (mm)											
2600	0	0	0	0	0	0	0	0	0	0	0	0
2500	400	400	350	300	300	300	300	300	250	150	100	0
2400	550	550	550	500	450	450	400	400	300	250	100	0
2200	800	750	750	700	650	650	600	550	400	250	0	0
2000	950	950	850	850	800	750	700	550	400	0	0	0
1800	1100	1100	950	950	850	800	750	550	0	0	0	0
1600	1150	1150	1100	1000	900	850	750	450	0	0	0	0
1400 ①	1200	1200	1100	1000	900	850 ②	650	0	0	0	0	0
1200	1200	1200	1100	1000	850	800	0	0	0	0	0	0
1000	1200	1150	1050	950	750	700	0	0	0	0	0	0
800	1150	1050	950	800	500	450	0	0	0	0	0	0
600	1050	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**	**1100**	**1200**	**1300**	**1400** ③	**1600**	**1800**	**2000**	**2200**	**2400**	**2600**

Example

- Resolution of the ESPE: > 40 mm
- Height **a** of the hazard zone: 1400 mm ①
- Resolution-dependent supplement **C**: 850 mm ②

The height **b** of the top edge of the ESPE's protective field must not be less than 1400 mm ③; if it is, the horizontal distance to the hazard zone shall be increased.

If the required height for the top edge of the protective field cannot be achieved, the supplement CRO shall 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 necessary horizontal distance **C** at the intersection between the two values.

Height **a** of the hazard zone (mm)	Additional horizontal distance **C** to the hazard zone (mm)											
2600	0	0	0	0	0	0	0	0	0	0	0	0
2500	400	400	350	300	300	300	300	300	250	150	100	0
2400	550	550	550	500	450	450	400	400	300	250	100	0
2200	800	750	750	700	650	650	600	550	400	250	0	0
2000	950	950	850	850	800	750	700	550	400	0	0	0
1800	1100	1100	950	950	850	800	750	550	0	0	0	0
1600	1150	1150	1100	1000	900	850	750	450	0	0	0	0
1400 ②	1200	1200	1100 ③	1000	900	850	650	0	0	0	0	0
1200	1200	1200	1100	1000	850	800	0	0	0	0	0	0
1000	1200	1150	1050	950	750	700	0	0	0	0	0	0
800	1150	1050	950	800	500	450	0	0	0	0	0	0
600	1050	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**	**1100** ①	**1200**	**1300**	**1400**	**1600**	**1800**	**2000**	**2200**	**2400**	**2600**

Example

- Three-beam standard ESPE (300/700/1100 mm)
- Height **b** of the top edge of the protective field: 1100 mm ①
- Height **a** of the hazard zone: 1400 mm ②
- Supplement determined by possible reaching over C_{RO}: 1100 mm ③ (instead of the 850 mm stated in the previous standard)

3 c

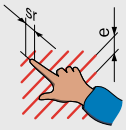
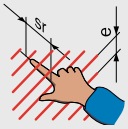
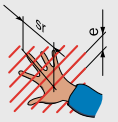
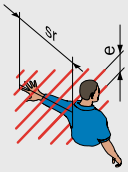
To take the possibility of reaching over into account, standard ISO 13855 includes the following table. This table is used to calculate the increased height of the top edge of the protective field or the increased minimum distance.

Height **a** of the hazard zone (mm)	Additional horizontal distance **C** to the hazard zone (mm)											
2600	0	0	0	0	0	0	0	0	0	0	0	0
2500	400	400	350	300	300	300	300	300	250	150	100	0
2400	550	550	550	500	450	450	400	400	300	250	100	0
2200	800	750	750	700	650	650	600	550	400	250	0	0
2000	950	950	850	850	800	750	700	550	400	0	0	0
1800	1100	1100	950	950	850	800	750	550	0	0	0	0
1600	1150	1150	1100	1000	900	850	750	450	0	0	0	0
1400	1200	1200	1100	1000	900	850	650	0	0	0	0	0
1200	1200	1200	1100	1000	850	800	0	0	0	0	0	0
1000	1200	1150	1050	950	750	700	0	0	0	0	0	0
800	1150	1050	950	800	500	450	0	0	0	0	0	0
600	1050	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**	**1100**	**1200**	**1300**	**1400**	**1600**	**1800**	**2000**	**2200**	**2400**	**2600**

Safety distance for guards

Guards must be at an adequate distance from the hazard zone if they have openings. This requirement also applies to openings between a protective device and a machine frame, jiggs, etc.

Safety distance as a function of the openings on guards according to ISO 13857

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

3 c

8007988/2015-07-07
Subject to change without notice

Safety distance for interlocking guards

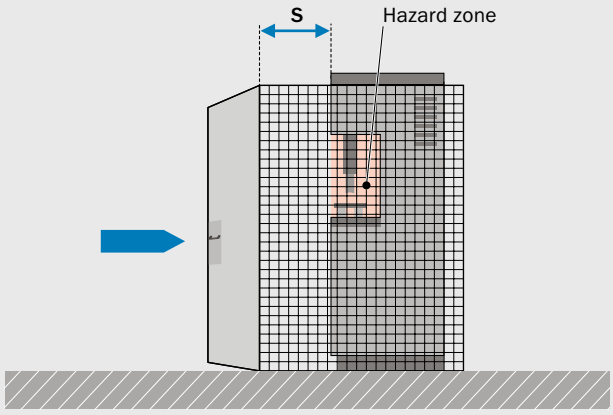
Where ...

- **S** is the minimum distance in millimeters, measured from the nearest hazardous point to the nearest door opening point.
- **K** is a parameter in millimeters per second, derived from the data for the approach speeds of the body or parts of the body, usually 1600 mm/s.
- **T** is the stopping/run-down time of the overall system in seconds.
- **C** is a safety distance taken from the corresponding table in ISO 13857: (safety distance as a function of opening in guards). 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.

For locked movable guards that initiate a stop, a safety 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.

General calculation formula

$$S = (K \times T) + C$$

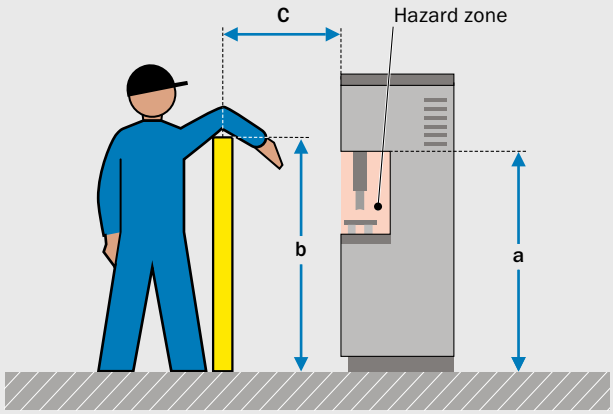


Safety distance for interlocking guards

→ Calculation of the minimum distance for interlocking guards: ISO 13855 (B-type standard)

Height requirements for guards

Similar to the procedure for ESPE, the same procedure is also to be used for guards. Different calculation tables are to be used depending on the potential hazard.
To prevent crawling beneath guards, it is normally sufficient if the guards start at 200 mm above the reference level.



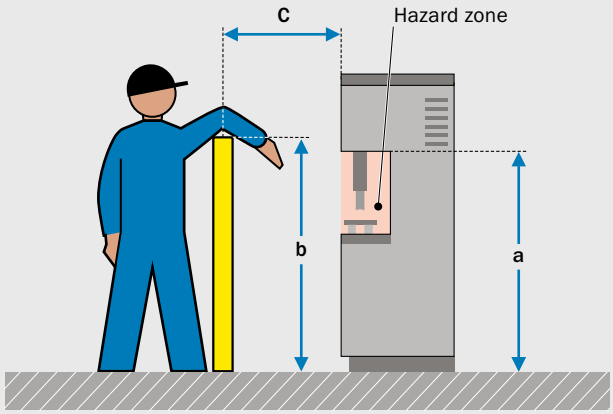
Parameters for determining the height requirements for guards

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

Height a of the hazard zone (mm)	Horizontal distance C to the hazard zone (mm)								
2500	0	0	0	0	0	0	0	0	0
2400	100	100	100	100	100	100	100	100	0
2200	600	600	500	500	400	350	250	0	0
2000	1100	900	700	600	500	350	0	0	0
1800	1100	1000	900	900	600	0	0	0	0
1600	1300	1000	900	900	500	0	0	0	0
1400	1300	1000	900	800	100	0	0	0	0
1200	1400	1000	900	500	0	0	0	0	0
1000	1400	1000	900	300	0	0	0	0	0
800	1300	900	600	0	0	0	0	0	0
600	1200	500	0	0	0	0	0	0	0
400	1200	300	0	0	0	0	0	0	0
200	1100	200	0	0	0	0	0	0	0
0	1100	200	0	0	0	0	0	0	0
	Height b of the guard (mm)								
	1000	1200	1400	1600	1800	2000	2200	2400	2500

8007988/2015-07-07
Subject to change without notice

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



Parameters for determining the height requirements for guards

Height a of the hazard zone (mm)	Horizontal distance C to the hazard zone (mm)									
2700	0	0	0	0	0	0	0	0	0	0
2600	900	800	700	600	600	500	400	300	100	0
2400	1100	1000	900	800	700	600	400	300	100	0
2200	1300	1200	1000	900	800	600	400	300	0	0
2000	1400	1300	1100	900	800	600	400	0	0	0
1800	1500	1400	1100	900	800	600	0	0	0	0
1600	1500	1400	1100	900	800	500	0	0	0	0
1400	1500	1400	1100	900	800	0	0	0	0	0
1200	1500	1400	1100	900	700	0	0	0	0	0
1000 ①	1500	1400	1000	800	0 ②	0	0	0	0	0
800	1500	1300	900	600	0	0	0	0	0	0
600	1400	1300	800	0	0	0	0	0	0	0
400	1400	1200	400	0	0	0	0	0	0	0
200	1200	900	0	0	0	0	0	0	0	0
0	1100	500	0	0	0	0	0	0	0	0
	Height b of the guard (mm)									
	1000	1200	1400	1600	1800 ③	2000	2200	2400	2500	2700

Proceed as follows to determine the necessary height for the top edge of the 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., 1000 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 guard in the bottom row, e.g., 1800 mm.

Example of high potential hazard

The guard shall, therefore, start 200 mm above the reference level and end at 1800 mm. If the height of the guard is to be 1600 mm, then the safety distance must be increased to at least 800 mm.

➜ Safety distances and required protective field height: ISO 13857

Minimum distance for position fixing protective devices

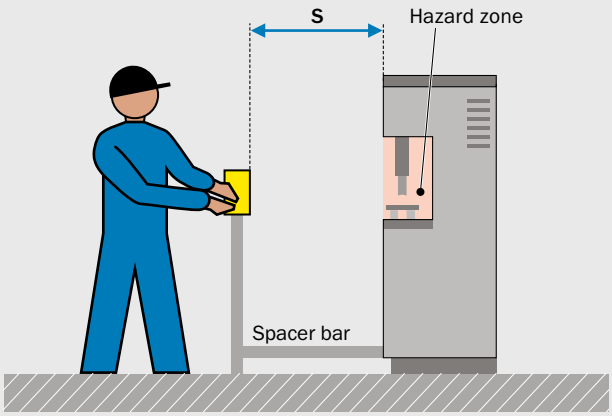
Where ...

- **S** is the minimum distance in millimeters measured from the control to the nearest hazardous point.
- **K** is a parameter in millimeters per second, derived from the data for the approach speeds of the body or parts of the body, usually 1600 mm/s.
- **T** is the stopping/run-down time of the overall system from when the control is released in seconds.
- **C** is a supplement: 250 mm. Might not be required in certain conditions (e.g., covering of the control switch).

If a two-hand control is fitted to a portable stand, then the maintenance of the necessary minimum distance must be ensured by a spacer bar or limited cable lengths (to prevent the operator carrying the control to a place where it will not provide the required safety).

Example: Minimum distance for two-hand control

$$S = (K \times T) + C$$



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

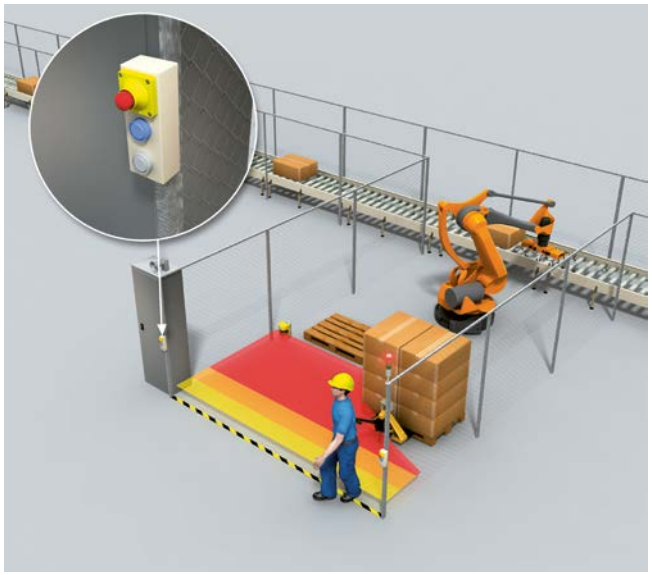
8007988/2015-07-07
Subject to change without notice

Application of reset and restart

If a protective device has issued a stop command, the stop state shall be maintained until a manual reset device is activated and the machine can subsequently be restarted. An exception to this rule is the use of protective devices that provide the constant detection of persons in the hazard zone (e.g., presence detection).

The manual reset function shall be provided by a separate, manually operated device. The device shall be designed so that it withstands the foreseeable load and the intended effect can only be obtained by intentional actuation (⚠ touch panels are unsuitable). According to ISO 13849-1 (Subclause 5.2.2) the reset shall only be generated by releasing the command device from its actuated (on) position. For this reason, signal processing is required to detect the falling edge of the signal from the command device. In other words, acknowledgment can only take the form of releasing the drive element from its (engaged) ON position. Reset is only permitted if all safety functions and protective devices are functional.

The command device for the reset shall be installed outside the hazard zone. It shall be possible from this position to completely oversee the hazard zone. By this means it can be checked that there is nobody in the hazard zone.



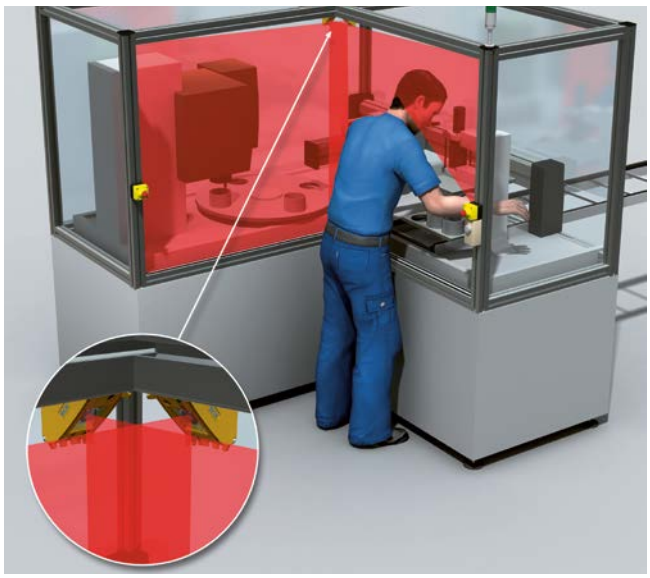
The position of the reset pushbutton allows a full view of the hazard zone for the resetting of the protective device.

The signal from the reset device is part of the safety function. As such, it shall:

- Either be discretely wired to the safety-related logic unit
- Or 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.

Hazardous point protection without reset



In this arrangement it is not possible to remain in the hazard zone without being detected. 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.

"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 an input element, logic unit, power control element as well as the actuator/work element.
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 faults. They are based on the principles of preventing and controlling faults.

8007988/2015-07-07

Control system			Aspects relating to safety technology	
Principle of operation of the control system		**Typical components**	**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 electropneumatic control systems. Service unit necessary for conditioning compressed air.
	Hydraulic 	• Accumulators • Pressure limiters • Multiway valves • Filters • Level gages • Temperature gages • Hoses • 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:
		  • Position switches
		  • Selector switches
		  • Pushbuttons
		• Switching amplifiers:
		  • Contactors
		  • Relays
		  • Circuit breakers
			• Protection class of the devices
			• Selection, dimensioning, and placement of the 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, e.g.,
		  • Transistors
		  • Resistors
		  • Capacitors
		  • Coils
		• Highly integrated components, e.g., 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 by component selection.

	Microprocessor-controlled 	• Microprocessors
		• Software
			• Installation fault in the hardware
			• Systematic faults including common mode faults
			• Programming faults
			• Handling faults
			• Operating faults
			• Manipulation
			• Viruses
				• Measures to prevent faults:
				  • Structured design
				  • Program analysis
				  • Simulation
				• Measures to control faults:
				  • Redundant hardware and software
				  • RAM/ROM test
				  • CPU test

Translation of text from: Alfred Neudörfer, Konstruieren sicherheitsgerechter Produkte, Springer Verlag, Berlin u. a., ISBN 978-3-642-33889-26 (5th Edition 2013)

The safety-related input elements have been described above with the safety sensors (protective devices). For this reason only the logic unit and the actuators are described below.
To assess the safety aspects of the actuators, reference is made to the power control elements. Faults and failures in actuator/work elements are normally excluded. (A motor without any power goes to the safe state.)

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 actuators.

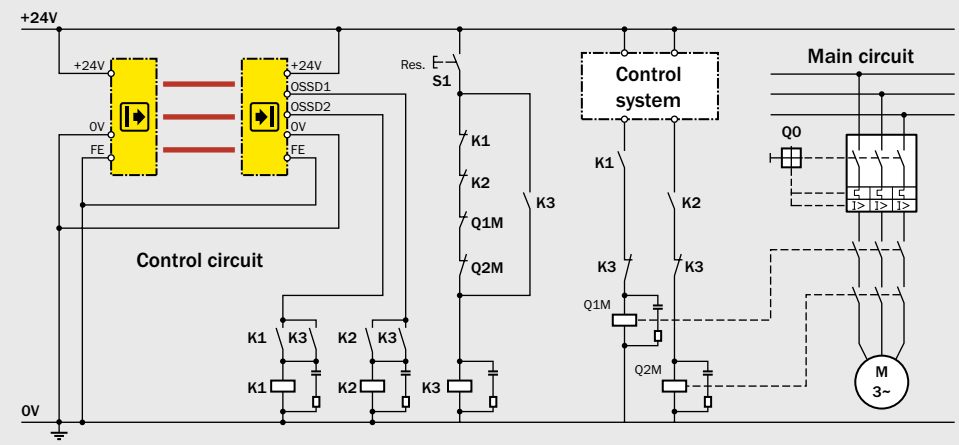
➜ You will find connection diagrams for the integration of protective devices at www.sick.com

Logic units

In a logic unit different input signals from safety functions are linked together to form output signals. Electromechanical, electronic, or programmable electronic components can be used for this purpose.

Warning: Depending on the required reliability, the signals from the protective devices shall not be processed only by standard control systems. If necessary additional cutoff paths shall be provided.

Logic unit made up of contactors

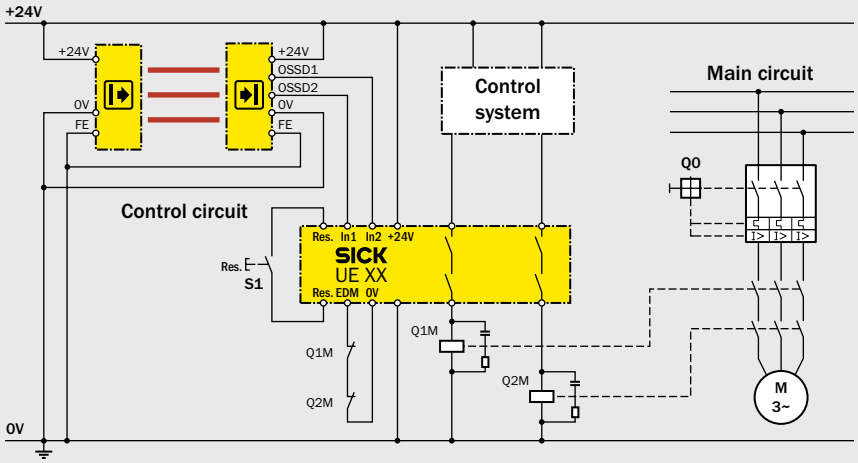


Using individual auxiliary contactors with positively guided contacts it is possible to design control systems with any level of complexity. Redundancy and monitoring by positively guided contacts are features of this safety principle. Wiring provides the logical operators.

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.

8007988/2015-07-07
Subject to change without notice

Logic unit as safety relay (safety interface)



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

The implementation of more complex safety applications is simplified. The certified safety relay also reduces the 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 language(s) supported by the firmware.

Parametrization

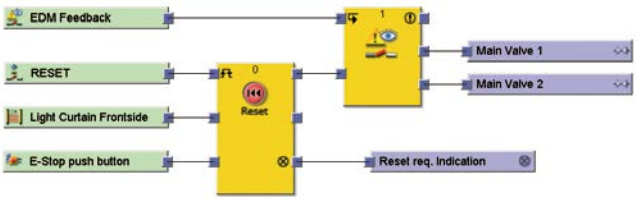
Is the selection of properties from a defined pool of functionality by selector switch/software parameters at the time of commissioning.

Features: low logic depth, AND/OR logic

Configuration

Flexible operators for defined function blocks in certified logic with a programming interface, parameterization of times and configuration of the inputs/outputs of the control system, for example.

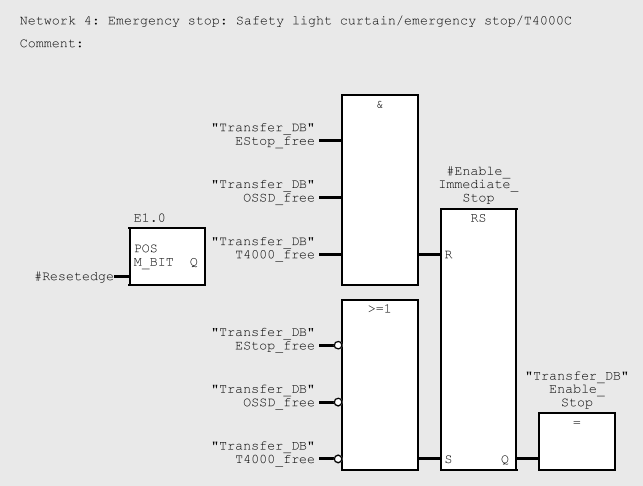
Features: any logic depth, binary logic



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

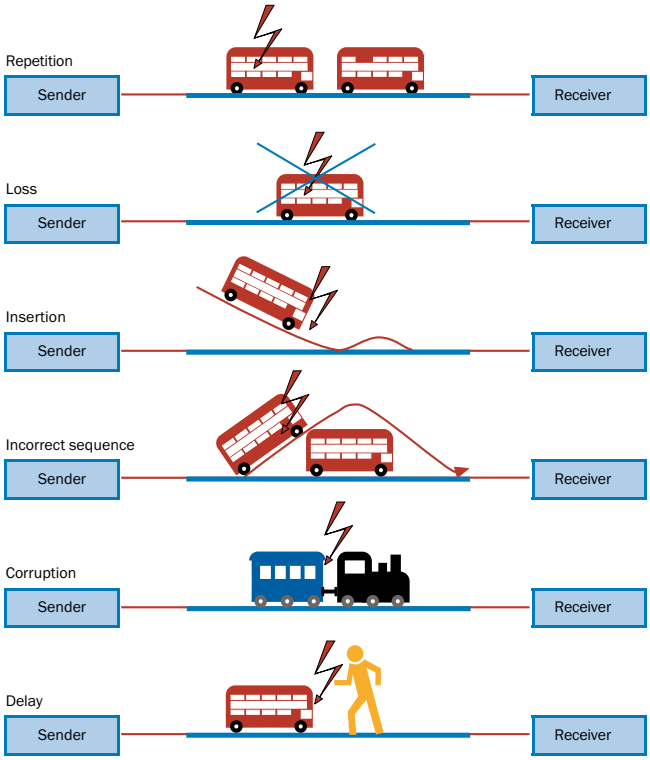


3 c

8007988/2015-07-07
Subject to change without notice

Reliable data transmission

Bus systems are used to transmit signals between the control system and sensors or actuators 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.



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

Several measures can be applied in the higher-level control system against the transmission faults mentioned above, e.g., sequential numbering of safety-related messages or defined times for incoming messages with acknowledgment. Protocol extensions based on the field-bus used include such measures.

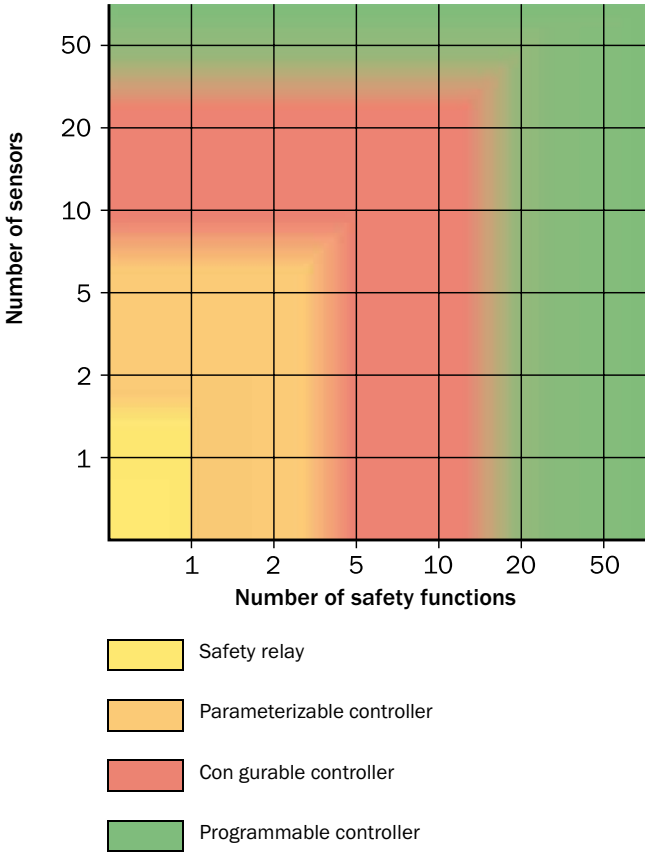
A detailed study of different faults and errors in hardware and software has shown that such faults mostly result in the same few transmission faults on bus systems.

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 field-bus systems are:

- AS-i Safety at Work
- DeviceNet Safety
- PROFIsafe

Selection criteria

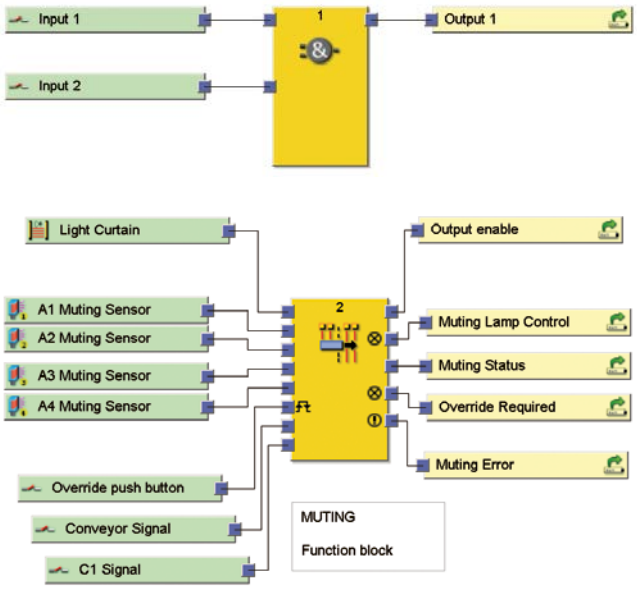
The criteria for the selection of a control system model are initially the number of safety functions to be implemented as well as the scope of the logical operators on the input signals.
The functionality of the logical operators — e.g., simple AND, flipflop, or special functions such as muting — also affects the selection.



Design matrix

0 = logic 0 or OFF
S = actuator enable (restart)
I = logic 1 or ON
– = any status

Safety inputs \ Case	Effect: Robots	Table on left	Table on right	⋮	⋮
	Safety outputs				
Position lost	0	–	–		
Robot left	S	–	–		
Robot right	S	–	–		
Robot center	S	–	–		
Access left	S	I	–		
Access right	–	–	I		
Emergency stop	0	0	0		
...					



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 faults in the logic. To detect systematic faults, 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 possible way of implementing this specification is what is known as the **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.
A review with all those involved in the project is sensible.
In the case of programs that are poorly documented and unstructured, faults occur during subsequent modifications; in particular, there is a danger of unknown dependencies or side effects, as they are often referred to. Good specifications and program documentation are very effective in preventing faults, particularly if the software is developed externally.

Power control elements

The safety function initiated by the protective devices and the logic unit shall stop hazardous machine functions. For this purpose, the actuator elements or work elements are switched off by power control elements

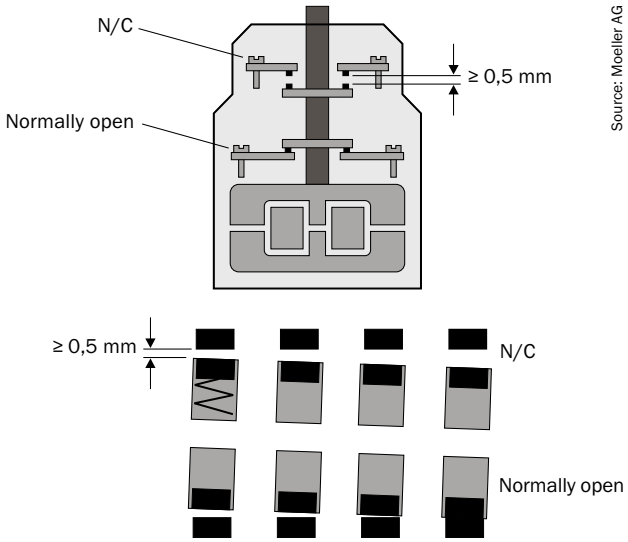
→ Principle of switch off/power shutdown: ISO 13849-2 (B-type standard)

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). 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 any 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.



Source: Moeller AG

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 (➜ 3-42). A simple diode for arc suppression can result in a release (switch to OFF) time up to 14 times longer.

Suppressor (across 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)

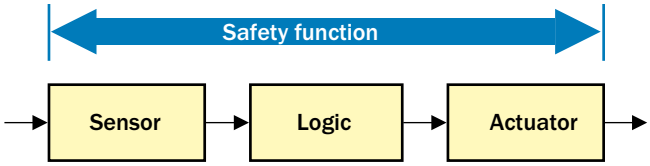
1) The element must be exactly matched to the inductance!

3 c

8007988/2015-07-07
Subject to change without notice

Drive technology

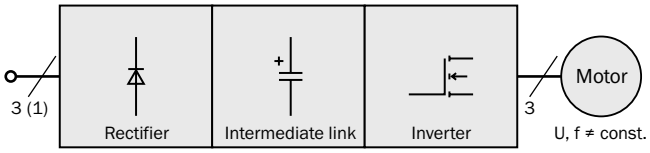
When considering safety functions, drives represent a central sub-function, as they pose a risk of unintentional movement, for example.
The safety function stretches from the sensor to the actuator (see figure).



The actuator can involve several components (contactor, drive controller, feedback), depending on 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.



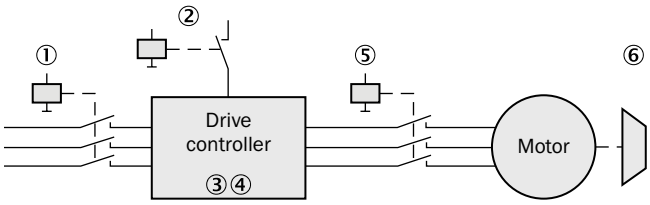
To limit transient overvoltages caused by switching loads in DC and AC circuits, interference suppression components are to be used, in particular if sensitive electronic assemblies are being used in the same control cabinet.

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 screened?
- 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

To implement the safety function, various switch-OFF paths are possible in the actuator subsystem:



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

A safety function can be implemented with a drive controller in various ways:

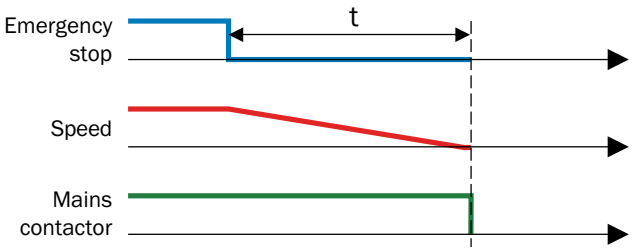
- By means of **disconnection of the supply of power**, e.g., using a mains contactor ① or a motor contactor ⑤.
- By means of **external circuits for monitoring**, e.g., by monitoring an encoder
- By means of **element safety functions integrated directly in the drive controller** (➜ 3-76)

3 c

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.



Speed detection with external monitoring units

To monitor the drive, external monitoring units require signals that provide information about the latest 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 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.

Element safety functions integrated in the drive controller

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 changing (actuator). In this context, safety-related functions integrated in the drive controller are to be considered element safety functions.

They are generally divided into two groups:

- Safe stopping and braking functions: These functions are used to stop the drive safely (e.g., safe stop)
- Safe movement 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. Secondary conditions include parameters such as the necessary braking distance, the presence of kinetic energy, etc.

The shutdown reaction varies depending on the element safety function chosen. 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.

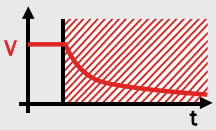
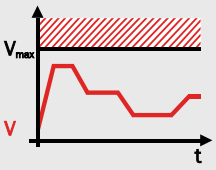
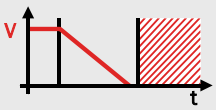
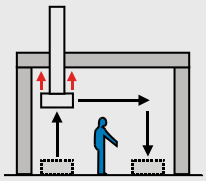
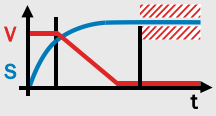
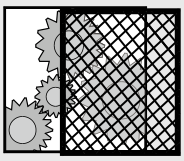
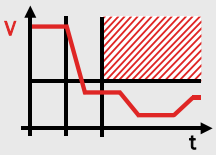
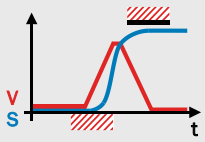
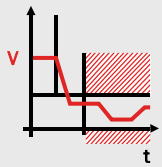
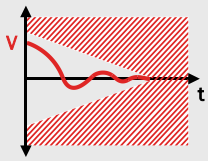
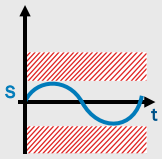
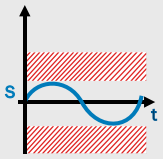
Possible interfaces for the implementation of safety sub-functions integrated directly in the drive are:

- Discrete 24-V signals
- Control communication (channel 1)/24 V discrete (channel 2)
- Safe communication systems (field-bus systems/network interface)

Control communication refers to a standard control system sending a setpoint for rotational speed or position to the drive via a field-bus or network that is not of safe design.

The majority of element safety 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”. Drive controllers 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

	Safe Torque Off (STO) • Corresponds to stop category 0 in accordance with 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 in accordance with 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 in accordance with 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 zone 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 (SMP) [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

Source: Bosch Rexroth AG

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.

→ Functional safety of power drives IEC 61800-5-2 (B-type 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 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, the valves are defined as power control elements. The failure of drives/work elements must also be considered according to the possible repercussions.

8007988/2015-07-07
Subject to change without notice

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)

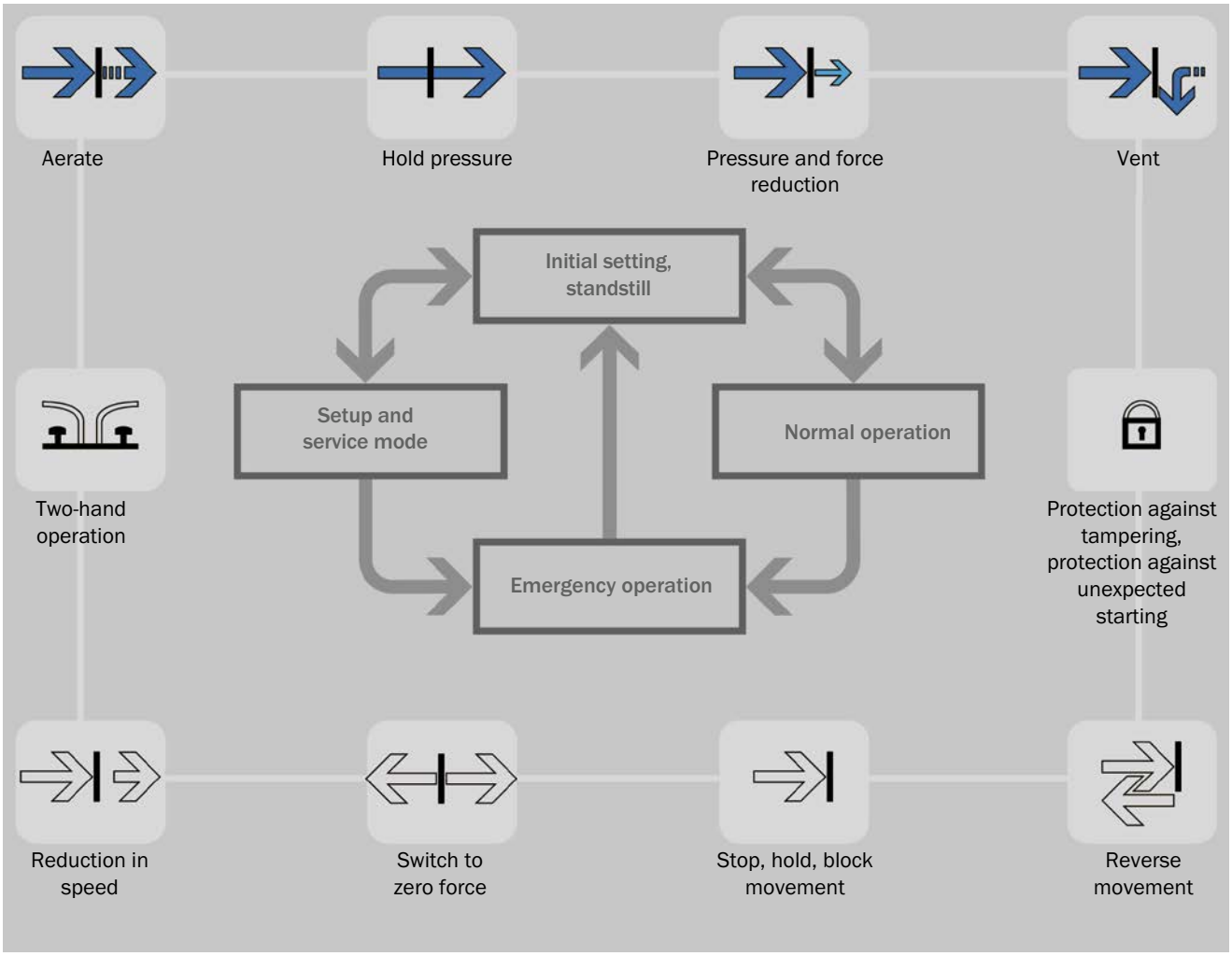
These contaminations must be reduced to an acceptable degree with the aid of filters.

A filter concept refers to the suitable selection of a filter principle for the task required as well as the arrangement of the filter in an appropriate 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.

→ Proven safety principles: ISO 13849-2 (B-type standard)
→ Safety-related requirements on hydraulic/pneumatic systems: ISO 4413, ISO 4414
→ Aging process on hydraulic valves: BIA report 6/2004

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 element safety 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 element safety functions that are purely pneumatic.

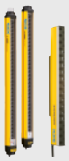
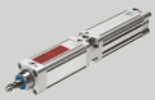
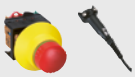
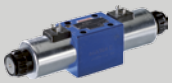
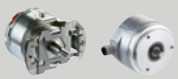


Direct pneumatic effect on movement
Indirect pneumatic effect on movement

Source: Festo AG & Co. KG – Safety Technology Guidelines

8007988/2015-07-07
Subject to change without notice

Product overview: Safety technology for machine safety

Sensors	Logic	Power control elements
Safety light curtains 	 Safety relays	 Electrical drives with element safety sub-functions [1]
Safety camera systems 		
Multiple light beam safety devices 		 Safety pneumatic valves [2]
Single-beam safety devices 		
Safety laser scanners 	 Safety controllers and motion control	 Contactors [3]
Interlocking devices		
With separate actuator 		 Frequency inverters [4]
With actuator for locking devices 		
For switching cam, turning lever 		 Brakes [2]
Magnetically coded 	 Safe sensor cascade	
RFID coded 		 Pneumatic valves [1]
Inductive 		
Emergency stop pushbutton enabling switch 		 Hydraulic valves [1]
Motor feedback systems, encoders 		
Photoelectric switches, magnetic and inductive sensors 		

Service solutions from SICK

With the approval of: 1) Bosch Rexroth AG, 2) FESTO AG & Co. KG, 3) Eaton Industries GmbH, 4) SEW-EURODRIVE GmbH & Co. KG.

→ All SICK products are listed in our online product finder at www.sick.com

3 c

Summary: Designing the safety function

General

- Draft a safety concept. During this process take into account the features of the machine, the features of the surroundings, human aspects, the features of the design, and the features of protective devices.
- Design the safety functions with the required level of safety. Safety functions are formed by the subsystems sensor, logic, and actuator.
- Determine the level of safety for each subsystem from the safety-related parameters structure, reliability, diagnostics, resistance, and 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), guards, movable 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 the correct 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).

8007988/2015-07-07

Step 3d: Design and verification of the safety function

During verification, analyses and/or checks are carried out to demonstrate that all aspects of the safety function meets the objectives and requirements of the specification.

Essentially, verification involves two stages:

- Verification of mechanical execution
- Verification of functional safety

Verification of the mechanical design of the protective device

In the case of mechanical protective devices, the realization shall 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 or radiation. Particular attention should be paid to compliance with ergonomic requirements.

Separating and/or distancing effect

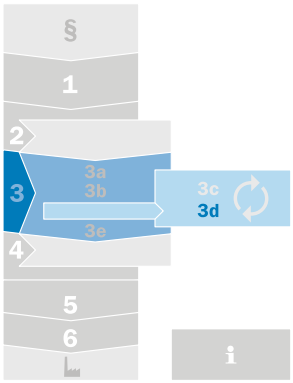
- Sufficient safety distance and dimensioning (reaching over, reaching under, etc.)
- Suitable mesh size or lattice spacing for barriers
- Sufficient rigidity and suitable mounting
- Selection of suitable materials
- Safe setup
- Resistance to aging
- Protective device set up so that climbing on it is not possible

Restraining of ejected parts and/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 lattice spacing for barriers
- Sufficient rigidity and suitable mounting
- Selection of suitable materials
- Safe setup
- Resistance to aging

Ergonomic requirements

- See-through or transparent (so that machine operation can be observed)
- Setup, color, aesthetics
- Handling (weight, actuation, etc.)



3 d

In this chapter ...

The thorough check on the effectiveness of a protective device can be undertaken using a checklist:

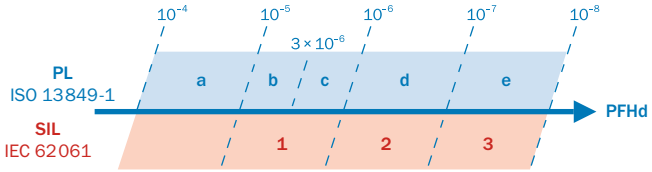
Example: Checklist for the manufacturer or installer when installing protective devices (e.g., an ESPE)			
1.	Have adequate measures been taken to prevent access to the hazard zone or hazardous point and can the hazard zone or hazardous point only be accessed via secured areas (ESPE, protective doors with interlocking device)?	Yes ☐	No ☐
2.	Have appropriate measures been taken to prevent (mechanical protection) or monitor unprotected presence in the hazard zone when protecting a hazard zone or hazardous point and have these been secured or locked to prevent their removal?	Yes ☐	No ☐
3.	Does the protective device conform to the reliability level (PL or SIL) required for the safety function?	Yes ☐	No ☐
4.	Has the maximum stopping and/or stopping/run-down time of the machine been measured and has it been entered and documented (at the machine and/or in the machine documentation)?	Yes ☐	No ☐
5.	Has the protective device been mounted such that the required safety or minimum distance from the nearest hazardous point has been achieved?	Yes ☐	No ☐
6.	Is reaching under, reaching over, climbing under, climbing over, or reaching around the protective device effectively prevented?	Yes ☐	No ☐
7.	Have the 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.	Is the control switch for resetting the protective device or restarting the machine present and correctly installed?	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 protective functions effective at every setting of the operating mode selector switch?	Yes ☐	No ☐
12.	Are the protective devices effective for the entire duration of the dangerous state?	Yes ☐	No ☐
13.	Once initiated, will a dangerous state be stopped when switching the protective devices off or when changing the operating mode, or when switching to another protective device?	Yes ☐	No ☐
14.	Are the notes included with the protective device attached so they are clearly visible for the operator?	Yes ☐	No ☐

8007988/2015-07-07

Verification of functional safety

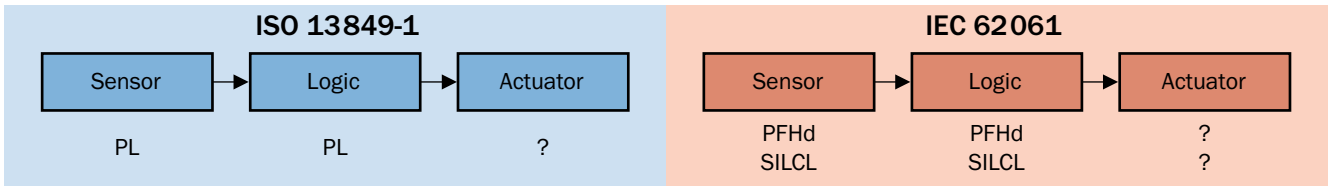
According to the standards for functional safety, the actual safety level shall match the intended safety level. Two different methods are available here:

- Determining the performance level (PL) achieved according to ISO 13849-1
- Determining the safety integrity level achieved (SIL) according to IEC 62061



Both methods can be used to check whether the required level of safety can be achieved. The PFHd value is determined as the corresponding quantitative measure.
In both of the examples that follow (➜ 3-93 and ➜ 3-98), sensor and logic data is available but actuator data is not.

- 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
- PFHd: Probability of a dangerous failure per hour
- SILCL: SIL claim limit (suitability). Discrete level for defining the integrity of the safety function.



3 d

Determining the performance level (PL) achieved as per ISO 13849-1

ISO 13849-1 sets out two methods for determining performance level:

- **Simplified method** (➜ 3-87):
  tabular determination of performance level based on the performance level of each subsystem
- **Detailed method** (➜ 3-88):
  calculation of the performance level based on the PFHd 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 shall also be taken into account.

Subsystems

A safety function that is implemented using control measures generally comprises sensor, logic unit, and actuator. Such a chain can include, on the one hand, discrete elements such as guard interlocking devices or valves and complex safety controllers. As a rule, it is therefore necessary to divide a safety function into subsystems.

In practice, certified subsystems are already used in many cases for certain safety functions. These subsystems can be light curtains, for example, but also safety controllers, for which "precalculated" PL or PFHd values are supplied by the component manufacturer.

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.

➜ More information about validation: ISO 13849-2
➜ Go to: www.dguv.de/bgia/13849 for comprehensive information about ISO 13849-1

8007988/2015-07-07
Subject to change without notice

Simplified method

This method also allows the overall PL for many applications to be estimated with sufficient accuracy without knowing individual PFHd 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 PFHd range of values for the various PL. Therefore, using the detailed method (see next section) may deliver more accurate results.

Procedure

- Calculate the PL of the subsystem or subsystems 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 a PL of "e", the lowest PL (low) is, therefore, "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 a PL of "d", two subsystems achieve a PL of "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".

PL (low) (lowest PL of a subsystem)	n (low) (number of subsystems with this PL)		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

→ If the PL is not known for all subsystems, the safety level can be determined as described in the section titled "Determining the safety level of a subsystem according to ISO 13849-1" below.

Detailed method

An essential – but not exclusive – criterion for determining the PL is the "probability of a dangerous failure per hour" (PFHd) of the safety components. The resulting PFHd value is made up of the sum of the individual PFHd values.

The manufacturer of a safety component may also have applied additional structural restrictions that must also be taken into account in the overall consideration.

➜ If the PFHd value is not known for all subsystems, its safety level can be determined.
See "Determining the level of safety of a subsystem according to ISO 13849-1" below.

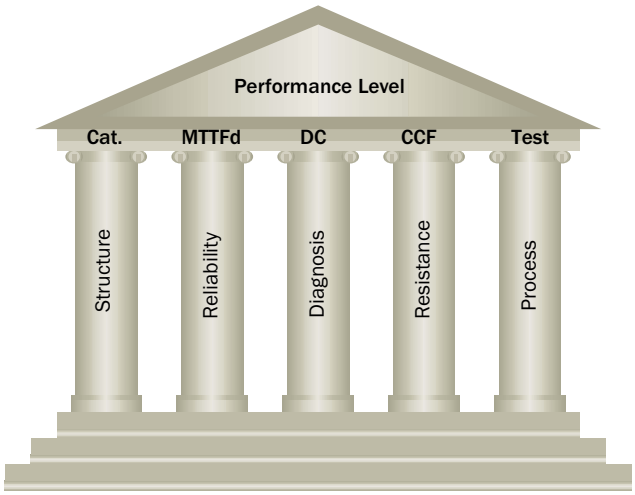
Determining the level of safety for a subsystem as per ISO 13849-1

A safety-related subsystem can be formed from many different individual components which may even be made by different manufacturers. Examples of such components include:

- Input side: 2 safety switches on a physical guard
- Output side: 1 contactor and 1 frequency inverter to stop a dangerous movement

In such cases, the PL for this subsystem 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 (category ➜ 3-89)
- MTTFd values of individual components (➜ 3-90)
- Diagnostic coverage (DC ➜ 3-91)
- Common cause failure (CCF ➜ 3-91)
- Software aspects that are relevant to safety
- Systematic failures



3 d

8007988/2015-07-07
Subject to change without notice

Category of safety-related parts of control systems (ISO 13849-1)

Subsystems are usually single-channel or dual-channel. Unless additional measures are in place, single-channel systems respond to faults with a dangerous failure. Faults 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.

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 a fault can result in the loss of the safety function.	Primarily characterized by component selection
1	The requirements of category B shall be met. Proven components and proven safety principles shall be used.	• The occurrence of a fault 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 proven safety principles used. The safety function must be checked by the machine controller at appropriate intervals (test rate 100 times higher than requirement rate).	• The occurrence of a fault can result in the loss of the safety function between checks. • The loss of the safety function is detected by the check.	Predominantly characterized by the structure
3	The requirements of category B shall be met and proven safety principles used. Safety-related parts shall be designed such that ... • An isolated fault in any of these parts will not lead to the loss of the safety function • Wherever it is reasonably possible, the isolated fault is detected.	• When the isolated fault occurs, the safety function is always retained. • Some, but not all faults are detected. • Accumulation of undetected faults may lead to loss of the safety function.	
4	The requirements of category B shall be met and proven safety principles used. Safety-related parts shall be designed such that: • An isolated fault in any of these parts will not lead to the loss of the safety function **and** • The isolated fault is detected on or before the next request for the safety function **or** • If this is not possible, an accumulation of faults will not lead to the loss of the safety function.	• The safety function is always retained when faults occur. • The faults are detected in a timely manner to prevent the loss of the safety function.	

Mean time to dangerous failure (MTTFd)

MTTF stands for Mean Time To Failure. From the point of view of ISO 13849-1, only dangerous failures need to be considered (hence "d").

This value represents a theoretical parameter expressing the probability of a dangerous failure of a component (not the entire subsystem) within the service life of that component. The actual service life of the subsystem is always shorter.

The MTTF value can be derived from the failure rates. The following rules apply:

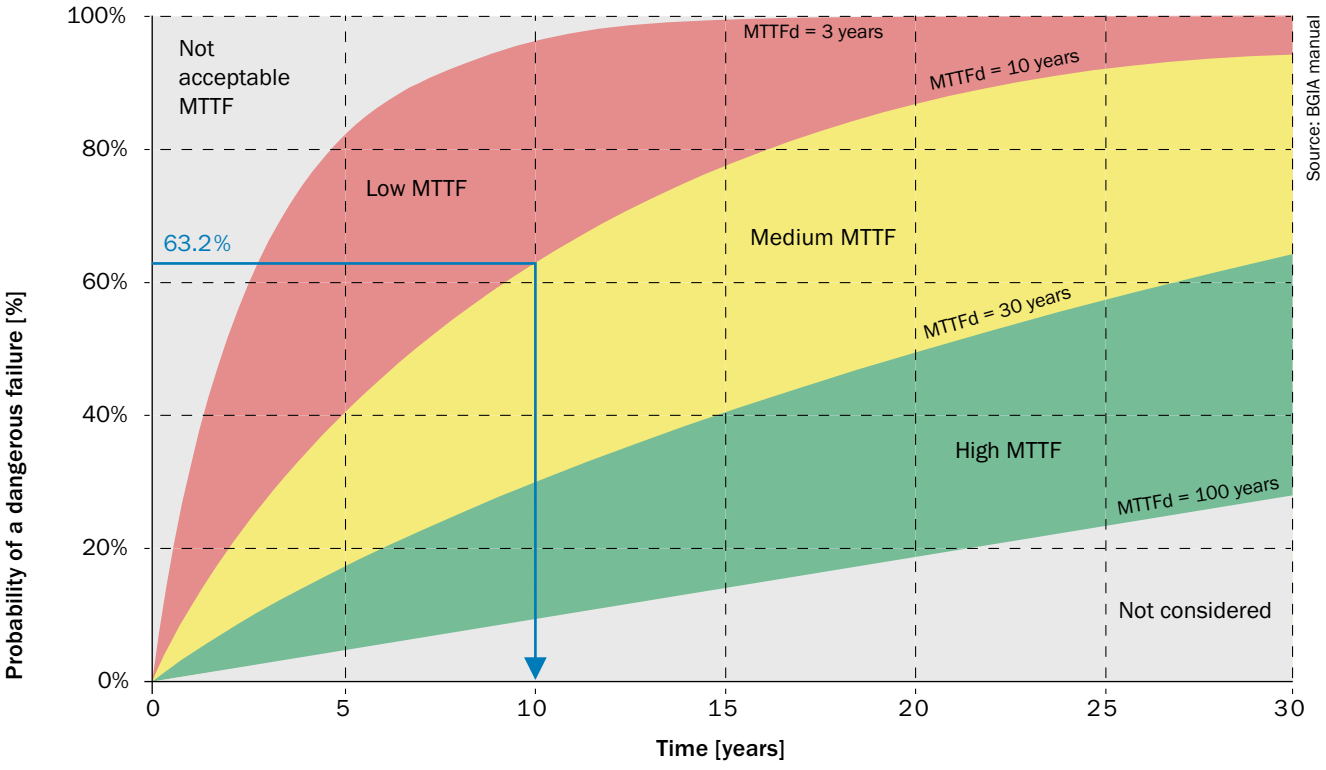
- B_{10} values for electromechanical or pneumatic components. Here, wear and thus the maximum permissible application time are determined by the switching frequency. B_{10} indicates the number of switching cycles until 10% of components fail.
- The B_{10d} value indicates the number of switching cycles until 10% of components fail dangerously. If the B_{10d} value is not available, a blanket $B_{10d} = 2 \times B_{10}$ can be assumed.
- Electronic components: failure rate λ. Failure rates are often expressed as FIT (Failures In Time). One FIT is one failure per 10^9 hours.

ISO 13849-1 combines the MTTFd figures into ranges:

Designation	Range
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd < 100 years

The mean time to a dangerous failure in years (MTTFd) can be calculated for the overall system from the component values. To avoid overrating the impact of reliability, the useful maximum value for the MTTFd has been limited to 100 years.

3 d



8007988/2015-07-07
Subject to change without notice

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 capability to detect dangerous faults. Poor diagnostics only detect a few faults, good diagnostics detect a large number of or even all failures.

Instead of detailed analysis (FMEA), ISO 13849-1 proposes measures and quantifies the DC. Here too, there are a number of different ranges:

Designation	Range
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

Common cause failures – Resistance

External influencing factors (e.g., voltage level, overtemperature) can render identical components unusable regardless of how rarely they fail or how well they are tested. (Even with two eyes it is impossible to continue reading a newspaper if the lights suddenly go out.) These common cause failures are always to be prevented (CCF – common cause failure).

Annex F to ISO 13849-1 offers a simplified method based on a points system to determine whether adequate measures are in place to counter CCF. Each measure applied is given a points score. A score of 65 or higher indicates that adequate CCF measures are in place.

Requirement		Maximum value	Minimum requirement
Separation	Separation of signal circuits, separate routing, isolation, air paths, etc.	15	**Total figure ≥ 65**
Diversity	Different technologies, components, principles of operation, designs	20	
Layout, 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 fault analysis to avoid common cause faults	5	
Competence, training	Training for designers so that they understand and can avoid the causes and consequences of CCF	5	
Effect of the environment	Test the system for susceptibility to EMC	25	
	Test the system for susceptibility to temperature, shock, vibration, etc.	10	

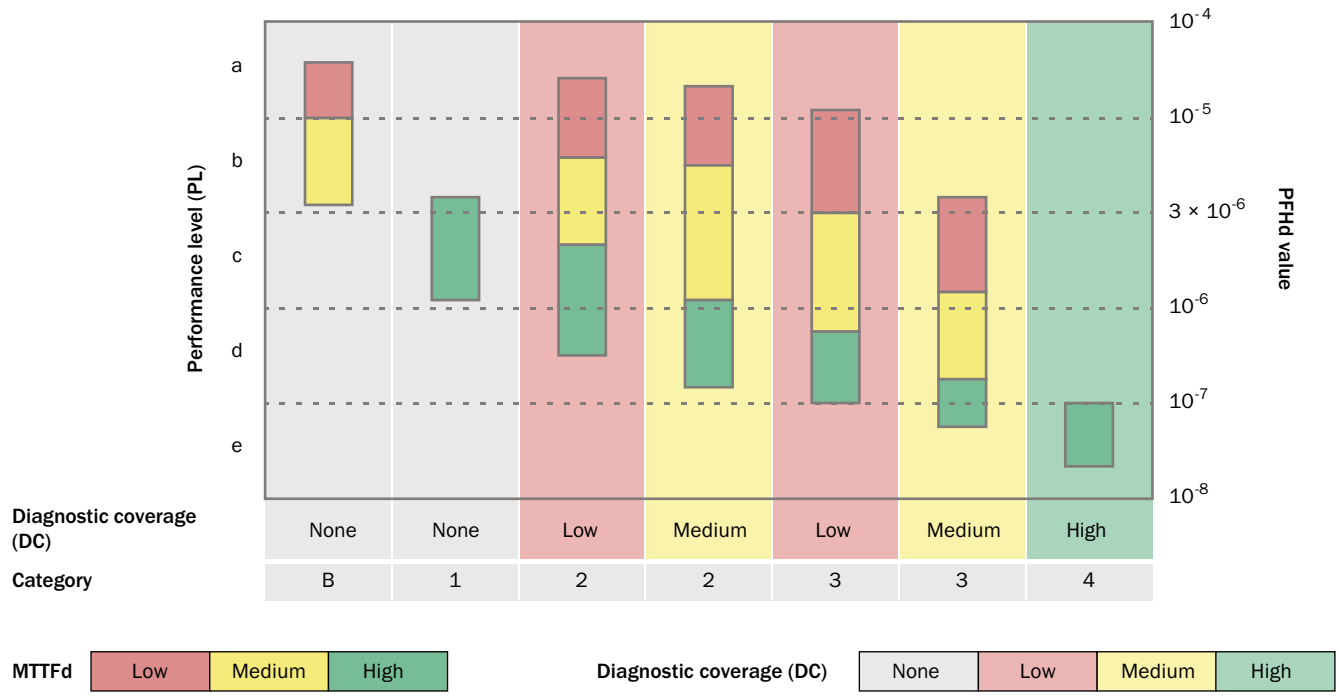
Process

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 (principle of counter-checking by a second person), and that version and change history information is readily available in comprehensive documentation.

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 figure below shows the relationship between the MTTFd value (per channel), the DC, and the category.

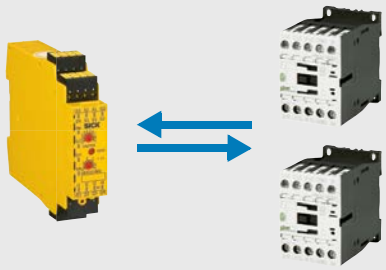


A performance level of "d" can be achieved with a dual-channel control system (category 3), for example. This can be reached either with components of good quality (MTTFd = medium) if almost all faults are detected (DC = medium) or with components of very good quality (MTTFd = high) if many faults are detected (DC = low).

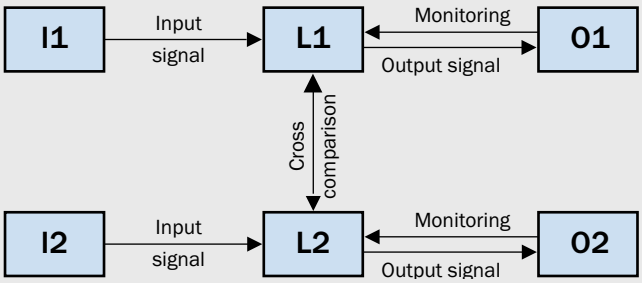
A complex mathematical model which is unnoticed by the user underlies this method. For pragmatic application, the category, MTTFd, and DC parameters are predefined in this model.

Example: Determining the "actuator" subsystem

1) Definition of the "actuator" subsystem
The "actuator" 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 UE logic unit itself is not part of the "actuator" subsystem but is used for diagnostic purposes.



2) Definition of the category
Single-fault safety (with fault detection) makes the equipment **suitable for Category 3 or 4**.
Note: The category is not defined definitively until the DC value has been specified.



3) Determination of the MTTFd per channel
As contactors are subject to wear, the B10d value and the estimated switching frequency (nop) must be used to calculate the MTTFd. The following formula applies:
The figure for the switching frequency comprises operating hours/day [hop], working days/year [dop], and the switching frequency per hour [C]:
General conditions according to the manufacturer:

- B_{10d} = 2,600,000
- C = 1/h (assumed value)
- d_{op} = 220 d/a
- h_{op} = 16 h/d

These general conditions result in an **MTTFd of 7,386 years** per channel, which is interpreted as "high".

$$MTTFd = \frac{B_{10d}}{0,1 \times n_{op}}$$

$$MTTFd = \frac{B_{10d}}{0,1 \times d_{op} \times h_{op} \times C}$$

MTTFd	Range
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd < 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

3 d

Example: Determining the "actuator" subsystem

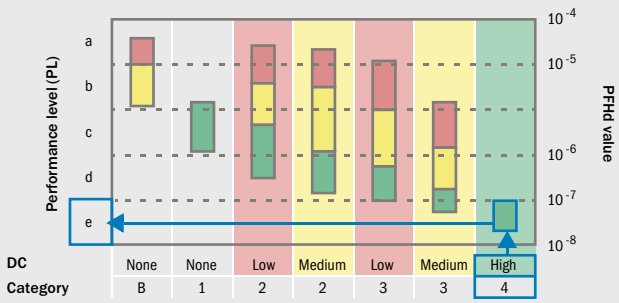
5) Evaluation of the measures to prevent common cause failures
Measures to avoid the common cause effect are implemented in multi-channel systems. An evaluation of the measures gives them **a score of 75**. This meets the minimum requirement.

Requirement	Value	Minimum requirement
Separation	15	Overall value 75 ≥ 65
Diversity	20	
Layout, application, experience	20	
Analysis, evaluation	5	
Competence/training	5	
Effect of the environment	35	
	75	

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

✔

7) Result
From the illustration for the determination of the PL for the subsystem (➜ 3-86) the PL for the subsystem can be determined. In this case, the **PL is "e"**.
The resulting **PFHd figure of 2.47 × 10^{-8}** for this subsystem can be taken from a detailed table in ISO 13849-1. The high DC means that the dual-channel structure meets the requirements of **Category 4**.



➜ 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 performance level (PL) achieved as per ISO 13849-1" on page ➜ 3-86).

Alternative: Determining the safety integrity level achieved (SIL) according to IEC 62061

The safety integrity level (SIL) achieved is determined based on the following criteria:

- The safety integrity of the hardware
  - Structural restrictions (SILCL)
  - The probability of dangerous hardware failures (PFHd)
- The requirements for systematic safety integrity
  - Avoidance of failures
  - Management of systematic faults

Here – similar to ISO 13849-1 – the safety function is initially broken down into function blocks and then transferred to subsystems.

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 SILCL of a subsystem restricts the maximum SIL that can be achieved by the overall system.
- The PFHd of the overall control system from the sum of the individual PFHd does not exceed the values in figure "Verification of functional safety" on page ➜ 3-99.

Example

In the figure above, all subsystems achieve SILCL3. The addition of the PFHd 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 must be taken for systematic safety integrity.

The measures for avoiding systematic hardware faults include:

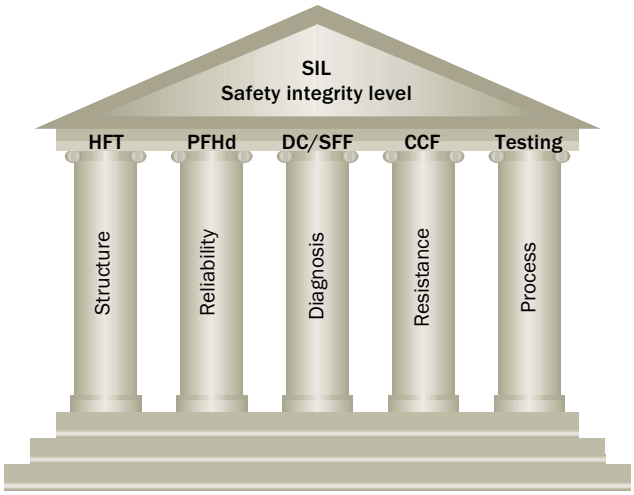
- Layout conforming to the plan for functional
- safety
- Correct selection, combination, arrangement, assembly, and installation of subsystems, including cabling, wiring, and other connections
- Use within the manufacturer's specifications
- Compliance with application instructions provided by the manufacturer (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 management of systematic faults, for example:

- Cutting off the power supply to induce a safe status
- Measures to manage the effects of faults and other effects arising out of a shared data communication process, including transmission faults, 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.



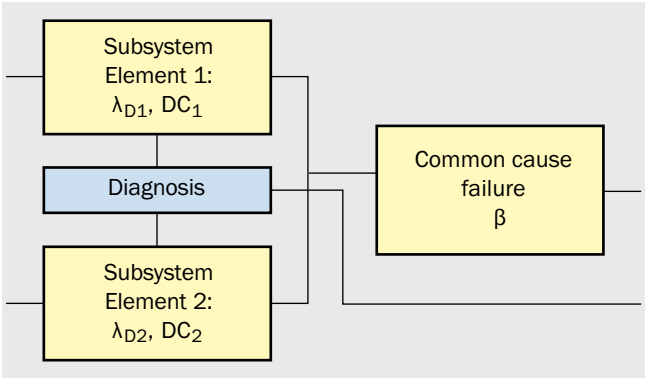
The safety integrity level achieved for a subsystem is made up of the following parameters:

- Hardware fault tolerance (HFT)
- PFHd 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).



The probability of dangerous hardware failures (PFHd)

Alongside structural restrictions, the "probability of dangerous hardware failures" must also be taken into account for each subsystem. Based on a mathematical model, there is a formula to determine the PFHd value for each type of subsystem, whereby the following parameters feature in the calculation:

- Diagnostic coverage
- Mission time
- Diagnostic test interval
- Failure rate of components (λ_D)
- Common cause failure (common cause factor β)

HFT = 1

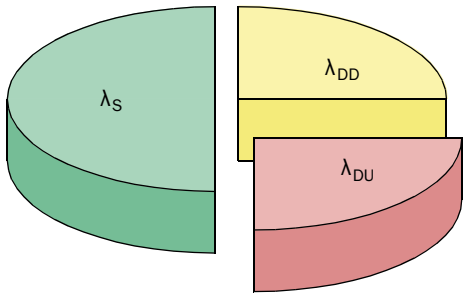
Diagnostics with DC_1 and DC_2

$$PFHd = (1-\beta)^2 \times \left\{ \frac{\lambda_{D1} \times \lambda_{D2} \times (DC_1 + DC_2) \times T_D}{2} + \frac{\lambda_{D1} \times \lambda_{D2} \times (2 - DC_1 - DC_2) \times T_P}{2} + \beta \times \frac{\lambda_{D1} + \lambda_{D2}}{2} \right\}$$

$$PFHd \approx \beta \times \frac{\lambda_{D1} + \lambda_{D2}}{2}$$

Safe failure fraction (DC/SFF)

DC = 50 %
SFF = 75 %



The "safe failure fraction" (SFF) consists of the diagnostic coverage DC (λ_{DD} /λ_{DU}) and the "safe failure" fraction (λ_S).

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D}$$

8007988/2015-07-07

Common cause failure – Resistance

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.

Requirement		Maximum value
Separation	Separation of signal circuits, separate routing, isolation, air paths, etc.	**15**
Diversity	Different technologies, components, principles of operation, designs	**20**
Layout, 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 fault analysis to avoid common cause faults	**5**
Competence, training	Training for designers so that they understand and can avoid the causes and consequences of CCF	**5**
Effect of the environment	Test the system for susceptibility to EMC	**25**
	Test the system for susceptibility to temperature, shock, vibration, etc.	**10**

Value	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 procedures for software development 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), a manufacturer 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, PFHd, 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 (SILCL)

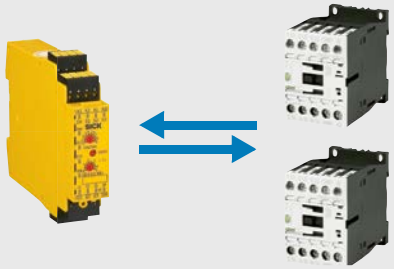
Once the hardware tolerance (architecture) has been specified, the maximum achievable SIL (SIL claim limit) can be determined for the subsystem.

Safe failure fraction (SFF)	Hardware fault tolerance	
	0	1
< 60%	–	SIL1
60 to < 90%	SIL1	SIL2
90 to < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

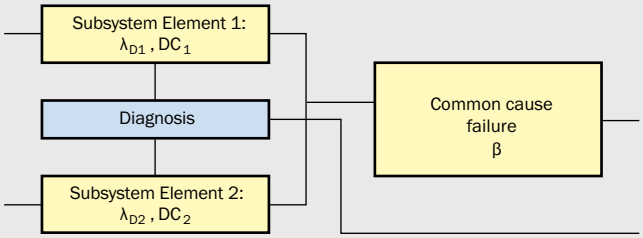
A dual-channel system with HFT1 can claim SILCL3 with an SFF of 90%.

Example: Determining the SILCL and PFHd of the "actuator" subsystem

1) Definition of the “actuator” subsystem
The "actuator" subsystem comprises two contactors with "feedback". As the contactors are positively guided, a safety-relevant failure of the contactors can be detected (EDM).
The logic unit UE410 is itself not part of the “actuator” subsystem, but it is used for diagnostics purposes.



2) Definition of hardware fault tolerance (HFT)
Single-fault safety (with fault detection) results in an HFT of 1.



3) Determining the PFHd
a) Based on the fault rate λD
As contactors are subject to wear, the B10d 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. Therefore, the fault rate λD is determined based on ISO 13849-1. It is assumed that the fault rate remains constant during application.
General conditions according to the manufacturer:

- B10d = 2,600,000
- C = 1/h (assumed value)

These general conditions result in an λD of $3.8 \times 10^{-8}\ \frac{1}{h}$.

b) Based on the CCF factor (β)
Measures to avoid the common cause effect are required in multi-channel systems. The effect is determined based on measures as per the requirements of IEC 62061. In the example, the factor is 5% (see below: "5) Evaluation of measures to avoid common cause faults") PFHd ≈ 1.9 × 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%

$$PFHd \approx \beta \times (\lambda_{D1} + \lambda_{D2}) \times ½$$

$$\approx \beta \times \lambda_D$$

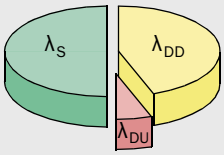
$$\approx 0.05 \times 0.1 \times \frac{C}{B_{10d}}$$

$$PFHd \approx 1.9 \times 10^{-9}$$

Example: Determining the SILCL and PFHd of the "actuator" subsystem

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 faults λD for contactors are detected. Accordingly, the
SFF = 30% + 69.3% = 99.3%.

DC = 99 %
SFF = 99.3 %



5) Evaluation of measures to avoid common cause faults
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%.

Value	CCF factor (β)
≤ 35	10%
36 to 65	5%
66 to 85	2%
86 to 100	1%

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

✔

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 SILCL3.

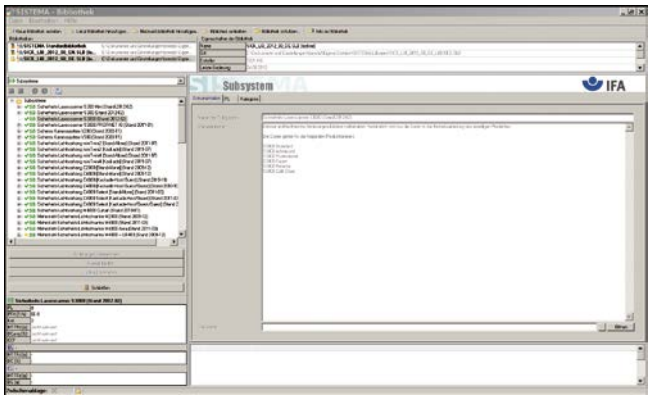
Safe failure fraction (SFF)	Hardware fault tolerance	
	0	1
< 60%	–	SIL1
60 to < 90%	SIL1	SIL2
90 to < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

PFHd ≈ 1.9×10^{-9}

➜ With the resulting SILCL data and the PFHd figure for the subsystem, the SIL achieved for the entire safety function can be determined as described above (see “Safety integrity of the hardware” on page ➜ 3-95).

Useful support

The verification methods described require know-how and experience of the concepts of performance level (PIL) and safety integrity level (SIL). SICK offers associated services (➜ "How SICK supports you" on page ➜ i-1). A suitable software tool can assist you in a systematic approach.
The SISTEMA software assistant, which was developed by IFA and is available free of charge, supports an effective method for calculating performance level. SICK is able to offer a library of certified safety components for this tool.
Furthermore, our seminars can provide you with practical know-how for the tasks you have to deal with on a day-to-day basis.



➜ For further information about SISTEMA, the component library from SICK, and training, please refer to www.sick-safetyplus.com

3 d

Summary: Verification of the safety function

General

- Verify that the intended safety functions conform to the required safety level. To do this, verify mechanical and functional safety.

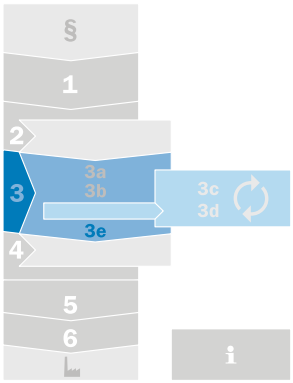
Methods

- Determine the resulting level of safety as per ISO 13849-1 (PL). Available methods:
  - Simplified method (based on PL)
  - Detailed method (based on PFHd values)
- If neither the PL nor the PFHd value is known, determine the safety level of the subsystem from the following parameters: 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.

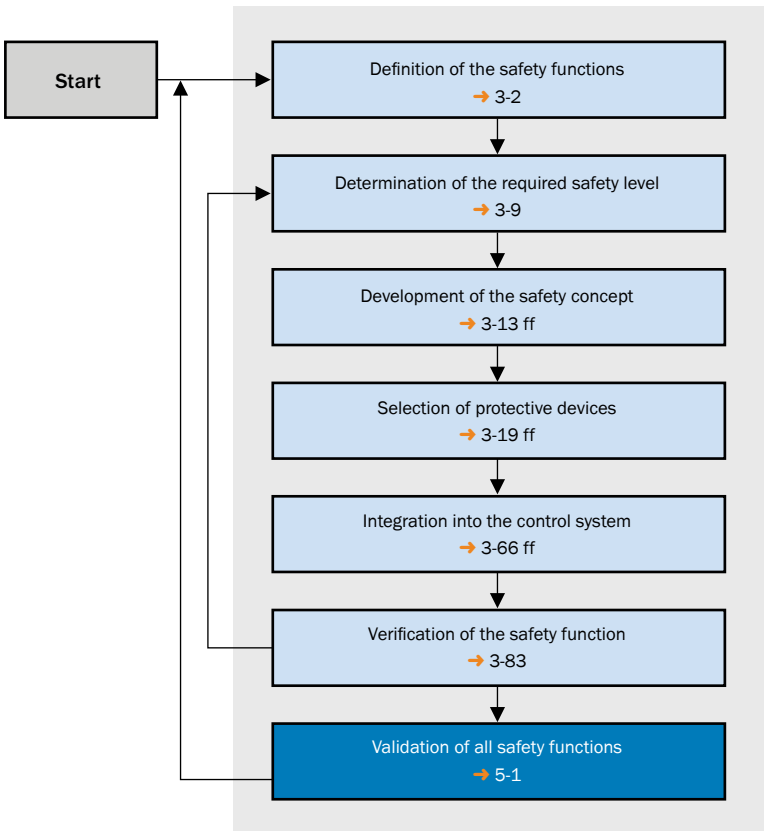
Help

- Use the recommended tools and take advice.

Step 3e: Validation of 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.



3 e

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 faults 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 body-in-white 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 tresspassing this field. The validation process shall uncover such aspects.

A validation process involves a number of procedures being applied which complement each other.
These include:

- 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

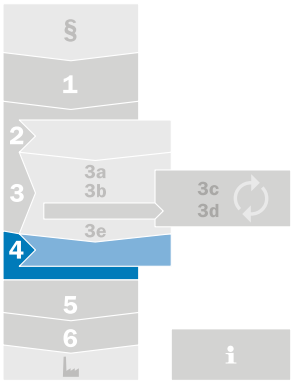
8007988/2015-07-07

Step 4: User information about residual risks

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 informed of the necessity to take further protective measures (in particular to use personal protective equipment).

Information for use about residual risks may include:

- Acoustic and optical warning devices
- Information and warnings on the machine
- Warnings in the instruction handbook
- Operating procedures, training requirements, or briefing of users
- Instructions about the use of personal protective equipment



Information for use shall not be a replacement for other measures!

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

4

Acoustic and optical warning devices

If the operation of a machine is not monitored, warnings must be provided on the machine providing information about 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. The manufacturer has a duty to inform of residual risks that remain.

Information and warnings on the machine

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 official languages are acceptable. 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.

4

Warnings and safety notes in the instruction handbook

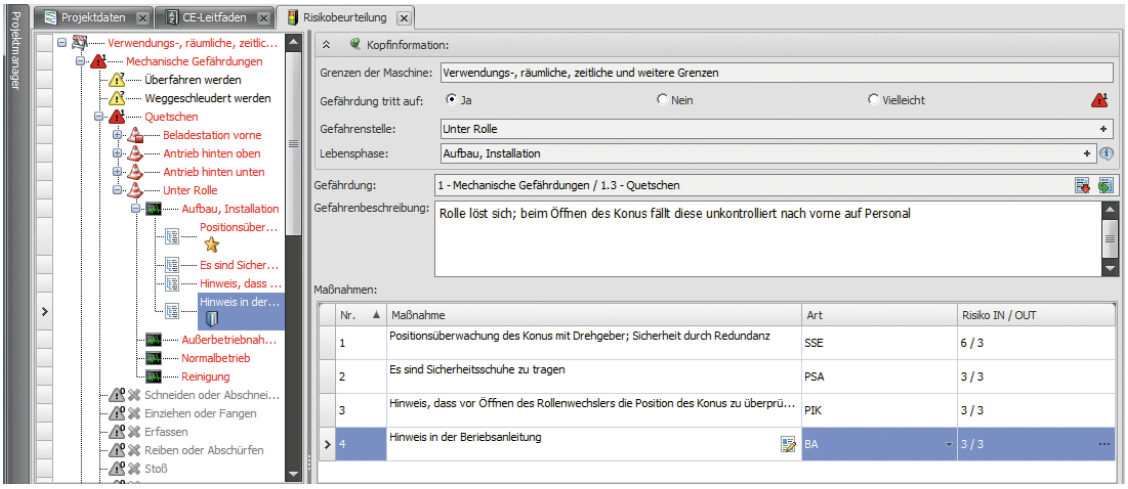
The instruction handbook shall include all safety-relevant information for the machine, in particular:

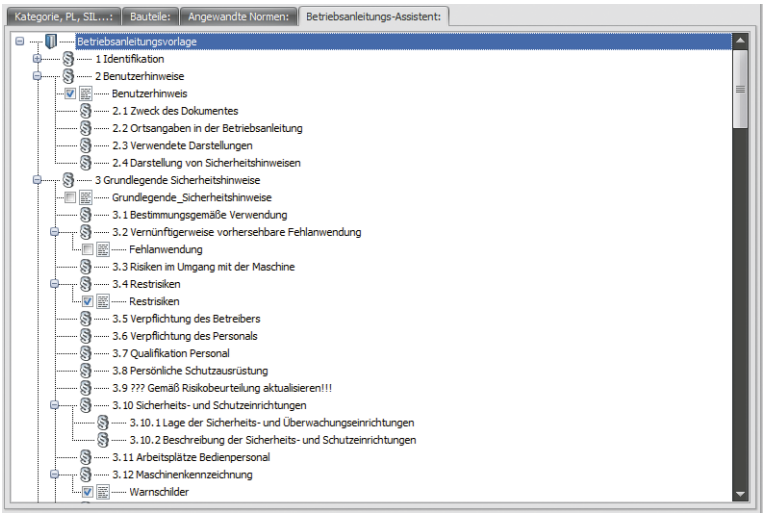
- Warnings relating to possible misuse of the machine that experience has shown might occur
- Notes about commissioning and operation of the machine as well as about required training and/or briefing of operating personnel
- Information about residual risks which remain in spite of measures taken to integrate safety in the design and use of protective devices and supplementary 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 life cycle phases of the machine
- 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

8007988/2015-07-07
Subject to change without notice

Documentation with Safexpert®

The Safexpert® software (➜ page 1-5) provides assistance in meeting requirements with regard to technical documentation. For instance the user can integrate information from the risk assessment directly in the instruction handbook.





Safexpert® operating instructions assistant

4

Summary of Steps 2, 3, and 4: Risk reduction

General

To reduce the risk(s) posed by the hazard analyzed, 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. Inform about residual risks. Define and provide proper information for the user to reduce residual risks.

Technical protective devices

- 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 necessary 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 reached.

8007988/2015-07-07
Subject to change without notice

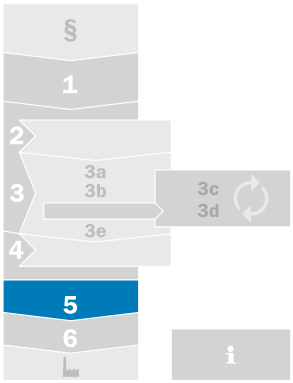
Step 5: Overall validation

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.

In practice, therefore, it may be the case that an individual technical measure does not reduce risk but in the overall context a satisfactory result is achieved. 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?

- Has the 3-step method been applied?
- 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?

During a safety inspection, SICK safety specialists check the entire machine for relevant hazards.

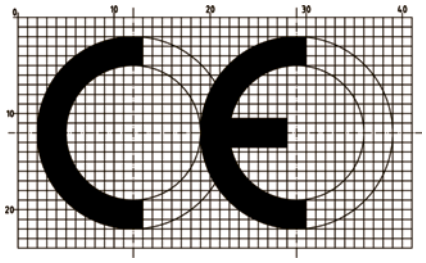


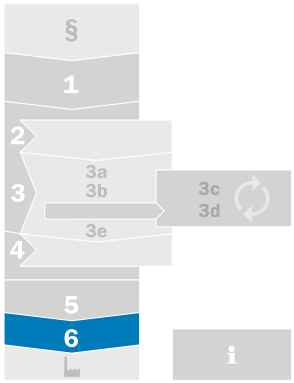
5

8007988/2015-07-07
Subject to change without notice

Step 6: Placing products 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 mark added to the machine. The declaration of conformity shall take into account all European directives applicable to the machine.





Technical documentation

The scope of the technical documentation is described in Annex VII, Section A of the Machinery Directive. For incomplete machines, the specific 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 cover the design, build, and function of the machine.

It shall be drafted in one or more of the official languages of the European Union; the instruction handbook for the machine, to which the specific provisions of Annex I, Number 1.7.4.1 apply, is an exception to this rule.

Custody period and deadlines

The technical documentation must be held ready for the responsible authorities of the member states:

- 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). However, the person designated in the EC declaration of conformity shall be able to make the technical documentation available by a reasonable deadline.

Warning: If technical documentation is not made available to the responsible national authorities further to a reasoned request, this can be sufficient reason to question the ability of the machine concerned to comply with essential health and safety requirements.

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 (➜ 1-1) from which the procedure applied can be derived:
  - List of essential health and safety requirements applicable for 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 EC declaration of conformity
- If applicable, copy of the EC declarations of conformity for the other machines or products incorporated into the machine
- If applicable, declaration of incorporation and mounting instructions for incomplete machines

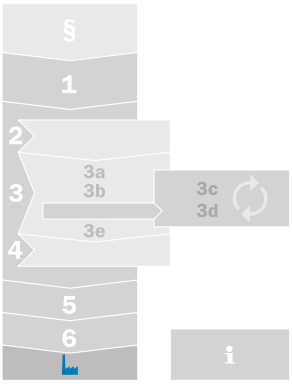
Instruction handbook

An instruction handbook in the official language of the country of use shall be supplied with the machine. This instruction handbook shall be the "original instruction handbook" or a translation of the "original instruction handbook"; in the latter case the original instruction handbook shall also be supplied. For more information, see “Step 4: Information for use on residual risks”, ➜ 4-1.

8007988/2015-07-07
Subject to change without notice

User's responsibilities

The employer is responsible for the safety of the 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 procured?

The acquisition process is a key stage in a project to build or modernize production facilities. The decisions that are made at this stage can determine success of failure.

- 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 the 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 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 regulations and standards or specific regulations can be taken as a starting point when building or modernizing production facilities. These stipulate that the user of the systems concerned shall ensure that operational safety is inspected and formally specified.
In so doing, the operator 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 shall be met:

1. Type of inspection
2. Scope of inspection
3. Depth of inspection
4. Deadlines for inspection
5. Checker's level of qualification

A safety inspection by SICK provides you with a fast overview of the safety status of your machines.
The SICK sales headquarters in Düsseldorf and our Czech subsidiary have already been accredited as inspection centers.
Accreditation by an independent body verifies that SICK is capable of carrying out the activities specified in the accreditation scope with high levels of reliability and with delivery of the required quality.
We discuss potential for improvement with you and work in partnership to realize them.

DAkkS Deutsche Akkreditierungsstelle D-IS-12060-01-01

I 4051

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
   - 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 kept 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.

8007988/2015-07-07

How SICK supports you

The efficient integration of the safety function in a machine or machine concept requires advanced safety expertise. This expertise covers not only skills, topicality, and scope in relation to safety knowledge but also experience in the application of suitable processes. Only a safety partner who is able to combine all of these factors can be considered an expert in safety.

SICK has more than 60 years' experience in machine safety and can provide you with customized services that deliver the expertise that is necessary to implement safety in your machines in compliance with directives.

In so doing, SICK is making a contribution to the ongoing development of the safety culture in your organization with the aim of ...

- 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

You are quite right to expect your partner to meet exacting requirements. A partner must:

- Have many years of experience
- Come up with innovative ideas
- Be international in how it is organized

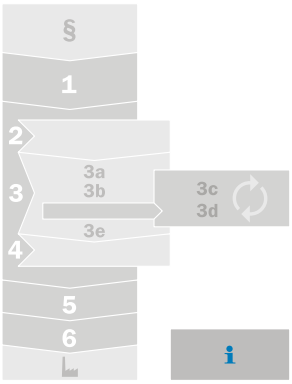
If you consult SICK experts at an early stage ...

- 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.

The SICK process for services for the conformity and design of safe machines and systems

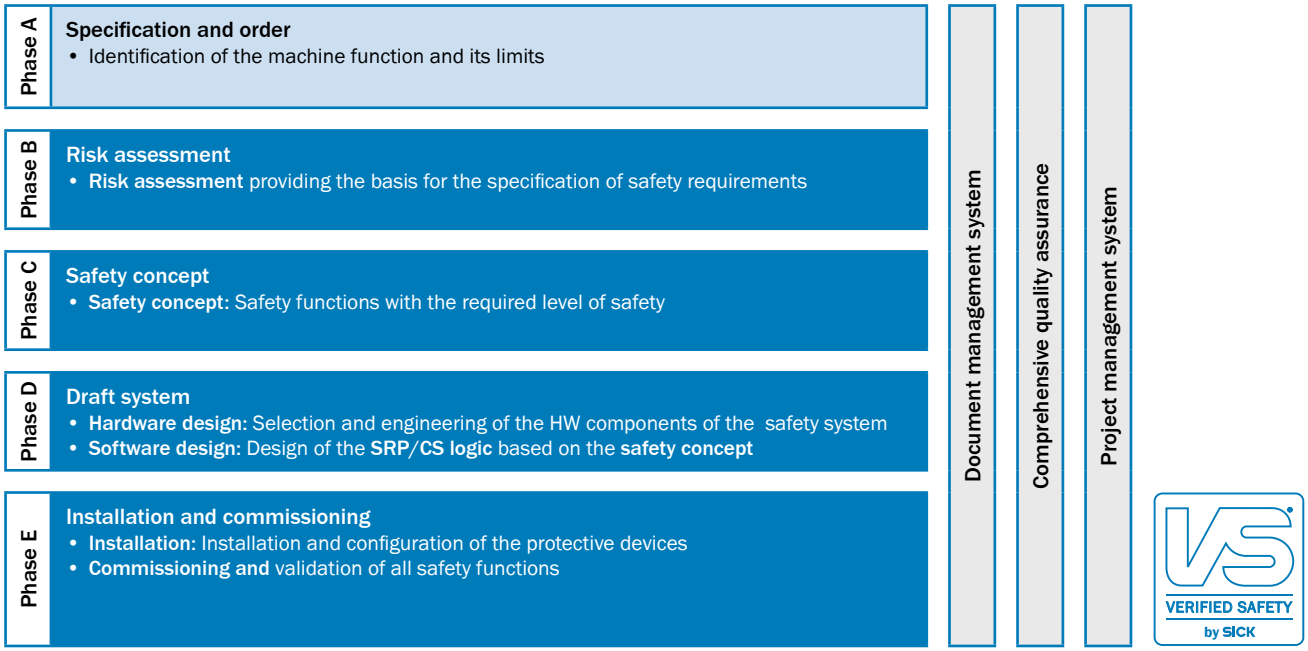
Services from SICK in the area of "consultancy and design for machine safety" are delivered according to the process mapped out below. The service products provided by SICK during each phase are clearly identifiable. They can be purchased from SICK individually or as a comprehensive service solution within the scope of a CE conformity process process.



In this chapter ...

The SICK process for services for the conformity and design of safe machines and systems

Services from SICK in the area of "consultancy and design for machine safety" are delivered according to the process mapped out below. The service products provided by SICK during each phase are clearly identifiable. They can be purchased from SICK individually or as a comprehensive service solution within the scope of a CE conformity process process.



Training seminars and workshops

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. It is for this reason that the focus of our training and workshops lies very much in practical applications.

Customized training provision
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:

- Training
- Workshops
- e-learning
- Modular training concepts
- Update training

Safeguarding advances in knowledge
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 know-how 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

Strengthening application safety
Our training seminars are product-based in order to ensure integration into the intended applications in a way that is both efficient and safe in the long term. Delegates are introduced to the fundamental knowledge they will need for safe and efficient working with the device concerned (analysis and diagnostic options are also covered).
The general structure of our training seminars takes in the various phases of the process to select and integrate a product:

- Selection
  - Safety aspects
  - Product features and possible applications
- Integration
  - Adding to the application (assembly) and wiring
  - Programming
  - Commissioning
- Safe operation
  - Fault diagnosis and rectification

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.

➜ 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 seminars outside Germany, contact your SICK representative or visit us at www.sick.com

If you wish, we can come to you with our seminars and user training workshops. Contact us!

SICK – At your side throughout your system's product life cycle

With certified safety products and services customized to meet your needs, SICK is able to support you throughout the life cycle of your machine, from planning through commissioning and beyond to maintenance and upgrades.

Services from SICK	A safe machine in 6 steps				
	§ Laws, directives, standards	Step 1 Risk assessment	Steps 2 through 4 Risk reduction: The 3-step method	Steps 5 through 6 Overall validation and placing on the market	Responsibility of the operating organization
Consulting and design					
• Risk assessment		✔			
• Safety concept			✔		
• Hardware design			✔		
• Software design			✔		
• Installation			✔		
• Commissioning			✔		
• CE-conformance check				✔	
• Plant walk-through					✔
Verification and optimization					
• Initial inspection				✔	✔
• Periodic inspection					✔
• Machine safety inspection				✔	✔
• Electrical equipment check				✔	✔
• Accident investigation					✔
• Stoptime measurement				✔	✔
Training and advanced learning					
• Seminars	✔	✔	✔	✔	✔
• User training					✔
• WebTraining	✔	✔	✔	✔	✔
Modernization and retrofitting					
• Upgrade kits					✔
Product and system support					
• Commissioning check					✔
• Helpline support					✔
• On-site troubleshooting					✔
• Exchange units					✔
• Spare parts					✔
• Workshop repairs					✔

Components (products)
Using certified products makes it easier for machine manufacturers to prove conformity with the requirements of the Machinery Directive and various standards. As a provider of solutions, SICK offers the machine manufacturer a wide range of products from the simple single-beam photoelectric safety switch through safety light curtains, safety laser scanners, safety camera systems, and safety switches to modular safety controllers with network support and software solutions for the conformity of machinery.

Consultancy: Our knowledge to the advantage of your applications
SICK has subsidiaries or representatives in 87 industrial countries worldwide, where you can access the specialist consultancy and advisory services you need from our technical experts. Our team will support you not only by providing technical knowledge about our products but also with their knowledge of the market and national legislation and standards.

➜ Product overview for safety technology ➜ 3-81
➜ 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 www.sick-safetyplus.com

An overview of the relevant standards

Type	European standard EN	Harmonized	International standard ISO/IEC	Title/Reference
A	EN ISO 12100 replaces the following standards	✔	ISO 12100	Safety of machinery - General principles for design - Risk assessment and risk reduction
	EN ISO 12100-1		ISO 12100-1	Safety of machinery - Basic concepts and general principles for design • Part 1: Basic terminology, methodology
	EN ISO 12100-2		ISO 12100-2	Safety of machinery - Basic concepts, general principles for design • Part 2: Technical principles
	EN ISO 14121-1		ISO 14121-1	Safety of machinery - Risk assessment • Part 1: Principles
B	EN 349	✔	ISO 13854	Minimum gaps to avoid crushing of parts of the human body
	EN 574	✔	ISO 13851	Two-hand control devices - Functional aspects and design principles
	EN 953	✔	ISO 14120	Guards - General requirements for the design and construction of fixed and movable guards (*currently being revised for future publication as EN ISO 14120)*
	EN 1037	✔	ISO 14118	Prevention of unexpected startup
	EN 1088 ISO 14119	✔		Interlocking devices associated with guards - Principles for design and selection
	EN ISO 13849-1	✔	ISO 13849-1	Safety-related parts of control systems • Part 1: General principles for design
	EN ISO 13849-2	✔	ISO 13849-2	• Part 2: Validation
	EN ISO 13850 (replaces EN 418)	✔	ISO 13850	Emergency stop - Principles for design
	EN ISO 13855 (replaces EN 999)	✔	ISO 13855	Positioning of protective devices with respect to the approach speeds of parts of the human body
	EN ISO 13857 (replaces EN 294 and EN 811)	✔	ISO 13857	Safety distances to prevent hazard zones being reached by upper and lower limbs
	EN 60204-1	✔	IEC 60204	Electrical equipment of machines • Part 1: General requirements
	EN 61496-1	✔	IEC 61496-1	Electro-sensitive protective equipment • Part 1: General requirements and tests
	CLC/TS 61496-2	–	IEC 61496-2	• Part 2: Particular requirements for equipment using active optoelectronic protective devices (AOPDs)
	CLC/TS 61496-3	–	IEC 61496-3	• Part 3: Particular requirements for active optoelectronic protective devices responsive to diffuse reflection (AOPDDR)
	CLC/TS 62046	–	IEC/TS 62046	Application of protective equipment to detect the presence of persons
	EN 62061	✔	IEC 62061	Functional safety of safety-related electrical, electronic and programmable electronic control systems

8007988/2015-07-07
Subject to change without notice

Type	European standard EN	Harmonized	International standard ISO/IEC	Title/Reference
C	EN 1114-1	✔	–	Plastics and rubber machines - Extruders and extrusion lines • Part 1: Safety requirements for extruders
	EN 12622	✔	–	Hydraulic press brakes
	EN 13736	✔	–	Pneumatic presses
	EN 1459	✔	–	Safety of machinery – Variable-reach trucks
	EN 1525	–	–	Safety of industrial trucks - Driverless trucks and their systems
	EN 1526	✔	–	Safety of industrial trucks - Additional requirements for automated functions on trucks
	EN 1612-1	✔	–	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
	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	✔	–	Rail dependent storage and retrieval equipment - Safety requirements
	EN 692	✔	–	Mechanical presses
	EN 693	✔	–	Hydraulic presses
	EN 710	✔	–	Safety requirements for foundry molding and coremaking machinery and plant and associated equipment
	EN 869	✔	–	Safety requirements for pressure metal diecasting units
	EN ISO 1010-X	✔*	ISO 1010-X	Printing and paper converting machines (*:Parts -1 to -4 of this standard are harmonized)
	EN ISO 10218-1 (replaces EN 775)	✔	ISO 10218-1	Industrial robots - Safety requirements • Part 1: Robots
	EN ISO 10218-2	✔	ISO 10218-2	• Part 2: Robot systems and integration
	EN ISO 11111-X	✔*	ISO 11111-X	Textile machinery (*: Parts -1 to -7 of this standard are harmonized)

Useful links

Where do I find ...?	
Text of directives (EU)	Full texts from directives can be found on the Internet, for example on the European Union's law portal: ➜ eur-lex.europa.eu
Lists of standards	Official journal of the European Union Federal Institute for Occupational Safety and Health (Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA)): ➜ www.baua.de German Engineering Federation (Verband Deutscher Maschinen- und Anlagenbau (VDMA)): ➜ www.vdma.org European Commission ➜ 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
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 Great Britain (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
Up-to-the-minute information about German Notified Bodies, other EU member states and/or EFTA states and other states with whom the EU has concluded a Mutual Recognition Agreement (MRA) can be obtained from the EU's NANDO information system.	The Federal Institute for Occupational Safety provides a list of certification bodies currently notified by EU member states: ➜ ec.europa.eu/enterprise/newapproach/nando

Where do I find ...?	
National bodies for occupational safety in Germany (structure varies by state)	Baden-Württemberg: ➜ www.gewerbeaufsicht.baden-wuerttemberg.de Bavaria: ➜ www.lgl.bayern.de/arbeitsschutz/index.htm Berlin: ➜ www.berlin.de/lagetsi Brandenburg: ➜ www.arbeitsschutzverwaltung.brandenburg.de Bremen: ➜ www.gewerbeaufsicht.bremen.de Hamburg: ➜ www.hamburg.de/arbeitsschutz Hessen: ➜ www.sozialnetz.de/ca/b/b Mecklenburg-Vorpommern: ➜ www.lagus.mv-regierung.de Lower Saxony: ➜ www.gewerbeaufsicht.niedersachsen.de North Rhine-Westphalia: ➜ www.arbeitsschutz.nrw.de/bp/index.html Rheinland-Pfalz: ➜ www.masgff.rlp.de/arbeit/arbeitsschutz Saarland: ➜ www.lua.saarland.de Saxony: ➜ www.arbeitsschutz.sachsen.de Sachsen-Anhalt: ➜ www.verbraucherschutz.sachsen-anhalt.de/arbeitsschutz Schleswig-Holstein: ➜ www.schleswig-holstein.de/DE/Themen/A/arbeitsschutz Thüringen: ➜ www.thueringen.de/th7/tlv/arbeitsschutz
Austria	Austrian work inspectorate: ➜ www.arbeitsinspektion.gv.at CD-ROM “ArbeitnehmerInnenschutz expert” (in German) ➜ www.a-expert.at
Switzerland	Swiss work inspectorate: ➜ www.seco.admin.ch
List of expert committees within Employers' Liability Insurance Associations (Germany)	Reorganization of expert committees and groups within the German Social Accident Insurance Association (Deutsche Gesetzliche Unfallversicherung, DGUV). DGUV guideline no. 401 "Divisions and specialist fields of the DGUV" lays the foundations for an integrated network of skills and expertise for all aspects of health and safety that is fit to face the challenges of the future. The existing committees are being replaced by the new divisions. ➜ www.dguv.de/de/Pr%c3%a4vention/Fachbereiche-der-DGUV/index.jsp
Addresses of Employers' Liability Insurance Associations (Germany)	➜ www.dguv.de/de/Berufsgenossenschaften-Unfallkassen-Landesverbände
Accident insurers	Germany: German Social Accident Insurance: ➜ www.dguv.de Austria: General accident insurance: ➜ www.auva.at Switzerland: Swiss Accident Insurance Fund: ➜ www.suva.ch

Glossary/Index

Abbreviation/Term		Definition	Index

λ	**Failure rate per hour**	λ: Failure rate per hour, λ_S and λ_D added together
		• λ_S: Safe failure rate
		• λ_D: Dangerous failure rate, can be divided into:
		  • λ_{DD}: Dangerous failure rate for failures detected by diagnostic functions
		  • λ_{DU}: Dangerous failure rate for failures that go undetected
			→ 3-96
			→ 3-98

β factor		Susceptibility to common cause failures (IEC 62061) → CCF	→ 3-97 → 3-98
A			
AOPD	**Active opto-electronic protective device**	Device with a sensor function produced by optoelectronic send and receive elements which detect a break in the optical radiation generated in the device due to the presence of an opaque object in the defined protective field (or in the case of a photoelectric switch: on the axis of the light beam) (CLC/TS 61496-2). In DIN EN 692 “Mechanical presses”, EN 693 “Hydraulic presses”, and EN 12 622 “Hydraulic press brakes” the abbreviation **AOS** is used as a synonym for **AOPD**.	→ 3-30
AOPDDR	**Active opto-electronic protective device responsive to diffuse reflection**	Device with a sensor function produced by optoelectronic send and receive elements which detects the diffuse reflection of optical radiation generated in the device due to the presence of an object in a defined two-dimensional protective field (IEC/TS 61496-3, CLC/TS 61496-3).	→ 3-31
B			
B_{10d}		Number of cycles after which a dangerous failure has occurred on 10% of the components (for pneumatic and electromechanical components, for example).	→ 3-17 → 3-93
BGIA		→ IFA	
C			
Category		Categorization of the safety-related parts of a control system in relation to their resistance to faults and their subsequent behavior in the event of a fault.	→ 3-18 → 3-89
CCF	**Common cause failure**	Failure of various units due to a single event where these failures are not caused by each other.	→ 3-16 → 3-95 → 3-97 → 3-98
CENELEC	**Comité Européen de Normalisation Electrotechnique**	European Committee for Electrotechnical Standardization. Responsible for the harmonization of electrotechnical standards within the European Union and the entire European Economic Area. → www.cenelec.eu	→ §-7
CLC		Prefix for standards adopted by CENELEC.	→ §-7
D			
DC	**Diagnostic coverage**	Measure of the effectiveness of the diagnostics that can be determined as the ratio of the failure rate of detected dangerous failures to the failure rate of all dangerous failures.	→ 3-95 → 3-96 → 3-98
d_{op}		Mean operating time in days per year.	→ 3-93
E			
E/E/PES	**Electrical, electronic and programmable electronic safety-related systems**	Electrical, electronic, and programmable safety-related systems (IEC 62061/EN 62061)	
EDM	**External device monitoring**	Means by which the electro-sensitive protective equipment (ESPE) monitors the status of control devices which are external to the ESPE (IEC 61496-1/ EN 61496-1). The use of EDM is not limited to ESPE.	→ 3-73 → 3-93 → 3-98
EFTA	**European Free Trade Association**	An international organization founded by European states.	→ §-7
Element safety functions		The part of a safety function that is provided by a safety-related element (e.g., actuator) for risk reduction.	→ 3-76
EMC	**Electromagnetic compatibility**	→ EMC	
EMC	**Electromagnetic compatibility**	Ability of an item of electrical equipment to work satisfactorily in its electromagnetic environment and at the same time not to excessively interfere with this environment, in which there are other items of equipment.	→ 2-9 → 3-95 → 3-97

8007988/2015-07-07

Abbreviation/Term		Definition	Index
ESPE	**Electro-sensitive protective equipment**	Assembly of devices and/or components working together for protective tripping or presence-sensing purposes and comprising as a minimum (IEC 61 496-1/ EN 61 496-1): • Sensor element • Control and/or monitoring devices • Switching outputs (OSSD) They are used to provide personal protection at machines and systems where there is a risk of physical injury. They cause the machine or system to adopt a safe state before a person can be exposed to a dangerous situation.	→ 3-29 f
F			
FIT	**Failure in time**	Failure rate in 10^{-9} hours → $\lambda = 1 \times 10^{-9}$ 1/h	→ 3-16
FMEA	**Failure mode and effects analysis**	Procedure for analyzing the effects of failures (IEC 812/EN 60812).	→ 3-17
Functional safety		Part of the overall safety related to the machine and the machine control system that depends on the correct function of the → SRECS, the safety-related systems in other technologies, and the external equipment for risk reduction.	→ 3-1 → 3-85
H			
HFT[n]	**Hardware fault tolerance**	Ability to continue to perform a required function in the presence of faults or failures (IEC 62061/EN 62061).	→ 3-96
h_{op}	**Operating hours**	Mean operating time in hours per day.	→ 3-93
I			
IFA	**Institut für Arbeitsschutz**	Institute for Occupational Safety and Health of the German Social Accident Insurance Association. Until 2009: BGIA.	→ §-12
Interlocking		An interlocking device is a mechanical, electrical, or other device the purpose of which is to prevent the operation of a machine element under certain circumstances.	→ 3-21 ff
L			
Lambda λ		→ λ	→ 3-96 → 3-98
Light curtain		An AOPD with a resolution of ≤ 116 mm.	→ 3-29 f → 3-47
M			
Minimum distance		Calculated distance between the protective device and the hazard zone necessary to prevent a person or part of a person reaching into the hazard zone before the termination of the dangerous machine function.	→ 3-47 ff
MTTFd	**Mean time to failure**	Expected value for the mean time to dangerous failure (ISO 13849-1/EN ISO 13849-1).	→ 3-90
Muting		Muting function. Temporary automatic muting of one or more safety functions by safety-related parts of the control system (IEC 61496-1/EN 61496-1).	→ 3-38
N			
N/C	**Normally closed**	Normally closed	→ 3-21
N/O	**Normally open**	Normally open	→ 3-45 → 3-73
n_{op}	**Number of operations per year**	Text from EN ISO 13849-1: Mean number of operations per year (ISO 13849-1/ EN ISO 13849-1) $n_{op} = \frac{d_{op} \times h_{op} \times 3600 \frac{s}{h}}{t_{cycle}}$ d_{op} is the mean operating time in days per year h_{op} is the mean operating time in hours per day t_{cycle} is the mean time between the start of two sequential cycles of a part in seconds per cycle	→ 3-93
O			
On-delay time		Time by which the response of the contacts is delayed. Variable on-delay times can be set on switching amplifiers with response delay.	

Abbreviation/Term		Definition	Index
OSSD	**Output signal switching device**	The part of the electro-sensitive protective equipment (ESPE) that is connected to the machine control and that changes to the OFF state when the sensor section is triggered during intended operation.	→ 3-18 → 3-66 f
P			
PDF	**Proximity device with defined behavior under fault conditions**	Proximity device with defined behavior under fault conditions.	
PFHd	**Probability of dangerous failure per hour**	Mean probability of a dangerous failure per hour (1/h).	→ 3-85 → 3-94 → 3-95
PL	**Performance level**	Discrete level used to specify the ability of the safety-related parts of a control system to perform a safety function under foreseeable conditions (ISO 13849-1/ EN ISO 13849-1).	→ 3-86
Placing on the market		According to the German Equipment and Product Safety Act: Placing on the market for the first time	→ 6-1
Positive opening		Positive opening on switches signifies that there must be positive transmission of force between actuator and switching element. The actuating mechanism must be designed so that even in the event of mechanical failure (a spring fracturing or contact welding, for example) the contacts open reliably and remain open in the actuated state (IEC 60947-5-1/EN 60947-5-1).	→ 3-24
Presence detection		Secondary protective device for machines and/or systems that can be accessed from the floor and on which the system must be prevented from starting while the operator is inside (safety function: preventing start).	→ 3-50 ff
Protective field		The area in which the test object specified by the manufacturer is detected by the electro-sensitive protective equipment (ESPE). • Safety light curtain: The protective field lies between the sender unit and the receiver unit. It is defined by the protective field height and the protective field width. • Safety laser scanner: The protective field secures the hazard zone on a machine or vehicle. The field is defined by the scanning range, scanning angle, response time, and resolution of the device used (see technical specifications).	→ 3-47
R			
Reset		Resetting the protective device to the monitored status. • Manual reset is provided by a separate device to be operated manually, e.g., using a reset button. • Automatic reset by the protective device is only permitted in exceptional cases: It must not be possible for persons to be in the hazard zone without the protective device triggering or it must be ensured there are no persons in the hazard zone during and after reset.	→ 3-46 → 3-65
Resolution/Sensor detection capability		The limit for the sensor parameter that causes the electro-sensitive protective equipment (ESPE) to respond. It is defined by the manufacturer.	→ 3-31
Response time		The maximum time between the occurrence of an event which activates the sensor unit and the switching outputs (OSSDs) being switched to the OFF state.	→ 3-47
Restart		Putting the machine back into operation. After the triggering of the protective function or after a fault, the protective device can be reset to make it possible to subsequently restart the machine.	→ 3-4 f → 3-55 → 3-75
Restart interlock		Means of preventing automatic restarting of a machine following triggering of the safety function during a dangerous part of the machine operating cycle. after a change in the operating mode of the machine or and after a change to the device used to control starting of the machine (IEC 61496-1/EN 61496-1). • Operating modes include: inching, single stroke, automatic • Startup control devices include: foot switch, two-hand control device, single-break PSDI triggering or double-break PSDI triggering by the ESPE's sensor function • Restart interlock (RES): The machine stops and the restart interlock (RES) is engaged on interruption of at least one light beam. This interlock ensures that the machine can only be restarted if the light path is clear and the reset button has been pressed and released again.	
S			
Safety function		Function of a machine whose failure can result in an immediate increase of the risk(s) (ISO 12100). A safety function is provided by safety-related parts of control systems (SRP/CS).	→ 3-2
Sensor detection capability/Resolution		The limit for the sensor parameter that causes the electro-sensitive protective equipment (→ ESPE) to respond. It is defined by the manufacturer.	→ 3-32

Abbreviation/Term		Definition	Index
SFF	**Safe failure fraction**	Safe failures as a fraction of the overall failure rate of a subsystem that does not result in a dangerous failure (IEC 62 061/EN 62 061).	→ 3-96
SIL	**Safety integrity level**	Discrete level (one out of a possible three) for specifying the safety integrity of the safety functions assigned to the safety-related system, where safety integrity level 3 has the highest level of safety integrity and safety integrity level 1 has the lowest (IEC 62061/EN 62061).	→ 3-96
SILCL	**SIL claim limit**	Safety integrity level claim limit (for a subsystem): Maximum SIL that can be claimed for an → SRECS subsystem in relation to architectural constraints and systematic safety integrity (IEC 62061/EN 62061).	→ 3-85 → 3-97 → 3-99
Single-break/double-break PSDI mode:		This operating mode is advantageous if parts must be inserted or removed by hand periodically. In this mode, the machine cycle is automatically re-initiated after the protective field becomes clear again following single or double break. The reset device must be activated under the following conditions: • When the machine starts • On restart if the → AOPD is interrupted within a dangerous • movement • To initiate a restart after more than 30 s has elapsed (see IEC 61496-1/ EN 61496-1) → More information: EN 692 However, it is necessary to check that no hazard to the operator can arise during the work process. This limits use to small machines where the hazard zone cannot be accessed and presence detection is in place. Suitable measures must also be taken to secure all other sides of the machine. If this operating mode is activated, the resolution of the AOPD must be less than or equal to 30 mm (see ISO 13855 and EN 692, EN 693). As a general rule, when assembling protective devices, the following faults must be excluded: reaching over, reaching under, reaching around, standing behind.	→ 3-41
SRECS	**Safety-related electrical control system**	Electrical control system for a machine the failure of which will result in an immediate increase in the risk or risks.	
SRP/CS	**Safety-related part(s) of control system**	Part of a control system that responds to safety-related input signals and generates safety-related output signals (ISO 13849-1/EN ISO 13849-1).	→ 3-85
T			
Test rod		An opaque cylindrical element used to verify the detection capability of the active optoelectronic protective device (AOPD) (IEC/TS 61496-2, CLC/TS 61496-2)	
T_{10d}		Limit for the operating time of a component. Mean time until a dangerous failure has occurred on 10% of the components. $T_{10d} = \frac{B_{10d}}{n_{op}}$ The MTTFd determined for components subject to wear only applies for this time.	
V			
VBPD	**Visual based protection device**	Protective devices based on image evaluation, e.g., safety camera systems.	

Co-authors – Acknowledgment

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 AG & Co. KG
- Pablo Ruiz, Festo AG & Co. KG
- SEW-EURODRIVE GmbH & Co KG

8007988/2015-07-07 · 2M/MK · Pre USmod en44

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

SICK
Sensor Intelligence.