



GUIDELINES FOR SAFE MACHINERY

Six Steps to Machine Safety

SICK
Sensor Intelligence.

Six steps to a safe machine

§	Laws, directives, standards, liability	→ §-1		
	<ul style="list-style-type: none"> • Regulatory requirements → §-1 • European directives → §-4 • Obligations of the machine manufacturer → §-5 • Standards → §-9 • International/European standards → §-11 • Nationally recognized testing labs → §-14 • Test bodies, insurance providers, and authorities → §-15 			
1	Risk assessment	→ 1-1		
	<ul style="list-style-type: none"> • The risk assessment process → 1-1 • Functions of the machine → 1-3 • Identification of tasks and hazards → 1-4 • Risk estimation and risk evaluation → 1-5 • Documentation → 1-6 			
	2	Safe design	→ 2-3	
		<ul style="list-style-type: none"> • Mechanical design → 2-3 • Operating and maintenance concept → 2-4 • Electrical installation → 2-5 • Enclosure ratings → 2-8 • Lock-out/tag-out → 2-10 • Stop functions → 2-11 • Electromagnetic compatibility (EMC) → 2-12 • Fluid technology → 2-14 • Use in potentially explosive atmospheres → 2-15 		
		3	Technical protective measures	→ 3-1
			<ul style="list-style-type: none"> a Definition of the safety functions → 3-2 b Determination of the required safety level → 3-9 	
Implementation of the safety functions				
<ul style="list-style-type: none"> e Validation of all safety functions → 3-95 				
c			Design of the safety function	→ 3-13
		<ul style="list-style-type: none"> • Development of the safety concept → 3-13 • Selection of the protective devices → 3-18 • Positioning and dimensioning of protective devices → 3-44 • Integration of protective devices into the control system → 3-65 • Product overview for safeguarding → 3-76 		
	d Verification of the safety function	→ 3-79		
4	Administrative measures / information about residual risks	→ 4-1		
5	Overall validation of the machine	→ 5-1		
6	Deployment of machinery	→ 6-1		
	<ul style="list-style-type: none"> • Technical documentation → 6-3 			
i	Annex			
	<ul style="list-style-type: none"> • How SICK supports you → i-1 • Overview of relevant standards → i-6 • Useful links → i-12 • Glossary/Index → i-14 • Space for your own notes → i-18 			





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 supplier and user should 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 supplier and user shall define, select, and apply suitable engineering controls. If the remaining risk is not acceptable, administrative controls such as organizational procedures should be implemented. Information on the residual risks should also be provided.
- 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 previous page.

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 people against accidents taking into account the applicable laws, regulations, directives, and standards. The examples and statements given are the result of our many years of practical experience and are to be considered generic, not specific, applications.

This guide describes the legal requirements relating to machinery in North America and their implementation. The safety requirements relating to machinery in other regions (e.g., Europe, 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. Review of this guide is not a substitute for your own, independent, legal analysis.

We refer only to the latest published regulations and standards 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.

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

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.)

LEGAL DISCLAIMER

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, SICK, REGARDLESS OF THE CAUSE OF ACTION, SHALL HAVE NO LIABILITY OF ANY KIND ARISING OR RELATED TO THIS SAFETY GUIDE, OR THE CONTENTS FOR INJURY, DEATH, DAMAGE TO PROPERTY, LOSS OF USE, LOSS OF OPPORTUNITY, LOSS OF PROFITS, INCREASED COSTS, OR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL OR PUNITIVE DAMAGES. THE SAFETY GUIDE IS MADE AVAILABLE TO YOU "AS IS." TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, SICK DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. SICK DOES NOT WARRANT ANY COMPLETENESS OF CONTENT, ACCURACY, OR VERIFICATION OF THE CONTENTS, NOR ANY IMPLIED WARRANTIES OF USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE WITH RESPECT TO THIS SAFETY GUIDE.

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 – using modern methods, the opposite is actually possible.
- Higher levels of safety result in increased motivation and satisfaction and, as a result, higher productivity.

Safety is a management task

It is very important that the needs of operators, maintenance personnel and others 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.

Involvement of the employees results in acceptance

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, most accidents are due to human error. To reduce accidents, experts call for a wide-ranging “safety culture” within the organization.

Expert knowledge is required

The safety of machinery depends to a large extent on the correct application of regulations and standards. Such regulations describe general requirements that are specified in more detail by standards. Standards are updated regularly and represent accepted solutions for safety.

directives describe general requirements that are specified in more detail by standards. European standards are also often accepted outside Europe.

In Europe, national legal requirements are harmonized through European directives such as the Machinery Directive. These

Implementing all these requirements in a practical manner requires extensive expert knowledge, application knowledge, and many years of experience.

“Everyone, and that includes you and me, is at some time careless, complacent, overconfident and stubborn. At times, each of us becomes distracted, inattentive, bored and fatigued. We occasionally take chances, we misunderstand, we misinterpret and we misread. These are completely human characteristics. Because we are human and because all of these traits are fundamental and built into each of us, the equipment, machines and systems that we construct for our use have to be made to accommodate us the way we are, and not vice versa.”

**-Al Chapanis,
former Professor of Human Factors Engineering, Johns Hopkins University.**

U.S. regulatory requirements



Worker safety regulations in the United States are enforced through the Occupational Safety and Health Administration (OSHA). The United States Congress, through the Occupational Safety and Health Act, established OSHA on December 29, 1970.

The goal of this act was to ensure safe and healthy working conditions for working men and women by:

- Authorizing enforcement of the requirements developed under the Act
- By assisting and encouraging the States in their efforts to assure safe and healthy working conditions
- By providing for research, information, education and training in the field of occupational safety and health.

Some examples of specific types of machinery regulations are:

- 1910.212 – General requirements for all machines
- 1910.213 – Woodworking machinery requirements
- 1910.216 – Mills and calenders in the rubber and plastics industries
- 1910.217 – Mechanical presses
- 1910.219 – Mechanical power transmission apparatus

Two important clauses from 1910.212 “General requirements for all machines” state:

1910.212(a)(1) Types of guarding. One or more methods of machine guarding shall be provided to protect the operator and other employees in the machine area from hazards such as those created by point of operation, ingoing nip points, rotating parts, flying chips and sparks. Examples of guarding methods are-barrier guards, two-hand tripping devices, electronic safety devices, etc.

This information may be obtained at OSHA's internet web site at:
[→ www.osha.gov/index.html](http://www.osha.gov/index.html)

In addition, Section 18 of the OSHA Act of 1970, OSHA also encourages the States to develop and operate their own job safety and health programs.

OSHA provides contact information and an OSHA profile for each of these State Plans, which may include additional regulations. The following states and territories of the United States have recognized programs:

This information may be obtained at OSHA's internet web site at:
[→ http://osha.gov/dcsp/osp/index.html](http://osha.gov/dcsp/osp/index.html)

The OSHA General Duty Clause states in Section 5a that each employer:

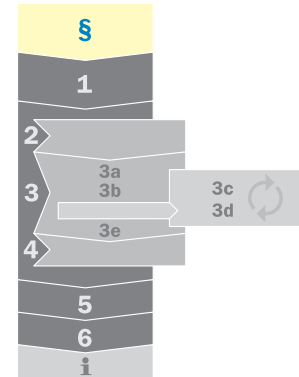
1. Shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;
2. Shall comply with occupational safety and health standards promulgated under this Act.

Occupational and Health Requirements in the United States are defined in Title 29 of the Code of Federal Regulations Part 1910, which is broken down into a number of subparts. Subpart O deals specifically with Machinery and Machine Guarding and defines general requirements for all machines as well as requirements for certain specific types of machinery.

1910.212(a)(3)(ii) The point of operation of machines whose operation exposes an employee to injury, shall be guarded. The guarding device shall be in conformity with any appropriate standards therefore, or, in the absence of applicable specific standards, shall be so designed and constructed as to prevent the operator from having any part of his body in the danger zone during the operating cycle.

• Alaska	• New Mexico
• Arizona	• New York ¹⁾
• California	• North Carolina
• Connecticut ¹⁾	• Oregon
• Hawaii	• Puerto Rico
• Illinois ¹⁾	• South Carolina
• Indiana	• Tennessee
• Iowa	• Utah
• Kentucky	• Vermont
• Maryland	• Virgin Islands ¹⁾
• Michigan	• Virginia
• Minnesota	• Washington
• Nevada	• Wyoming
• New Jersey ¹⁾	

¹⁾ Connecticut, Illinois, New Jersey, New York and Virgin Islands plans cover public sector (State and Local Government) employment only.



The requirements for the safety of machinery as for the use of protective devices are defined by differing legislative stipulations and technical standards in the various countries.

In this chapter ...

U.S. regulatory requirements	§-1
Canada regulatory requirements . . .	§-2
Mexico regulatory requirements . . .	§-3
Brazil regulatory requirements	§-3
European directives	§-4
The Machinery Directive	§-5
The Work	
Equipment Directive	§-5
Obligations for the machine manufacturer	§-5
Standards	§-15
European standardization	§-12
Nationally recognized testing labs	§-14
Test bodies, insurance providers, and authorities	§-15
Summary	§-16



Canada regulatory requirements



In March of 2004, Federal amendment Bill C-45 was passed into law and became a new section called 217.1 in the criminal code. This law was a recommendation as a result of a Royal commission

of Inquiry into a methane gas explosion in a coal mine in Nova Scotia that killed 26 workers.

217.1 states: Every one who undertakes, or has the authority, to direct how another person does work or performs a task is under a legal duty to take reasonable steps to prevent bodily harm to that person, or any other person, arising from that work or task.

Typically this law is intended to establish the legal duties for all persons directing the work of others. It does not interfere or replace any existing laws or regulations. This law is enforced by the police and the crown. Whereas local Occupation Health and Safety Laws (province dependant) are enforced by Ministries of Labour or Workmens Compensation Boards.

The Canada Labour Code (CLC) governs, among other items, occupational safety and health in federal works, undertakings and businesses including employment on ships, trains and aircraft while in operation, and employment in the oil and gas industry in Canada Lands. More specifically, Part II of the CLC is intended to prevent accidents and injury to health arising out of, linked with or occurring in the course of employment.

Part II of the Canada Labour Code provides an employee with three fundamental rights:

- The right to know
- The right to participate
- The right to refuse

Below is a link to local authorities:

→ <http://www.ccohs.ca/oshanswers/information/govt.html>

Ontario regulations

For example, four separate safety regulations (Regulation for Industrial Establishments, Construction Sites, Mines, and Health Care Facilities) have been defined in the Province of Ontario. Canada expects that employers, supervisors, owners and constructors, among others, have an obligation to know and comply with the regulations that have been passed under the Act.

Section 7 of the Regulation for Industrial Establishments defines a process for Pre-Start Health and Safety Reviews. The intent of this section is to ensure that a timely professional review identifies and either removes or controls specific hazards, before a machine or process is started up.

The requirements for a Pre-Start Health and Safety Review are triggered when applicable sections of the Regulation for Industrial Establishments and Sections 24, 25, 26, 28, 31 or 32 also apply.

Please consult the following links:

→ Prestart Health and Safety Reviews: http://www.labour.gov.on.ca/english/hs/pdf/gl_psr.pdf

→ Occupational Health and Safety Act: <http://www.labour.gov.on.ca/english/hs/pubs/ohsa/index.php>

Purpose of Part II of the Canada Labour Code:

Under subsection 122.1, the purpose of the Canada Labour Code, Part II is to prevent accidents and injury to health arising out of, linked with or occurring in the course of employment to which this Part applies. Under subsection 122.2, preventive measures should consist first of the elimination of hazards, then the reduction of hazards and finally, the provision of personal protective equipment, clothing, devices or materials, all with the goal of ensuring the health and safety of employees.

The Occupational Health and Safety Act provides a means of power for each Province to make regulations, set general principles and duties for workplace parties. Worker safety regulations in Canada are enforced by the province in which the machine is located. In Ontario, regulations are enforced by the Ministry of Labour. If the machine is located outside of the Province of Ontario, please check to ensure that National, Provincial and Local regulations have been satisfied.

In addition to these requirements, other Acts beyond the Occupational Health and Safety Act may also apply and may vary based on which Canadian Province the machine is located. The following examples are based on both Federal Government and the Province of Ontario.

- The Building Code Act and Ontario Building Code (as amended)
- The Fire Marshals Act and Ontario Fire Code (as amended)
- The Electricity Act and Ontario Electrical Safety Code (as amended)
- Canadian Electrical Code
- National Building Code (NBC)
- National Fire Code (NFC)

In this case, any of the following are used as protective elements in connection with a machine or apparatus:

- Safeguarding devices that signal the machine to stop, including but not limited to, safety light curtains and screens, area scanning safeguarding systems, radio frequency systems, two-hand control systems, two-hand tripping systems, and single or multiple beam systems;
- Barrier guards that use interlocking mechanical or electrical safeguarding devices.

Additional provisions outside the scope of this guideline may also trigger a Pre-Start Health and Safety Review.

Many workplaces that regularly employ 20 or more workers are required to establish Joint Health and Safety Committees. These committees meet regularly to discuss health and safety concerns, review progress and make recommendations. Joint Health and Safety Committees are an advisory group comprised of both worker and management representatives.

Mexico regulatory requirements



The main regulation of Health and Safety in Mexico is covered in “The Federal Regulation for Occupational Health, Safety and environment,” or RFSHMAT (El Reglamento Federal de Seguridad, Higiene y Medio Ambiente de Trabajo).

It specifies the training of employees, Health and Safety Documentation that is required in the workplace, and a description and format for the necessary preventive measures to ensure a safe work place. The regulation (DOF 21.10.1997) states in:

- Article 35 that Machines shall comply with the related standards
- Article 36 that machines, movable parts and safeguarding equipment shall be inspected regularly, maintained and repaired properly

A Mexican Health and Safety Program is based on the outline of this Regulation.

The federal agency responsible for labor issues in Mexico is the Secretary of Labor and Social Welfare, or STPS (Secretaría del Trabajo y Previsión Social). It issues and performs Health and Safety audits on this regulation.

The Official Mexican Norms (NOM) are the specific work place rules issued to ensure compliance with Mexican labor laws and regulations. NOMs do not have to be approved by the legislature, but Federal government agencies (like STPS) have the jurisdictional authority to develop and issue NOMs. The NOMs detail each one of the sections of the regulation, such as noise, fire prevention, vibrations, etc. The NOMs are similar to OSHA regulations.

NOM-004-STPS is the official Mexican standard that defines the requirements of protection systems and safety devices for machinery and equipment used in the workplace.

Brazil regulatory requirements



The regulatory standards which address safety and occupational health in Brazil, known as NRs (“Normas Regulamentadoras”), are mandatory for public and private companies, public institutions of direct and indirect administration, as well as government organizations having employees under the Labor Laws Consolidation – CLT (“Consolidação das Leis do Trabalho”), a set of laws that includes the NRs. The main NR regulation addressing safety of machinery is the NR 12, which was revised in 2010.

In addition to the NRs, there are additional laws addressing safety of the workplace, including Law No. 6.514, which dates from 1977 and belongs to the Decree-Law (“Decreto-Lei”) No. 5452 from 1943. This law declares that machinery and equip-

ment shall be provided with devices for starting and stopping and others that may be necessary for the prevention of labor accidents, especially regarding the risk of accidental activation. This regulation also states that it is prohibited to manufacture, import, sell, lease and use machinery and equipment that do not meet the provisions of this article. Furthermore, NR 3 declares that emergency embargo or ban measures must be applied upon discovery of work places where there is serious and imminent risk to the worker, and equipment cannot be returned to work until the safety measures indicated by NR 12 and other applicable standards have been fulfilled.

Below is a link to local authorities (Portuguese only):

→ <http://portal.mte.gov.br/legislacao/normas-regulamentadoras-1.htm>



European directives

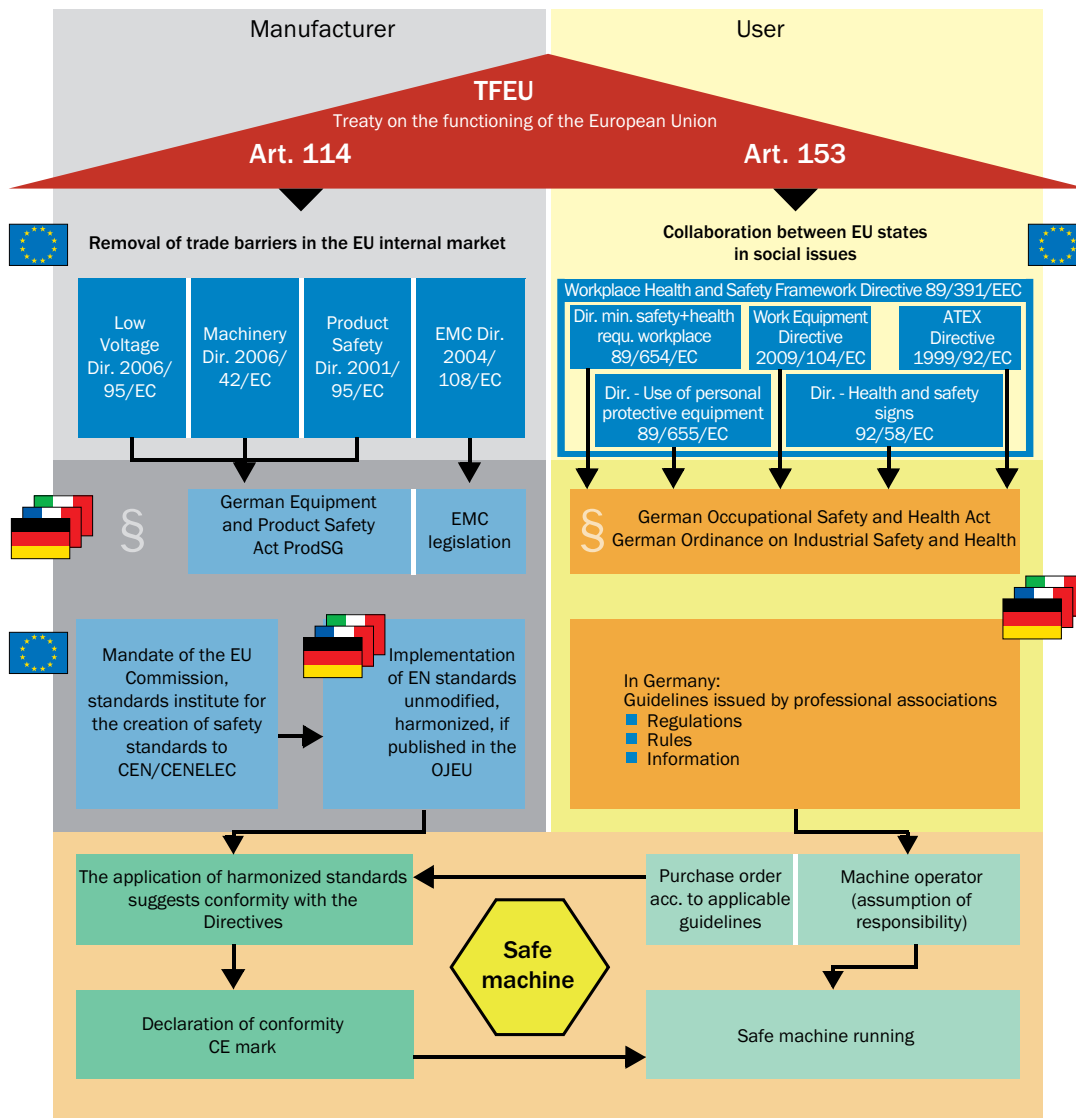


One of the fundamental principles of the European Community is the protection of the health of its citizens, both in the private and in the professional sphere. A further fundamental principle is the creation of a single market with free movement of goods.

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 manufacturer 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 <http://eur-lex.europa.eu/>

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 North America or Asia).

- 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 29 December 2009.

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

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.

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.



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
- Be archived for at least ten years from the last day of manufacture of the machine (or the machine type)
- 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 (→ "EC conformity assessment procedure for machinery and safety components" → §-7):

- **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 as well as 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



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 (QMS) that has been assessed:** 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.

Attention! 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.)

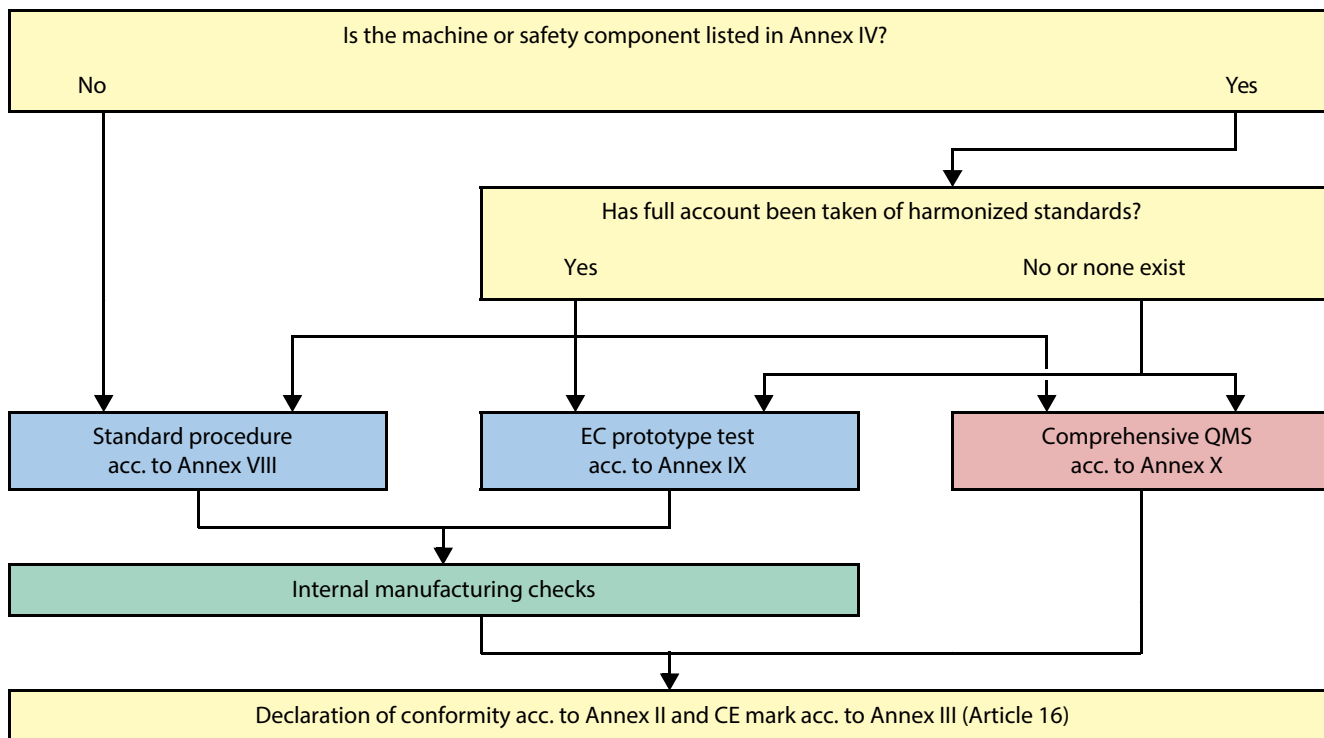
Special case: Partly completed machinery

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 without an end-effector, 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 manufacturer 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" §-15.

EC conformity assessment procedure for machinery and safety components



Summary: European laws and 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.

Standards

This Guide essentially references the most prominent national standards in the Americas. A list of relevant standards is provided in the annex.

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 by or agreed upon by governments or authorities. Standards describe the state-of-the-art at the time they are prepared. Over the last 100 years, a change from national standards to globally applicable stan-

dards 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 suppliers, integrators, and users 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)

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.



National Standards

U.S.A.

In addition to the referenced OSHA requirements above, OSHA also may enforce National Consensus Standards as though they are OSHA requirements. The term “national consensus standard” means any standard or modification thereof, which:

1. Has been adopted and promulgated by a nationally recognized standards-producing organization under procedures whereby it can be determined by the Secretary of Labor that persons interested and affected by the scope or provisions of the standard have reached substantial agreement on its adoption
2. Was formulated in a manner which afforded an opportunity for diverse views to be considered
3. Has been designated as such a standard by the Secretary (of Labor) after consultation with other appropriate Federal agencies
4. By an international standard that covers a subject, which is not covered by a standard in the United States

It is important to note that OSHA utilizes these national consensus standards to further define machine safeguarding requirements in addition to Subpart O.

For instance, in 1910.212(a)(3)(ii), the following statement is made:

“The point of operation of machines whose operation exposes an operator to injury, shall be guarded. The protective device shall be in conformity with any appropriate standards, or, in the absence of applicable specific standards, shall be so designed and constructed as to prevent the operator from having any part of his body in the danger zone during the operating cycle.”

“Any appropriate standards” refers to national consensus standards that are generally accepted in industry. Where possible, OSHA promulgates these national consensus standards and established federal standards as safety standards. The American National Standards Institute (ANSI), The National Fire Protection Agency (NFPA) and in some instances Underwriters Laboratories (UL) are examples of national consensus standards bodies that may be referenced by OSHA.

Canada

The Standard Council of Canada recognizes CSA as the primary Standards body for writing machine specific safety standards. ISO/ IEC Standards are also accepted.

Mexico

The Supreme Justice Court of the Nation (La Suprema Corte de Justicia de la Nación) stated that international treaties are binding for the whole Mexican State, and therefore international standards (ISO-IEC) have to be considered as the base for all technical regulations.

**Brazil**

Founded in 1940, the Brazilian Association of Technical Standards (ABNT) is the organization responsible for technical standardization in the country, providing the necessary basis to the Brazilian technological development. These standards are generally referred to as NBRs (“Normas do Brasil” - Brazilian Standards), more precisely, ABNT NBR.

ABNT is a private, nonprofit civil association, recognized as the only National Standardization Forum through Resolution No. 07 of CONMETRO dated 24 August 1992. It is a founding member of ISO (International Organization for Standardization), COPANT (Panamericana Technical Standards Commission) and AMN (MERCOSUR Standardization Association).

General

A summary of important safety standards by region is presented in the tables in the annex. Consult local, state and federal regulations for any additional requirements that may apply to your specific application.

ABNT is the sole and exclusive representative in Brazil of the ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) international organizations, as well as the regional standardization bodies COPANT (Panamericana Commission of Technical Standards) and AMN (Mercosur Association for Standardization).

Besides the ABNT NBR technical standards, there are the Regulatory Standards (“Normas Regulamentadoras” - NRs) which belongs to the Labor Laws Consolidation (CLT). These are compulsory requirements and include NR 12, which addresses safety of machinery.

International/European Standards

This section of the Guide essentially references international standards (ISO and IEC). A list of relevant standards is provided in the annex.

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

Different types of standards

There are three different types of standards:

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:

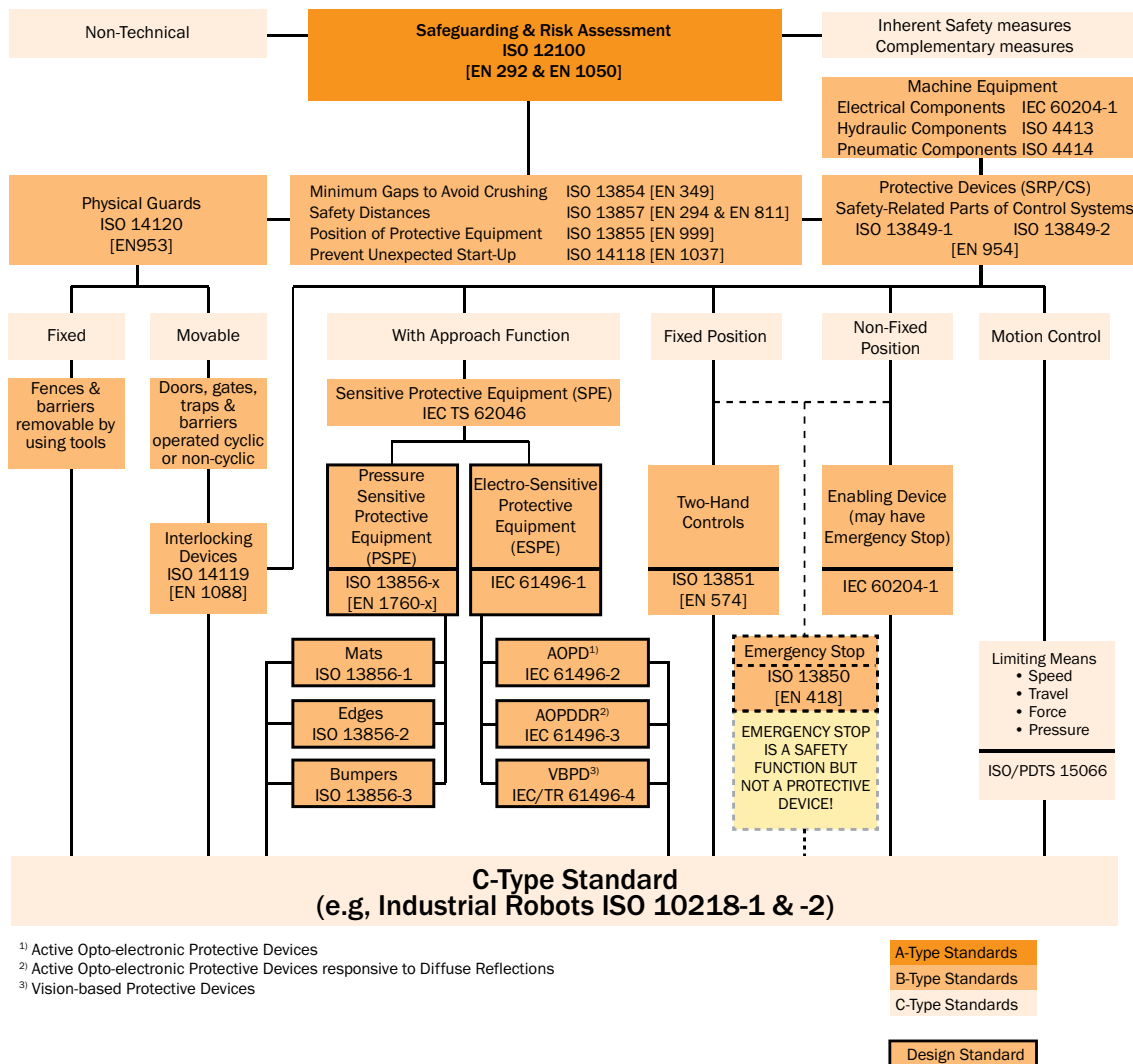
- **B1-type standards** on special safety aspects, e.g., the electrical safety of machinery, the calculation of safety distances, requirements for control systems
- **B2-type standards** on protective devices, e.g., two-hand controls, physical guards and electro-sensitive protective equipment

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 legal requirements of the region shall be met.

→ 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



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 in Europe

As a rule, each EU member state has its own standardization organization, e.g., DIN in Germany, ON in Austria, BSI in the United Kingdom, AFNOR in France. 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 EU 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: <http://www.normapme.com/>

→ A list of the standards with presumption of conformity with the directives is available at <http://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 applicable in that region 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.



Nationally recognized testing laboratories

OSHA Safety Regulations, which are U.S. law, contain requirements for “approval” (i.e., testing and certification) of certain products by a Nationally Recognized Testing Laboratory (NRTL). These Safety requirements are found in Title 29 of the Code of Federal Regulations (29 CFR), and the provisions for NRTL certification are generally in Part 1910 (29 CFR Part 1910). The requirements help protect workers by ensuring products are designed for safe use in the workplace. An NRTL generally certifies products for a manufacturer.

Many of these OSHA requirements pertain to equipment for which OSHA does not require an NRTL certification. The only products covered under the NRTL Program are those for which OSHA regulations require certification by an NRTL. Whether or not OSHA requires NRTL certification, an employer subject to OSHA’s requirements must ensure it complies with the provisions of the Safety Standards applicable to its operations.

An NRTL is an organization that OSHA has “recognized” as meeting the legal requirements in 29 CFR 1910.7. In brief, these requirements are the capability, control programs, complete independence, and reporting and complaint handling procedures to test and certify specific types of products for workplace safety. This means, in part, that an organization must have the necessary capability both as a product safety testing laboratory and as a product certification organization to receive OSHA recognition as an NRTL. OSHA’s recognition is not a government license or position, or a delegation or grant of government authority. Instead, the recognition is an acknowledgment that an organization

has the necessary qualifications to perform safety testing and certification of the specific products covered within its scope of recognition. As a result, OSHA can accept products “properly certified” by the NRTL. “Properly certified” generally means:

- The product is labeled or marked with the registered certification mark of the NRTL
- The NRTL issues the certification for a product covered within the scope of a test standard for which OSHA has recognized it
- The NRTL issues the certification from one of its sites (i.e., locations) that OSHA has recognized.

Note: OSHA does not approve or disapprove products specifically. In terms of OSHA’s usage, “NRTL” is not treated as an acronym but just as a group of initials. As such, the indefinite article “an” precedes these initials in singular usage.

Some people think that a product must have UL certification when in fact any of the OSHA recognized NRTLs for the specific product are appropriate. Some of the recognized NRTLs for the U.S.A. and Canada include but are not limited to TUV, CSA, and UL.

Link to OSHA NRTL information:

→ <http://www.osha.gov/dts/otpc/nrtl/>



Test bodies, insurance providers, and authorities

European 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 standards in the "Useful links" section of the Annex [g i-12](#).



Summary: Regulations and standards

Regulations

- National regulations require safe and healthy working conditions.
- Regulations typically state that where hazards exist, safeguarding needs to be used.
- In addition to federal regulations, certain areas may have specific requirements. Consult local, state and federal authorities to determine what may apply to your specific application.

Standards

- Technical standards specify in detail the objectives defined in the regulations.
- In the absence of a national standard or regulation, international standards can be used.
- The application of harmonized European / International standards justifies the “presumption of conformity”, i.e., the presumption the machine meets the requirements of the Machinery 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.

Testing laboratory:

- Regulations may require the use of products certified by recognized testing laboratories.

Step 1: Risk assessment

When designing, modifying or using 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.

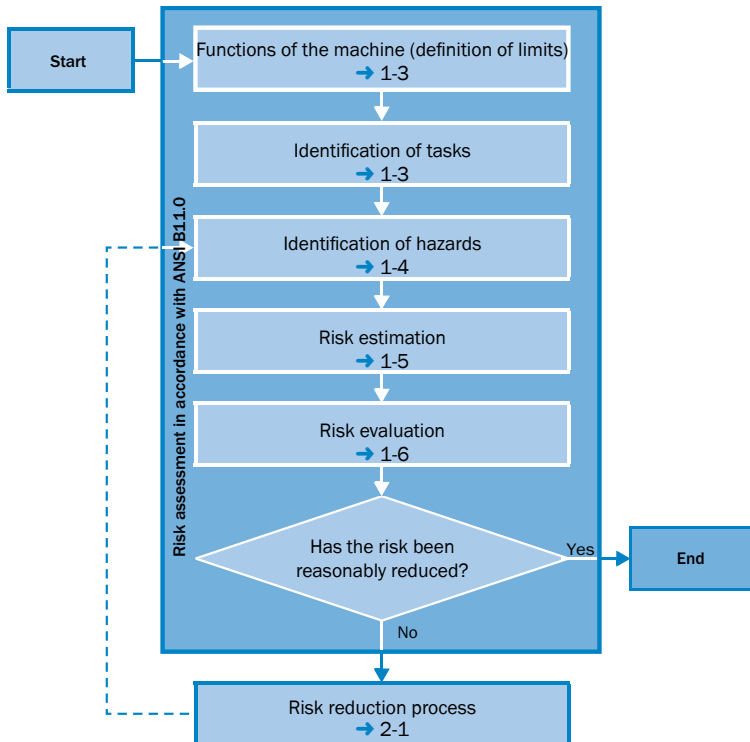
Where necessary, a risk assessment is followed by risk reduction, which is achieved by applying suitable protec-

tive measures. A new risk should not result from the application of protective measures, otherwise it to must be assessed and reduced. 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. When possible, the user should participate in the supplier’s risk assessment of the machine design.

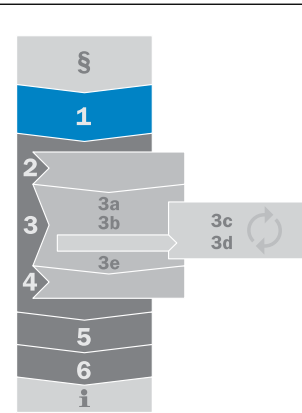
In many C-type standards, the risk assessment is defined to suit the specific machine and application. If no C-type standards are applicable or they are insufficient, the requirements in the A-type and B-type standards can be used.

→ Safe design, risk assessment, and risk reduction: ISO 12100, ANSI B11.0, ANSI/PMMA B155.1, CSA Z432

The risk assessment process



- 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.



In this chapter ...

The risk assessment process.	1-1
Functions of the machine.	1-3
Identification of hazards.	1-4
Risk estimation and evaluation.	1-5
Documentation	1-6
Summary	1-7

1

Using an iterative process and considering personnel

The process of performing a risk assessment and risk reduction strategy for a machine or system is an iterative process. After the initial risk reduction strategy has been implemented, it is imperative that the task and associated hazard be re-evaluated based on the additional protective measure and a new risk estimation is determined. If the subsequent risk estimation determines that residual risk is viewed as “acceptable,” then the next task and associated hazard are evaluated. If the residual risk is not determined to be acceptable, then implementation of additional risk reduction measures should occur followed by a new risk estimation. This iterative process repeats until the residual risk is viewed as acceptable.

Also consider that personnel potentially affected by the tasks and hazards associated with the machine / system could include:

- Operators or helpers
- Maintenance personnel
- Engineers
- Technicians
- Sales personnel
- Installation personnel
- Removal personnel
- Administrative personnel
- Trainees
- Passers-by
- Designers
- Manager
- Supervisors
- Safety personnel
- Safety committees
- Safety consultants
- Loss control administrators
- And others

Other factors that should be considered

- The level of training and experience of each personnel type shown above
- Machine task history, including statistical data, history of harm, history of “near misses”
- Workplace environment related to layout, lighting, noise, ventilation, temperature, humidity, etc.
- The ability to maintain protective measures required to provide adequate level of protection
- Human factors – e.g., errors resulting from omitting steps in the process, adding steps or performing steps out of sequence, personnel interaction, ability to execute required tasks, motivation to deviate from established safety procedures, accumulated exposure, and reduced vision.
- Reliability of safety functions, including mechanical, electrical, hydraulic, and pneumatic control system integrity
- Potential for circumvention of protective measures, including incentives to defeat protective measures e.g., protective measure prevents task from being performed, protective measure may slow down production, protective measure may interfere with other activities or may be difficult to use.



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

Machine limits	Examples
Use Limits	Intended use of the machine, production rates, cycle times, etc.
Space Limits	Range of movement, maintenance, etc.
Time Limits	Maintenance and wear of tools, fluids, etc.
Environmental Limits	Temperature, humidity, noise, location, etc.
Interface Limits	Other machines and auxiliary equipment, energy sources, etc.

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 no matter what 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 faults 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

Identification of the expected tasks to be completed on/by the machine

Once the machine/system limits have been defined, the next step in the process is to identify the various tasks and associated hazards of operating the machine. The following list provides some basic task categories that should be considered. It is important to note that this list is not exhaustive and that additional task categories may apply.

- Packing and transportation
- Unloading and unpacking
- System installation
- Start-up and commissioning
- Setup and try out
- Operation – all modes
- Sanitation and cleaning
- Housekeeping
- Tool change
- Planned maintenance
- Unplanned maintenance
- Major repair
- Recovery from crash
- Troubleshooting
- Decommissioning
- Disposal

Identification of the hazards associated with each task

After the tasks associated with the machine or system have been identified, corresponding hazards should be considered for each task. These tasks and hazards should account for

both the intended use of the machine and any reasonably foreseeable misuse of the machine.

Identification of other hazards


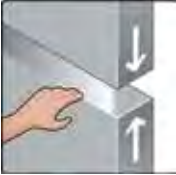








In addition to identifying hazards directly associated with specific tasks of the machine, the risk assessment must also

include the systematic identification of foreseeable hazards, hazardous situations, and/or hazardous events.

1

Hazards may include but are not limited to the following in all phases of the service life of the machine.
<ul style="list-style-type: none"> • Mechanical hazards • Electrical hazards • Thermal hazards • Hazards generated by noise • Hazards generated by 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 	<ul style="list-style-type: none"> • 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. A variety of standards and technical reports have been developed to assist with this process.

$$\text{Risk} = \text{Extent of injury} \times \text{Probability of occurrence}$$

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/people to the hazard
 - The frequency 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.

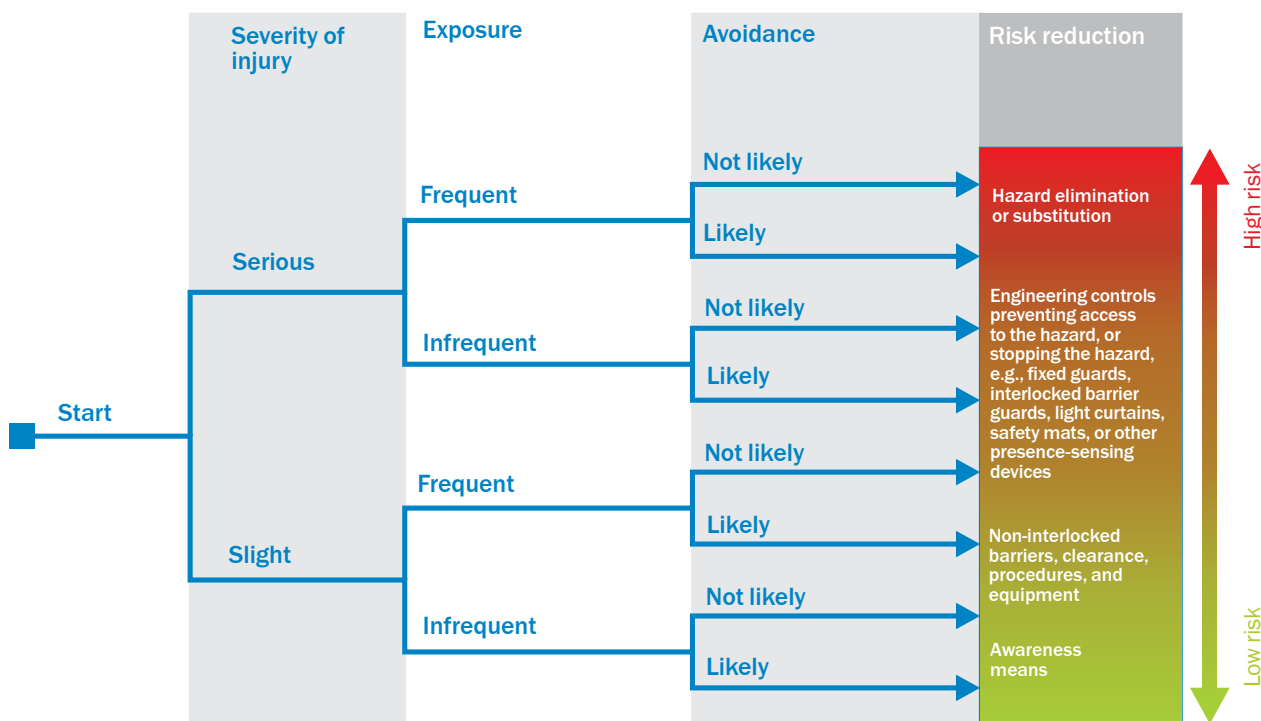
Various standards and technical reports addressing risk assessment utilize different approaches in considering these factors. Based on applicable national, regional and local regulations, please reference one or more of the following standards for further guidance relating to the factors to be evaluated during the risk assessment process:

Standard	Description
ANSI B11.0	Safety of Machinery – General Requirements and Risk Assessment
ANSI/PMMI B155.1	Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery
SEMI S10	Safety Guideline for Risk Assessment and Risk Evaluation Process
CSA Z432	Safeguarding of machinery
ISO 12100	Safety of machinery – General principles for design – Risk assessment and risk reduction
ISO/TR 14121-2	Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods
ANSI/ASSE Z590.3	Prevention through Design Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes
ANSI/AIHA/ASSE Z10	Occupational Health & Safety Management Systems
CSA Z1002	Occupational health and safety – Hazard identification and elimination and risk assessment and control
MIL-STD-882	Department of Defense Standard Practice – System Safety
ISO 13849-1	Safety of machinery - Safety-related parts of control systems – Part 1: General principles for design
IEC 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

Risk evaluation process

During the “risk evaluation,” it is defined, based on the results of the risk estimation, whether the application of protective measures is necessary and when the necessary risk reduction has been achieved.

The following chart shows one way of evaluating risk and the hierarchy of possible risk reduction measures.



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, etc.
- All hazards and hazardous situations identified and hazardous events considered
- Data used and their 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 used and prepared during the risk assessment

While various standards and directives, including the Machinery Directive, require that a risk assessment be performed, many do not require the risk assessment documentation be provided with the machine. However, machine users may request the results of the risk assessment performed by the machine builder or integrator to maintain the overall effectiveness of risk control throughout the entire life cycle of the equipment, including future changes or modifications to the equipment or the associated process.

Summary: Risk assessment

General

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

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 faults.
- Identify the tasks performed by affected personnel (operators, maintenance personnel, etc.). Take into account the level of training, experience and other human factors, such as incentives to defeat protective measures.
- 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.
- Estimate the risks posed by the hazards. These depend on the extent of injury and the probability of occurrence of the harm.
- Document the results of the risk assessment.

1

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

The following principles shall be applied during the selection of the measures, and in the order given:

1. Safe design: elimination or minimization of residual risks as far as possible (integration of safety in the design and construction of the machine or process)
2. Technical protective measures: Take the necessary protective measures (engineering controls) against risks that cannot be eliminated by design
3. Administrative measures to inform and warn about the residual risks



→ General principles of risk reduction: ISO 12100, ANSI B11.0, ANSI/PMMI B155.1, RIA TR R15.406, ANSI/ASSE Z244.1, CSA Z432



Risk reduction strategies

According to industry standards, the goal of implementing a risk reduction strategy is to reduce risk to personnel to an “acceptable” level. The definition of an “acceptable” level of residual risk is ultimately the decision of the owner of the equipment.

In general, there is industry agreement that a risk reduction strategy should utilize a hierarchical approach.

These indicate that the most effective solution begins with:

1. Elimination or substitution, working through to
2. Engineering controls, followed by
3. Awareness means, and then
4. Training and procedures, followed by
5. Personal protective equipment (the least effective solution).

A comprehensive approach to risk reduction may include any or all of the risk reduction strategies identified in the following table.

Risk Reduction Strategy	Examples
1. Elimination or substitution by changes in machine design	<ul style="list-style-type: none"> • Eliminate human interaction in the process • Eliminate pinch points (increase clearance) • Automated material handling
2. Engineering control (safeguarding technology)	<ul style="list-style-type: none"> • Mechanical hard stops • Barriers • Interlocks • Presence sensing devices • Two-hand controls
3. Administrative measures	<p>Awareness Means:</p> <ul style="list-style-type: none"> • Lights, beacons and strobes • Computer warnings • Signs • Restricted space painted on floor • Beepers • Horns • Labels <p>Training and Procedures:</p> <ul style="list-style-type: none"> • Safety job procedures • Safety equipment inspections • Training <p>Personal Protective Equipment:</p> <ul style="list-style-type: none"> • Safety glasses • Ear plugs • Face shields • Gloves

2

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.

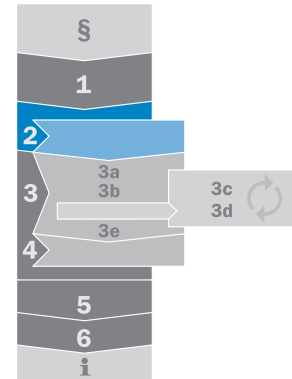
Aspects of safe design relate to the machine itself and the interaction between the person at risk and the machine.

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 damage to the machine and the environment is also to be taken into consideration.

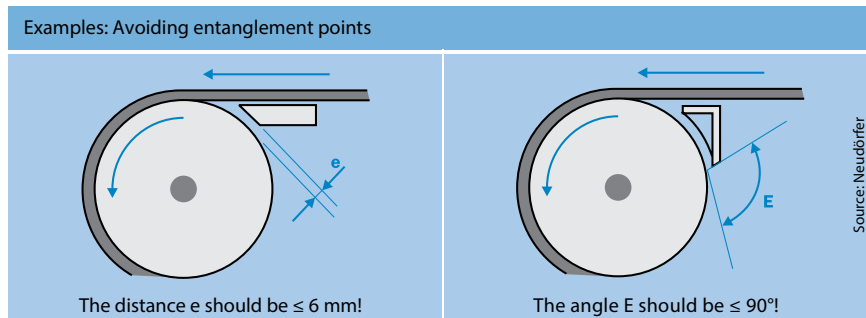
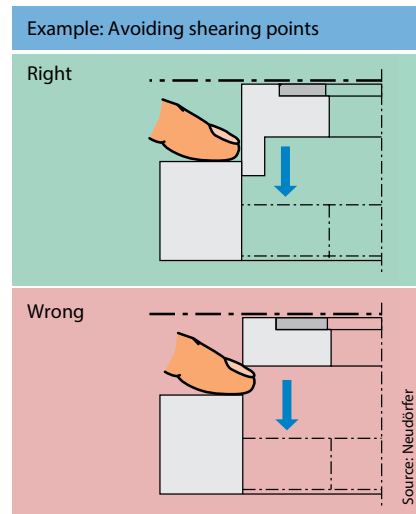
All elements of the machine design are to be specified so that they function within specified limits. The design should also always be as simple as possible. Safety-related functions are to be separated from other functions as far as possible.



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



→ Alfred Neudörfer: Konstruieren sicherheitsgerechter Produkte, Springer-Verlag, Berlin u. a., ISBN 978-3642191886 (4th Edition 2011)

In this chapter ...

Mechanical design	2-3
Operating and maintenance concept	2-4
Electrical equipment	2-5
Enclosure ratings	2-8
Lock-out/Tag-out	2-10
Stop functions	2-11
Electromagnetic compatibility (EMC)	2-12
Fluid technology	2-14
Use in potentially explosive atmospheres	2-15
Summary	2-16

Operating and maintenance concept

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

- Automatic loading and unloading stations
- Setup and maintenance work from outside the hazardous area(s)
- 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.

2

→ Color coding convention for industrial machinery: NFPA 79, IEC 60204-1

Color	Condition of Machine/Process (preferred purpose, unless otherwise agreed)	
	Status	Action by Operator
	Red	Emergency (hazardous condition)
Yellow Amber	Abnormal (abnormal or impending critical condition)	Monitoring and/or intervention (for example by re-establishing the intended function)
Green	Normal	Optional
Blue	Mandatory Action	Mandatory Action
Clear White Gray Black	Neutral (no specific meaning assigned – may be used whenever doubt exists about the application of RED, YELLOW, GREEN, or BLUE)	Monitoring

Color	Purpose	
	Safety of People or Environment	State of Equipment
	Status	Status
Red	Danger	Faulty
Yellow Amber	Warning / Caution	Abnormal
Green	Safe	Normal
Blue	Mandatory Action	Mandatory Action
Clear White Gray Black	Neutral (no specific meaning assigned)	Neutral (no specific meaning assigned)

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 safety standards: NFPA 70, NFPA 70E, NFPA 79, CSA Z462, NR-10, 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.

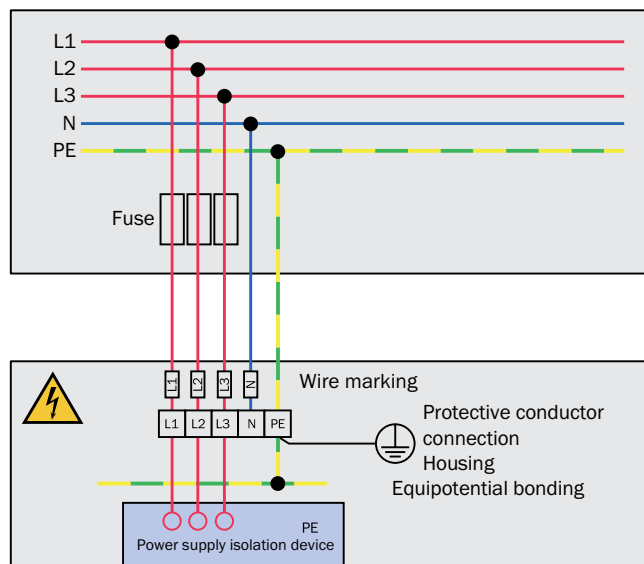
A stable power supply is particularly important in safety-related applications. For this reason, the voltage supplies should be able to withstand brief power failures.

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.

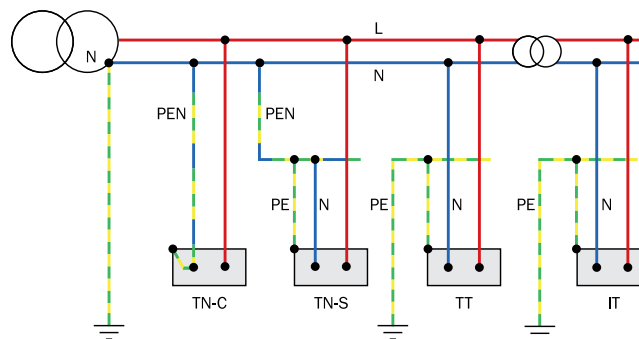


- Protective measures: IEC 60364-4-41, with varying national amendments
- Similar requirements can be found in NFPA 79

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



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).

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.

	<p>Protection class I</p> <p>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.</p>
	<p>Protection class II</p> <p>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.</p>
	<p>Protection class III</p> <p>Equipment in protection class III operates with a safety extra-low voltage and, therefore, does not require any explicit protection.</p>

Safety extra-low voltage SELV/PELV

AC voltages up to 50 V_{rms} 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)

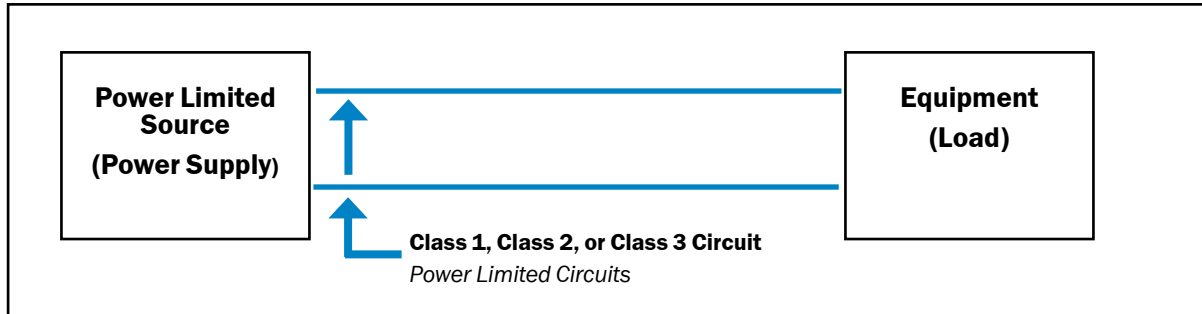
A safety extra-low voltage shall not be generated from the mains using autotransformers, voltage dividers, or series resistors.

		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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • AC ≤ 25 V or • DC ≤ 60 V 	No additional measures required	Basic protection by means of: <ul style="list-style-type: none"> • Insulation or casings in accordance with standards or • Body and active parts connected to main earthing rail

- Protection classes: EN 50178
- Safety of transformers: EN-61588 series
- Concepts of SELV and PELV: NFPA 79, ANSI/UL 60950-1, IEC/UL 61010A-1, and IEC 60364-4-1

NFPA 70, the National Electric Code (NEC), is the general North American guideline for all electrical installations.

It is also the source of power limiting circuit definition, known as Class 1, Class 2 and Class 3.



Most common is a Class 2 circuit, which offers protection for fire initiation and electric shock. For a 24 V DC power supply (the most commonly used Class 2 voltage), the maximum power allowed is 100 W. The power supply must be listed to applicable standards.

The advantage of using a Class 2 power supply is reduced requirements for insulation, wiring methods, installation materials and device approvals (UL). Class 2 can be regarded as a U.S. specialty.

Another option to provide protection against electric shock is to use safety extra-low voltage. Similar to the classes in the U.S., there are special requirements for the power source, creepage distances, insulation, etc.

A differentiation is made between:

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

These concepts are in correlation with NFPA and international standardization.

- Electrical installation methods: NFPA 70 - National Electric Code
- Limited power source as one option to achieve Class 2: UL 60950 (UL 1950), IEC 60950
- Electrical Standard for machinery, Protection against electrical shock: NFPA 79

Enclosure ratings

Typically electrical equipment enclosures need to meet the requirement for enclosure ratings. Two widely accepted rating systems are the NEMA types/number and the IP rating code. NEMA, short for National Electric Manufacturers' Association,

and their type number system is commonly specified at installations in the U.S and is similar to UL and CSA equivalents. IP, which is an abbreviation for International Protection, is derived from the IEC. Typically control cabinets should be NEMA 13.

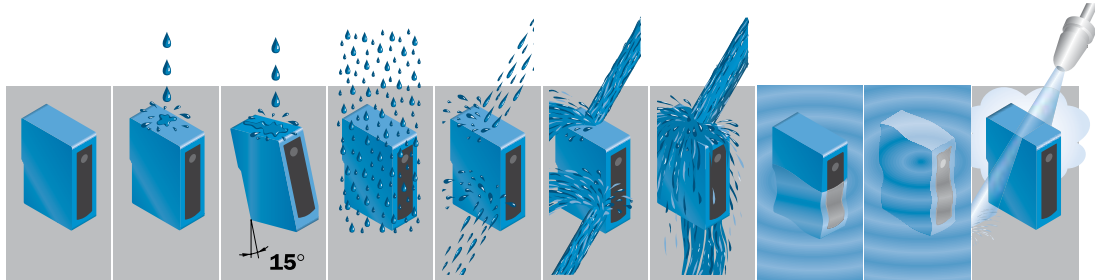
The NEMA classifications are as follows.

Standard NEMA	NEMA 1	NEMA 2	NEMA 3	NEMA 3S	NEMA 4	NEMA 4X	NEMA 6	NEMA 6P	NEMA 12	NEMA 13
Suggested Usage	Inside	Inside	Outside	Outside	Inside or Outside	Inside or Outside	Inside or Outside	Inside or Outside	Inside	Inside
Accidental Bodily Contact	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Falling Dirt	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dust, Lint, Fibers (non volatile)			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windblown Dust			Yes	Yes	Yes	Yes	Yes	Yes		
Falling Liquid and Light Splash		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hosedown and Heavy Splash					Yes	Yes	Yes	Yes		
Rain, Snow and Sleet			Yes	Yes	Yes	Yes	Yes	Yes		
Ice Buildup				Yes						
Oil or Coolant Seepage									Yes	Yes
Oil or Coolant Spray and Wash										Yes
Occasional Submersion							Yes	Yes		
Prolonged Submersion								Yes		
Corrosive Agents						Yes		Yes		

2

The enclosure IP 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
	None-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... Non-protected	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... Dust-protected	IP 50			IP 53	IP 54	IP 55	IP 56			
IP 6... Dust-tight	IP 60					IP 65	IP 66	IP 67		IP 69K

- Enclosure ratings: NEMA 250, IEC 60529
- Comparison between NEMA enclosure types and IEC IP rating: NFPA 79

Lock-Out/Tag-Out

Lock-Out/Tag-Out (LOTO) is an essential safety procedure that protects employees who are exposed to hazardous energy during servicing/maintenance activities. Lock-Out involves applying a physical lock to all hazardous energy sources on the equipment after they have been shut off and de-energized. Energy sources can be mechanical, electrical, pneumatic or hydraulic. The source is then Tagged-Out with an easy-to-read tag that alerts other workers in the area that a lock has been applied.

Some minor servicing operations like minor tool changes or adjustments may have to be performed during normal production operations, and an employer may be exempt from LOTO in some instances. Operations are not covered by LOTO if they are

routine, repetitive and integral to the use of the machine for production and if work is performed using alternative effective protective measures.

A hazardous energy control program is a critical part of an overall safety strategy and should include:

- Annual training and audits
- Machine Specific LOTO procedures as part of the manual (see general checklist)
- Corporate policy

Lock-Out/Tag-Out (LOTO) is supplementing – not substituting – proper machine safeguarding.

2

- OSHA Booklet 3120: Control of Hazardous Energy Lock-Out/Tag-Out
- OSHA Standard 29 CFR 1910.147, Control of hazardous energy (Lock-Out/Tag-Out)
- ANSI/ASSE Z244.1, Control of Hazardous Energy – Lockout/Tagout and Alternative Methods
- CSA Z460, Control of Hazardous Energy – Lockout and Other Methods

Lock-Out/Tag-Out Checklist (Source NIOSH)

When performing Lock-Out/Tag-Out on equipment, you can use the checklist below.

- Identify all sources of energy for the equipment or circuits in question.
- Disable backup energy sources such as generators and batteries.
- Identify all shut-offs for each energy source.
- Notify all personnel that equipment and circuitry must be shut off, locked out, and tagged out. (Simply turning a switch off is NOT enough.)
- Shut off energy sources and lock switchgear in the OFF position. Each worker should apply his or her individual lock. Do not give your key to anyone.
- Test equipment and circuitry to make sure they are de-energized. This must be done by a qualified person.*
- Deplete stored energy by bleeding, blocking, grounding, etc.
- Apply a tag to alert other individuals that an energy source or piece of equipment has been locked out.
- Make sure everyone is safe and accounted for before equipment and circuits are unlocked and turned back on. Note that only a qualified person* may determine when it is safe to re-energize circuits.

*OSHA designates a “qualified person” as someone who has received mandated training on the hazards and on the construction and operation of equipment involved in a task.



Stop functions

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 as defined in NFPA 79 and IEC 60204-1 are not to be mistaken for the categories defined in ISO 13849-1.

Stop Category 0	An uncontrolled stop by immediately removing power to the machine actuators (drive elements)
Stop Category 1	A controlled stop with power to the machine actuators available to achieve the stop, then remove power when the stop is achieved
Stop Category 2	A controlled stop with power left available to the machine actuators

→ Stop functions: NFPA 79, 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 interferences can be caused by:

- Fast, transient, electrical disturbances (bursts)
- 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 radio frequency (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

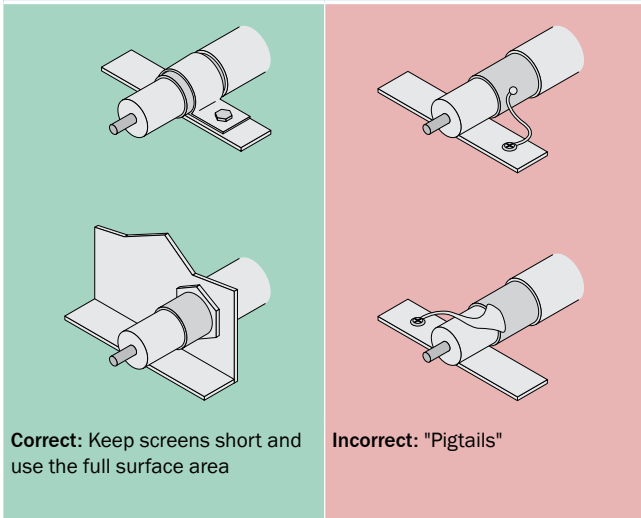
Example: Typical distances from mobile phone systems for different field strengths

Area of application	3 V/m	10 V/m	100 V/m	Note
Wireless home phone	Approx. 1.5 m	Approx. 0.4 m	≤ 1 cm	Base station or hand-held unit
Cell phone	Approx. 3 m	Approx. 1 m	≤ 1 cm	Maximum transmission power (900 MHz)
Cell 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 grounding/functional earth (FE) provided
- Connect any available communication cables carefully. Twisted cables are often required to transmit data (fieldbus)

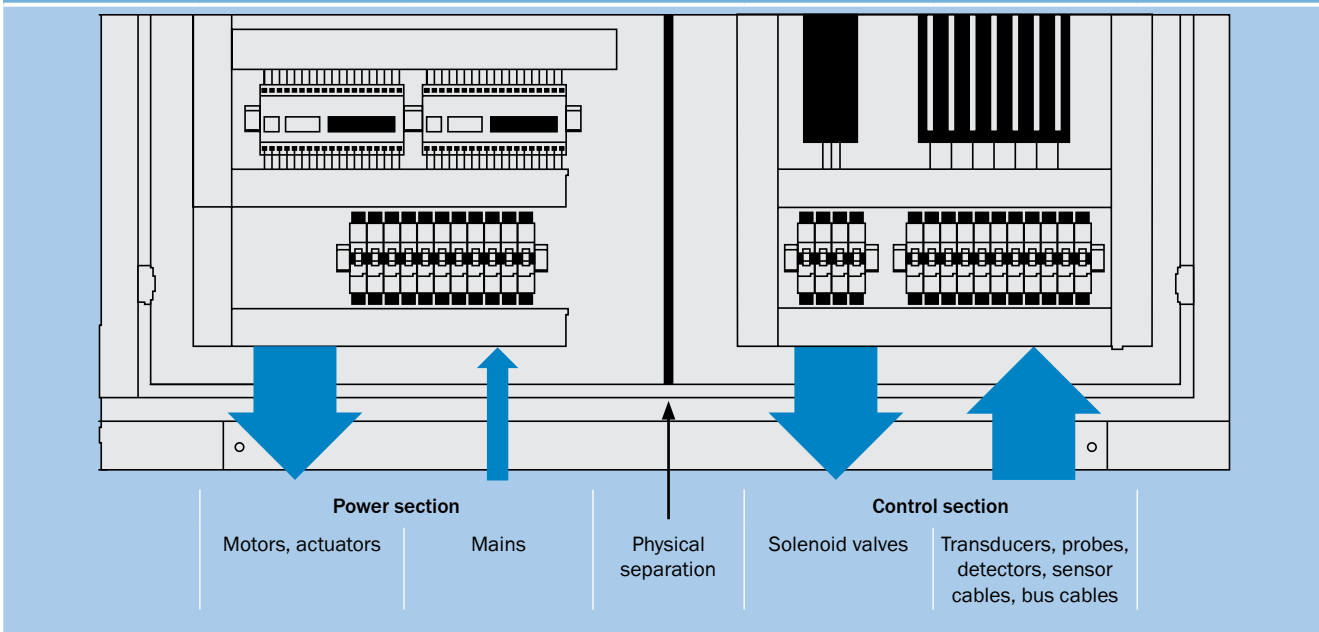
Example: Connecting shield correctly



Example: Providing equipotential bonding



Example: Physical separation



- EMC standards: EN 61000-1 to -4
- EMC requirements on safety components: UL 61496-1, IEC 61496-1, IEC 62061

Fluid technology (hydraulic and pneumatic)

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

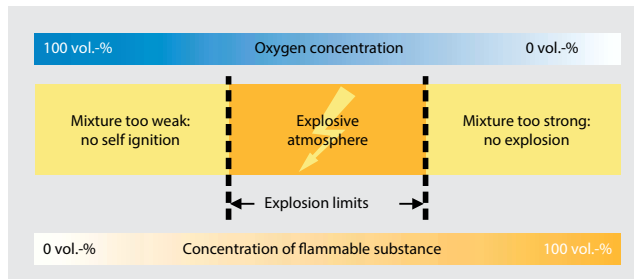
All parts of a fluid-related system are to be protected against pressures that exceed the maximum operating pressure of a subsystem or the rated pressure of a component. A hazard shall not be caused by leaks in a component or in the pipework/hoses. Acoustic attenuators are to be used to reduce the noise caused by escaping air. The use of acoustic attenuators shall not produce any additional hazard, and shall not cause any damaging back-pressure.

- ISO 4413, Hydraulic fluid power – General rules and safety requirements for systems and their components
- ISO 4414, Pneumatic fluid power – General rules and safety requirements for systems and their components

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.



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		

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 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					

→ Directive 1994/9/EC (ATEX 95 – manufacturer)
ATEX standard EN 1127-1

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/shutting down

- 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.
- Establish a hazardous energy control program (Lock-Out/Tag-Out).

EMC

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

Step 3: Technical protective measures

Technical protective measures, also known as engineering controls, 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. For example, a fixed guard (barrier, cover) which does not need to be removed frequently may achieve adequate risk reduction by the correct design of the guard alone.

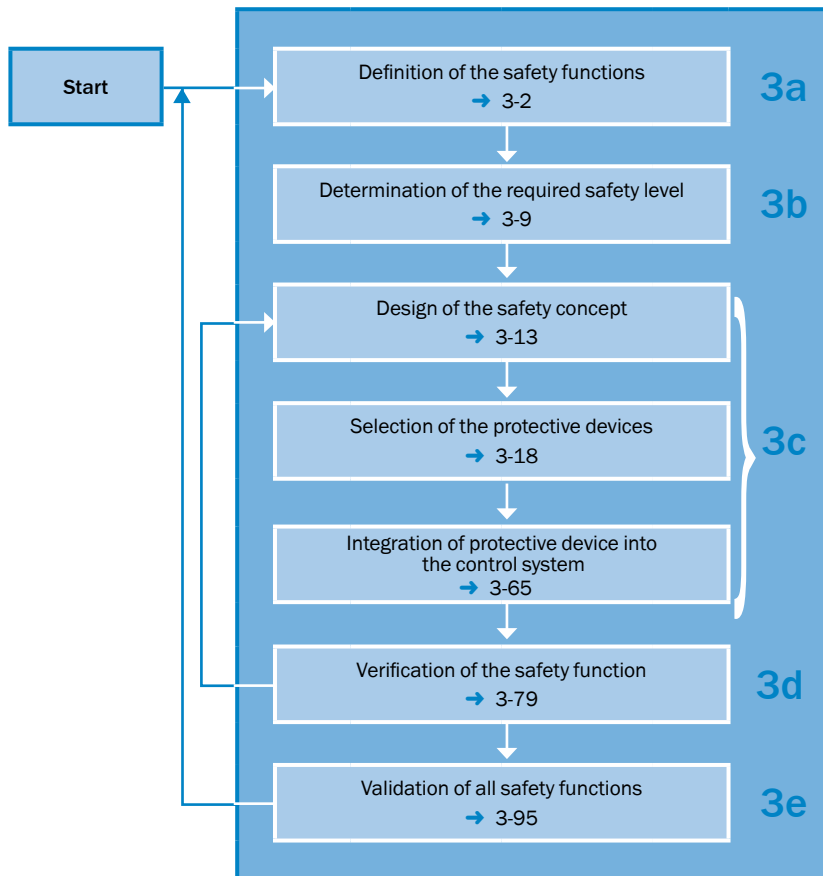
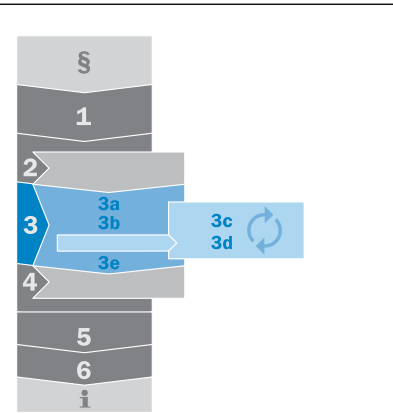
Functional safety

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.

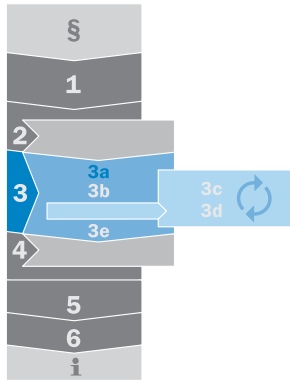
Validation

The validation of all engineering control 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



Step 3a: Definition of the safety functions

The safety functions define how risks are reduced by engineering controls. 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 risk reduction 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 2/2008e, "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
- 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



In this chapter ...

Permanently preventing access 3-2

Temporarily preventing access 3-2

Retaining parts/substances/
radiation 3-3

Initiating a stop 3-3

Avoiding unexpected startup 3-4

Preventing start 3-4

Combination of initiating a stop/
preventing start 3-4

Allowing material passage 3-5

Monitoring machine parameters . . . 3-5

Disabling safety functions
manually and for a limited time . . . 3-6

Combining or switching safety
functions 3-6

Emergency stop 3-7

Safety-relevant indications
and alarms 3-7

Other functions 3-8

Summary 3-8

Temporarily preventing access

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

Example:

- 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.

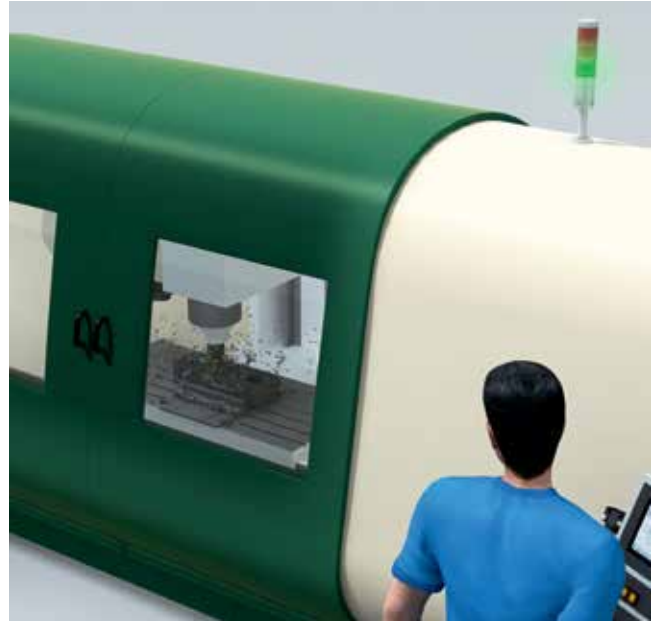


Retaining parts/substances/radiation

If parts can be ejected from 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 (NFPA 79 and EN 60204-1 → 2-11) 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 function
- Interrupting the light beams on a multiple light beam safety device providing access protection (see figure)

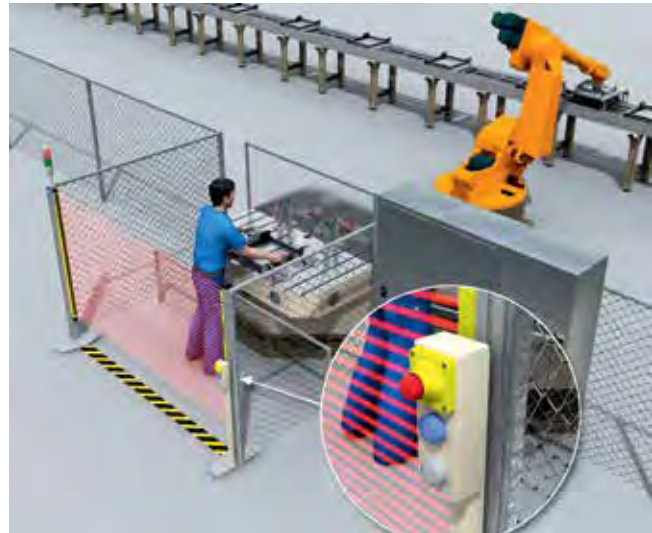


Avoiding unexpected startup

After actuating 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” → 3-64).

Examples:

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



Preventing start

After an “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 protective field of the vertical 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 people or parts of the body detected 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)



Allowing material passage

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 more detailed information, see section “Safety functions that can be integrated in ESPE” → 3-35.



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

Certain operations, such as set-up or process monitoring, may require the machine to operate with a guard displaced or removed and/or a protective device disabled. In these instances, additional measures must be provided for risk reduction and may only be allowed if the follow conditions are met:

- An operating mode selector switch capable of supervisory control (e.g., key switch) with a corresponding operating position shall be used
- Automatic control shall be disabled and 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 hold-to-run controls (devices requiring sustained action, such as two-hand control or enabling devices)
- Hazardous machine functions are only permitted under reduced risk conditions (e.g., limitation of speed, force, movement distance, duration of function)
- All individuals exposed to the hazardous machine function must be provided with and be in direct control of their own control device



3
a

Example:

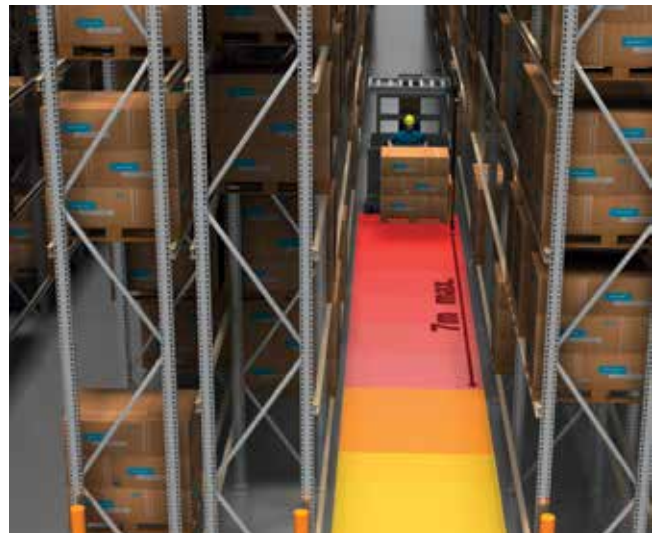
- Movement only at reduced speed with enabling button engaged and +/- buttons actuated (see figure)

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 must 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)



Emergency stop

Emergency stop is a complementary protective measure and not considered a primary safeguard because it does not prevent or detect access to a hazard point. However, an emergency stop can be used to further reduce 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 "Actions in an emergency" → 3-43).

→ See NFPA 79, ANSI B11.19, 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, pre-start warning) 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 be easily checked and inspected
- The warning equipment should be regularly inspected in accordance with the information for use provided by the supplier
- Over saturation of sensory inputs should be avoided, in particular where audible alarms are concerned

Examples:

- Interlocking indications
- AGV speed and start-up warning devices (see figure)
- Muting lamps



Other functions

Other functions can also be executed by safety-related devices, even if they are not used to protect people. When used, other functions must be implemented so as not to impair the safety functions themselves.

Examples:

- Tool and machine protection
- Presence Sensing Device Initiation (PSDI) mode (cycle initiation → 3-38)
- 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
- Avoiding unexpected startup
- Preventing start
- Combination of initiating a stop/preventing start
- Allowing material passage
- Monitoring machine parameters
- Disabling safety functions manually and for a limited time
- Combining or switching safety functions
- Emergency stop
- Safety-relevant indications and alarms

3
a

Step 3b: Determination of the required safety level

Often, machine-specific (C-type) standards specify the required safety level.

The required safety level must be defined separately for each safety function, and applies for all devices involved, such as:

- The sensor(s)/protective device(s)
- The evaluating logic unit(s)
- The actuator(s) (e.g., contactors, valves)

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 may be determined using one of the following standards:

- ANSI B11.0
- ANSI B11.19
- ANSI B11.26
- ANSI B11.TR4
- CSA Z432
- IEC 62061
- IEC 61508
- ISO 13849-1

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.

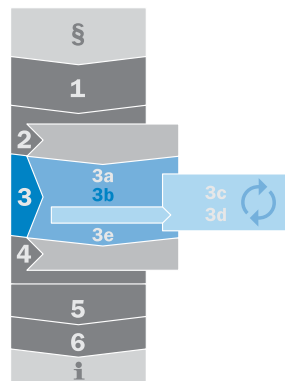
In addition, there can be different risks on the same machine in different phases of the life of the machine at different hazardous points. Here, safety functions are to be defined individually for each phase of life and hazard.

Most standards are based on the following parameters from the risk evaluation:

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

The combination of the parameters determines the safety level required.

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 ...

System performance requirements in ANSI / CSA	3-10
Required performance level (PLr) according to ISO 13849-1	3-10
Safety integrity level (SIL) according to IEC 62061	3-11
Area of application of ISO 13849-1 and IEC 62061	3-11
Summary	3-11

System performance requirements in ANSI / CSA

Many North American standards require the use of a risk graph or matrix, which results in various circuit performance requirements. Many of these standards discuss circuit performance in terms of “control reliability” levels, including single channel, single channel with monitoring, dual (redundant) channels, and dual channel with monitoring.

Of these standards, many do not require that a specific format be used to determine which circuit performance is used, as long as the methodology applied results in levels at least as stringent as the approach provided. As always, it is important to review the industry- or machine-specific standard appropriate for the application for further guidance.

Examples of North American standards and technical reports which define safety performance:

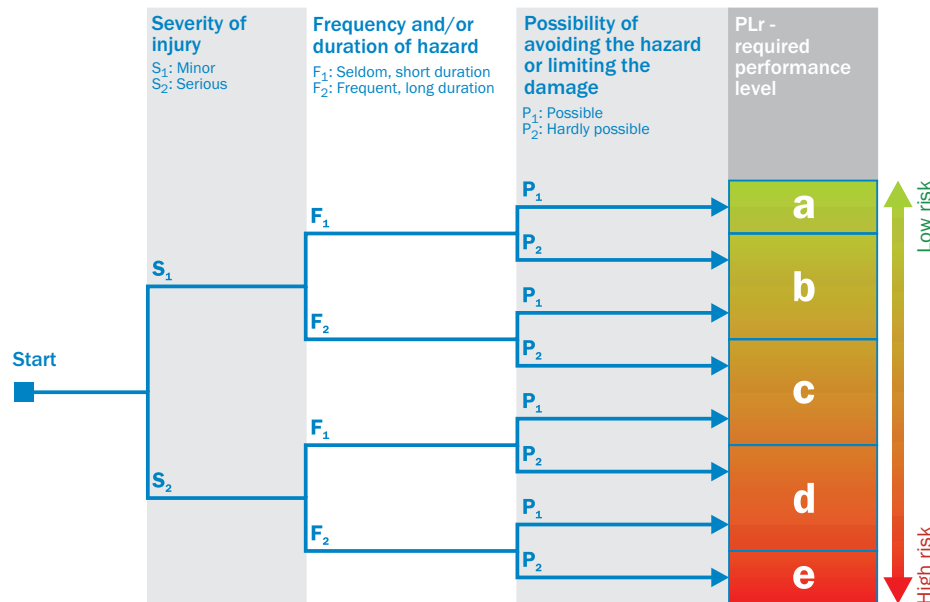
→ ANSI B11.19, ANSI B11.26, CSA Z432

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

This standard also uses a risk graph to determine the required safety level. The parameters severity, frequency and probability

are used to determine the magnitude of the risk. The result of the procedure is a “required performance level” (PLr).

3
b



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” → 3-15. In addition, further measures to avoid design faults are required.

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	4
1× per day > F ≥ 1× in 2 weeks	3
1× in 2 weeks > F ≥ 1× per year	2
1× per year > F	1

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 avoidance **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” → 3-15).

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,” “possibility of avoidance,” and sometimes “probability of occurrence” determine the required level of safety.

Applicable standards

- Many North American standards address the system performance in terms of “control reliability.”
- 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).



**3
b**

Step 3c: Design of 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 compo-

nents. 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.

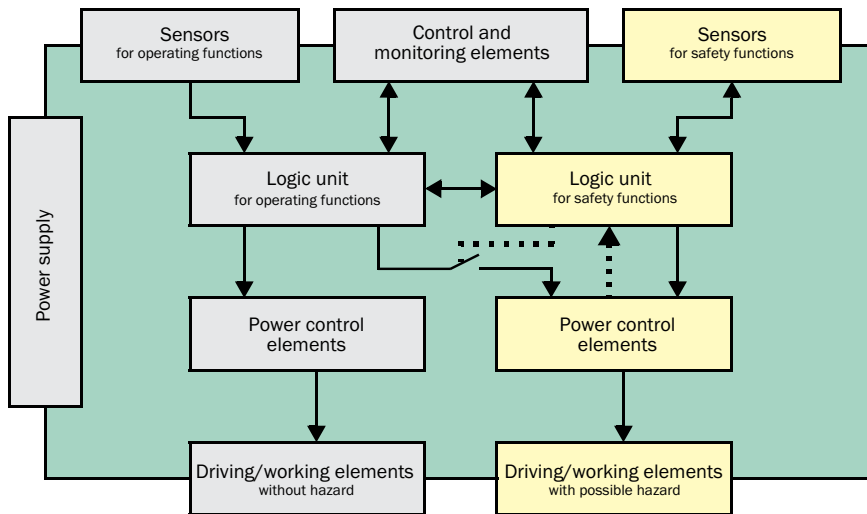
Development of the safety concept

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, "Functional safety of machine controls" at <http://www.dguv.de/medien/ifa/en/pub/rep/pdf/rep07/biar0208/rep22008e.pdf>

Functional layout of a machine control

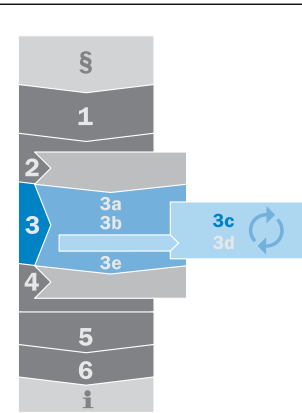


The safety-related parts of control systems are to be selected to suit the safety functions and the necessary level of safety. These parts include sensors, logic units, power control elements, for example, as well as drive and work elements. This selection is generally made in the form of a safety concept.

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 by 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.

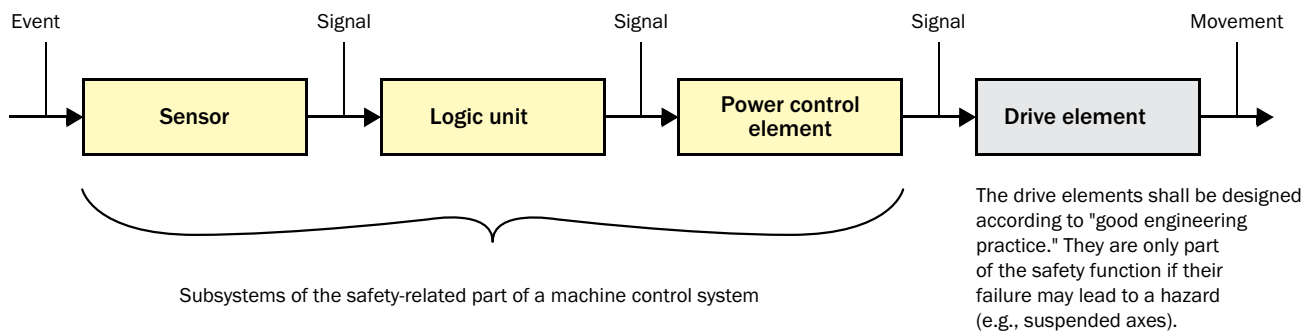


3
C

In this chapter ...

- Development of safety concept . . . 3-13
- Functional layout of a machine control 3-13
- Technology, selection, and use of safeguarding 3-17
- Positioning and dimensioning of protective devices 3-44
- Application of reset and restart . . . 3-64
- Integration of protective devices into the control system 3-65
- Fluid control systems 3-74
- Safety-related pneumatics 3-75
- Product overview for safety technology 3-76
- Summary 3-77

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 (→3-17)

Which protective devices are to be selected 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 operator
- Expected number of people in the area
- Approach speed (K)
- Possibility of defeating the protective devices
- Foreseeable misuse

Features of the design

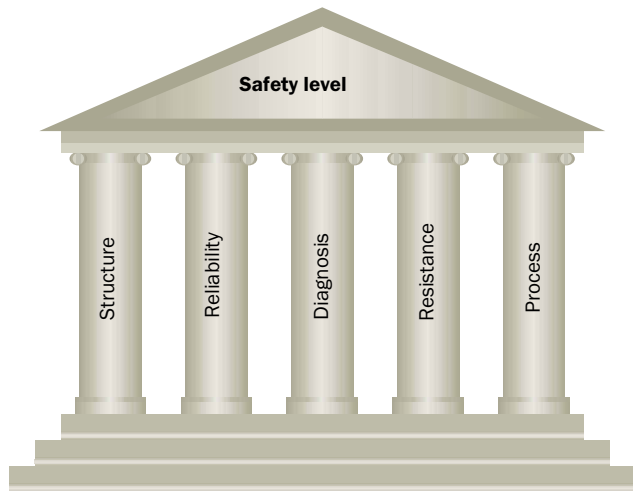
It is always advisable to implement safety functions with certified safety components. Certified safety components will simplify the design process and subsequent verification. A safety function is performed by several subsystems.

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:

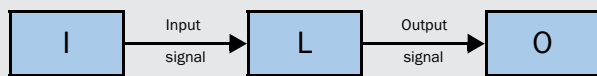
- Structure
- Reliability of the components/devices
- Diagnostics for detecting faults
- Resistance to common cause faults
- Process



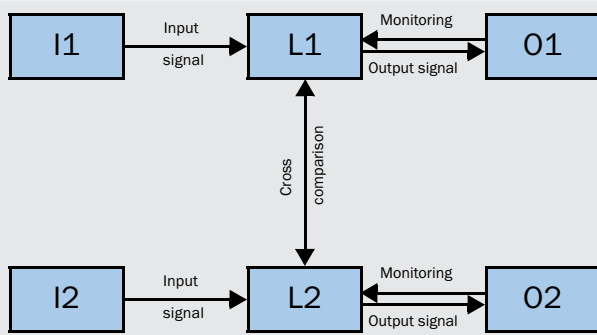
Structure

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



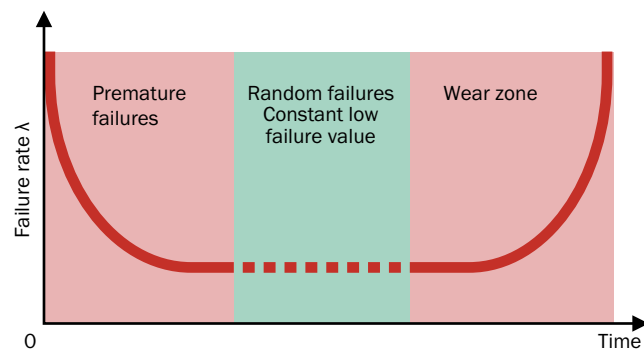
Dual-channel safety components



Reliability of the components/devices

Any failure of a safety component will result in an interruption 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:

- **B₁₀ figures** for electromechanical or pneumatic components. Here, life limit is determined by switching frequency. B₁₀ indicates the number of switching cycles until 10% of components fail.
- **Failure rate λ** (lambda value) for electronic components. Often the failure rate is stated in FIT (Failures In Time). One FIT is one failure per 10⁹ hours.



Diagnostics for fault detection

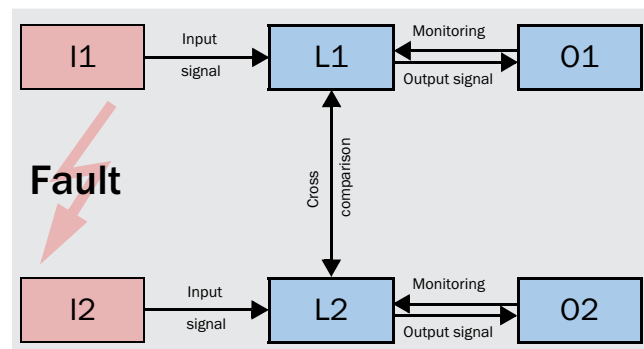
Certain faults can be detected by diagnostics measures. These include plausibility monitoring, current and voltage monitoring, watchdog functionality, brief function test, etc.

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 failures

The term "common cause failure" (CCF) 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.

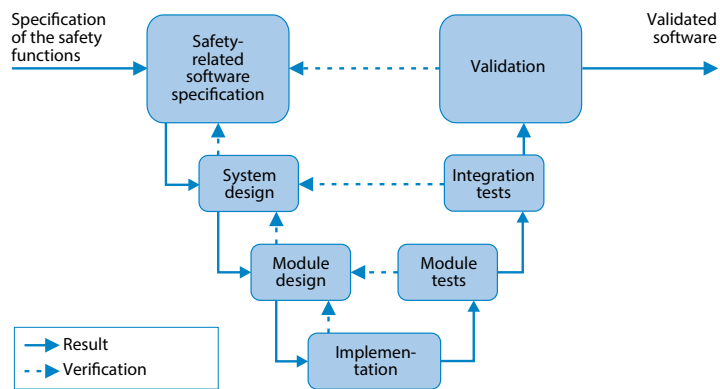


Process

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

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

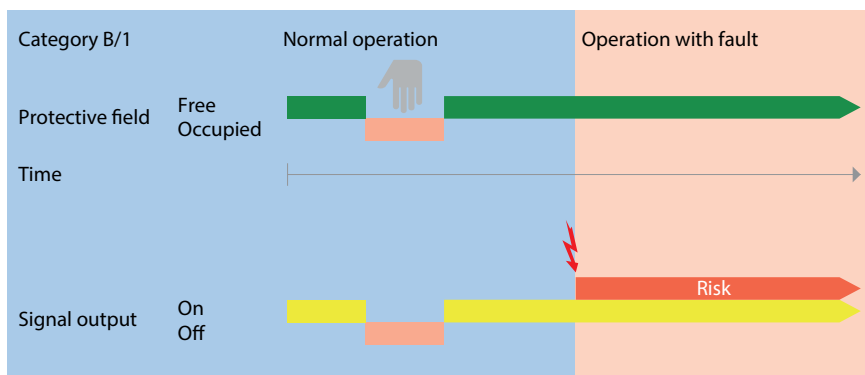
In the safety technology market, a process based on the V-model has proven particularly effective in practice for software design (see figure).



Architecture of safety systems

In ISO 13849-1, the safety-related architecture is interpreted with the aid of the categories. These basic principles are also retained in North American standards through the description of the system performance.

3
C

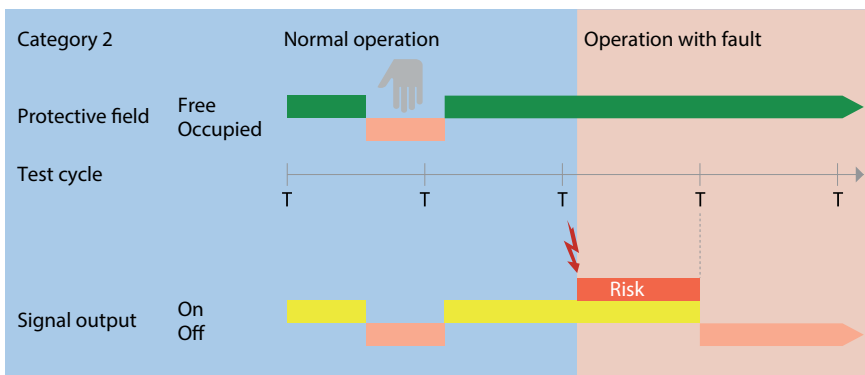


Category B/Category 1

Simple/single channel

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

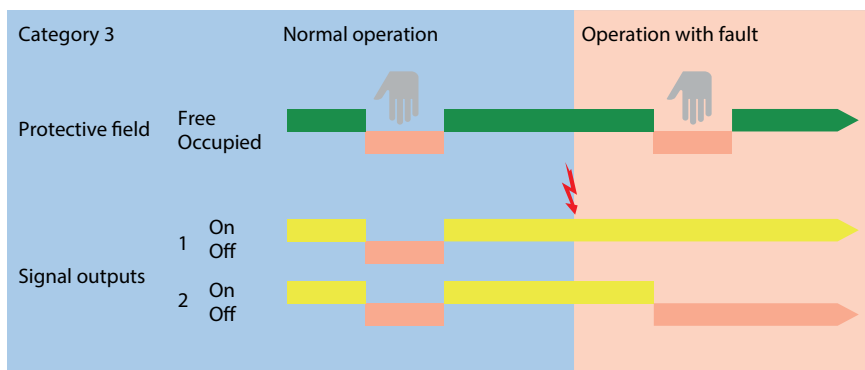
The risk can be minimized with reliable and proven components (Category 1).



Category 2

Single channel with monitoring

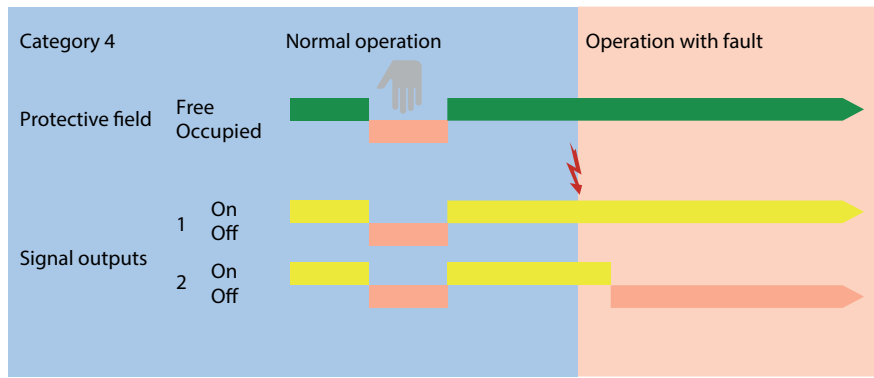
Faults are detected by carrying out a test. A risk prevails during the time between the occurrence of the fault and the next test. The test rate according to ISO 13849-1 shall be considered.



Category 3

Dual channel with monitoring (Control reliable)

In the event of a fault, the safety function is retained. The failure 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

Dual channel with multiple fault monitoring (Control reliable)

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).

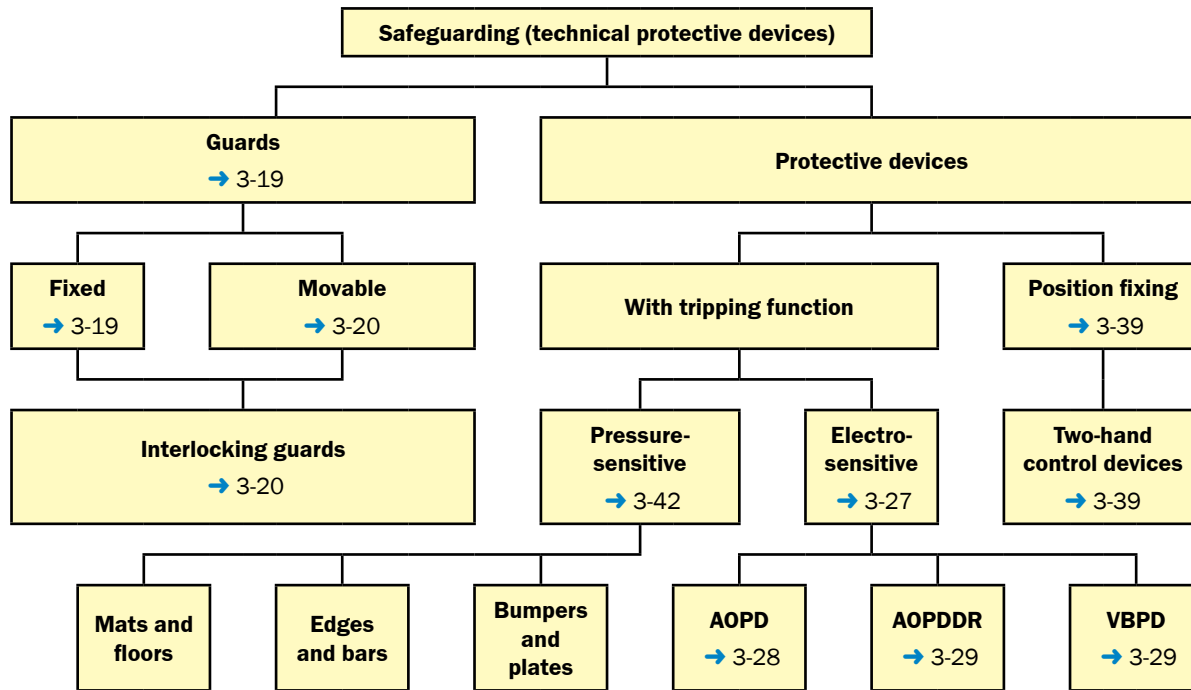
Characteristics of safeguarding

Characteristics of safeguarding to be considered are: The following sections describe these points in detail.

- Properties and applications of guards and protective devices (electro-sensitive, separating, etc. → 3-18)
- Position/dimension of guards and protective devices (→ 3-44)
- Integration of protective devices into the control system (→ 3-65)



Technology, selection, and use of safeguarding



Selection of the protective devices

The following table gives a simplified overview about advantages and disadvantages of the various protective devices and their possible misuse.

Protective Device	Parts can fly out / Radiation hazard	Frequent load/ unload activities	Multi operator protection	Machine can not be stopped safely / in time	Productivity	Maintenance free	Special Features *	Critical / foreseeable misuse
Fixed Guards	+	-	+	+	-	+	-	Removed, wrong dimensioning or location
Movable Guards	+	●	+	●	●	●	-	Easy defeat of interlock possible, wrong dimensioning or location
Opto-Electronic Devices	-	+	+	-	+	+	+	Wrong dimensioning or location, allowing reaching over /under, standing behind possible
Two-Hand Devices	-	●	-	-	●	●	-	Only one devices used for multi operator processes, wrong location
Mats, Bumpers	-	+	+	-	+	-	●	Defeated after mechanical defect, wrong dimensioning or location

* (Man / Material detection, use on mobile applications)

Explanation of symbols:

- = neutral
- + = preferred
- = not recommended

A comprehensive explanation about the features and the right use of the protective devices is described in the following sections.

- OSHA 3170-02R: Safeguarding Equipment and Protecting Employees from Amputations (→ www.osha.gov/Publications/osha3170.pdf)
- ANSI B11.19
- RIA TR R15.406

Guards

Guards are physical barriers, designed as part of the machine or installed around it, 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. Generally speaking, barriers are used to prevent access of individuals to the hazardous point, whereas shields are used to contain hazards which could be expelled or emitted from the hazardous point. In some applications, physical guards may be designed to fulfill the function of both a barrier and a shield.

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 life cycle of the machine.
- They shall not cause any additional hazards.
- 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 to the hazardous machine function.
- As far as possible, they should not remain in the protective position if unfastened.

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 personnel.

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

See ANSI B11.19 for additional requirements of vision/viewing panels expected to perform as a safeguard.

- Guards: ANSI B11.19, RIA TR R15.406, CSA Z432, NR-12, ISO 13857, ISO 14120
- Principles for safe machine design: ANSI B11.0, ISO 12100 (A-type standards)

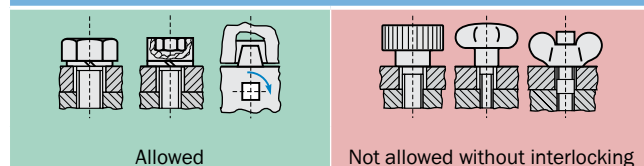
Mounting guards

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).

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



Adjustable physical guards

Adjustable guards provide a means of adapting the guard to the specific work piece or stock being introduced into the workspace. They must be kept in place with fasteners that make removal or opening impossible without the use of appropriate tools. These guards should not become a hazard between themselves and moving machine parts. While they

can be adapted to many types of operations, they may require frequent adjustments which may lead the operator to make them ineffective. These types of guards are not as secure and tamper resistance as a fixed guard but can offer the same level of protection if applied correctly.

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

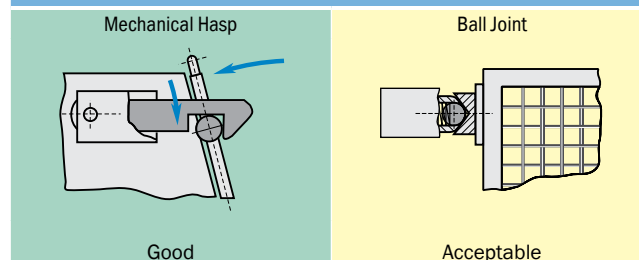
Ergonomic aspects are also significant during the design of protective devices. Guards will only be accepted by employees if they do not hinder setup, maintenance, and other similar activities any more than necessary. Movable guards must meet the following ergonomic criteria:

- 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



Interlocking of guards

Guards must be interlocked if they:











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

“Interlocking” means that the opening of the guard is converted into a control 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)

There are four types of interlocking devices associated with guards as described in ISO 14119:

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
	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 shall 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.

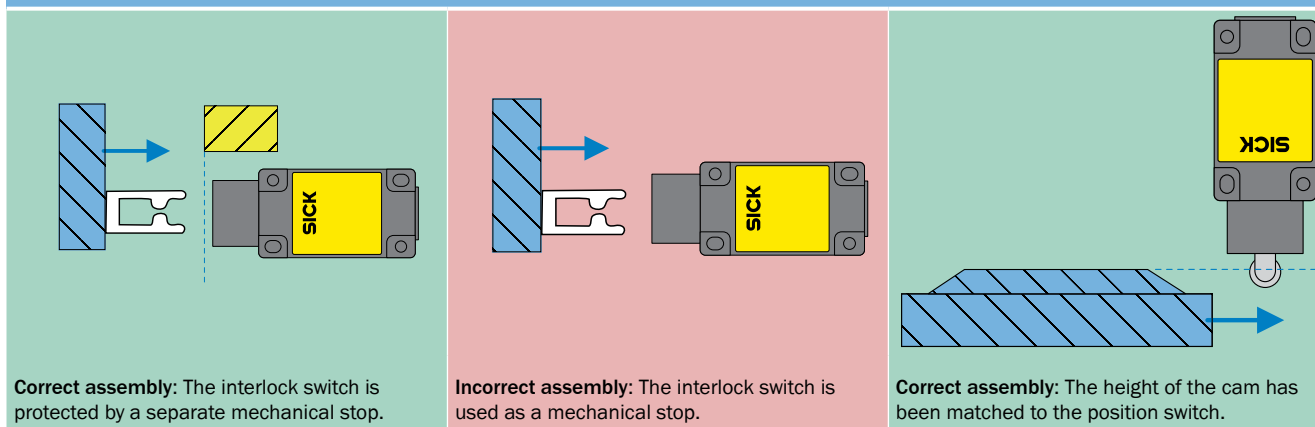
Depending on the technology of the position switch used and the functional safety requirements, either one or more interlocking devices will be required for a guard.

Mechanical attachment

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

- They shall be fitted such that they are protected against damage due to foreseeable external effects.
- They shall not be used as a mechanical stop.
- Their placement and design shall protect them against inadvertent operation and damage.
- They must be arranged, installed, 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.

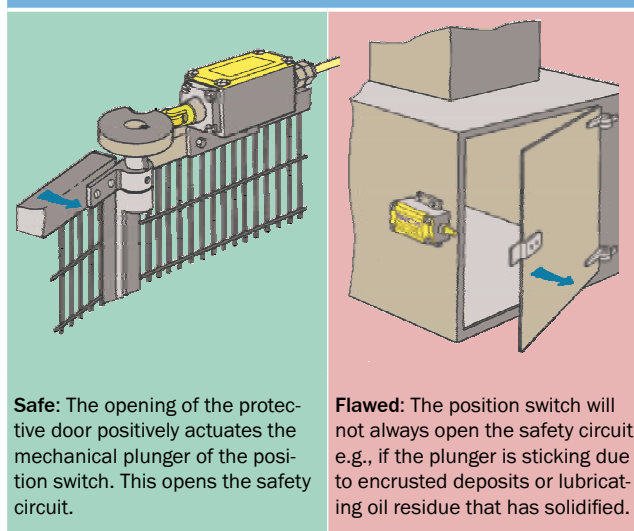
Example: Mechanical attachment of position switches



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 the possibility of manipulation.

Example: Positive mechanical actuation



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 the 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

Prevention of manipulation

When designing interlocking devices, designers shall consider the possible motivation for manipulation of the protective device and take 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 installation 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)



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

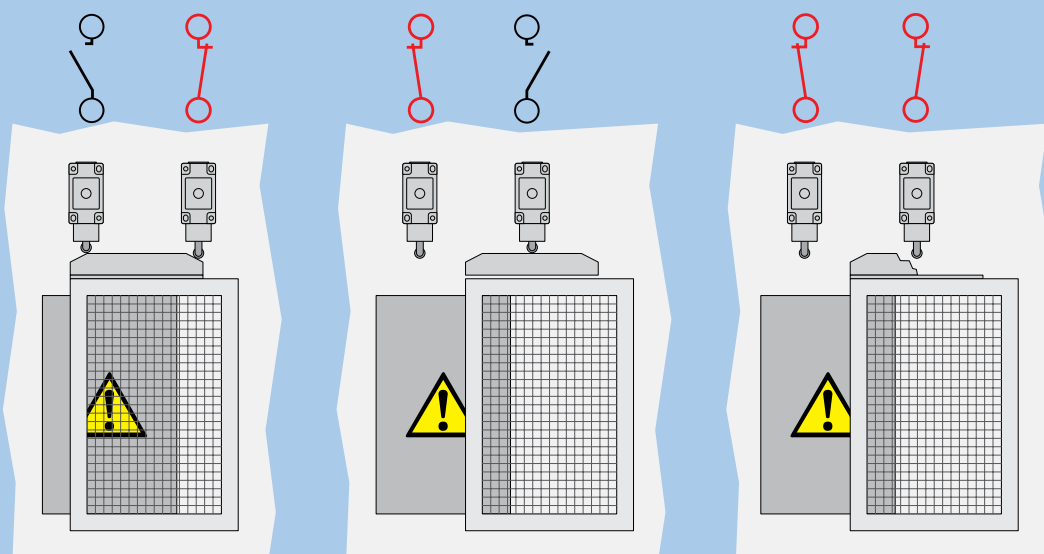
The use of both redundantly monitored electronic outputs from electro-sensitive position switches is considered equivalent to positive opening. If a Type 3 or Type 4 interlocking device is the only interlocking device on a guard, it must meet the requirements of IEC 60947-5-3.

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, which requires two mechanical switches.

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



Mechanical failure of actuator is detected by redundant diverse arrangement

Non-contact version

Non-contact interlocking devices are of redundant internal design or use special principles such as magnetic coding, inductive coupling, or transponders with codes.



- Requirements for safety switches/interlocking devices: ISO 14119, ANSI B11.19, RIA TR R15.406, CSA Z432, NR-12
- Principle of positive opening: IEC 60947-5-1
- Additional requirements for horizontal injection molding machines for the plastics industry: ANSI/SPI B151.1

Safety locking devices

The safety function “temporarily prevent access” is normally accomplished using locking devices. Locking devices are necessary if the dangerous movement takes a long time to stop (protection of personnel) or if a process is not allowed to be interrupted (process protection).

Safety locking devices are devices that prevent the opening of physical guards until there is no longer a risk of injury. Typically a differentiation is made between the following variants:

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 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.

Principle		By shape			By force	
Principle of operation	Actuation (locking)	Spring	Power ON	Power ON	Power ON	
	Locking	Power ON	Spring	Power ON	Power OFF	
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
- When used for safeguarding purposes, the time-control or automatic signal to release the locking device must come from a certified safety component

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


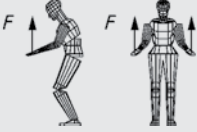
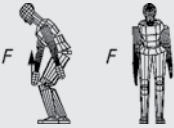
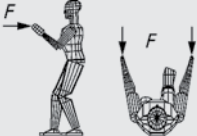
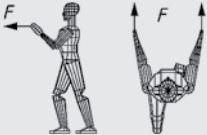
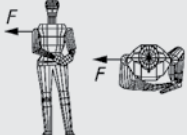

An essential criterion when selecting a locking device is the force required to hold the guard. Annex I of ISO 14119:2013 specifies maximum static forces that can be applied to the most commonly used movable guards.

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, signifying the guard is open. These contacts may be positive opening, but this is not always required.



Required holding force for guards according to Annex I of 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 grips	700

Trapped key systems

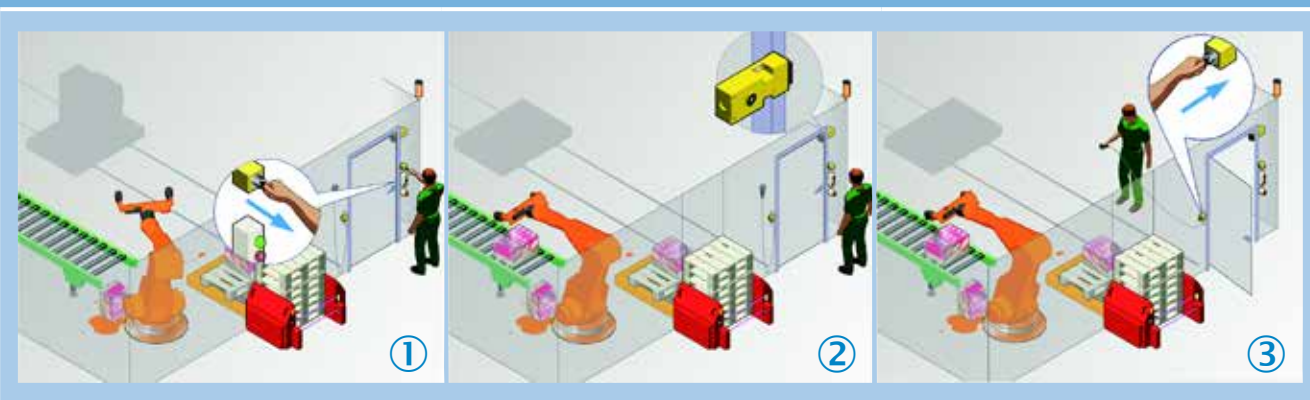
Guards have the disadvantage that after entering the hazard zone and the subsequent closing of the protective device, restarting cannot be effectively prevented. Additional measures are necessary, such as a reset device or the insertion of a U-lock in a Type 2 interlocking device actuator (referred to as an “interlock blocking device” in ANSI B11.19). These organizational measures are dependent, however, on the willingness or awareness of the user.

One possible way to prevent an unintentional start is trapped key systems in combination with interlocking devices. A key inserted outside the hazardous area enables automatic operation and keeps the door locked.

When the key is removed (Figure ①), the dangerous state is stopped. In the safe state (e.g., at standstill) the door can be opened (Figure ②). A key inserted in the interior can enable set-up operating modes (Figure ③). Automatic operation is disabled in this situation, even if the door is closed.

Note: These measures are not a substitute for Lock-Out/Tag-Out procedures because the interlocking device is typically not used as an energy isolation device.

Example: Trapped key system



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 standards IEC 61496-1, UL 61496-1, ANSI B11.19, RIA TR R15.406, and CSA Z432 define 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 people 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).

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 standards IEC 61496-2, UL 61496-2, ANSI B11.19, RIA TR R15.406, and CSA Z432 define safety requirements for AOPDs.

Typical AOPDs include single-beam and multiple light beam safety devices and safety light curtains. AOPDs with a capability to detect a body or arm and not a finger or hand are called multiple light beam safety devices. They are used to protect access to hazard zones (see figure). International standards define this as devices with a detection capability more than 40 mm, whereas North American standards define this limit as more than 64 mm.



Access protection with a multiple light beam safety device

AOPDs with a smaller detection capability (40 mm or less according to international standards, and 64 mm or less for North American standards) 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 (→ 3-37).

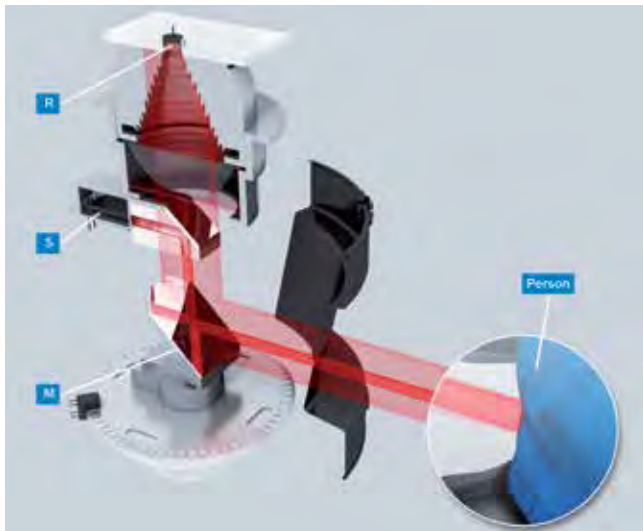
Safety laser scanners (AOPDDR)

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 below). 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 as well as 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 standards IEC 61496-3, ANSI B11.19, RIA TR R15.406, and CSA Z432 state the safety requirements for AOPDDRs.

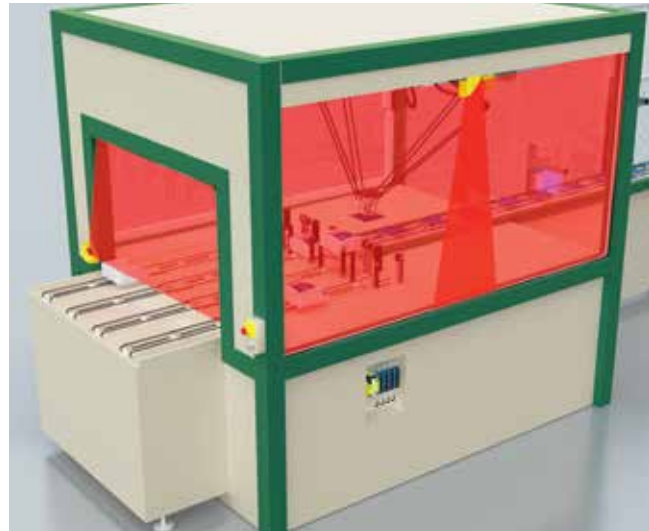
Vision-based protective devices (VBPD)

VBPDs are camera-based protective devices and use image capturing and processing technologies for safety detection of people (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 people, including:

- Interruption of the light 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 the size of the smallest object detected by the ESPE within the defined monitored area (protective field).

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

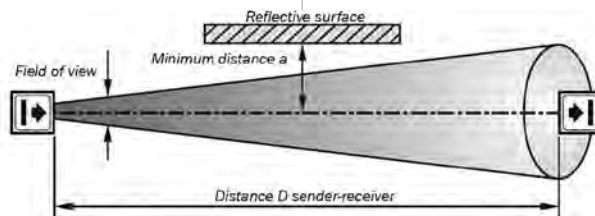
For safety laser scanners (AOPDDR), the detection capability is dependent upon the distance to the object, the angle between the individual beams of light (pulse), and the shape and size of the transmitted beam.

The reliability of the detection capability is determined by the type classification in the IEC 61496 and UL 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.

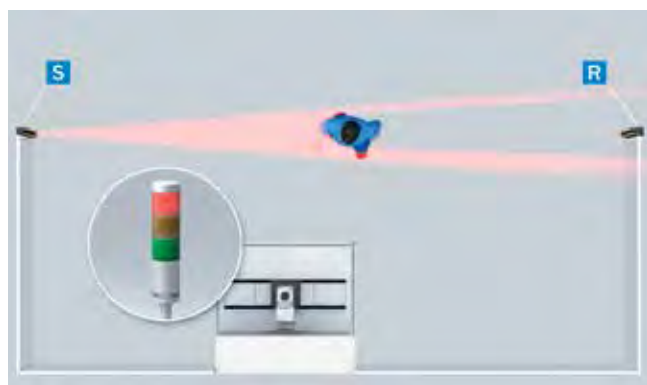
	Type 2	Type 4
Functional safety	The protective function may be lost if a fault occurs between test intervals	The protective function is maintained even if multiple faults occur
EMC (electromagnetic compatibility)	Basic requirements	Increased requirements
Maximum aperture angle of the lens	10°	5°
Minimum 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	$= \text{distance} \times \tan(10^\circ/2)$	$= \text{distance} \times \tan(5^\circ/2)$
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



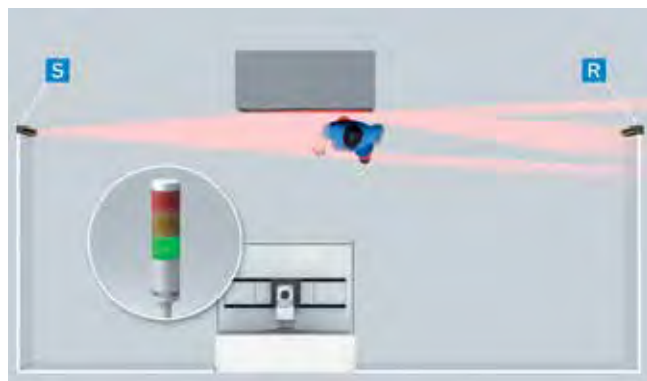
Main differences of type 2 and type 4 AOPDs according to IEC 61496 and UL 61496

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.



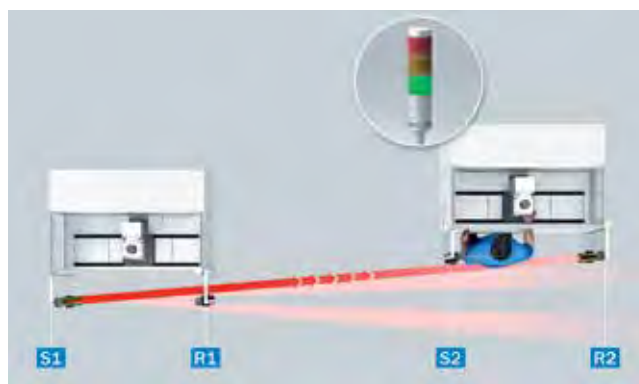
Reflection impedes detection by the ESPE and the hazardous movement is not stopped.

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" → 3-30).

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).



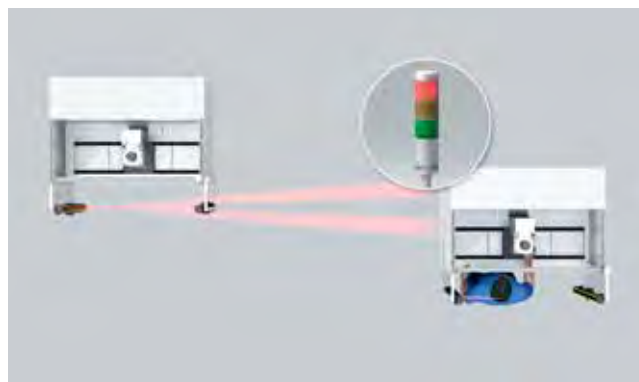
Mutual interference impedes detection by the ESPE and the hazardous movement is not stopped.

Installation 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 must 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 (detection capability)

What safety function is the ESPE expected to perform?

- Initiating a stop (→ 3-3)
- Avoiding unexpected startup (→ 3-4)
- Preventing start (→ 3-4)
- Combination: Initiating a stop and preventing start (→ 3-4)
- Allowing material passage (→ 3-5)
- Monitoring machine parameters (→ 3-5)
- Indications and alarms that are relevant to safety (→ 3-7)
- Other functions, e.g., PSDI mode, blanking, protective field switching, etc. (→ 3-37)

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 behavior 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, → 3-30).

→ Requirements to be met by ESPE: IEC 61496-1, UL 61496-1, IEC 61496-2, UL 61496-2, IEC 61496-3, IEC TR 61496-4, ANSI B11.19, RIA TR R15.406, and CSA Z432

Achievable reliability of safety functions with optoelectronic protective devices

		ISO 13849-1 (PL)					Example devices
		a	b	c	d	e	
ESPE type according to IEC 61496-1 and UL 61496-1	2						Safety light curtains, single-beam photoelectric safety switches, multiple light beam safety devices
	3						Safety laser scanners, safety camera systems
	4						
		1		2	3		
		IEC 62061 (SIL)					

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

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.

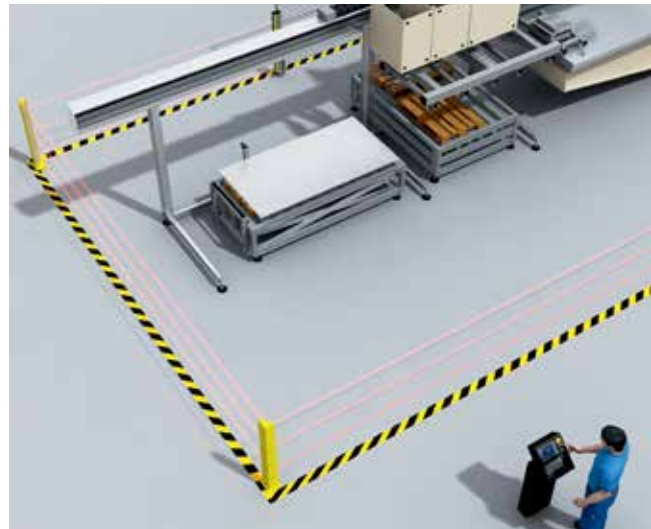
The advantage of this type of protective device is that it allows short minimum distance and the operator can work more ergonomically (e.g., during loading work on a press).



Access protection: Detection of a person on access to the hazard zone

In the case of access protection, the approach of a person is detected by detecting the body.

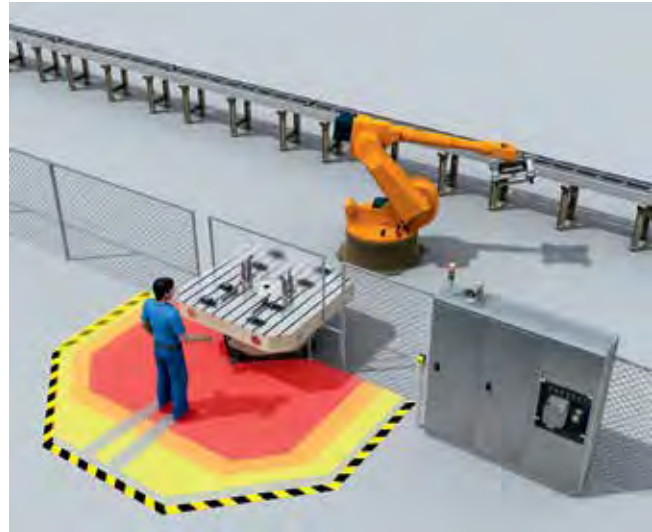
This type of protective device is used for protection of access to hazard zones. A stop signal is initiated if the hazard zone is entered. A person who is standing behind the protective device will not be detected by the ESPE!



Hazard area protection: Detection of the presence of a person in the hazard area

In the case of hazard 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 hazard area cannot be viewed completely from the position of the reset device. If the hazard area is entered, a stop signal is initiated and starting prevented.

**Mobile hazard area protection: Detection of a person approaching the hazard area**

Hazard area protection is suitable for AGV (automated guided vehicle), cranes and stackers, to protect people 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 trespassed) 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, such that 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, interlock, 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, ANSI B11.19, RIA TR R15.406, CSA Z432, NR-12

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 and any unmonitored areas are small enough to prevent undetected access to the hazard zone (see figure).

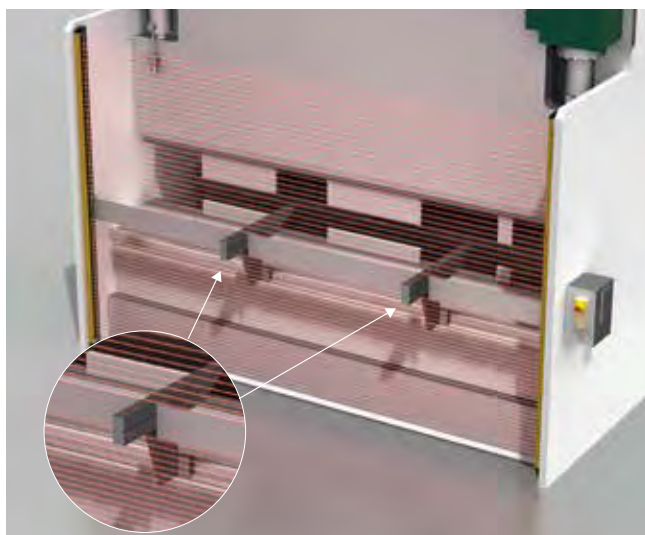


Material throughput with safety laser scanners, vertical protective fields, and protective field switching with suitably arranged sensors.

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).



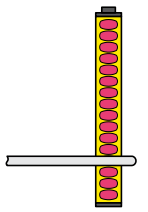
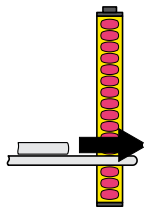
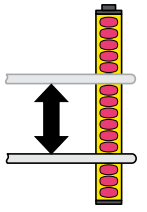
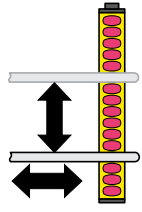
Fixed blanking of light curtain beams on a trimming press.

In the blanked area, the resolution capability of the ESPE is enlarged (deteriorates). Take this 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).

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).

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 <i>fixed size must</i> be at a specific point in the protective field.	On one side of the fixed blanking an object of <i>limited size is allowed</i> to move through the protective field.	An object of <i>fixed size must</i> be within a specific area of the protective field. The object is allowed to move.	An object of <i>limited size</i> is allowed in a specific area of the protective field. The object is allowed to move.
			



PSDI mode

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

Conforming to international standards, PSDI mode can only be executed with type 4 AOPDs and an effective resolution $d \leq 30$ 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 or mechanical obstruction).

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 trespassable. For presses, special conditions apply for PSDI mode.



Single break PSDI mode on an automatic assembly system with a safety light curtain. During loading, the tool is in the open position. After the operator leaves the protective field, the assembly cycle begins.

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

According to OSHA 29 CFR 1910.217 at the time of printing, PSDI is not allowed on mechanical power presses in the U.S. or U.S. territories.

Please check your local authority for applicability of PSDI.

- PSDI mode: B-type standards ANSI B11.19, CSA Z432, ISO 13855, IEC 61496-1, UL 61496-1
- PSDI mode on presses: C-type standards OSHA 1910.217, ANSI B11.1, ANSI B11.2, ANSI B11.3, CSA Z142, NR-12, EN 692, EN 693
- PSDI mode on robots: C-type standards RIA TR R15.406, CSA Z434

Fixed position protective devices

Fixed position 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 fixed position protective devices is given in:

- Alfred Neudörfer: Konstruieren sicherheitsgerechter Produkte (Designing Safety-related Products), Springer-Verlag, Berlin u. a., ISBN 978-3642191886 (4th Edition 2011)

Two-hand controls

A two-hand control only protects one person! If there are several operators, each person must actuate a separate 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 by location, orientation, and/or shrouding 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 closer to the hazard zone than the permitted safe mounting distance
- When more than one operator is provided with a two-hand control, all actuating devices (pushbuttons) must be actuated concurrently to initiate hazardous machine functions

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

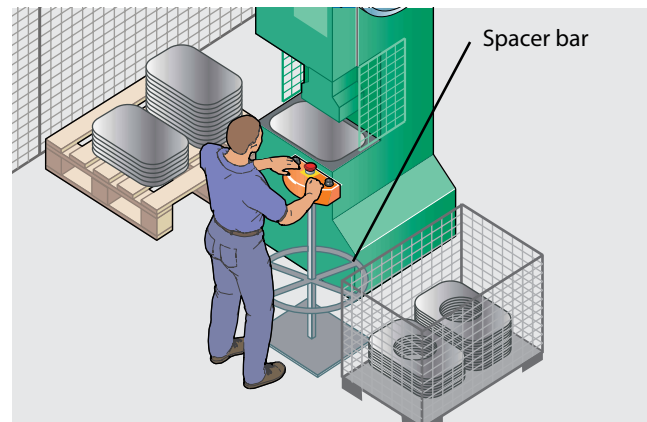
The following provisions also apply in the case of type III two-hand controls:

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

In North America, the functional requirements equivalent to type III described above are required when two-hand controls are intended to protect people from machine hazards.

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



Spacer bar

→ Requirements to be met by two-hand controls:

ISO 13851, OSHA 1910.217, ANSI B11.19, NFPA 79, RIA TR R15.406, CSA Z32, NR-12

→ See 3-63 for information about calculating the minimum distance for two-hand controls.

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 which obtain the operator's acknowledgement before allowing machine functions. 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 and are required by most North American standards.



These measures are not a substitute for Lock-Out/Tag-Out procedures.

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 reactivated 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.

The selection of activating an enabling device must be capable of supervisory control (e.g., keyswitch, password) to prevent unauthorized selection or de-selection while in use. When an enabling device is in use, the machine control systems must ensure that only one actuating control can initiate hazardous machine function.

When multiple people are in the hazard zone when protective devices are disabled, each person must have their own enabling device, and each selected device must be concurrently operated before hazardous machine functions can be initiated.

The means of returning the machine control to the operating mode must be located outside of the hazard zone such that it cannot be reached from within the hazard zone to ensure the hazard zone is clear of individuals.

Protection against manipulation shall be considered when using enabling devices.

→ Requirements for enabling devices: ANSI B11.19, ANSI/ASSE Z244.1, CSA Z432, NR-12, NFPA 79, IEC 60204-1 (B-type standards)

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 (→ 3-5).

Electro-sensitive safety inductive position switches are particularly suitable for this task. They monitor a certain part of the process (e.g., 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.



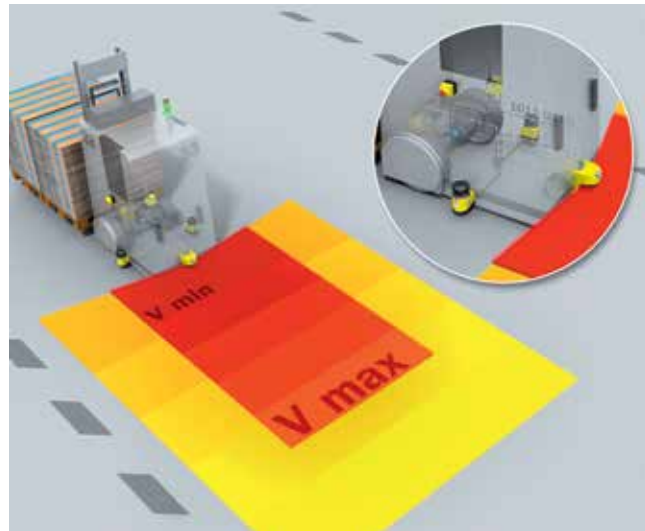
Safe position monitoring for a lift on an automobile production line

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.



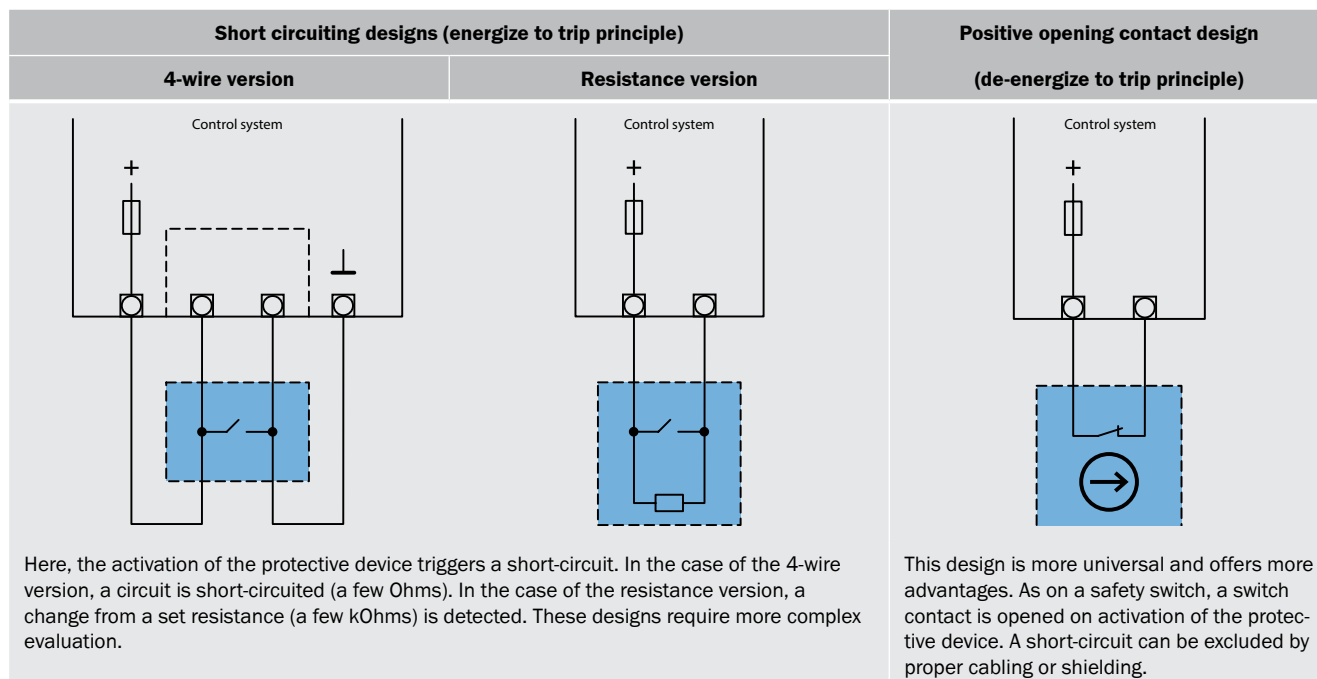
Speed monitoring for protective field switching on an automated guided vehicle

Mats and floors, 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.



→ Requirements of pressure sensitive protective devices: ANSI B11.19, RIA TR R15.406, CSA Z432, ISO 13856 series (B-type standards)

Foot switches (when not used for emergency stop)

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
- After the hazardous machine function has been stopped, restarting via the foot switch is only permitted after releasing and actuating the foot switch again
- If there are several operators, each shall actuate a separate switch

Some international standards include additional requirements, such as:

- A 3-position design similar to the enabling switch principle (see "Principle of operation of the 3-position enabling device" → 3-40)
- A means of manual reset upon actuation of the actuator beyond the pressure point
- Evaluation of at least one normally open contact and one normally closed contact

→ Requirements for foot switches: NFPA 79

Complementary protective measures

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

These might include:

- Emergency stop devices (→ 3-7)
- Measures to free and rescue people who have become trapped
- Measures for isolating and dissipating hazardous energy (→ 2-10)

- 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 section "Design of the safety function" → 3-13).

Actions in an emergency

Emergency stop (shut down in an emergency)

In an emergency it is not just necessary to stop all dangerous movements, sources of energy that produce hazards, e.g. stored energy shall be safely dissipated. This action is termed "emergency stop."

- Emergency stop devices shall be easy to reach and be accessible from all directions.
- Emergency stop devices shall end a dangerous state as quickly as possible without producing additional risks.
- The emergency stop command shall have 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 latching function shall be applied.
- The emergency stop shall be made as per stop Category 0 or 1.

Emergency switching off

If there is a possibility of hazards or damage due to electrical power, emergency switching off should be provided. Here the supply of power is shut down using electromechanical switchgear.

- It shall only be possible to switch on the supply of power after all emergency switching off commands have been reset.
- As a result, emergency switching off is stop Category 0.

Reset after emergency stop

If a device for use in an emergency is actuated, devices triggered by this action shall remain in the off state until the device for use in an emergency has been reset.

The reset of the emergency device shall be done manually at the specific location. The reset shall only prepare the machine to be put back in operation and not restart the machine.

Emergency stop and emergency switching off are additional measures but 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 device shall be positive opening normally closed contacts. The emergency stop device shall be red and any background shall be yellow. Examples:

- Switches actuated with mushroom head pushbuttons
- Switches actuated with wires, ropes or rails
- Foot switches without covers (for emergency stop)

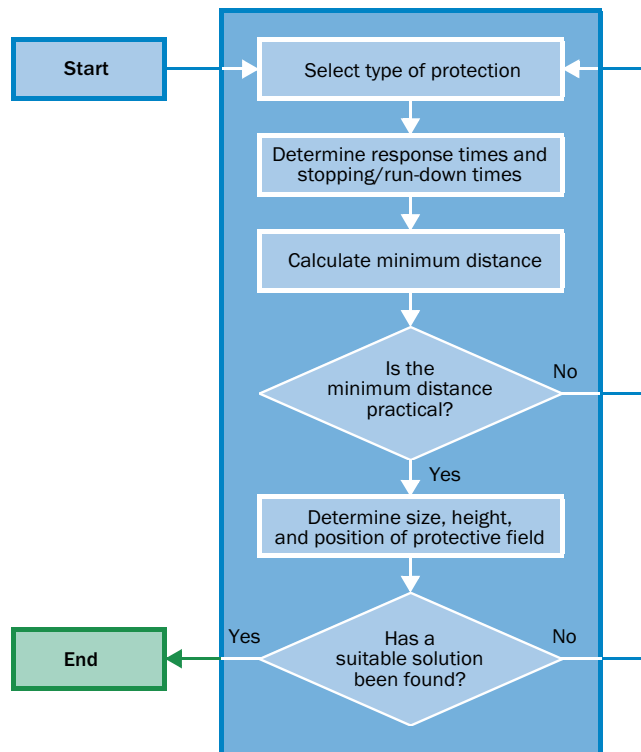
If wires and ropes are used as actuating elements for emergency devices, they shall be designed and fitted such that they are easy to actuate and when pulled or the wire/rope is cut. Reset mechanisms should be arranged in the manner that the entire length of the wire or rope is visible from the location of the reset mechanism.

- Design principles and requirements for emergency stop: NFPA 79, IEC 60204-1, ANSI B11.19 and ISO 13850
- See also section: "Emergency stop" (→ 3-7)
- Emergency operations: Machinery Directive 2006/42/EC

Positioning and dimensioning of protective devices

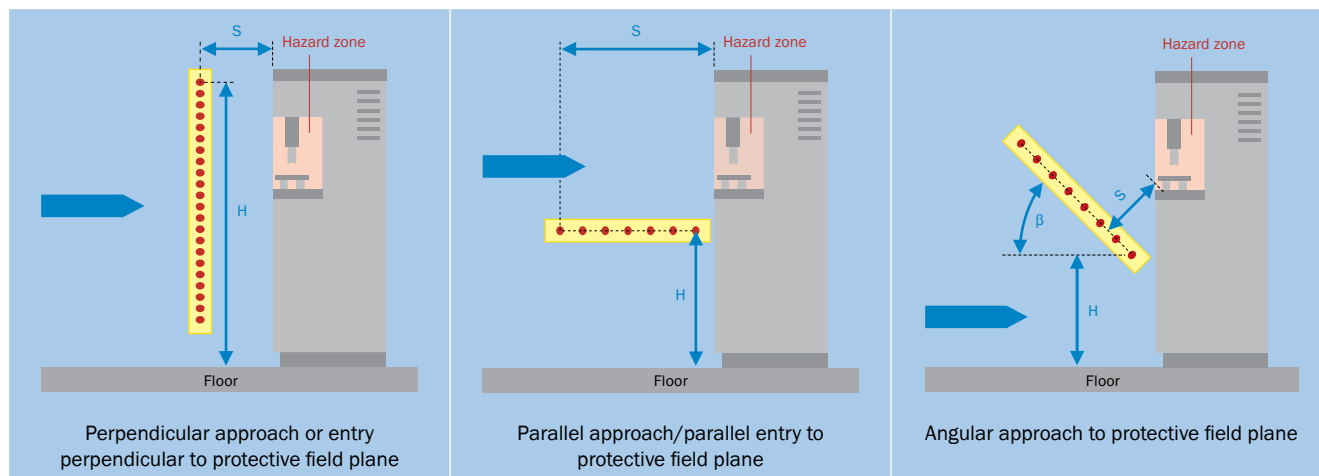
One essential aspect for the selection of an optimal protective device is the space available. It must be ensured that the dangerous state can be eliminated in time before the hazardous point is reached.

The necessary minimum distance is dependent on, among other aspects, the size and type of the protective device.



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.



After the ESPE has been selected for the safety function “initiating a stop,” 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 or response time shall be chosen. The possibility of someone standing between the protective field and the hazard zone shall be prevented.

→ Calculation of the minimum distance for an ESPE:
 OSHA 1910.217, ANSI B11.19, RIA TR R15.406,
 CSA Z432, NR-12, ISO 13855

Two similar calculations exist to accurately determine the appropriate minimum distance of safeguarding devices; one in North America and another in International standards. When applied accurately, either method has proven reliable.

Users and integrators should consider all local and regional regulatory requirements and consensus standards when selecting which methodology to apply.

General calculation formulas

North America:

$$D_s = (K \times T) + D_{pf}$$

Europe / International:

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

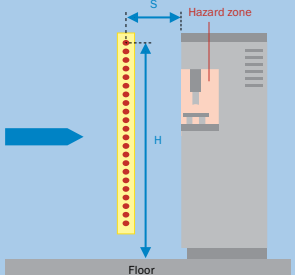
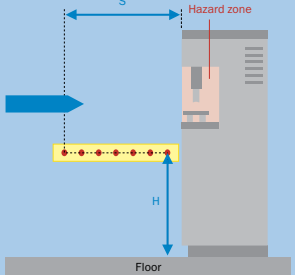
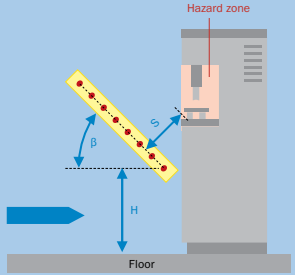
The table on pages 3-46 and 3-47 contains the formulas for the calculation of the factors to consider for determining the minimum distance, where:

- β is the angle between the detection plane and the approach direction
- H is the height of the protective field (detection plane) above the working surface
- d is the resolution of the ESPE (detection capability)

Where:

- D_s or 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
- D_{pf} or 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, the additional distance 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, the additional distance is determined by the height of the protective field and is referred to as C_{RO} (reach over).

NOTE: The resolution value d is also referred to as S or O_s in North American standards. For the examples in the table, the variable d will be used exclusively.

North America (based on ANSI B11.19, RIA TR R15.406, and CSA Z432)																									
Approach	Detection capability, d (resolution/object sensitivity)	Beam height, H (distance from floor)	Intrusion Factor, D _{pf}	Depth of field	Minimum Distance																				
Perpendicular: β = 90° (±5°) 	Finger/hand detection: d ≤ 64 mm	Calculation of the minimum height of the highest beam depending on the distance to the hazard zone (→3-56)	$D_{pf} = 3.4 \times (d - 7 \text{ mm})$	Not Applicable	$D_S = (K \times \sum T_{total}) + D_{pf}$ where K = 1600 mm/s																				
	Arm detection: 64 mm < d ≤ 600 mm	Height of the bottom beam ≤ 300 mm Height of highest beam ≥ 1200 mm	$D_{pf} = 900 \text{ mm}$																						
	Body detection: 64 mm < d ≤ 600 mm	Height of the bottom beam ≤ 300 mm Height of highest beam ≥ 900 mm	$D_{pf} = 1200 \text{ mm}$																						
Parallel: β = 0° (± 5°) 	Example of common detection capabilities:	Detection field height is determined by device resolution based on formula: H ≥ 15 (d - 50 mm) Where: 0 ≤ H ≤ 1000 mm	$D_{pf} = 1200 \text{ mm}$	Minimum depth of field (sensing area) addresses a different installation consideration than the penetration factor (D _{pf}) and must also be considered. The minimum depth of field must hinder an individual from stepping over the detection plane. If an individual can step over and pass unrestricted, minimum depth of field ≥ 1200 mm If supplemental safeguarding or physical barriers are used such that an individual must stand within the sensing area, minimum depth of field ≥ 900 mm	$D_S = (K \times \sum T_{total}) + D_{pf}$ where K = 1600 mm/s																				
	<table border="1"> <tr> <td>d = 14 mm</td> <td>0 mm</td> <td>1000 mm</td> </tr> <tr> <td>d = 20 mm</td> <td>0 mm</td> <td>1000 mm</td> </tr> <tr> <td>d = 24 mm</td> <td>0 mm</td> <td>1000 mm</td> </tr> <tr> <td>d = 30 mm</td> <td>0 mm</td> <td>1000 mm</td> </tr> <tr> <td>d = 34 mm</td> <td>0 mm</td> <td>1000 mm</td> </tr> <tr> <td>d = 40 mm</td> <td>0 mm</td> <td>1000 mm</td> </tr> <tr> <td>d = 50 mm</td> <td>0 mm</td> <td>1000 mm</td> </tr> <tr> <td>d = 70 mm</td> <td>300 mm</td> <td>1000 mm</td> </tr> </table>	d = 14 mm				0 mm	1000 mm	d = 20 mm	0 mm	1000 mm	d = 24 mm	0 mm	1000 mm	d = 30 mm	0 mm	1000 mm	d = 34 mm	0 mm	1000 mm	d = 40 mm	0 mm	1000 mm	d = 50 mm	0 mm	1000 mm
d = 14 mm	0 mm	1000 mm																							
d = 20 mm	0 mm	1000 mm																							
d = 24 mm	0 mm	1000 mm																							
d = 30 mm	0 mm	1000 mm																							
d = 34 mm	0 mm	1000 mm																							
d = 40 mm	0 mm	1000 mm																							
d = 50 mm	0 mm	1000 mm																							
d = 70 mm	300 mm	1000 mm																							
Angular : 5° < β < 85° 	If β > 30°, use the perpendicular approach defined above. If β < 30°, use the horizontal or parallel approach defined above. The minimum distance is based on the beam closest to the hazardous point. H ≥ 15 (d - 50 mm) refers to the lowest beam.				$D_S = (K \times \sum T_{total}) + D_{pf}$ where K = 1600 mm/s																				

Important note: Under no circumstances shall it be possible to reach the hazard. See → 3-55 for more information.

Europe / International (based on ISO 13855 and NR-12)			
Detection capability, d (resolution/object sensitivity)	Beam height, H (distance from floor)	Intrusion Factor, C	Minimum Distance
Finger/hand detection: d ≤ 40 mm	Calculation of the minimum height of the highest beam depending on the distance to the hazard zone (→ 3-56)	C = 8 x (d - 14 mm)	$S = (K \times \sum T_{total}) + C$ where K = 2000 mm/s . In this case, S shall be ≥ 100 mm. If S > 500 mm, then use: $S = (K \times \sum T_{total}) + C$ where K = 1600 mm/s . In this case, S cannot be < 500 mm.
Arm detection: 40 mm < d ≤ 70 mm	Height of the bottom beam ≤ 300 mm	C = 850 mm	$S = (K \times \sum T_{total}) + C$ where K = 1600 mm/s
	Height of highest beam ≥ 900 mm		
Body detection: d > 70 mm	Number of beams: Recommended heights: 4 300, 600, 900, 1200 mm 3 300, 700, 1100 mm 2 400, 900 mm	C = 850 mm	$S = (K \times \sum T_{total}) + C$ where K = 1600 mm/s
	(400 mm can only be used if there is no risk of crawling beneath the lowest beam.)		
Example of common detection capabilities:	Detection field height is determined by device resolution based on formula: H ≥ 15 (d - 50 mm) Where: 0 ≤ H ≤ 1000 mm		$S = (K \times \sum T_{total}) + C$ where K = 1600 mm/s
	Min. permissible height (where 0 mm is the working surface): d = 14 mm 0 mm d = 20 mm 0 mm d = 24 mm 0 mm d = 30 mm 0 mm d = 34 mm 0 mm d = 40 mm 0 mm d = 50 mm 0 mm d = 70 mm 300 mm d > 117 mm not permitted as a primary safeguarding device	Max. permissible height: 1000 mm 1000 mm 1000 mm 1000 mm 1000 mm 1000 mm 1000 mm 1000 mm	
		C = 1200 mm - (0.4 x H) In this case, C shall be ≥ 850 mm.	
If β > 30°, use the perpendicular approach defined above. If β < 30°, use the horizontal or parallel approach defined above. The minimum distance is based on the beam closest to the hazardous point and ≤ 1000 mm in height. H ≥ 15 (d - 50 mm) refers to the lowest beam.			$S = (K \times \sum T_{total}) + C$ where K = 1600 mm/s



Important note: Under no circumstances shall it be possible to reach the hazard. See →3-55 for more information.

Special cases

Press application

Unlike general standards, machine-specific C-type standards can contain special requirements.

In particular for metal-working presses, the following requirements apply when following European and International standards:

Calculation of the supplemental intrusion factor for presses

Resolution d of the ESPE	Supplement C	Stroke initiation by ESPE/PSDI mode
$d \leq 14 \text{ mm}$	0 mm	Allowed
$14 \text{ mm} < d \leq 20 \text{ mm}$	80 mm	
$20 \text{ mm} < d \leq 30 \text{ mm}$	130 mm	
$30 \text{ mm} < d \leq 40 \text{ mm}$	240 mm	Not allowed
$40 \text{ mm} < d$	850 mm	

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

ESPE for presence detection

This type of protection is recommended for large systems that are accessible from the working surface (floor). In this special case, starting of the machine ("preventing start" safety function → 3-4) must be prevented while there is an operator inside.

This is a secondary protective device which detects the presence of people 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 (→ 3-3), 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 machine as safety function position 1, initiating a stop and safety function position 2, preventing unexpected start

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 people. 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., three-position foot switch, automatic stopping performance measurement, etc.).

→ Safety of hydraulic press brakes: ANSI B11.3, CSA Z142, NR-12, EN 12622

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.

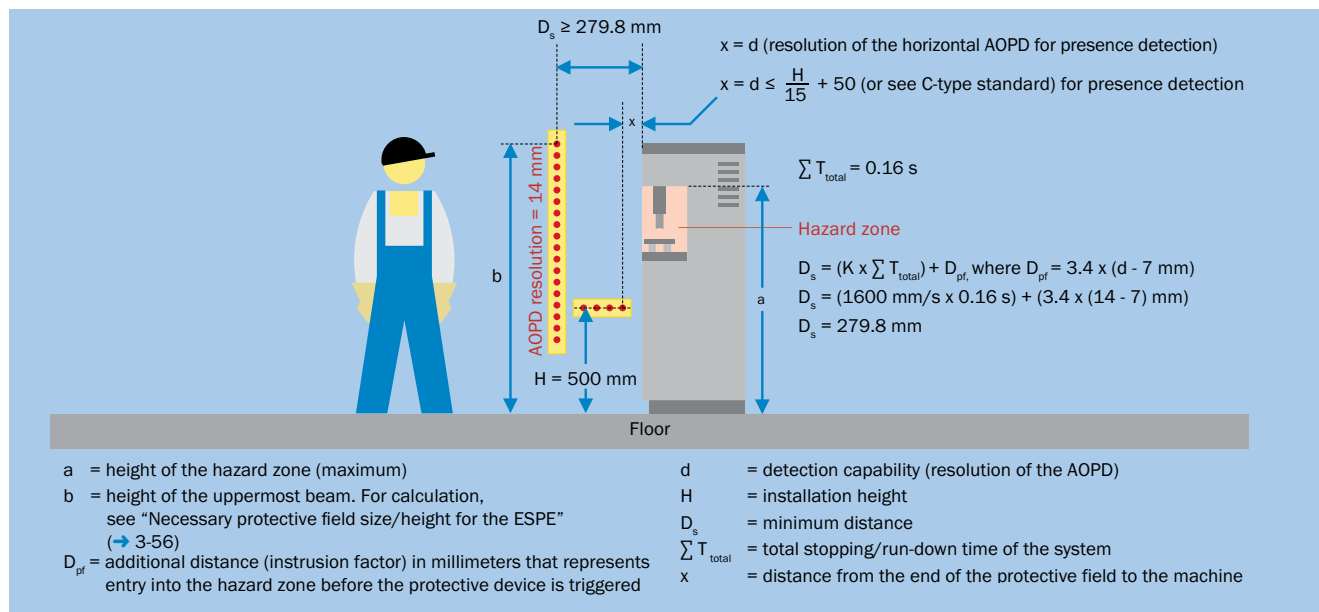
Examples for calculating the minimum distance

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

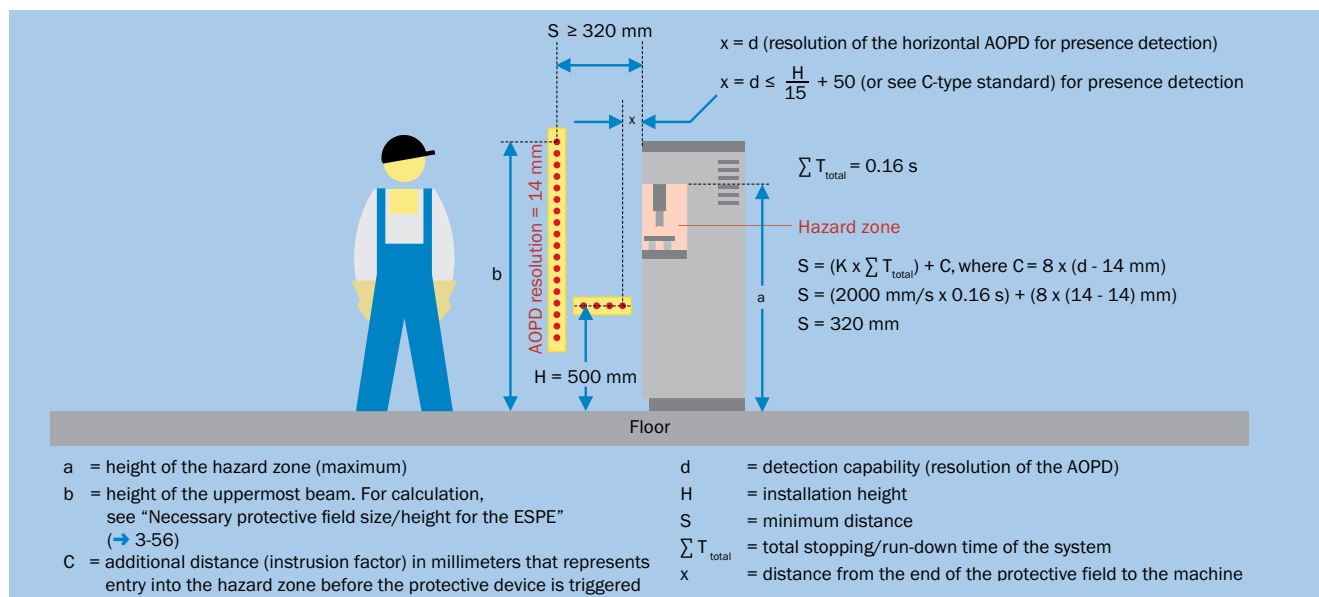
The calculations, as shown in the figures, yield different minimum distances depending on which approach is applied. In either case, the optimal minimum distance is achieved by using a safety light curtain with the best possible combination of resolution and response time.

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.

Perpendicular Approach using North American Calculation



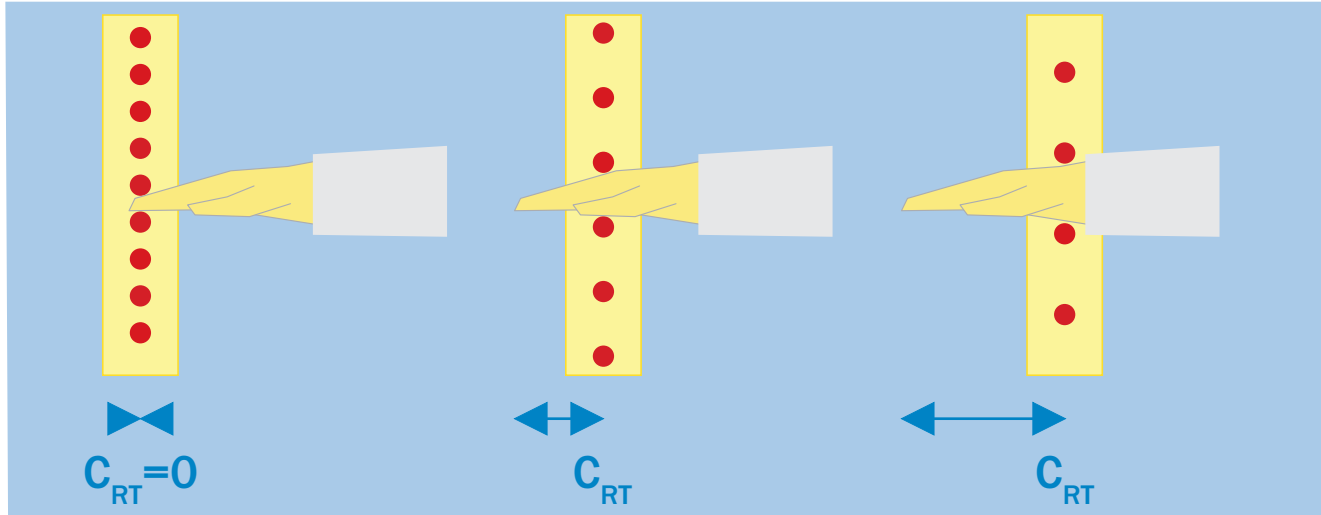
Perpendicular Approach using EN/ISO Calculation



Supplement determined by resolution

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. This value is referred to as C_{RT} in European and International standards, or as D_{pf} in North American standards.



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

Solution 2: Parallel approach — hazardous area protection

A horizontal AOPD is used. The figures below show the calculations of the minimum distance and the positioning of the AOPD. With an installation height of 500 mm, an AOPD with a resolution less than or equal to 83.33 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.

Parallel Approach using North American Calculation

The diagram illustrates a worker on the left and a machine on the right. A horizontal AOPD is positioned at a height $H = 500\text{ mm}$ from the floor. The AOPD resolution is 80 mm . The distance from the end of the protective field to the machine is x . The minimum distance is $D_s \geq 1456\text{ mm}$. The formula for x is $x = d \leq \frac{H}{15} + 50$ (or see C-type standard). The total stopping/run-down time is $\sum T_{total} = 0.16\text{ s}$. The hazard zone is indicated by a red box on the machine. The calculation for D_s is shown as follows:

$$D_s = (K \times \sum T_{total}) + D_{pf}$$

where $D_{pf} = 1200\text{ mm}$

$$D_s = (1600\text{ mm/s} \times 0.16\text{ s}) + 1200\text{ mm}$$

$$D_s = 1456\text{ mm}$$

Legend:

- D_{pf} = additional distance (intrusion factor) 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
- D_s = minimum distance
- $\sum T_{total}$ = total stopping/run-down time of the system
- x = distance from the end of the protective field to the machine

Parallel Approach using EN/ISO Calculation

The diagram is similar to the North American calculation but uses different formulas. The worker, AOPD, and machine are shown with the same dimensions ($H = 500\text{ mm}$, AOPD resolution = 80 mm). The distance from the end of the protective field to the machine is x . The minimum distance is $S \geq 1256\text{ mm}$. The formula for x is $x = d \leq \frac{H}{15} + 50$ (or see C-type standard). The total stopping/run-down time is $\sum T_{total} = 0.16\text{ s}$. The hazard zone is indicated by a red box on the machine. The calculation for S is shown as follows:

$$S = (K \times \sum T_{total}) + C$$

where $C = 1200\text{ mm} - (0.4 \times H) \geq 850\text{ mm}$

$$S = (1600\text{ mm/s} \times 0.16\text{ s}) + (1200\text{ mm} - (0.4 \times 500\text{ mm}))$$

$$S = 1256\text{ mm}$$

If the installation height (H) of the AOPD is decreased, the minimum distance is increased.

Legend:

- C = additional distance (intrusion factor) 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
- $\sum T_{total}$ = total stopping/run-down time of the system
- x = distance from the end of the protective field to the machine

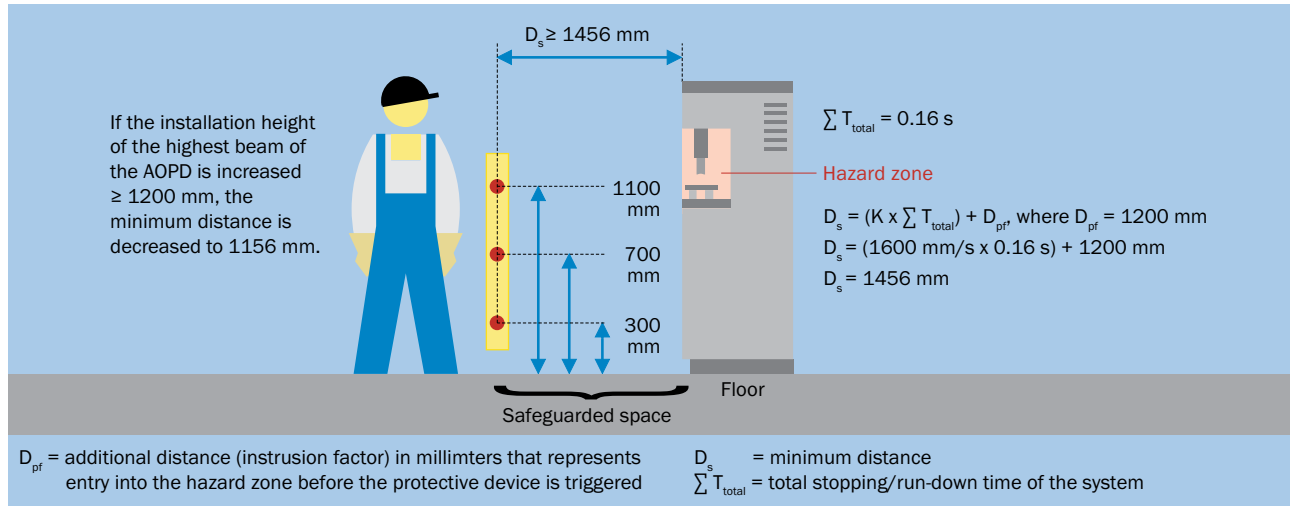
3
C

Solution 3: Access protection

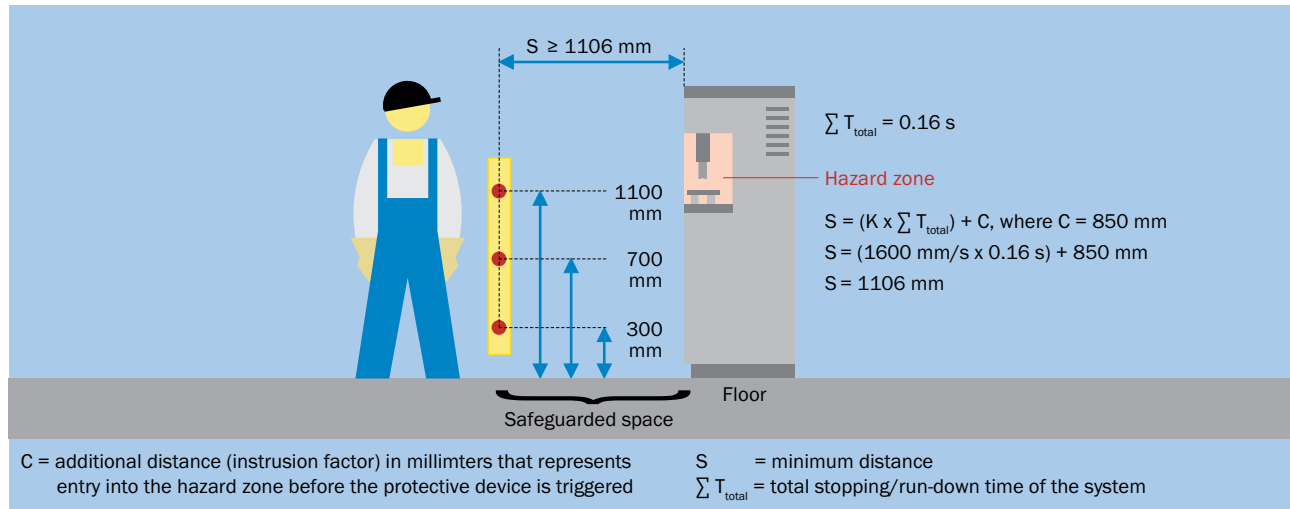
Access protection with 3 beams (at heights of 300 mm, 700 mm, and 1100 mm) allows perpendicular approach, and permits the operator to reach over the detection field undetected toward the hazard. This solution also allows the operator to stand between the hazard zone and the AOPD without being

detected. For this reason, additional safety measures shall be applied to reduce this risk. The control device (e.g., a reset pushbutton) shall be positioned so that the entire hazard zone can be overseen. It shall not be possible to reach the button from inside the safeguarded space.

Access protection using North American calculation



Access protection using EN/ISO calculation

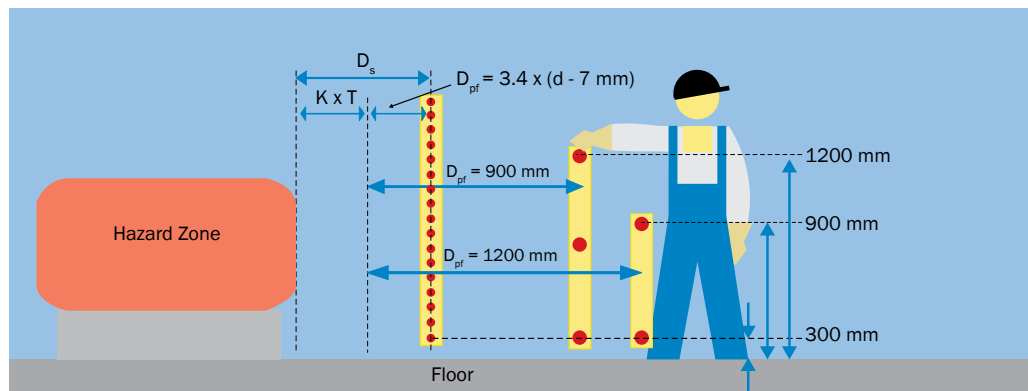


Comparison of the results

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

Solution	Minimum distance for stopping/run-down time = 0.16 s		Advantages	Disadvantages
	North American calculations	European / International calculations		
1 – Hazardous point protection	$D_s \geq 279.8 \text{ mm}$	$S \geq 320 \text{ mm}$	<ul style="list-style-type: none"> Increased productivity, as the operator is closer to the work process (short paths) Protection on several sides possible using deflector mirrors Automatic start possible PSDI mode possible when permitted by local regulations and C-type standard (mirrors not permitted) Very little space required 	<ul style="list-style-type: none"> Higher price for the protective device due to good resolution and presence detection
2 – Hazardous area protection	$D_s \geq 1456 \text{ mm}$	$S \geq 1256 \text{ mm}$	<ul style="list-style-type: none"> Automatic start possible Enables access to be protected independent of the height of the hazard zone 	<ul style="list-style-type: none"> The operator is much further away (long paths) More space required Lower productivity
3 – Access protection	$D_s \geq 1456 \text{ mm}$	$S \geq 1106 \text{ mm}$	<ul style="list-style-type: none"> Cost-effective solution Enables access to be protected independent of the height of the hazard zone Protection on several sides possible using deflector mirrors 	<ul style="list-style-type: none"> 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.

3
C



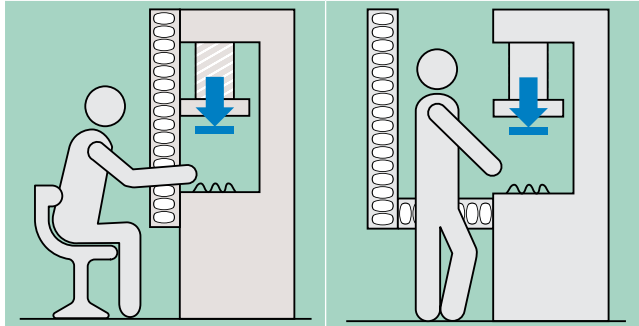
Example of guarding with various detection capabilities for the perpendicular approach according to North American standards.

Necessary protective field size/height of the ESPE

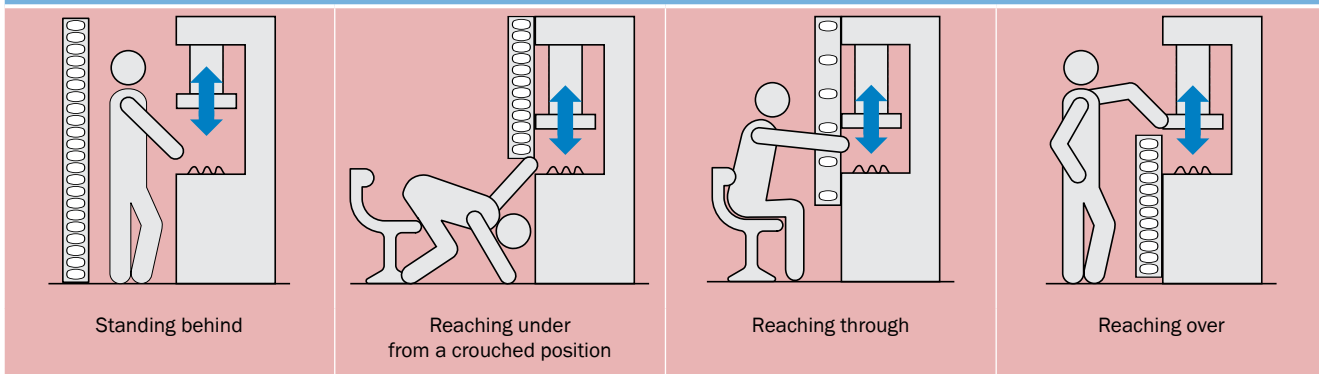
As a general rule, the following faults must be excluded when installing protective devices:

- 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.
- The location of the protective field must be in accordance with the calculated minimum distance for the application.
- If it is possible to stand behind protective devices, additional measures are required (e.g., restart interlock, secondary protective device).

Examples of correct installation



Examples of dangerous installation errors



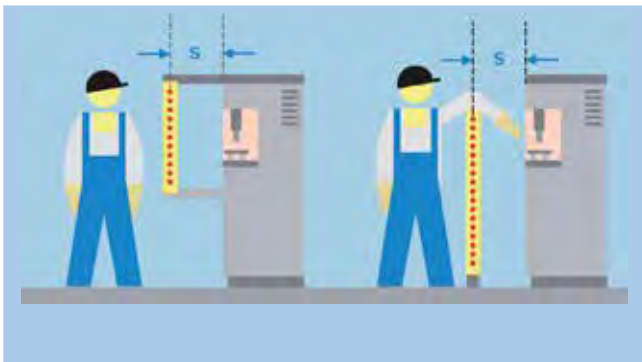
Once the minimum distance between the protective field and the nearest hazardous point has been calculated, the protective field height required must be determined in a further step.

This ensures the hazardous point cannot be accessed by reaching over the protective field 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. In this case, 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.

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. Guidance regarding this comparison can be found in 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 RIA TR R15.406 or ISO 13855 shall be used for both methods.

Increase height of top edge

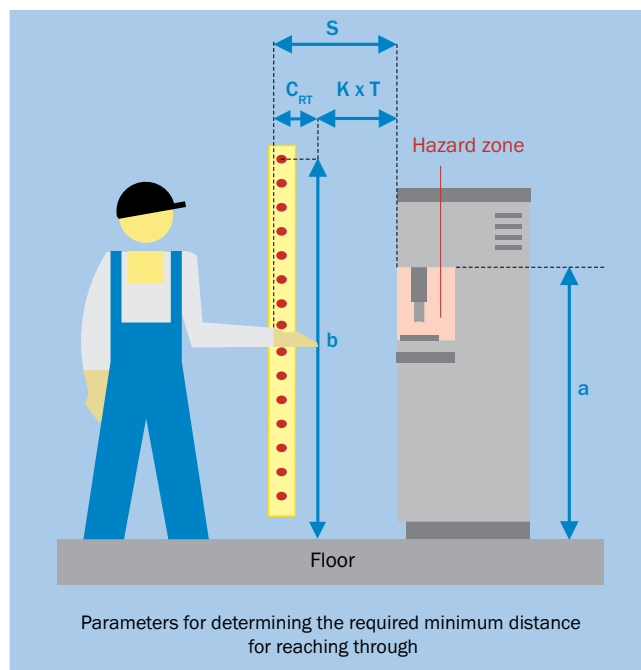
The height of the hazard zone **a** and the supplement determined by the resolution **C_{RT}** are used to calculate the required height of the top edge of the protective field **b** when the minimum distance **S** remains unchanged. With the top edge of the protective field calculated at this height,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

Consequences

In some applications, in which the ESPE used is a multiple beam system (arm or body detection), the minimum distance could increase or ESPE with a smaller resolution **d** for finger or hand detection (light curtains) shall be used. This situation applies for the application of RIA TR R15.406 or ISO 13855.

Some C-type standards differ from RIA TR R15.406 and ISO 13855 in the calculation of the minimum distances.

3
C

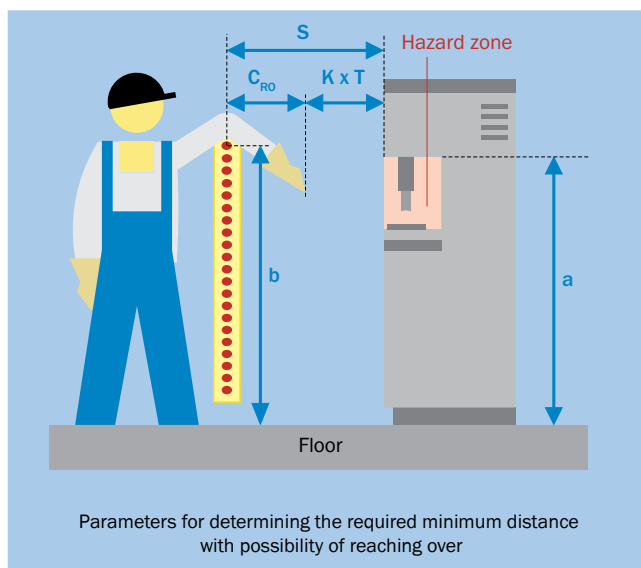


Increase minimum distance (height of top edge prescribed)

If the top edge of the protective field **b** is prescribed by a pre-existing product, the minimum distance **S** 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 below represents the intrusion distance **C_{RO}**. If **C_{RO} ≥ 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 shall be used to calculate the minimum distance.



The rule of thumb is:

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

The table from RIA TR R15.406 and ISO 13855 as well as practical examples can be found on the following pages.

To take the possibility of reaching over into account, RIA TR R15.406 and ISO 13855 include 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)												
	0	0	0	0	0	0	0	0	0	0	0	0	0
2600 ¹⁾	0	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	0
2400	550	550	550	500	450	450	400	400	300	250	100	0	0
2200	800	750	750	700	650	650	600	550	400	250	0	0	0
2000	950	950	850	850	800	750	700	550	400	0	0	0	0
1800	1100	1100	950	950	850	800	750	550	0	0	0	0	0
1600	1150	1150	1100	1000	900	850	750	450	0	0	0	0	0
1400	1200	1200	1100	1000	900	850	650	0	0	0	0	0	0
1200	1200	1200	1100	1000	850	800	0	0	0	0	0	0	0
1000	1200	1150	1050	950	750	700	0	0	0	0	0	0	0
800	1150	1050	950	800	500	450	0	0	0	0	0	0	0
600	1050	950	750	550	0	0	0	0	0	0	0	0	0
400	900	700	0	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	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	

1) Approach to the hazard zone by reaching over is impossible

Electro-sensitive protective equipment with a height of the:

- Upper edge of the detection zone below 900 mm is not included since they do not offer sufficient protection against circumventing or stepping over
- Lower edge of the detection zone above 300 mm in relation to the reference plane does not offer sufficient protection against crawling below

When vertical electro-sensitive protective equipment are combined with protective structures (guards) that allow people to lean on the structure, calculate the required height for guards (→ 3-61)

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:

North America	Europe/International
ESPE, resolution $d \leq 64$ mm: $C_{RT} = 3.4 \times (d - 7)$ mm	ESPE, resolution $d \leq 40$ mm: $C_{RT} = 8 \times (d - 14)$ mm
ESPE, resolution $d > 64$ mm and Height of highest beam ≥ 1200 mm: $C_{RT} = 900$ mm	ESPE, resolution $d > 40$ mm: $C_{RT} = 850$ mm
Height of highest beam ≥ 900 mm: $C_{RT} = 1200$ mm	

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.

3
C

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

Example using European / International values for C_{RT}

- Resolution of the ESPE: > 40 mm
 - Height **a** of the hazard zone: 1400 mm ①
 - Resolution-dependent supplement **C**: 850 mm
- 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 **C_{RO} 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)												
	0	0	0	0	0	0	0	0	0	0	0	0	0
2600	0	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	0
2400	550	550	550	500	450	450	400	400	300	250	100	0	0
2200	800	750	750	700	650	650	600	550	400	250	0	0	0
2000	950	950	850	850	800	750	700	550	400	0	0	0	0
1800	1100	1100	950	950	850	800	750	550	0	0	0	0	0
1600	1150	1150	1100	1000	900	850	750	450	0	0	0	0	0
1400	1200	1200	1100	1000	900	850	650	0	0	0	0	0	0
1200	1200	1200	1100	1000	850	800	0	0	0	0	0	0	0
1000	1200	1150	1050	950	750	700	0	0	0	0	0	0	0
800	1150	1050	950	800	500	450	0	0	0	0	0	0	0
600	1050	950	750	550	0	0	0	0	0	0	0	0	0
400	900	700	0	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	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	

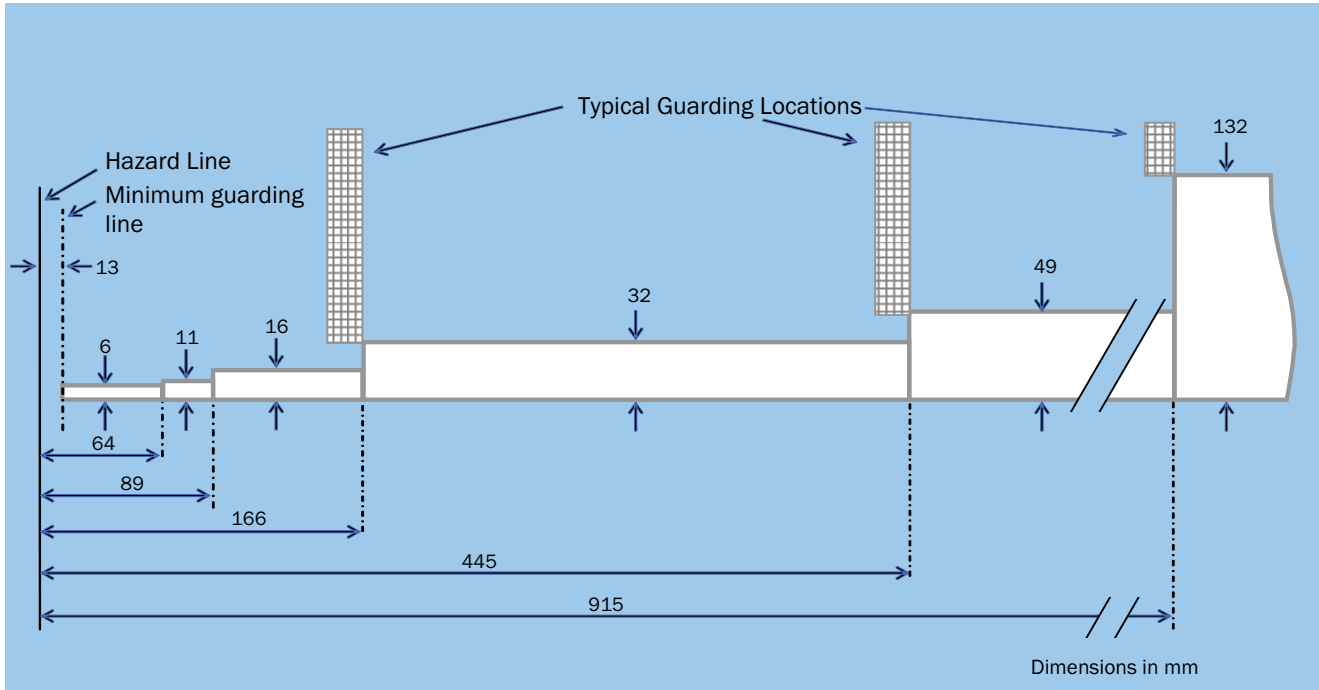
Example using European / International values for C_{RT}

- 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)

Safety distance for guards

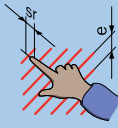
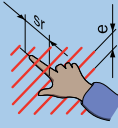
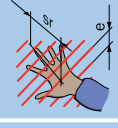
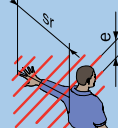
Guards must be at an adequate distance from the hazard zone if they have openings. This requirement also applies to openings between a protective device and a machine frame, jigs, etc. There are different distance requirements depending on the type of opening (slotted, square, circle).

Safety distance as a function of the openings on guards (for slotted opening) according to ANSI B11.19 and CSA Z432:



3
C

Safety distance as a function of the openings on guards according to RIA TR R15.406, NR-12, and ISO 13857

Part of the body	Opening e (mm)	Safety distance (mm)		
		Slot	Square	Circle
	$e \leq 4$	≥ 2	≥ 2	≥ 2
	$4 < e \leq 6$	≥ 10	≥ 5	≥ 5
 	$6 < e \leq 8$	≥ 20	≥ 15	≥ 5
	$8 < e \leq 10$	≥ 80	≥ 25	≥ 20
	$10 < e \leq 12$	≥ 100	≥ 80	≥ 80
	$12 < e \leq 20$	≥ 120	≥ 120	≥ 120
	$20 < e \leq 30$	$\geq 850^{a)}$	≥ 120	≥ 120
	$30 < e \leq 40$	≥ 850	≥ 200	≥ 120
	$40 < e \leq 120$	≥ 850	≥ 850	≥ 850

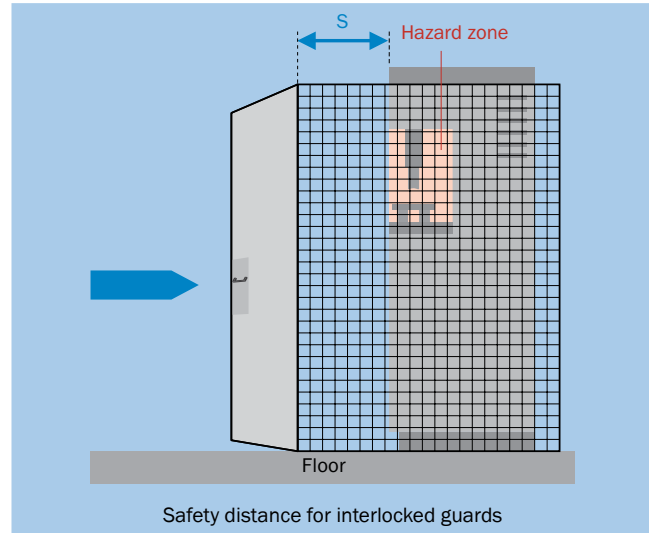
The bold lines within the table delineate the part of the body restricted by the opening size.

^{a)} If the length of the slot opening is ≤ 65 mm, the thumb will act as a stop and the safety distance can be reduced to 200 mm.

3
C

Safety distance for interlocking guards

For interlocked movable guards that initiate a stop, a safety distance must also be observed similar to the procedure for ESPE. Alternatively, interlocks with locking mechanisms may be used to prevent access until the hazard is no longer present see section "Locking devices" → 3-24).



General calculation formula

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

Where:

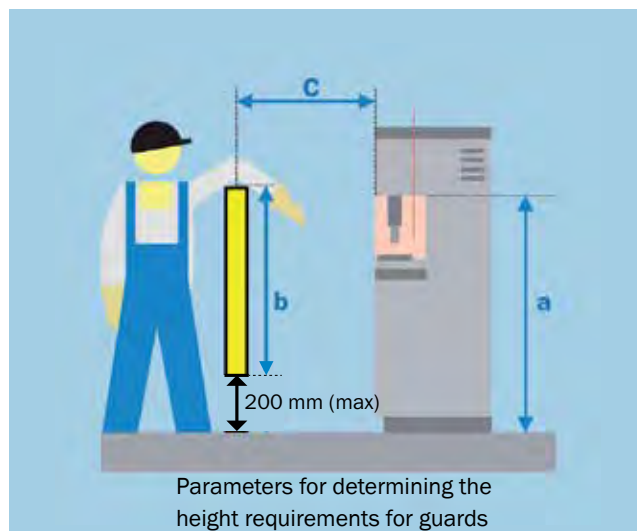
- **S** is the minimum distance in millimeters, measured from the nearest hazardous point to the nearest door opening point.
- **K** is a parameter in millimeters per second, derived from the data for the approach speeds of the body or parts of the body, usually 1600 mm/s.
- **T** is the stopping/run-down time of the overall system in seconds.
- **C** is a safety distance taken from the corresponding table in either ANSI B11.19 and CSA Z432, or ISO 13857 and RIA TR R15.406 (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.

Calculation of the minimum distance for interlocking guards: ANSI B11.19, RIA TR R15.406, ISO 13855

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 180 mm above the reference level (unless a C-Type standards states a more restrictive requirement).



Required height for guards in case of low risk according to ANSI B11.19, RIA TR R15.406, CSA Z432, and ISO 13857

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

Height b of the guard (mm)										
1000	1200	1400	1600	1800	2000	2200	2400	2500	2700	

- a) Protective structures less than 1000 mm in height are not included because they do not sufficiently restrict movement of the body.
- b) Protective structures lower than 1400 mm should not be used without additional safety measures.
- c) Low risk hazard zones at or above 2500 mm in height are considered adequately safeguarded by location.

Required height for guards in case of high risk according to ANSI B11.19, RIA TR R15.406, CSA Z432, NR-12, and ISO 13857

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

- a) Protective structures less than 1000 mm in height are not included because they do not sufficiently restrict movement of the body.
- b) Protective structures lower than 1400 mm should not be used without additional safety measures.
- c) High risk hazard zones at or above 2700 mm in height are considered adequately safeguarded by location.

3
C

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

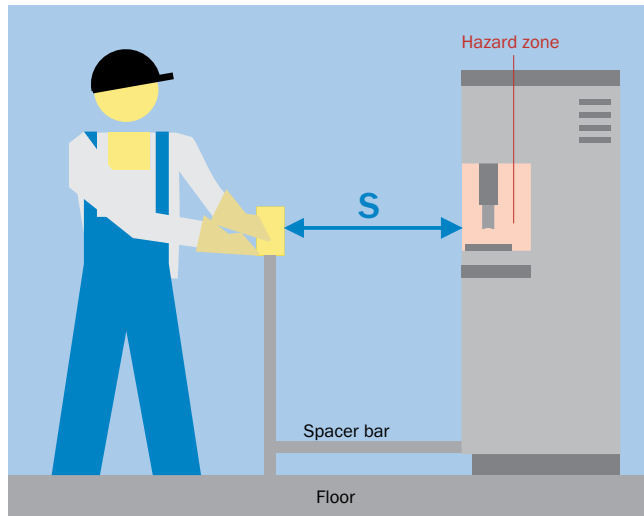
The guard shall, therefore, start 180 mm above the reference level (e.g., floor, working surface) and end at 1800 mm. If the height of the guard is to be 1600 mm, then the safety distance must be increased to at least 800 mm.

→ Safety distances and required guard height: ANSI B11.19, RIA TR R15.406, CSA Z432, NR-12, ISO 13857

Minimum distance for fixed position protective devices

Example: Minimum distance for two-hand control

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



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). This value is not required in some North American standards, but should be included as a best practice when considering minimum distance for a two-hand control device.

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).

3
C

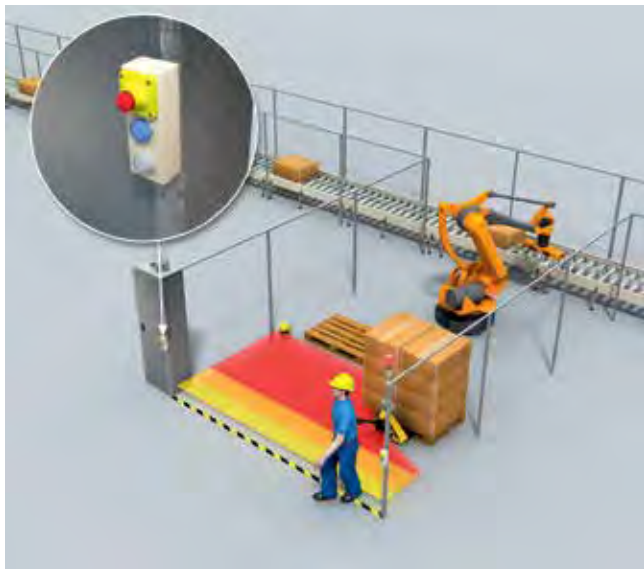
→ Calculation of the minimum distance: OSHA 1910.217, ANSI B11.19, RIA TR R15.406, CSA Z432, NR-12, ISO 13855

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 (Δ 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. 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 such that it is not accessible from within the safeguarded area. 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.



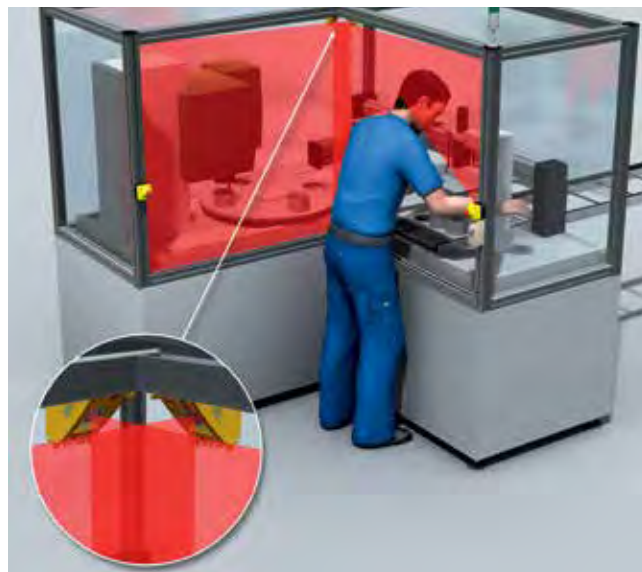
The position of the reset pushbutton allows a full view of the hazard zone for the resetting of the protective device.

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 require 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 into the control system






Along with mechanical aspects, a protective device must also be integrated into 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 978-3642191886 (4th Edition 2011)

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 (SRP/CS) 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.

Control system		Aspects relating to safety technology		
Principle of operation of the control system	Typical components	Interfering factors	Explanations	
Fluid	Pneumatic 	<ul style="list-style-type: none"> • Multiway valves • Vent valves • Manual shut-off valves • Filters with water trap • Hoses 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Accumulators • Pressure limiters • Multiway valves • Filters • Level gauges • Temperature gauges • Hoses • Threaded fittings 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Control switches: <ul style="list-style-type: none"> • Position switches • Selector switches • Pushbuttons • Switchgear: <ul style="list-style-type: none"> • Contactors • Relays • Circuit breakers 	<ul style="list-style-type: none"> • 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 positions, parts are insensitive to moisture, temperature fluctuations, and electromagnetic interference if selected correctly
	Electronic 	<ul style="list-style-type: none"> • Individual components, e.g.: <ul style="list-style-type: none"> • Transistors • Resistors • Capacitors • Coils • Highly integrated components, e.g., integrated circuits (IC) 	As listed under "Electromechanical" In addition: <ul style="list-style-type: none"> • Temperature fluctuations • Electromagnetic interference 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 	<ul style="list-style-type: none"> • Microprocessors • Software 	<ul style="list-style-type: none"> • Installation fault in the hardware • Systematic failures including common mode failures • Programming errors • Handling errors • Operating errors • Manipulation/tampering • Viruses 	<ul style="list-style-type: none"> • Measures to prevent faults: <ul style="list-style-type: none"> • Structured design • Program analysis • Simulation • Measures to control faults: <ul style="list-style-type: none"> • Redundant hardware and software • RAM/ROM test • CPU test

Translation of text from: Alfred Neudörfer, Konstruieren sicherheitsgerechter Produkte, Springer Verlag, Berlin u. a., ISBN 978-3642191886 (4th Edition 2011) (English version "The Design of Safe Machines" planned for 2015: ISBN 978-3-540-35791-9)

The safety-related input elements have been described above as 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 typically 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.

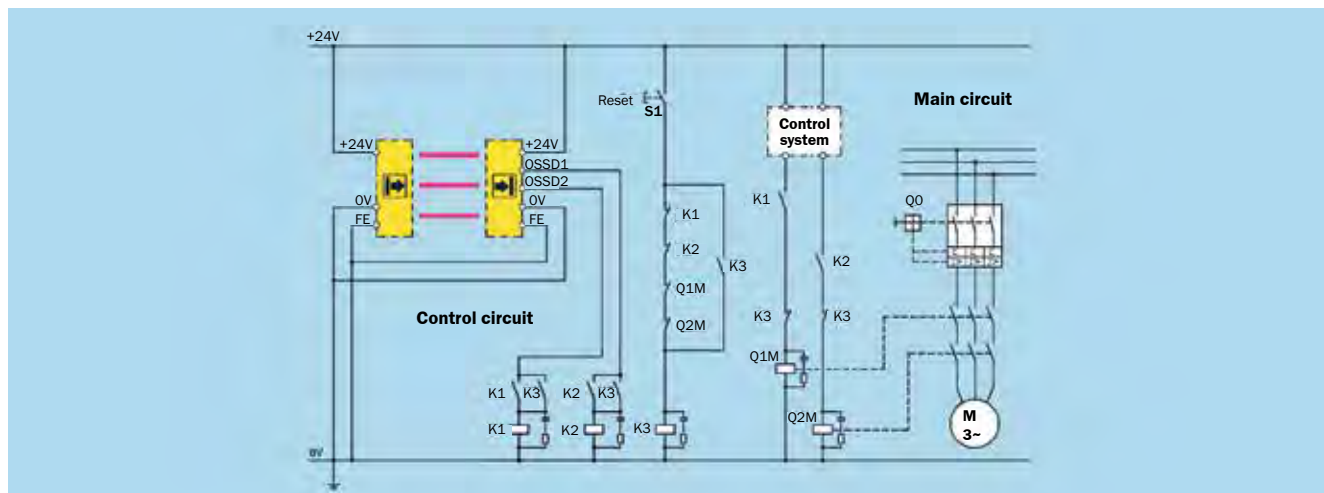
→ Connection diagrams for the integration of protective devices can be found at <http://www.sickusa.com/>

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 (e.g., PLC). There must also be redundant circuits for removing power.

Logic unit made up of separate contactors

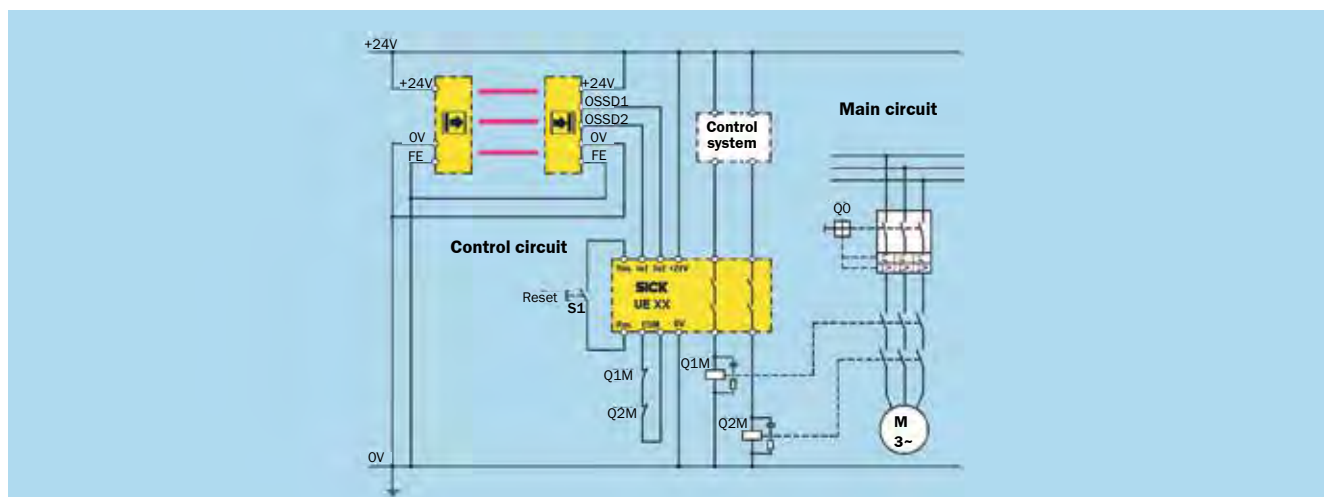


Using individual auxiliary contactors with positively guided contacts, it is possible to design control systems with any level of complexity. Redundancy and monitoring by positively guided contacts are features of this safety principle. Wiring provides the logical operators.

Function: If the contactors **K1** and **K2** are de-energized, pressing **S1** energizes the **K3** contactor and it remains energized. If no object is detected in the active protective field, the outputs

OSSD1 and **OSSD2** are conducting voltage. The contactors **K1** and **K2** are energized by the normally open contacts on **K3** and latch. **K3** is de-energized by releasing **S1**. Only then are the output circuits closed. On detection of an object in the active protective field, the **K1** and **K2** contactors are de-energized by the **OSSD1** and **OSSD2** outputs.

Logic unit using safety relay/safety interface module (SIM)



Safety relays combine one or more safety functions in one housing. They generally have automatic monitoring functions. 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 certified safety PLCs. The concept of “proven components” and “proven safety principles” are now available using 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 integrator using the language(s) supported by the firmware.

Parameterization

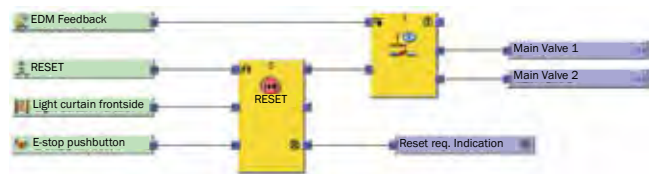
Parameterization is the selection of properties from a defined pool of functionality by selector switch/software parameters at the time of commissioning.

Features: low logic depth, AND/OR logic

Configuration

Configuration is the application of flexible operators for defined function blocks in certified logic with a programming interface, for example through parameterization of times or configuration of the inputs/outputs of the control system.

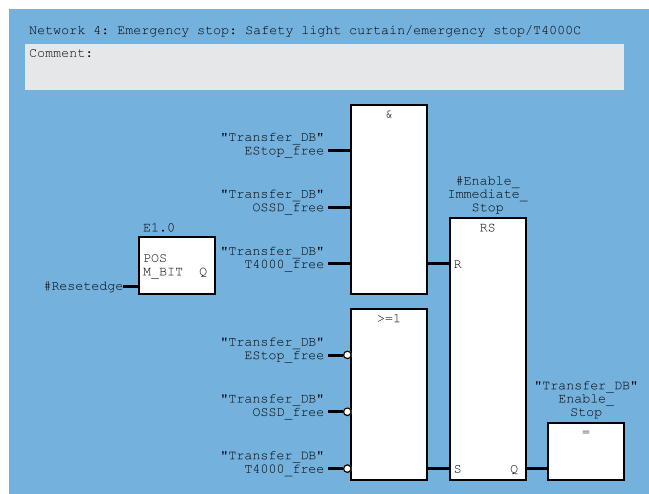
Features: any logic depth, binary logic



Programming

Programming defines the logic as required using the functionality defined by the predefined programming language, mostly using certified function blocks.

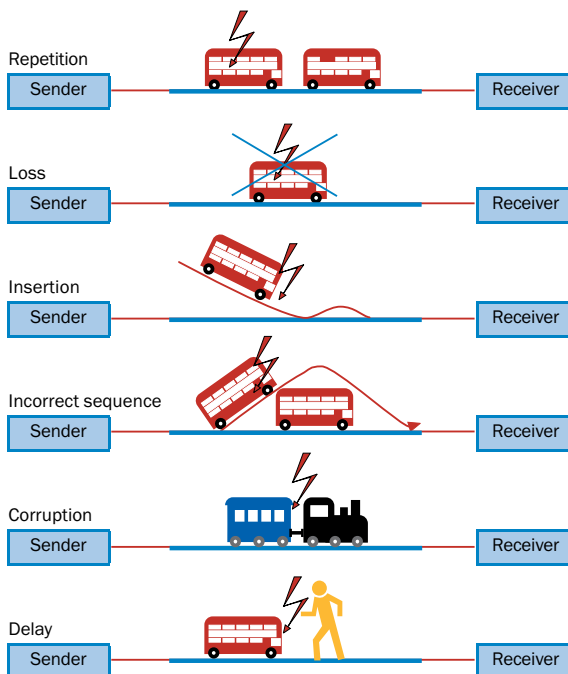
Features: any logic depth, word level



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.

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.



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

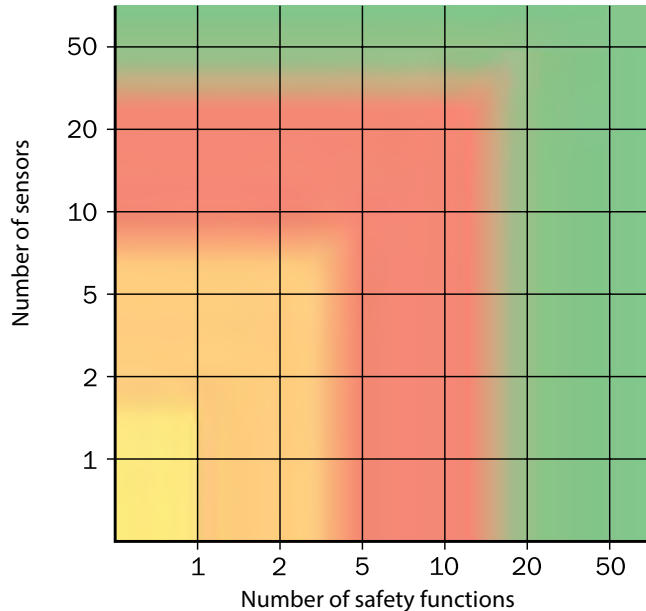
Several measures can be applied in the higher-level control system against the transmission faults mentioned above, e.g., sequential numbering of safety-related messages or defined times for incoming messages with acknowledgment. Protocol extensions based on the fieldbus used include such measures. In the ISO/OSI (Open Systems Interconnection) layer model, they act over the transport layer and, therefore, use the fieldbus with all its components as a “black channel,” without modification. Examples of established fieldbus systems include but are not limited to:

- AS-i Safety at Work
- DeviceNet Safety
- PROFI-safe

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.



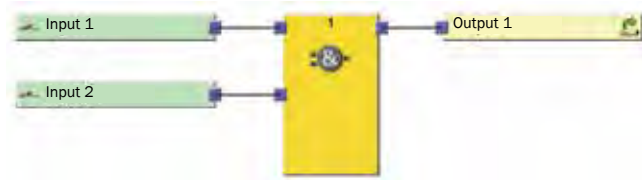
- Safety relay
- Parameterizable controller
- Configurable controller
- Programmable controller

Design matrix

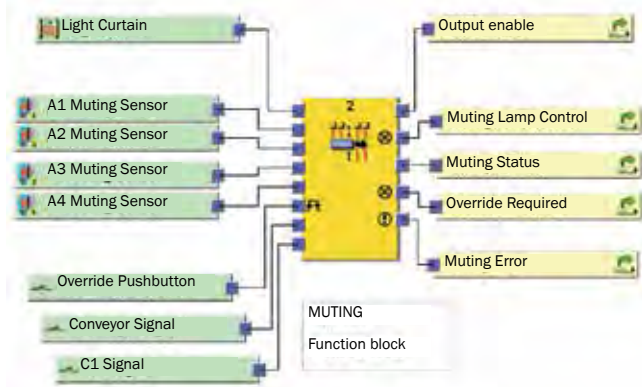
- 0** = logic 0 or OFF
- S** = actuator enable (restart)
- I** = logic 1 or ON
- = any status

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

Simple AND logic operator



Muting function logic operator



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 failures, 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 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 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

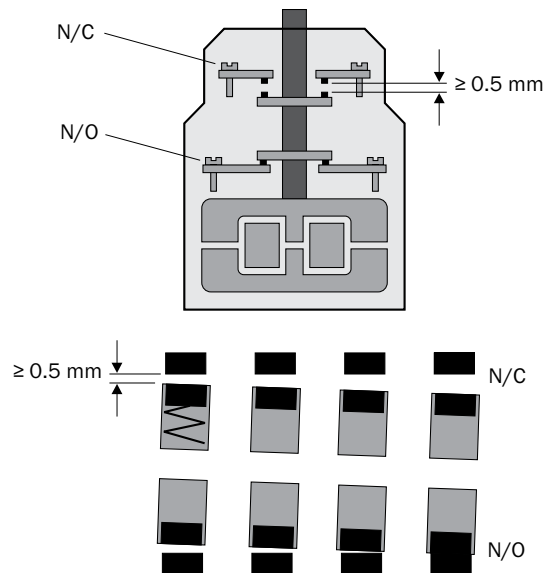
Electromechanical contactors are the most commonly used type of power control element. One or more contactors can form a safety function subsystem by combining special selection criteria, wiring, and technical measures. By protecting the contacts against overcurrent and short-circuits, over-sizing (normally 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, known as “external device monitoring” (EDM). This requirement can be met using a contactor with positively guided contacts. The contacts are positively guided when all contacts within a set are mechanically linked in such a way that normally open contacts and normally closed contacts can never be closed simultaneously 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). As with 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.

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



Source: Moeller AG

Contact system of a contactor with positively guided contacts. A normally open contact is welded.

an effect on the release delay and, therefore, on the required minimum distance of the protective device (→ 3-44). A simple diode for arc suppression can result in a time to respond (switch to OFF) up to 14 times longer. This must be taken into account for when calculating the minimum safety distance.

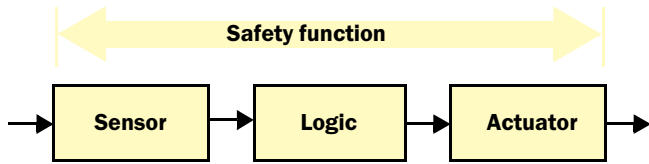
Suppressor (across inductance)	Diode	Diode combination	Varistor	RC element
Protection against overvoltage	Very high	High	Limited	High ¹⁾
Release delay (delay in switching OFF)	Very long (relevant to safety)	Short (but must be taken into account)	Very short (not relevant to safety)	Very short ¹⁾ (not relevant to safety)

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

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).



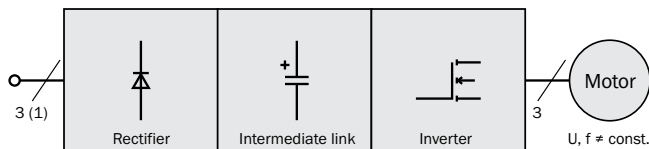
The actuator can involve several components (contactor, drive controller, feedback), depending on technical design and safety function. Braking systems and holding systems are also to be taken into account on axes subject to gravity.

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.



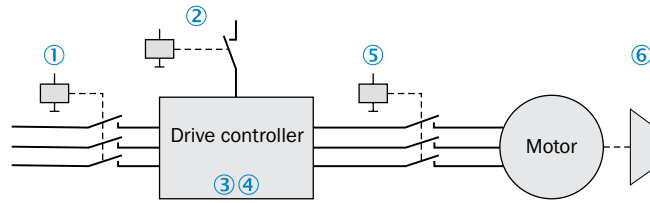
To limit transient overvoltages caused by switching loads in DC and AC circuits, interference suppression components are to be used, in particular if sensitive electronic assemblies are being used in the same control cabinet.

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

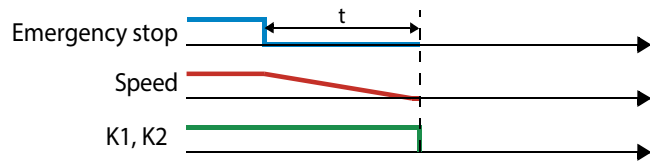
A safety function can be implemented with a drive controller in various ways:

- 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 (→ 3-72)

Disconnection of the power supply

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 needed 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), drive-controlled motion ramp down is initiated. A combination of drive-supported safety functions may also need to be implemented as a suitable measure to achieve adequate risk reduction.

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 (fieldbus systems/network interface)

“Control communication” refers to a standard control system sending a setpoint for rotational speed or position to the drive via a fieldbus 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

	<p>Safe Torque Off (STO)</p> <ul style="list-style-type: none"> • Corresponds to stop Category 0 in accordance with NFPA 79 and 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. 		<p>Safe Maximum Speed (SMS) ¹⁾</p> <ul style="list-style-type: none"> • Safe monitoring of the maximum speed independent of the operating mode.
	<p>Safe Stop 1 (SS1) ²⁾</p> <ul style="list-style-type: none"> • Corresponds to stop Category 1 in accordance with NFPA 79 and 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. 		<p>Safe Braking and Holding System (SBS) ¹⁾</p> <ul style="list-style-type: none"> • The safe braking and holding system controls and monitors two independent brakes.
	<p>Safe Stop 2/Safe Operating Stop (SS2, SOS) ²⁾</p> <ul style="list-style-type: none"> • Corresponds to stop Category 2 in accordance with NFPA 79 and IEC 60204-1. • Controlled stopping while maintaining the supply of power to the actuators. • After standstill: Safe monitoring of the drive shaft position within defined range. 		<p>Safe Door Locking (SDL) ¹⁾</p> <ul style="list-style-type: none"> • The door lock is only unlocked if all drives in a protective zone are in the safe state.
	<p>Safely Limited Speed (SLS)</p> <ul style="list-style-type: none"> • 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. 		<p>Safely Limited Increment (SLI)</p> <ul style="list-style-type: none"> • If an enable signal is given, a safely limited increment is monitored in a special operating mode. • The drive is then stopped and remains in this position.
	<p>Safe Direction (SDI)</p> <ul style="list-style-type: none"> • In addition to the safe movement, a safe direction (clockwise/counterclockwise) is monitored. 		<p>Safely Monitored Deceleration (SMD) ¹⁾</p> <ul style="list-style-type: none"> • Safe monitoring of deceleration on stopping with predetermining behavior.
	<p>Safely Monitored Position (SMP) ¹⁾</p> <ul style="list-style-type: none"> • 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). 		<p>Safely Limited Position (SLP)</p> <ul style="list-style-type: none"> • 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 mono-stable valves are generally designed for high endurance and can be considered proven in accordance with ISO 13849-2. However, fault exclusion 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 affected 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, the solenoid requires a suppressor similar to a contactor. 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.



Filter concept

The vast majority of failures of fluid control systems are due to malfunctions 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.

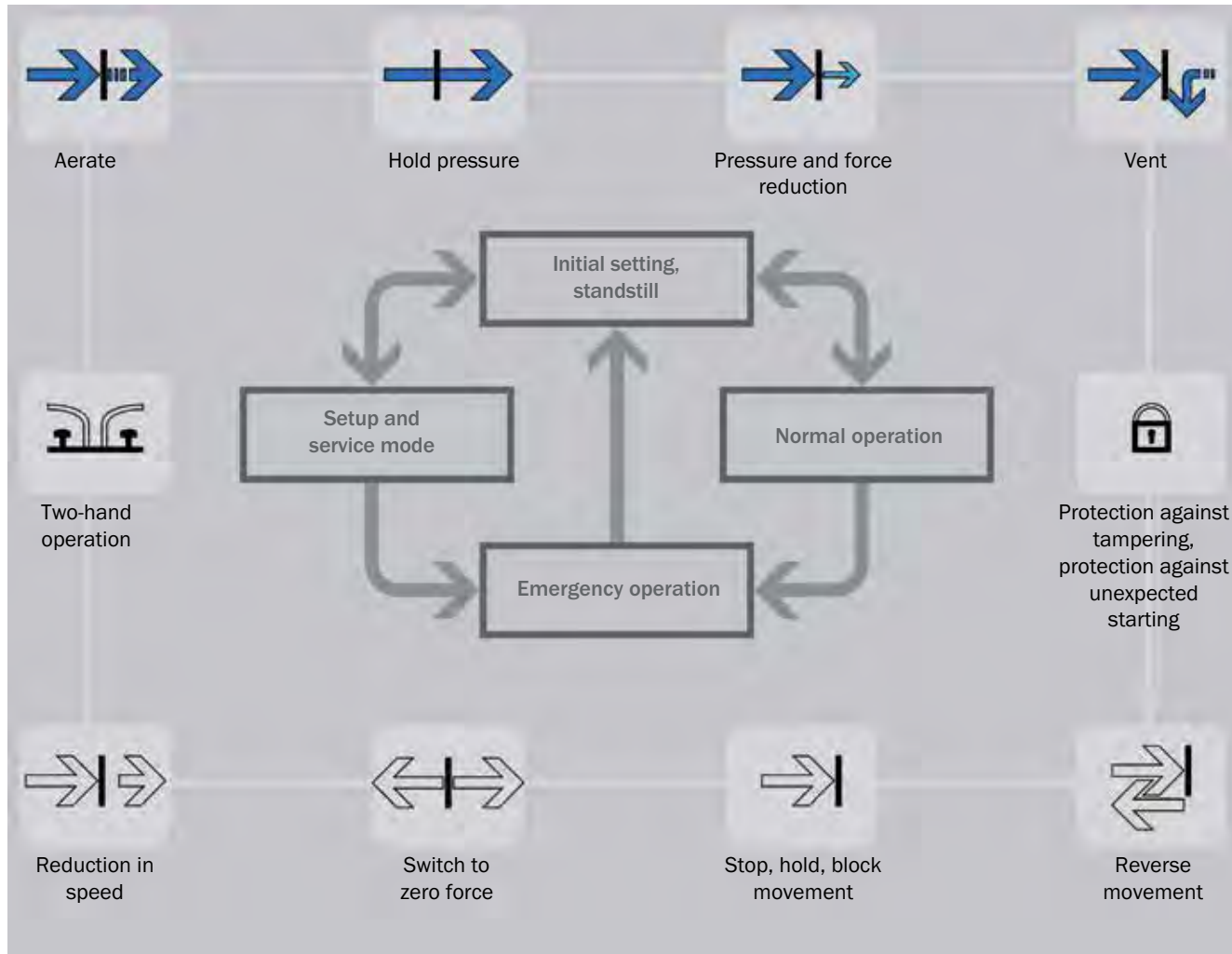
A filter concept refers to the suitable selection of a filter principle for the task required as well as the arrangement of the filter in an appropriate location. The filter concept must be designed so that it is able to retain in the filter the contamination added to the entire system in such a way 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

Product overview: Safety technology for machine safety

3
C

Sensors	Logic	Power control elements
Safety light curtains  Safety camera systems  Multiple light beam safety devices  Single-beam safety devices  Safety laser scanners 	 Safety relays	 Electrical drives with element safety sub-functions ¹
Interlocking devices: With separate actuator  With actuator for locking devices  For switching cam, turning lever  Magnetically coded  RFID coded  Inductive 		 Modular safety controllers and Motion control
Emergency stop pushbutton  Enabling switch 	 Safe sensor cascade	
Motor feedback systems  Encoders 		 Pneumatic valves ¹⁾
Photoelectric sensors  Magnetic and inductive sensors 	 Hydraulic valves ¹⁾	

Service solutions from SICK LifeTime Services (→ page i-1 in Annex i “How SICK supports you”)

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 <http://www.sickusa.com/>

Summary: Designing the safety function

General

- Draft a safety concept. During this process, take into account features of the machine, features of the surroundings, human aspects, features of the design, and 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 of 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 fixed position 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).

Step 3d: 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

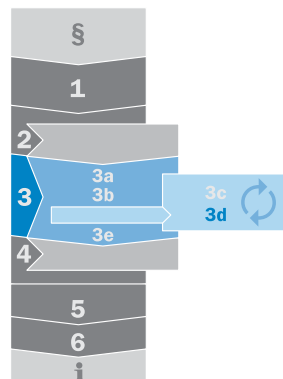
- Sufficient safety distance and dimensioning (reaching over, reaching under, etc.)
- Suitable mesh size or lattice spacing for barriers
- Sufficient rigidity and suitable mounting
- Selection of suitable materials
- Safe setup
- Resistance to aging
- Protective device design so that climbing on it is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

Containment 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 design
- Resistance to aging

Ergonomic requirements

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



3d

In this chapter ...

Verification of mechanical design 3-79

Verification of functional safety ... 3-81

Determining the performance level (PL) achieved as per ISO 13849-1 3-81

Alternative: Determining the safety integrity level (SIL) achieved according to IEC 62061 3-89

Useful support..... 3-93

Summary 3-94

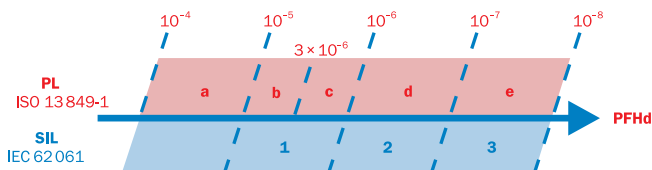
A thorough check of the effectiveness of a protective device can be undertaken using a checklist:

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 <input type="checkbox"/> No <input type="checkbox"/>
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 unauthorized removal?	Yes <input type="checkbox"/> No <input type="checkbox"/>
3.	Does the protective device conform to the reliability level (PL or SIL) required for the safety function?	Yes <input type="checkbox"/> No <input type="checkbox"/>
4.	Has the maximum stopping and/or 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 <input type="checkbox"/> No <input type="checkbox"/>
5.	Has the protective device been mounted such that the required safety or minimum distance from the nearest hazardous point has been achieved?	Yes <input type="checkbox"/> No <input type="checkbox"/>
6.	Is reaching under, reaching over, climbing under, climbing over, or reaching around the protective device effectively prevented?	Yes <input type="checkbox"/> No <input type="checkbox"/>
7.	Have the devices or switches been properly mounted and secured against manipulation after adjustment?	Yes <input type="checkbox"/> No <input type="checkbox"/>
8.	Are the required protective measures against electric shock in effect (protection class)?	Yes <input type="checkbox"/> No <input type="checkbox"/>
9.	Is the control device for resetting the protective device or restarting the machine present and correctly installed?	Yes <input type="checkbox"/> No <input type="checkbox"/>
10.	Are the components used for the protective devices integrated in accordance with the manufacturer's instructions?	Yes <input type="checkbox"/> No <input type="checkbox"/>
11.	Are the given protective functions effective at every setting of the operating mode selector switch?	Yes <input type="checkbox"/> No <input type="checkbox"/>
12.	Are the protective devices effective for the entire duration of the dangerous state?	Yes <input type="checkbox"/> No <input type="checkbox"/>
13.	Once initiated, will a dangerous state be stopped when switching the protective devices off, when changing the operating mode, or when switching to another protective device?	Yes <input type="checkbox"/> No <input type="checkbox"/>
14.	Are the notes included with the protective device attached so they are clearly visible for the operator?	Yes <input type="checkbox"/> No <input type="checkbox"/>

Verification of functional safety

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

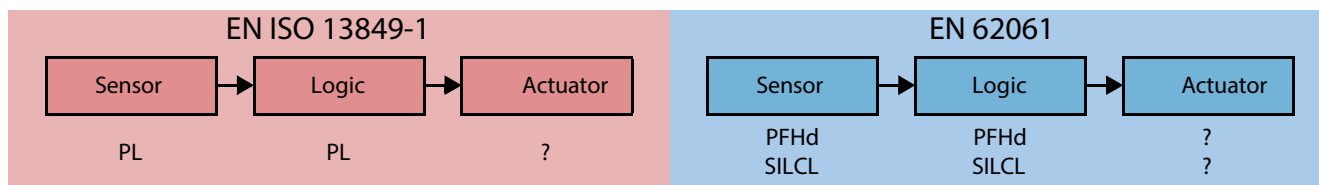
- Determining the performance level (PL) achieved according to ISO 13849-1
- Determining the safety integrity level achieved (SIL) according to IEC 62061



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 (→ 3-87 and → 3-90), 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:

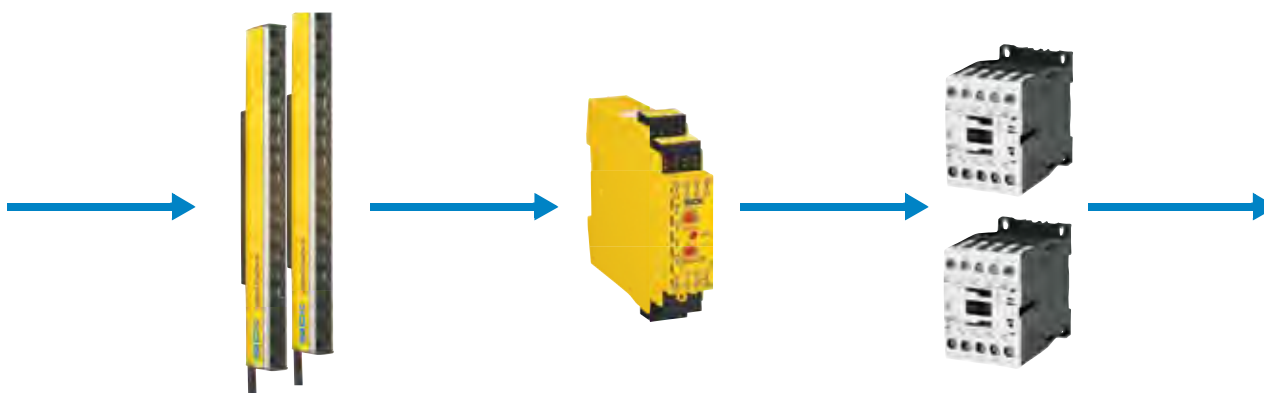
- **Simplified method** (→ 3-82):
Tabular determination of performance level based on the performance levels of each subsystem
- **Detailed method** (→ 3-82):
Mathematical determination of performance level based on the PFHd values of the subsystems (this method is only described indirectly in the standard)

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 "pre-calculated" PL or PFHd values are supplied by the com-

ponent 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 <http://www.dguv.de/ifa/Praxishilfen/Maschinensteuerungen/index.jsp> for comprehensive information about ISO 13849-1

Simplified method

This method 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.

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 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 PL (low) is, therefore, **c**.
- The number of subsystems with this PL is 2 (i.e., ≤2). Therefore, the overall PL achieved is **c**.

This method is based on mean values within the PFHd range of values for the various PL. Therefore, using the detailed method (see next section) may deliver more accurate results.

PL (low) (lowest PL of a sub-system)	n (low) (number of sub-systems 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

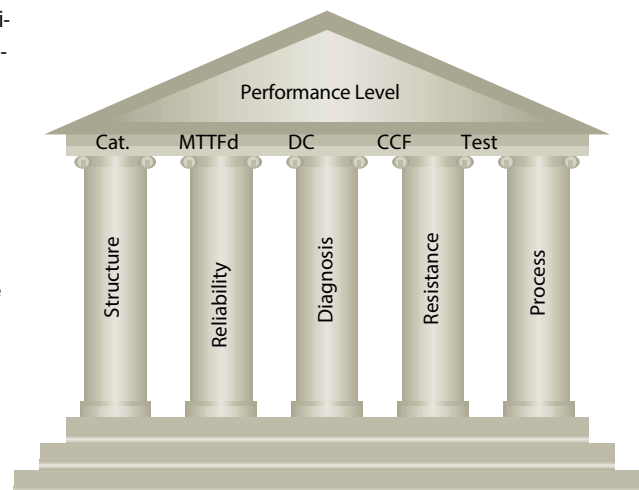
A safety-related subsystem can be formed from many different individual components which may even be made by different manufacturers. Examples of such components include:

- 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 → 3-83)
- MTTFd values of individual components (→3-84)
- Diagnostic coverage (DC → 3-85)
- Common cause failure (CCF → 3-91)
- Software aspects that are relevant to safety
- Systematic failures



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 designed, built, selected, assembled, and combined in compliance with applicable standards so that they are able to tolerate anticipated influencing factors.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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).	<ul style="list-style-type: none"> 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	<p>The requirements of category B shall be met and proven safety principles used. Safety-related parts shall be designed such that:</p> <ul style="list-style-type: none"> A single fault in any of these parts will not lead to the loss of the safety function Wherever it is reasonably possible, the single fault is detected. 	<ul style="list-style-type: none"> When the single 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	<p>The requirements of category B shall be met and proven safety principles used. Safety-related parts shall be designed such that:</p> <ul style="list-style-type: none"> A single fault in any of these parts will not lead to the loss of the safety function and The single fault is detected on or before the next request for the safety function. <p>If this is not possible, an accumulation of faults will not lead to the loss of the safety function.</p>	<ul style="list-style-type: none"> 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:

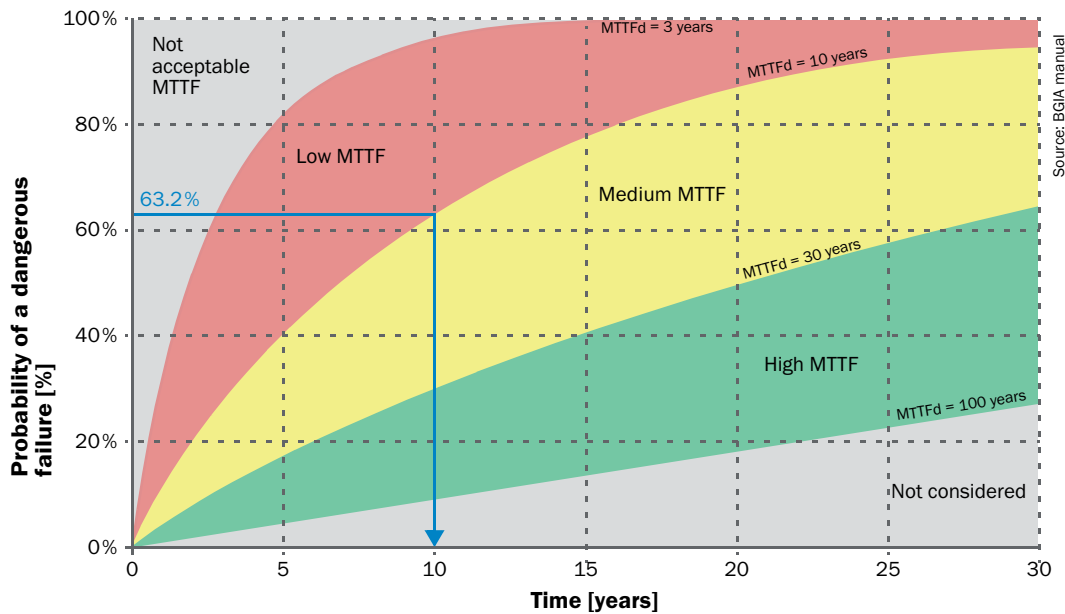
- B_{10} values for electromechanical or pneumatic components. Here, wear and thus the maximum permissible application time are determined by the switching frequency. B_{10} indicates the number of switching cycles until 10% of components fail.
- The B_{10d} value indicates the number of switching cycles 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 \leq MTTFd < 10 years
Medium	10 years \leq MTTFd < 30 years
High	30 years \leq 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.



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

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

Minimum requirement

Total figure ≥ 65



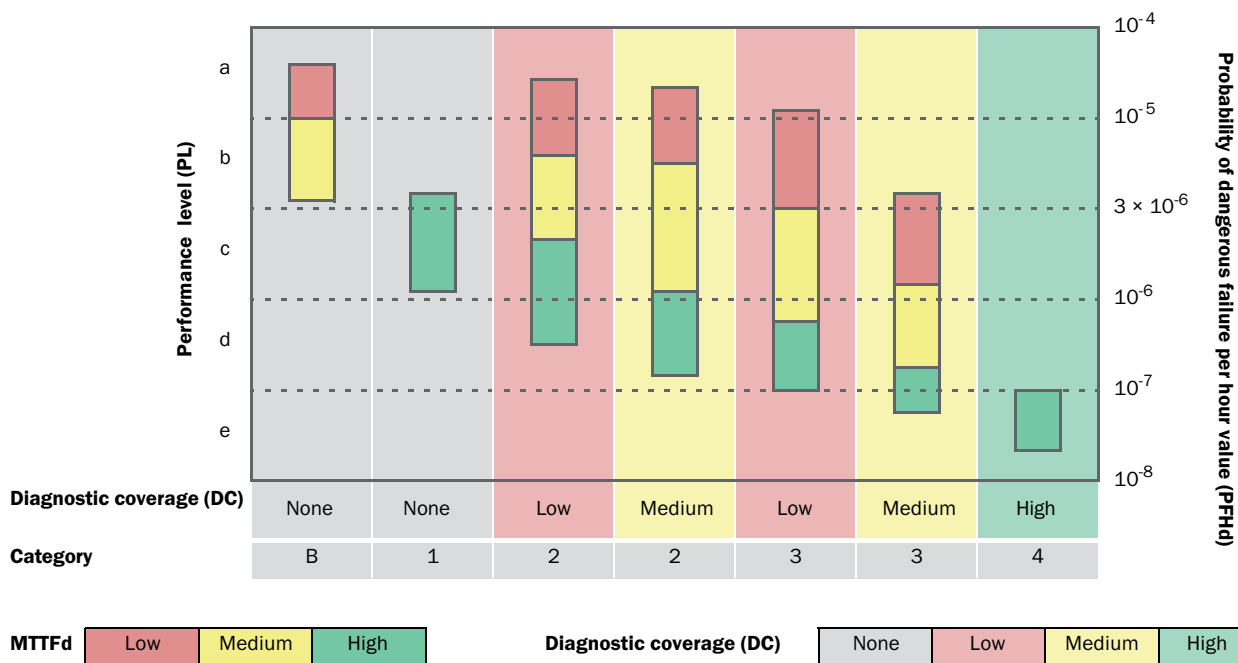
Process

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 a management task 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.



3
d

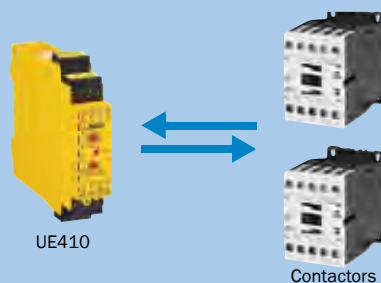
A performance level of **d** can be achieved with a dual-channel control system (category 3), for example. This can be reached either with components of good quality (MTTFd = medium) if almost all faults are detected (DC = medium) or with components of very good quality (MTTFd = high) if many faults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

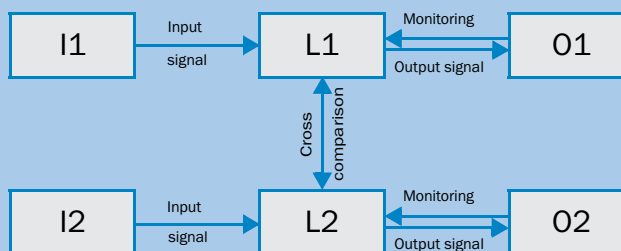
The "actuator" subsystem comprises two contactors with "feedback." As the contactor contacts are positively guided, a safety-relevant failure of the contactors can be detected (EDM). The UE410 logic unit itself is not part of the "actuator" subsystem but is used for diagnostic purposes.



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 B_{10d} value and the estimated switching frequency (n_{op}) must be used to calculate the MTTFd. The following formula applies:

The figure for the switching frequency comprises operating hours/day [h_{op}], working days/year [d_{op}] as well as the switching frequency per hour [C]:

General conditions according to the manufacturer:

- $B_{10d} = 2,600,000$
- $C = 1/\text{hour}$ (assumed value)
- $d_{op} = 220$ days/year
- $h_{op} = 16$ hours/day

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

Example: Determining the PL of the "actuator" subsystem

5) Evaluation of the measures to prevent common cause failures

Measures to avoid common cause failures 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:

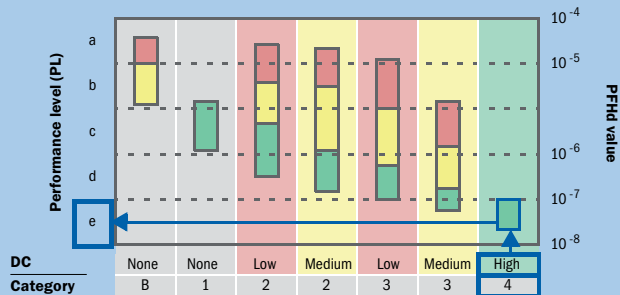
- Organization and competence
- Rules governing design (e.g., specification templates, coding guidelines)
- Test concept and test criteria
- Documentation and configuration management



7) Result

From the illustration for the determination of the PL for the subsystem (→ 3-81), 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" → 3-81).

Alternative: Determining the safety integrity level (SIL) achieved 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" → 3-81.

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:

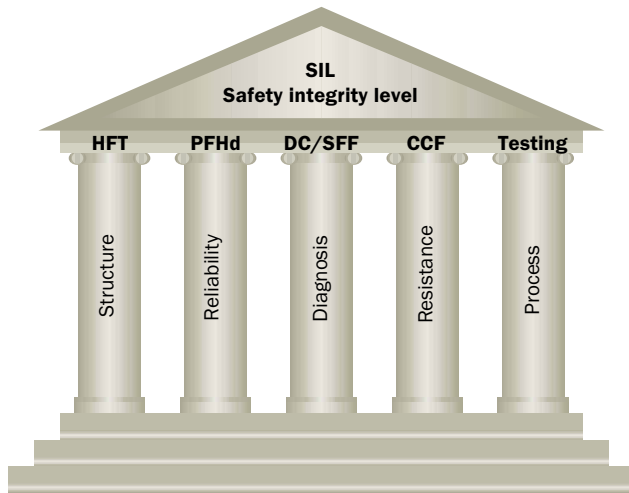
- Layout conforming to the plan for functional safety
- Correct selection, combination, arrangement, assembly, and installation of subsystems, including cabling, wiring, and other connections
- Use within the manufacturer's specifications
- Compliance with application instructions provided by the manufacturer (catalog data, installation instructions, and application of proven practical experience, for example)
- Observance of requirements with regard to electrical equipment in accordance with NFPA 79 or 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. (see "Reliable data transmission" →3-68).

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.



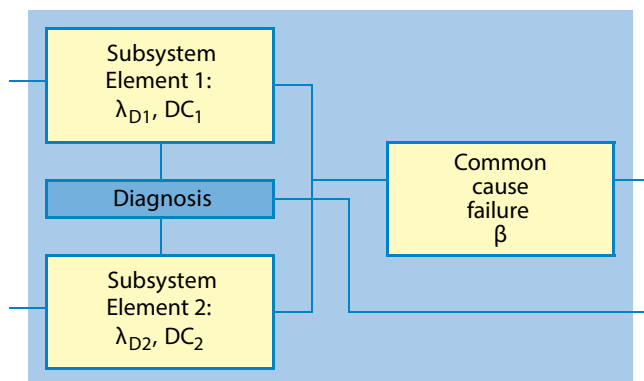
The safety integrity level achieved for a subsystem is made up of the following parameters:

- Hardware fault tolerance (HFT)
- Probability of dangerous failure per hour (PFHd)
- 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).



Probability of random dangerous hardware failures (PFHd)

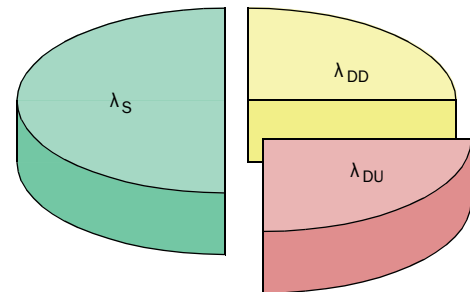
Alongside structural restrictions, the "probability of dangerous hardware failures" must also be taken into account for each subsystem. Based on a mathematical model, there is a formula to determine the PFHd value for each type of subsystem, whereby the following parameters feature in the calculation:

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

$$\begin{aligned}
 &HFT = 1 \\
 &\text{Diagnostics with } DC_1 \text{ and } DC_2 \\
 &PFHd = (1 - \beta)^2 \times \left\{ \frac{\lambda_{D1} \times \lambda_{D2} \times (DC_1 + DC_2) \times T_D}{2} \right. \\
 &\quad \left. + \frac{\lambda_{D1} \times \lambda_{D2} \times (2 - DC_1 - DC_2) \times T_P}{2} \right. \\
 &\quad \left. + \beta \times \frac{\lambda_{D1} + \lambda_{D2}}{2} \right\} \\
 &PFHd \approx \beta \times \frac{\lambda_{D1} + \lambda_{D2}}{2}
 \end{aligned}$$

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).

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

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.

Item	Score
Separation/segregation	
Are SRECS signal cables for the individual channels routed separately from other channels at all positions or sufficiently shielded?	5
Where information encoding/decoding is used, is it sufficient for the detection of signal transmission errors?	10
Are SRECS signal and electrical energy power cables separate at all positions or sufficiently shielded?	5
If subsystems elements can contribute to a CCF, are they provided as physically separate devices in their local enclosures?	5
Diversity/redundancy	
Does the subsystem employ different electrical technologies for example, one electronic or programmable electronic and the other an electromechanical relay?	8
Does the subsystem employ elements that use different physical principles (e.g., sensing elements at a guard door that use mechanical and magnetic sensing techniques)?	10
Does the subsystem employ elements with temporal differences in functional operation and/or failure modes?	10
Do the subsystem elements have a diagnostic test interval of ≤ 1 min?	10
Complexity/design/application	
Is cross-connection between channels of the subsystem prevented with the exception of that used for diagnostic testing purposes?	2
Assessment/analysis	
Have the results of the failure modes and the effects analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?	9
Are field failures analyzed with feedback into the design?	9
Competence/training	
Do subsystem designers understand the causes and consequences of common cause failures?	4
Environmental control	
Are the subsystem elements likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc. over which it has been tested, without the use of external environmental control?	9
Is the subsystem immune to adverse influences from electromagnetic interference up to and including the limits specified in Annex E?	9

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 certified 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.

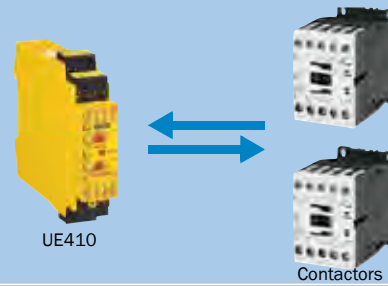
Safe failure fraction (SFF)	Hardware fault tolerance	
	0	1
< 60%	-	SIL1
60 to < 90%	SIL1	SIL2
90 to < 99%	SIL2	SIL3
$\geq 99\%$	SIL3	SIL3

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

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

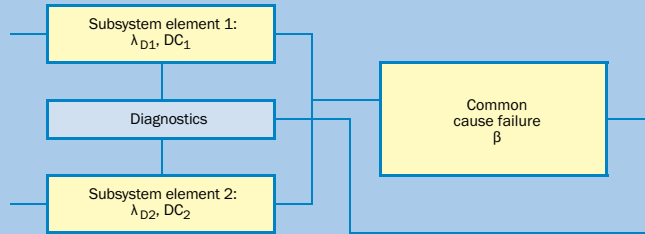
1) Definition of the "actuator" subsystem

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 λ_D

As contactors are subject to wear, the B_{10d} value and the estimated switching frequency must be used to calculate the switching frequency per hour [C].

IEC 62061 contains no statements about the behavior of mechanical components. Therefore, the fault rate λ_D is determined based on ISO 13849-1. It is assumed that the fault rate remains constant during application.

General conditions according to the manufacturer:

- $B_{10d} = 2,600,000$
- $C = 1/\text{hour}$ (assumed value)

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

b) Based on the CCF factor (β)

Measures to avoid common cause failures 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") $PFHd \approx 1.9 \times 10^{-9}$.

$$\lambda_D = \frac{1}{MTTF_d} = \frac{0.1 \times C}{B_{10d}}$$

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

$$PFHd \approx \beta \times (\lambda_{D1} + \lambda_{D2}) \times \frac{1}{2}$$

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

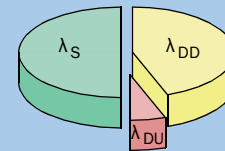
$$\approx 0.05 \times 0.1 \times \frac{C}{B_{10d}}$$

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

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 λ_D 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 common cause failures 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%

3
d

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

6) Evaluation of process measures

Similarly, systematic aspects for the avoidance and management of faults must be taken into account. For example:

- Organization and competence
- Rules governing design (e.g., specification 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" → 3-89).

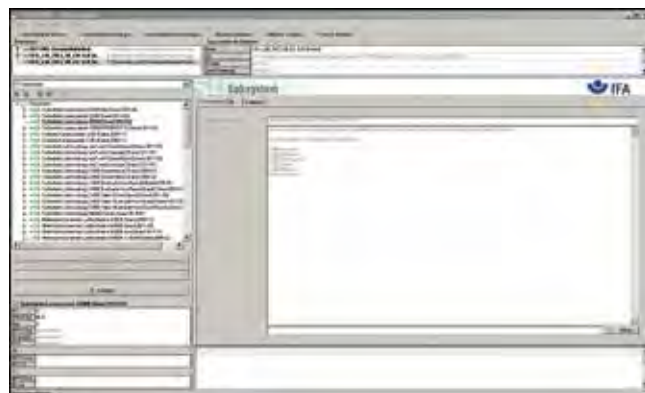


Useful support

The verification methods described require know-how and experience of the concepts of performance level (PL) and safety integrity level (SIL). SICK offers associated services (see "How SICK supports you" → 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 <http://www.sick-safetyplus.com/>

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 it is also possible to determine the safety level of a subsystem that is not certified.

Help

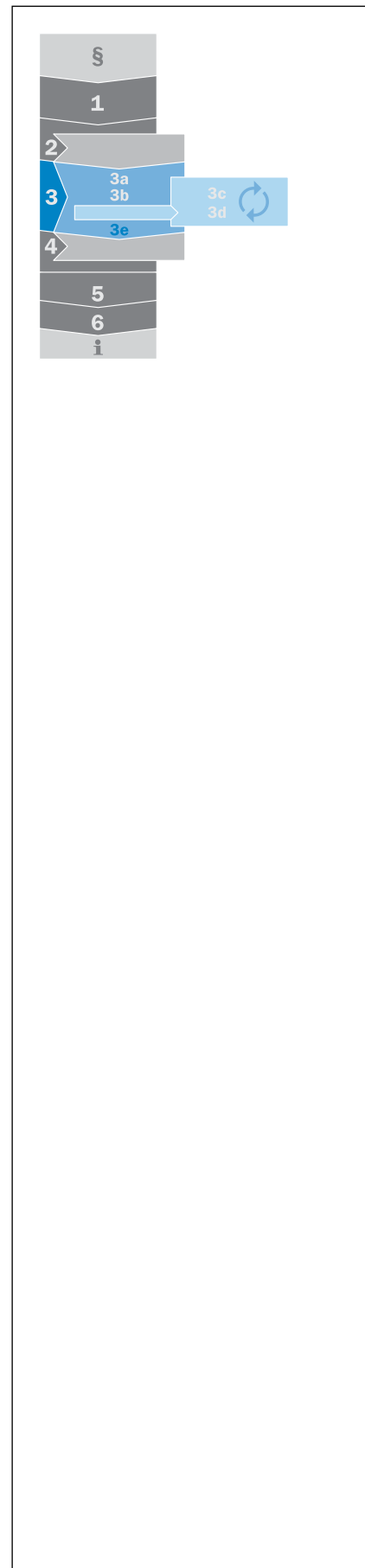
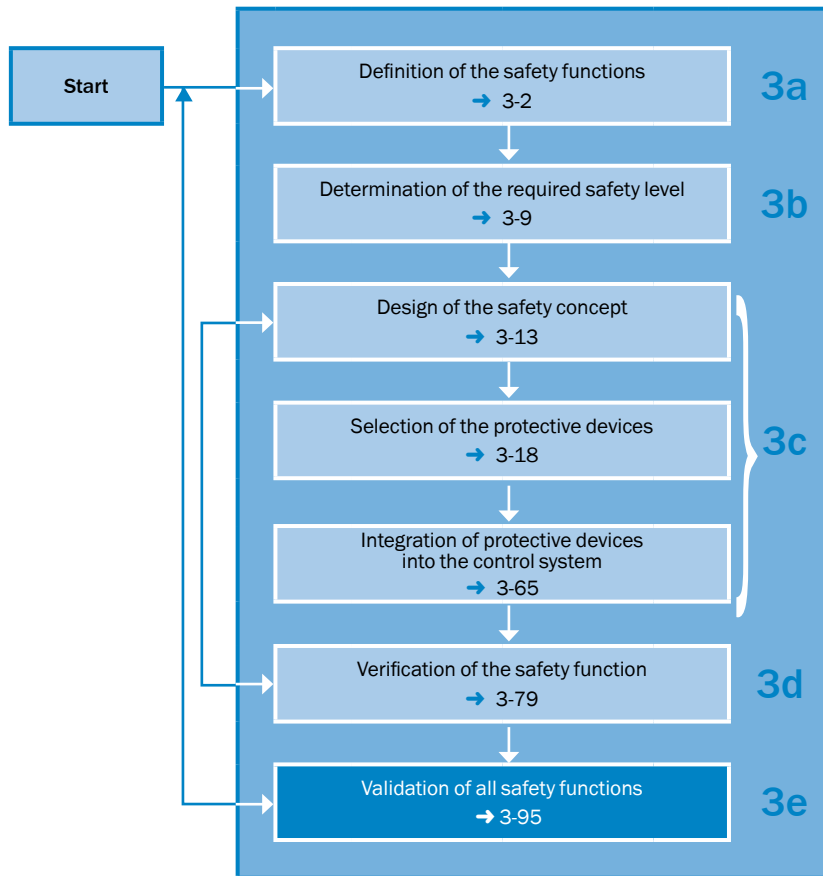
- Use the recommended tools and seek advice.

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 appropriate safety standards (such as ISO 13849-2), in particular the requirements for the level of safety defined.

Insofar as is reasonable, validation should be carried out by people who were not involved in the design of the safety-related parts of the control systems. In some provinces of Canada, this is part of the Pre Start and Health and Safety Review (PSR), and in Brazil, this is part of the Technical Responsibility Annotation of the Regional Council of Engineering and Architecture (ART/CREA).

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 manufacturing 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, particularly if it is possible to stand behind the protective field undetected. 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 using 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

Step 4: Administrative measures / Information for use on 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).

Administrative measures are acceptable only when guards or safeguarding devices (that prevent people from being exposed to machine hazards) cannot be installed due to reasons of infeasibility.

Administrative measures may supplement safe design and engineering controls; however, these administrative measures must not be used in place of them.

Within these administrative measures, standards indicate the use of the following hierarchy:

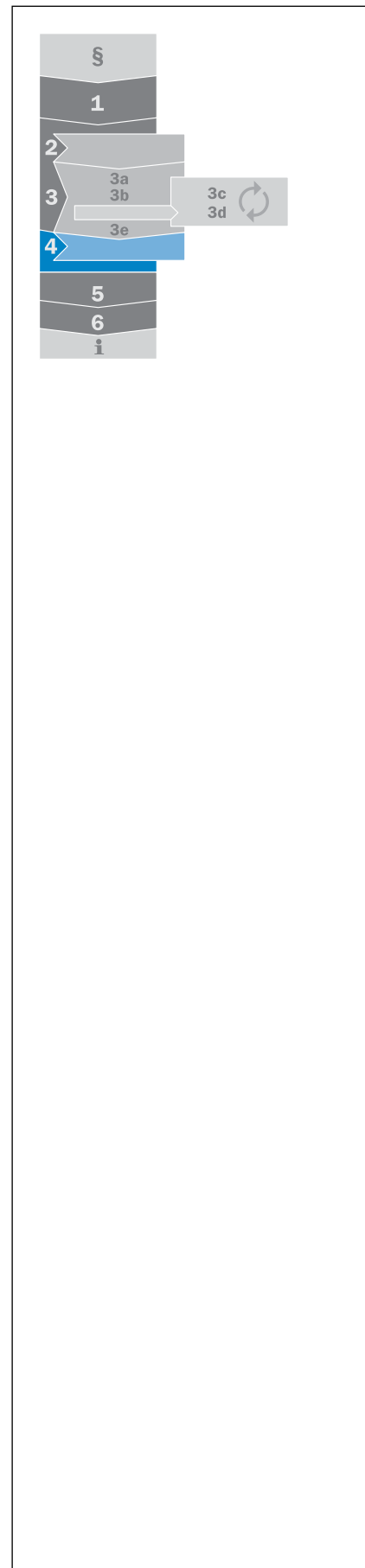
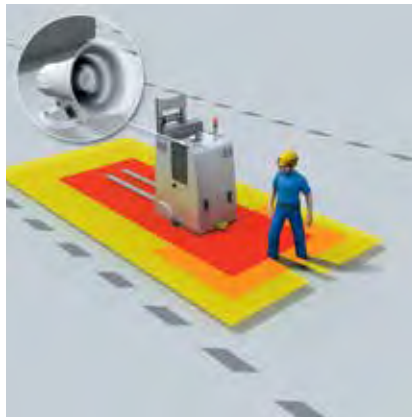
- Awareness means (e.g., signs, lights, horns, beepers, restricted space painted on floor)
- Training and procedures (e.g., safe work procedures, Lockout / Tagout procedures, training of personnel)
- Personal protective equipment (PPE) (e.g., safety glasses, gloves, ear plugs)

→ Hierarchical approach for risk reduction: ANSI B11.0, ANSI/ASSE Z244.1, ANSI/PMMI B155.1-2011, RIA TR R15.406, CSA Z432

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

Acoustic and optical warning devices

When machine hazards may be initiated independent of human action, warnings must be provided on the machine providing information about hazards. 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. Both the supplier(s) and employer have 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.



→ Safety alerting standards: OSHA 1910.145, ANSI Z535 series, NR 26, ISO 3864 series, ISO 7010

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

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 risks are eliminated as far as possible.
2. Define, apply, and check the required protective measures.
3. Define and provide information about residual risks and information about administrative measures.

Technical protective measures

- Either of the ANSI B11.26, 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.

4

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. Adequate 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 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.

Special requirements

It is the law in some regions that before workers operate any machinery, an employer must first have a report prepared by a professional engineer stating which measures need to be taken in order to ensure the safeguarding is adequate and properly applied.

Canada: In some provinces of Canada, including Ontario, the law requires that this report be completed. The report is called a Pre-Start Health and Safety Review (PSR) and is required by PSR Legislation, Section 7 of the Occupational Health and Safety Act. (http://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_900851_e.htm)

Brazil: In Brazil, the standard NR-12 requires that any substantial transformation of the operating system, including retrofitting, shall only be performed by designs prepared by a legally qualified professional, accompanied by a Technical Responsibility Annotation (ART). The ART is a function of the Regional Council of Engineering and Architecture (CREA).



5

Step 6: Deployment of machinery

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

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 or failure.

- For complex assemblies of machines, designate a "site manager" when following the Machinery Directive.
- Clarify in advance the procedure for the machinery or machine components provided.

Safety inspections

Experience shows that in practice, machine safety is not perfect. Protective devices are often manipulated in order to work without interfering with tasks. Other problems are the incorrect positioning of protective devices and improper integration into control systems.

During the operation and maintenance of the machine, the user (typically defined as the employer) shall ensure that the risk level is maintained at an acceptable level, as determined by the risk assessment. The user shall operate and maintain the machine within the established operating limits, and consistent with the information from the supplier addressing operation and maintenance.

The user must also establish and follow a program of periodic and regular inspection and maintenance to ensure that all parts, auxiliary machinery, and safeguards are in a state of safe operating condition, adjustment, and repair in accordance with the supplier's information.

If the user deviates from the supplier information for operation and maintenance or the established operating limits, the user shall consult with the equipment and/or component supplier(s) and shall use the risk assessment process to maintain risk at an acceptable level. See ANSI B11.0 for additional information.

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.

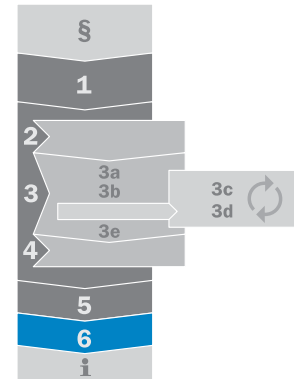
- Draw up a contract specifying how additional documentation is to be provided (e.g., risk assessment, PSR/ART, etc.) so that it will be easier to make changes downstream.
- Define, as far as possible, which standards will be applied (e.g., ANSI consensus standards, harmonized standards in the EU) as the basis.
- Agree upon the procedure in the event of deviations from harmonized standards.

In Europe, the safe 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 employer 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 five parameters shall meet the requirements of the national transposition of the Directive:

1. Type of inspection
2. Scope of the inspection
3. Depth of the inspection
4. Deadlines for the inspection
5. Skills and capabilities of the people responsible for carrying out the inspection

A safety inspection by SICK provides you with a fast overview of the safety status of your machines. We discuss potential for improvement with you and work in partnership to realize them.

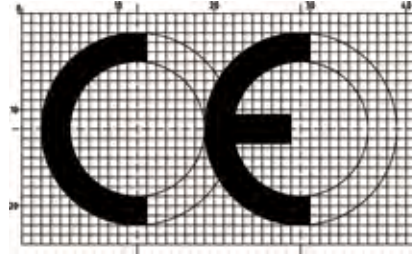


Work Equipment Directive, Article 4a: Inspection of work equipment

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 people 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 people within the meaning of national laws and/or practices
 - Special inspections by competent people 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 (e.g., 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. EC member states shall determine the conditions under which such inspections are made.

Placing products on the European 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, are 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.

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 (→ 1-6) 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 to 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

Warning: If technical documentation is not made available to the responsible national authorities in response 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.

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: Administrative measures / Information for use on residual risks," → 4-1.

6

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

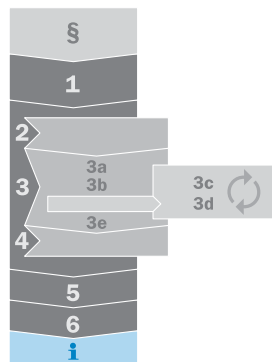
You are quite right to expect your partner to meet exacting requirements. A partner must:

- 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, you can ensure:

- Safety will be planned as an integral part of your project
- Potential weaknesses will be identified early in the process
- Over specifying safety requirements will be avoided
- Effectiveness and competitiveness will be ensured





Services from SICK increase safety and add value.



SICK safety services for the support and design of safe machines and systems

Safety services from SICK are available during each phase of the machine lifecycle. They can be purchased from

SICK individually or as a comprehensive service solution within the scope of a safe machine or system design.

Consulting & Design	
 <ul style="list-style-type: none"> • Risk Assessment • Safety Concept • Hardware & Software Design • Safety Integration • Project Management 	SICK's on-site experts can assist you on the front end of your project. Bringing in SICK's globally available experts at the beginning of your project saves time and money while ensuring you are using the latest technologies appropriately.
Product & System Support	
 <ul style="list-style-type: none"> • Installation • Commissioning 	With reliability and support you can trust, day in and day out. SICK LifeTime Services ensure that the sensor systems and safety devices on your machines and systems are always fully operational.
Verification & Optimization	
 <ul style="list-style-type: none"> • Validation • Inspection • Stop Time Measurement 	Lines change and safety regulations evolve. Our experts can help you make sure your existing machines and solutions continue to run at optimal levels and meet current safety requirements.
Training & Education	
 <ul style="list-style-type: none"> • Safety Education • Product Training — Safety Devices 	Our training programs will give you and your colleagues confidence when working with SICK's products and systems. Safety education from the industry experts ensure you are up to date on current safety regulations.

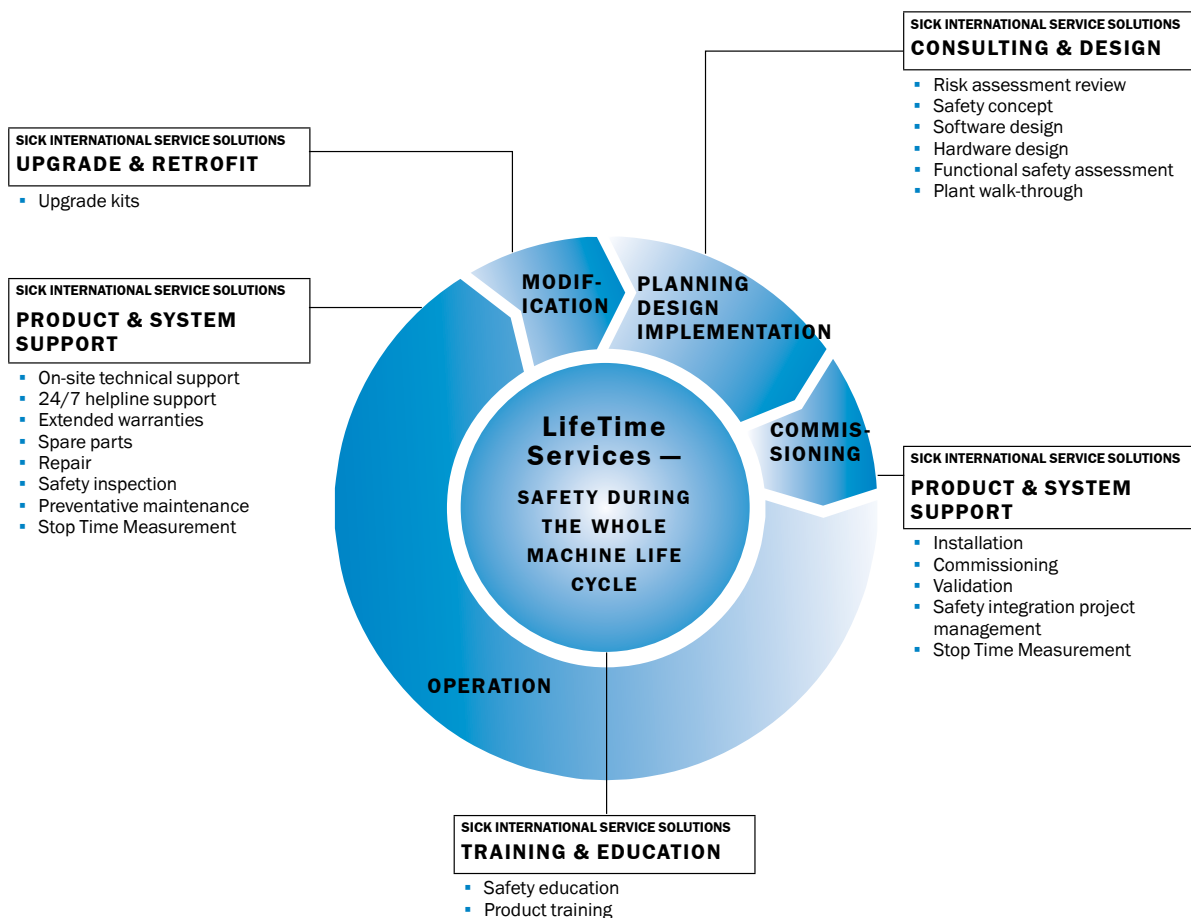
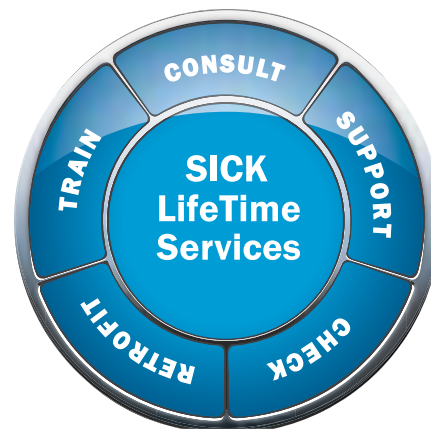
In this chapter ...

SICK safety services	i-1
Training seminars and workshops	i-3
Overview of relevant standards	i-6
Useful links	i-12
Glossary/Index	i-14

SICK – we support your system over the entire product life cycle

Our services are a natural extension of the high-quality products we offer. They ensure reliable and safe performance over the lifetime of the product and machine. They not only protect your initial investment, but also protect your operations and processes from costly downtime and expense, and ensure longer asset life and usefulness. Our staff of professionals are trained to provide the highest level of support and are there when you need them most. Among the many benefits of using SICK's LifeTime Services are:

- Identification of risk to eliminate potentially costly hazards
- Improved solution performance to maximize return on investment
- Rapid response to quickly resolve problems
- Higher productivity and throughput for more cost-effective operations
- Structured responses and predictable resolution planning
- Documentation for more accurate record keeping and future reference



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.

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 product training and safety education 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 customers and the training content to be delivered, we will select the best way of sharing knowledge and safeguarding through:

- Product training
- Safety education
- 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 regulations

Strengthening application safety

Our training seminars are oriented in order to ensure integration of safeguarding solutions into the intended applications in a way that is both efficient and safe in the long term. Attendees 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 (mounting and 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 Product Training & Support, including courses and schedules, please contact your SICK representative or visit us at www.sick.com/us/en-us/home/service/training.

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

Services from SICK	A safe machine in 6 steps			
	§ Laws, regulations, directives, standards	Step 1 Risk assessment	Steps 2 through 4 Risk reduction: The 3-step method	Steps 5 & 6 Overall validation and deployment
Consulting & Design				
• Risk Assessment		✓		
• Safety Concept			✓	
• Hardware & Software Design			✓	
• Safety Integration Project Management		✓	✓	✓
Verification & Optimization				
• Safety Inspection				✓
• Safety Validation				✓
• Stop Time Measurement			✓	✓
Training & Education				
• Safety Education	✓	✓	✓	✓
• Product Training			✓	
Upgrade & Retrofit				
• Upgrade Kits				✓
Product & System Support				
• Installation				✓
• Commissioning				✓
• 24/7 Helpline Support			✓	✓
• On-site Technical Support			✓	✓
• Extended Warranty				✓
• Repair				✓
• Spare Parts				✓



Components (products)

Using certified products makes it easier for machine manufacturers and integrators to prove conformity with the requirements of various standards, regulations, or directives. As a provider of solutions, SICK offers 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.

Consulting: Our knowledge to the advantage of your applications

SICK has subsidiaries or representatives in 87 industrial countries worldwide, where you can access the specialist consulting 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.

- Safety product overview →3-76
- All products are listed in our online product finder at www.sickusa.com/
- To find out more about the services available in your country, contact your national SICK representative or visit us at sick-safetyplus.com/

An overview of the relevant standards

Dated: September 2014

U.S. safety standards

Summary of important consensus standards and technical reports related to machinery safeguarding

American National Standards Institute (ANSI)	
ANSI B11.0	Safety of Machinery – General Requirements and Risk Assessment
ANSI B11.1	Safety Requirements for Mechanical Power Presses
ANSI B11.2	Safety Requirements for Hydraulic and Pneumatic Power Presses
ANSI B11.3	Safety Requirements for Power Press Brakes
ANSI B11.4	Safety Requirements for Shears
ANSI B11.5	Iron Workers – Safety Requirements for Construction, Care and Use
ANSI B11.6	Safety Requirements for Manual Turning Machines with or without Automatic Control
ANSI B11.7	Cold Headers and Cold Formers – Safety Requirements for Construction, Care and Use
ANSI B11.8	Safety Requirements for Manual Milling, Drilling and Boring Machines with or without Automatic Control
ANSI B11.9	Safety Requirements for Grinding Machines
ANSI B11.10	Safety Requirements for Metal Sawing Machines
ANSI B11.11	Safety Requirements for Gear and Spline Cutting Machines
ANSI B11.12	Safety Requirements for Roll-forming and Roll-bending Machines
ANSI B11.13	Single- and Multiple-Spindle Automatic Bar and Chucking Machines – Safety Requirements for Construction, Care and Use
ANSI B11.15	Safety Requirements for Pipe, Tube, and Shape Bending Machines
ANSI B11.16	Safety Requirements for Powder/Metal Compacting Presses
ANSI B11.17	Safety Requirements for Horizontal Hydraulic Extrusion Presses
ANSI B11.18	Safety Requirements for Machine and Machinery Systems for Processing or Slitting Coiled or Non-coiled Metal
ANSI B11.19	Performance Criteria for Safeguarding
ANSI B11.20	Safety Requirements for Integrated Manufacturing Systems
ANSI B11.21	Safety Requirements for Machine Tools Using a Laser for Processing Materials
ANSI B11.22	Safety Requirements for Turning Centers and Automatic, Numerically Controlled Turning Machines
ANSI B11.23	Safety Requirements for Machining Centers and Automatic, Numerically Controlled Milling, Drilling and Boring Machines
ANSI B11.24	Safety Requirements for Transfer Machines
ANSI B11.25	Safety Requirements for Large Machines
ANSI B11.26	Functional Safety for Equipment (Electrical/Fluid Power Control Systems) – Application of ISO 13849 – General Principles for Design
ANSI B11.TR1	Ergonomic Guidelines for the Design, Installation and Use of Machine Tools
ANSI B11.TR2	Mist Control Considerations for the Design, Installation, and Use of Machine Tools Using Metalworking Fluids
ANSI B11.TR3	Risk Assessment and Risk Reduction – A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine Tools
ANSI B11.TR4	Selection of Programmable Electronic Systems (PES/PLC) for Machine Tools
ANSI B11.TR6	Safety Control Systems for Machine Tools
ANSI B11.TR7	Designing for Safety and Lean Manufacturing – A guide on integrating safety and lean manufacturing principles in the use of machinery
ANSI/ITSDF B56.5	Safety Standard for Driverless, Automatic Guided Industrial Vehicles and Automated Functions of Manned Industrial Vehicles
ANSI B65-1	Graphic technology – Safety Requirements for graphic technology equipment and systems – Part 1: General requirements

ANSI/SPI B151.1	American National Standard for Plastics Machinery – Horizontal Injection Molding Machines – Safety Requirements for Manufacture, Care, and Use
ANSI/SPI B151.27	American National Standard for Plastics Machinery – Safety Requirements for the Integration of Robots with Injection Molding Machines
ANSI/PMMI B155.1	Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery
ASME B20.1	Safety Standard for Conveyors and Related Equipment
ANSI/ASSE Z244.1	Control of Hazardous Energy – Lockout/Tagout and Alternative Methods
ANSI O1.1	American National Standard for Woodworking Machinery – Safety Requirements
ANSI/RIA R15.06	American National Standard for Industrial Robots and Robot Systems – Safety Requirements
RIA TR R15.406	Technical Report for Industrial Robots and Robot Systems – Safety Requirements – Safeguarding
RIA TR R15.506	Technical Report for Industrial Robots and Robot Systems – Safety Requirements – Applicability of ANSI/RIA R15.06-2012 for Existing Industrial Robot Applications
ANSI Z535.1	Safety Colors
ANSI Z535.2	Environmental and Facility Safety Signs
ANSI Z535.3	Criteria for Safety Symbols
ANSI Z535.4	Product Safety Signs and Labels
ANSI Z535.5	Safety Tags and Barricade Tapes (for Temporary Hazards)
ANSI Z535.6	Product Safety Information in Product Manuals, Instructions, and Other Collateral Materials
National Fire Protection Agency (NFPA)	
NFPA 70E	Standard for Electrical Safety in the Workplace®
NFPA 79	Electrical Standard for Industrial Machinery
Underwriters Laboratories (UL)	
UL 508	Industrial Control Equipment
UL 61496-1	Standard for Electro-Sensitive Protective Equipment, Part 1: General Requirements and Tests
UL 61496-2	Standard for Electro-Sensitive Protective Equipment, Part 2: Particular Requirements for Equipment Using Active Opto-Electronic Protective Devices (AOPDs)
Semiconductor Equipment and Materials International (SEMI)	
SEMI S2	Environmental, Health, and Safety Guideline for Semiconductor Manufacturing Equipment
SEMI S10	Safety Guideline for Risk Assessment and Risk Evaluation Process
Department of Defense (DoD)	
MIL-STD-882E	Department of Defense Standard Practice – Systems Safety

NOTE: This list of standards and technical reports is not comprehensive, but rather a sampling of the more commonly referenced industry standards and practices used in machine safeguarding.

Canadian safety standards

CSA Z142	Code for power press operation: Health, safety, and safeguarding requirements
CSA Z432	Safeguarding of Machinery
CSA Z434	Industrial Robot and Robot Systems – General Safety Requirements
CSA Z460	Control of hazardous energy – Lockout and other methods
CSA Z1002	Occupational health and safety – Hazard identification and elimination and risk assessment and control

Mexican safety standards

NOM-004-STPS	Protection Systems and Safety Devices for Machinery and Equipment Used in the Workplaces
NOM-029-STPS	Maintenance of Electrical Installations in the Workplace – Safety Conditions

Brazilian regulatory standards (NR)

NR 01	General Provisions
NR 02	Preview Inspection
NR 03	Embargo or Ban
NR 04	Specialized Services in Safety Engineering and Occupational Medicine
NR 05	Internal Commission for Accident Prevention
NR 06	Personal Protective Equipment
NR 07	Programs for Medical Control of Occupational Health - PCMSO / Order SSST (Technical Note)
NR 09	Programs for Prevention of Environmental Risk
NR 10	Safety in Installations and Services in Electricity
NR 11	Transportation, Handling, Storage and Material Handling
NR 11 Annex I	Technical Regulation on Procedures for Transportation, Storage and Handling for Marble Sheets, Granite and Other Rocks
NR 12	Safety in Machinery and Work Equipment
NR 17	Ergonomics
NR 26	Safety Signaling
NR 27	Safety of Work Technician Professional Registry in MTB
NR 28	Inspection and Penalties

Brazilian Association of Technical Standards (ABNT)

Type	Standard	Title/Reference
A	ABNT NBR ISO 12100	Safety of machinery – General principles for design – Risk assessment and risk reduction
B	ABNT NBR NM ISO 13854	Safety of machinery – Minimum clearances to avoid crushing of parts of human body
	ABNT NBR 14152	Safety of machinery – Two-hand control devices – Functional aspects and design principles
	ABNT NBR NM 272	Safety of machinery – Guards – General requirements for the design and construction of fixed and movable guards
	ABNT NBR 14154	Safety of machinery – Prevention of unexpected start
	ABNT NBR NM 273	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection
	ABNT NBR 14153-1	Safety of machinery – Safety related parts of control systems – Part 1: General principles for design
	ABNT NBR 13759	Safety of machinery – Emergency stop equipment – Functional aspects – Principles for design
	ABNT NBR ISO 13855	Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body
	ABNT NBR NM ISO 13852	Safety of machinery – Safety distances to prevent danger zones being reached by the upper limbs
	ABNT NBR NM ISO 13853	Safety of machinery – Safety distances to prevent danger zones being reached by the lower limbs
	ABNT NBR 5410	Electrical installations of buildings – Low voltage electrical installations
	ABNT NBR 13970	Safety of machinery – Temperatures of touchable surfaces – Ergonomic data for setting temperature limits of hot surfaces
	C	ABNT NBR 13930
ABNT NBR ISO 23125		Machine tools – Safety – Turning machines
NBR 13862		Continuous conveyors – Belt conveyors – Safety requirements for project
NBR 13536		Injection molding machines for plastics and rubber – Technical safety requirements for design, construction and use
NBR 13996		Blow molding machines Intended for the production of hollow plastic articles – Safety requirements for design and construction

European / International safety 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
	EN 1037	✓	ISO 14118	Prevention of unexpected start-up
	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 safeguards with respect to the approach speeds of parts of the human body
	EN ISO 13857 (replaces EN 294 and EN 811)	✓	ISO 13857 (replaces ISO 13852 and ISO 13853)	Safety distances to prevent hazard zones being reached by upper and lower limbs
	EN 60204-1	✓	IEC 60204-1	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)
			✓	IEC 61508
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	
			IEC 61800-5-2	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional

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 ...?				
<p>Information about laws and standards</p>	<p>United States</p> <p>U.S. — OSHA: → www.osha.gov/index.html</p> <p>U.S. — National Fire Protection Association: → www.nfpa.org</p> <p>American Society of Mechanical Engineers (ASME): → www.asme.org</p> <p>American Society of Safety Engineers (ASSE): → www.asse.org</p>	<p>Canada</p> <p>Canada: → www.ccohs.ca/oshanswers/information/govt.html → www.csa.ca</p> <p>Ontario: Pre Start Health and Safety Reviews: → www.labour.gov.on.ca/english/hs/pdf/gl_psr.pdf</p> <p>Occupational Health and Safety Act: → www.labour.gov.on.ca/english/hs/pubs/ohsa/index.php</p> <p>Electrical Safety in Ontario, Electrical Safety Authority: → www.esasafe.com</p> <p>Electrical approvals: → www.labour.gov.on.ca/english/hs/guidelines/liveperformancegl_live_apx_a.html → www.labour.gov.on.ca → www.iapa.ca</p>	<p>Mexico</p> <p>Information about Mexican regulations: → www.mexicanlaws.com → www.stps.gob.mx/bp/secciones/english/index.html</p>	<p>Brazil</p> <p>Information about Brazilian regulations: → portal.mte.gov.br/legislacao/normas-regulamentadoras-1.htm</p> <p>Information about Brazilian standards: → www.abnt.org.br</p>
<p>Order standards</p>	<p>→ web.ansi.org → www.global.ihs.com → www.nssn.com</p>			<p>→ www.abntcatalogo.com.br/default.aspx</p>
<p>Machine related</p>	<p>Machine Tools (B11 Series): → b11standards.org</p> <p>Industrial Robotics: → www.robotics.org</p> <p>Packaging and Process Technologies: → www.pmmi.org</p> <p>Plastics Industry: → www.plasticsindustry.org</p> <p>Printing, Publishing and Converting Technologies: → www.npes.org</p> <p>Industrial Trucks: → www.itsdf.org</p> <p>Semiconductor Equipment: → www.semi.org/en</p>			




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: → www.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: → ec.europa.eu/enterprise/policies/european-standards/documents 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 (SNV): → 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

Glossary/Index

Abbreviation/Term	Definition	Index
λ Failure rate per hour	<p>λ: Failure rate per hour, λ_S and λ_D added together</p> <ul style="list-style-type: none"> • λ_S: Safe failure rate • λ_D: Dangerous failure rate, can be divided into: <ul style="list-style-type: none"> • λ_{DD}: Dangerous failure rate for failures detected by diagnostic functions • λ_{DU}: Dangerous failure rate for failures that go undetected 	<p>→ 3-15</p> <p>→ 3-90</p>
β factor	<p>Susceptibility to common cause failures (IEC 62061)</p> <p>→ CCF</p>	<p>→ 3-90</p> <p>→ 3-91</p>
A		
AOPD Active optoelectronic protective device	<p>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).</p> <p>In DIN EN 692 “Mechanical presses”, EN 693 “Hydraulic presses”, and EN 12622 “Hydraulic press brakes” the abbreviation AOS is used as a synonym for AOPD.</p>	→ 3-28
AOPDDR Active optoelectronic protective device responsive to diffuse reflection	<p>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).</p>	→ 3-29
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).	→ 3-87
BGIA	→ IFA	→ §-15
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.	→ 3-83
CCF Common cause failure	Failure of various units due to a single event where these failures are not caused by each other.	<p>→ 3-15</p> <p>→ 3-85</p> <p>→ 3-91</p>
CENELEC Comité Européen de Normalisation Electrotechnique	<p>European Committee for Electrotechnical Standardization. Responsible for the harmonization of electrotechnical standards within the European Union and the entire European Economic Area.</p> <p>→ www.cenelec.eu/</p>	→ §-12
CLC	Prefix for standards adopted by CENELEC.	→ §-13
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.	→ 3-85
d_{op}	Mean operating time in days per year.	→ 3-87
Dpf Depth penetration factor	The distance that an individual could extend toward the hazard through the plane or field of a safeguarding device and penetrating the hazard area before the safeguard initiates the stop command	→ 3-45
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.	<p>→ 3-70</p> <p>→ 3-87</p> <p>→ 3-92</p>
EFTA European Free Trade Association	An international organization founded by European states.	→ §-12
Element safety functions	The part of a safety function that is provided by a safety-related element (e.g., actuator) for risk reduction.	→ 3-72
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.	→ 2-12

Abbreviation/Term		Definition	Index
ESPE	Electro-sensitive protective equipment	<p>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):</p> <ul style="list-style-type: none"> • Sensor element • Control and/or monitoring devices • Switching outputs (→ OSSD) <p>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.</p>	→ 3-27
F			
FIT	Failure in time	<p>Failure rate in 10^{-9} hours</p> <p>→ $\lambda = 1 \times 10^{-9} 1/h$</p>	→ 3-15
FMEA	Failure mode and effects analysis	Procedure for analyzing the effects of failures (IEC 60812/EN 60812).	→ 3-15 → 3-85
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
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).	→ 3-90
h_{op}	Operating hours	Mean operating time in hours per day.	→ 3-87
I			
IFA	Institut für Arbeitsschutz	Institute for Occupational Safety and Health of the German Social Accident Insurance Association. Until 2009: BGI.	→ §-15
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.	→ 3-20
L			
Lambda λ		→ λ	→ 3-15 → 3-90
Light curtain		<p>An AOPD with a resolution of ≤ 116 mm.</p> <p>In many North American standards, a resolution ≤ 64 mm is suitable for finger and hand protection, while Brazilian, International and European standards require a resolution ≤ 40 mm.</p>	→ 3-27 → 3-44
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.	→ 3-44
MTTFd	Mean time to dangerous failure	Expected value for the mean time to dangerous failure (ISO 13849-1/EN ISO 13849-1).	→ 3-84
Muting		Muting function. Temporary automatic suspension of one or more safety functions by safety-related parts of the control system (IEC 61496-1/EN 61496-1).	→ 3-35
N			
N/C	Normally closed	Normally closed contact	→ 3-70
N/O	Normally open	Normally open contact	→ 3-70
n_{op}	Number of operations per year	<p>Mean number of operations per year (ISO 13849-1/EN ISO 13849-1)</p> $n_{op} = \frac{d_{op} \times h_{op} \times 3600 \frac{s}{h}}{t_{cycle}}$	→ 3-87
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.	
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.	→ 3-28

Abbreviation/Term		Definition	Index
P			
PFHd	Probability of dangerous failure per hour	Mean probability of a dangerous failure per hour (1/h).	→ 3-81
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).	→ 3-81
Placing on the market		Making available for the first time in the European Community machinery or partly completed machinery with a view to distribution or use, whether for reward or free of charge (Machinery Directive 2006-42-EC)	→ 6-3
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).	→ 3-23
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).	→ 3-48
Protective field		The area in which the test object specified by the manufacturer is detected by the electro-sensitive protective equipment (→ ESPE). <ul style="list-style-type: none"> • 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). 	→ 3-30
PSDI	Presence-Sensing Device Initiation	Operating mode of indirect manual initiation of a single cycle by a presence-sensing device when it senses that work motions of the operator related to feeding or removing parts are completed and all parts of the operator's body are withdrawn from the sensing field of the device (ANSI B11.19).	→ 3-38
R			
Reset		Resetting the protective device to the monitored status. <ul style="list-style-type: none"> • 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 people in the hazard zone during and after reset. 	→ 3-43 → 3-64
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.	→ 3-30
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.	→ 3-44
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.	→ 3-64
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, and after a change to the device used to control starting of the machine (IEC 61496-1/EN 61496-1). <ul style="list-style-type: none"> • 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. 	→ 3-55
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.	→ 3-30

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 62061/EN 62061).	→ 3-90
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).	→ 3-89
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).	→ 3-89
Single-break/double-break PSDI mode:		<p>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:</p> <ul style="list-style-type: none"> • 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/ RIA TR R15.406, CSA Z432, EN 61496-1) <p>→ More information: EN 692</p> <p>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 protect all other sides of the machine.</p> <p>If this operating mode is activated, the resolution of the AOPD must be less than or equal to 30 mm (see ANSI B11.19, CSA Z432, ISO 13855, RIA TR R15.406, EN 692, and EN 693).</p> <p>As a general rule, when mounting protective devices, the following faults must be excluded: reaching over, reaching under, reaching around, standing behind.</p>	→ 3-38
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).	→ 3-65
T			
T_{10d}		<p>Limit for the operating time of a component. Mean time until a dangerous failure has occurred on 10% of the components.</p> $T_{10d} = \frac{B_{10d}}{n_{op}}$ <p>The MTTFd determined for components subject to wear only applies for this time.</p>	
T_{cycle}		The mean time between the start of two sequential cycles of a part in seconds per cycle	
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)	
V			
VBPD	Vision-based protection device	Protective devices based on image evaluation, e.g., safety camera systems.	→ 3-29























SICK AT A GLANCE

SICK is a leading manufacturer of intelligent sensors and sensor solutions for factory, logistics, and process automation. With more than 6,000 employees and over 40 subsidiaries 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/Luxembourg, Brazil, Czech Republic, Canada, China, Denmark, Finland, France, Germany, Great Britain, Hungary, India, Israel, Italy, Japan, Mexico, Netherlands, Norway, Poland, Romania, Russia, Singapore, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Turkey, United Arab Emirates, USA

Please find detailed addresses and additional representatives and agencies in all major industrial nations at: www.sick.com