Guidelines for Safe Machinery

safety PLUS®

Six steps to a safe machine

SICK
Sensor Intelligence.

Six steps to a safe machine

For safe machinery, the supplier and user need to work together from the beginning. There are regulations for the protection of user personnel. Regulations may be subject to regional variations. However, there is a general process to be employed during the manufacture and upgrade of machinery:

- During the design and manufacture of machinery, the supplier and user shall identify and evaluate all possible hazards and hazardous points by undertaking a risk assessment.
- Depending on this risk assessment, the supplier and user should agree how to eliminate or reduce the risk by suitable measures. If the risk cannot be eliminated by design measures, the supplier and user shall define and select suitable engineering controls. If the remaining risk is not acceptable, administrative measures such as organizational procedures should be implemented.
- To ensure the intended measures work correctly, overall validation is necessary. This overall validation shall evaluate the design and engineering controls, as well as the administrative measures.

We will guide you to a safe machine in six steps. You will find the procedure on page P-3.

About these guidelines

What are the guidelines?

This document contains an extensive set of guidelines about the safety of machinery and the selection and usage of protective devices. SICK will show you various ways in which you can protect machinery and people against accidents. This is not an exhaustive list. The examples given are the result of our many years of practical experience and are to be considered generic, not specific, applications.

These general guidelines describe the safety 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 these guidelines. Review of these guidelines is not a substitution for your own, independent, legal analysis.

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

We refer only to the latest, published regulations and standards at the time of publishing, if not mentioned otherwise.

Target audience for the guidelines?

These guidelines are aimed at manufacturers, operating organisations, designers, system engineers and all individuals who are responsible for machine safety. (For reasons of legibility, we will use mostly male terms in the following information.)

Editorial Team

Safety experts: Rolf Agner, Ian Brough, Juergen Bukowski, Howard DeWees, Mark Esau, John Keinath and our European colleagues for their version of the guideline.

Editors:

Lindsay Hartfiel, Tracie Manor


§
Laws, regulations, standards → §-1
Regulations → §-1
Standards → §-4
Testing laboratories → §-5
1
Risk assessment → 1-1
Process of risk assessment → 1-1
Identify the hazards → 1-3
Risk estimation → 1-4
Risk evaluation → 1-5
Risk reduction — The 3-step method 2-2
2
Safe design → 2-3
Mechanical design → 2-3
Operating and maintenance concept → 2-4
Electrical Equipment → 2-5
Lock-out / Tag-out → 2-8
Stop functions and actions in an emergency → 2-9
Electromagentic compatibility (EMC) → 2-10
Fluid technology → 2-11
3
Engineering controls → 3-1
a Defining the safety functions → 3-2
b Determining the necessary safety performance → 3-7
Implementation of the safety functions
c Designing the safety function → 3-11
Selection of the protective devices → 3-16
Positioning/dimensioning the protective devices → 3-30
Integration of the protective devices in the control system → 3-40
Product selection → 3-48
d Verifying the safety function → 3-51
e Validating all safety functions → 3-69
4
Administrative measures → 4-1
5
Overall validation of the machine → 5-1
6
Operating the Machine → 6-1
Annex
How SICK supports you → i-1
Overview of relevant standards → i-4
Useful links → i-7
Glossary → i-8
Space for your notes → i-11

Safeguarding people

The requirements for the protection of machinery have changed more and more with the increasing use of automation. In the past, sometimes safeguarding machinery was viewed as a nuisance. As a result, safety devices were often not used at all. Innovative technology has enabled protective devices to be integrated into the work process. If properly applied, they are no longer a hindrance for the operator. Indeed they often improve productivity. For this reason, reliable protective devices integrated into the workplace are essential.

Safety is a basic need

Safety is a basic need of people. Studies show that people who are continually 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:
Machine operator, maintenance personnel and others shall be able to rely on the safety of a machine.
It is often said that more “safety” reduces productivity — if done correctly, the opposite can actually be the case. Higher levels of safety result in increased motivation and satisfaction, and as a result higher productivity.

Safety is a management task

Decision makers in industry are responsible for their employees as well as for smooth, cost-effective production. Only if the management make safety part of every day business will the employees be receptive to the subject.

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

Involvement of the employees results in acceptance

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

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.

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.A. regulatory requirements

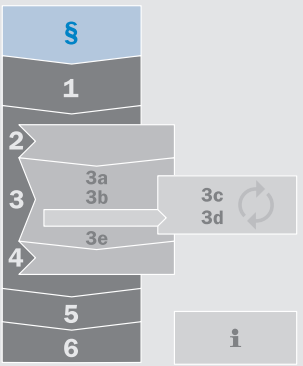
Worker safety regulations in the United States are enforced through the Occupational Safety and Health Administration (OSHA). The United States Congress, through the Occupational Safety and Health Act, established OSHA on December 29, 1970.

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.

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



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.

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.

This information may be obtained at OSHA’s internet web site at:
→ http://osha.gov/dcsp/osp/index.html
→ 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:

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

1) The Connecticut, New Jersey and New York State Plans cover public sector (State and Local Government) employment only.

§

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: Everyone 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

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)

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.

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, ... , two-hand control 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.

For additional information on Prestart Health and Safety Reviews, please consult the following link:
➜http://www.labour.gov.on.ca/english/hs/guidelines/prestart/index.html

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. NOM 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-1999 is the official Mexican standard that defines the requirements of protection systems and safety devices for machinery and equipment used in the workplace.

§

Standards

Standards are agreements made between the various interested parties (manufacturers, users, 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 hundred years, a change from national standards to globally-applicable standards has taken place. Depending on the place the machine or product is to be used, different legal stipulations may apply that make it necessary to apply different standards. The correct selection of the standards to be applied is an aid for the machine manufacturer for compliance with the legal requirements.

Organizations and structures for worldwide standardization

ISO (International Standardization Organization)

ISO is a worldwide network of standardization organizations from 157 countries. ISO prepares and publishes international standards focused on non-electrical technologies.

IEC (International Electrotechnical Commission)

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

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 occupational safety and health 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.

A summary of important ANSI and other safety standards 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.

§

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/otpca/nrtl/

§

Summary: Laws, directives, standards

Regulations

- National regulations ensure 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

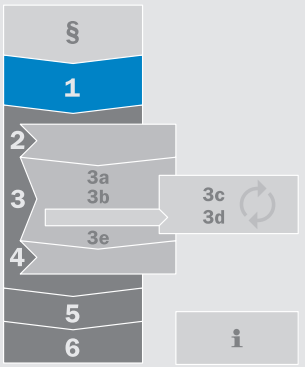
- Technical standards specify in detail the objectives defined in the regulations.
- In the absence of a national standard or regulation, international standards can be used.

Testing laboratory:

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

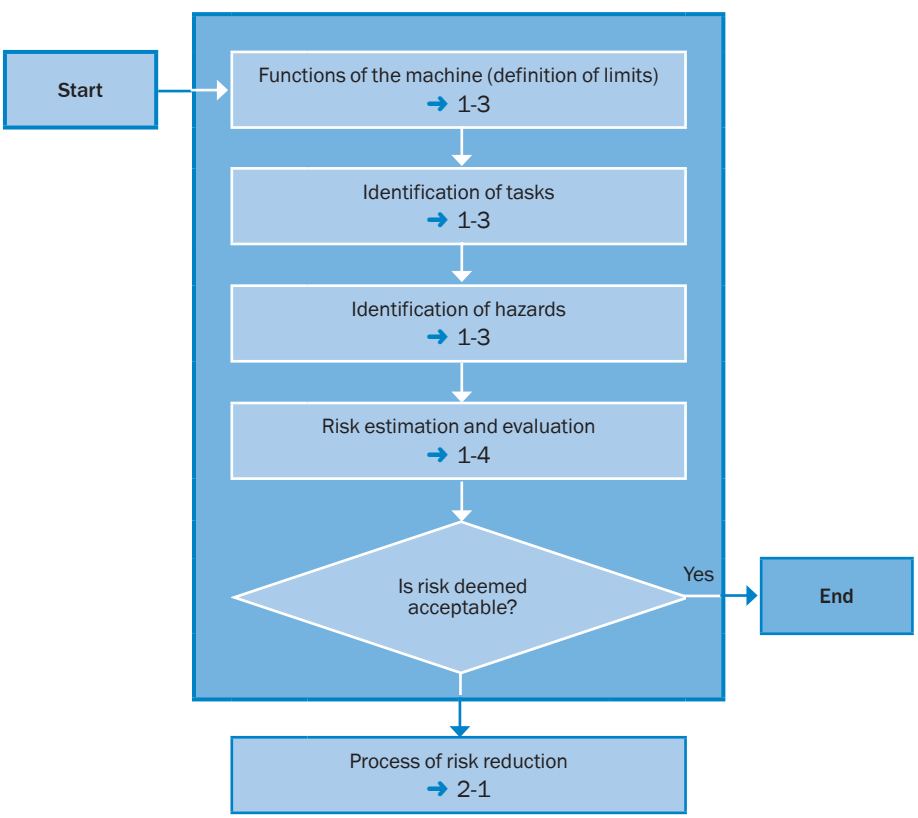
Step 1: Risk assessment

When designing or using a machine, the potential risks must be assessed and evaluated. Where necessary, additional protective measures must be implemented to protect operators and other individuals from hazards such as crushing, shearing, cutting, snatching, clamping, trapping, perforation, puncturing, risk of shock, and more. A risk assessment is a sequence of logical steps that permit the systematic analysis and evaluation of risks. The machine shall be designed and used taking into account the results of the risk assessment. Where necessary, risk reduction follows a risk assessment by applying suitable protective measures. A new risk shall not result from the application of protective measures. The repetition of the entire process, risk assessment and risk reduction, may be necessary to eliminate hazards as far as possible and to sufficiently reduce the risks identified. When possible, the user should participate in the supplier's risk assessment of the machine's design.



→ Risk assessment — ANSI B11.TR3, ANSI B11.2008, ANSI RIA 15.06, CSA Z434, ISO 14121

The risk assessment process



- The process shall be performed for all hazards. It shall be repeated (iterative process) until acceptable risk has been achieved.
- The risk assessment shall be documented.

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, 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 could be:

- the specification for the machine (what is produced, maximum production performance, materials to be used)
- physical boundaries and expected place of use
- the planned service life
- the intended functions and operating modes
- the malfunctions and faults to be expected
- the people involved in the machine process
- the products related to the machine
- the correct use, and 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.

Reasonably foreseeable misuse

The 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 failure during the usage of the machine
- incorrect action due to lack of concentration or carelessness
- incorrect action 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 faults to be expected

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

- reversing of roller movement (such that hands are drawn in)
- movement of a robot outside its normal working area

Identify the 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

Identify 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.

1

Hazards may include but are not limited to the following...	...in all phases of the service life of the machine.
■mechanical hazards ■electrical hazards ■thermal hazards ■hazards due to noise ■hazards due to vibration ■hazards due to radiation ■hazards due to materials and substances ■hazards due to neglecting ergonomic principles during the design of machinery ■hazards due to slipping, tripping and falling ■hazards related to surroundings in which the machine is used ■hazards resulting from a combination of the above mentioned hazards	■transport, assembly and installation ■commissioning ■setup ■normal operation and troubleshooting ■maintenance and cleaning ■decommissioning, dismantling and disposal

Risk estimation & risk evaluation

The next step is to perform a risk estimation for each task and its associated hazard(s). A variety of standards and technical reports have been developed to assist users with this process.

The risk related to the hazardous situation considered depends on the following elements:

Risk = **Extent of injury** × **Probability of occurrence**

■the extent of injury that can be caused by the hazard (minor injury, serious injury, etc.) and

■the probability of occurrence of this injury. This is given by:
- the exposure of a person/people to the hazard
- the occurrence of the hazardous event and
- the technical and human possibilities for the prevention or limitation of injury

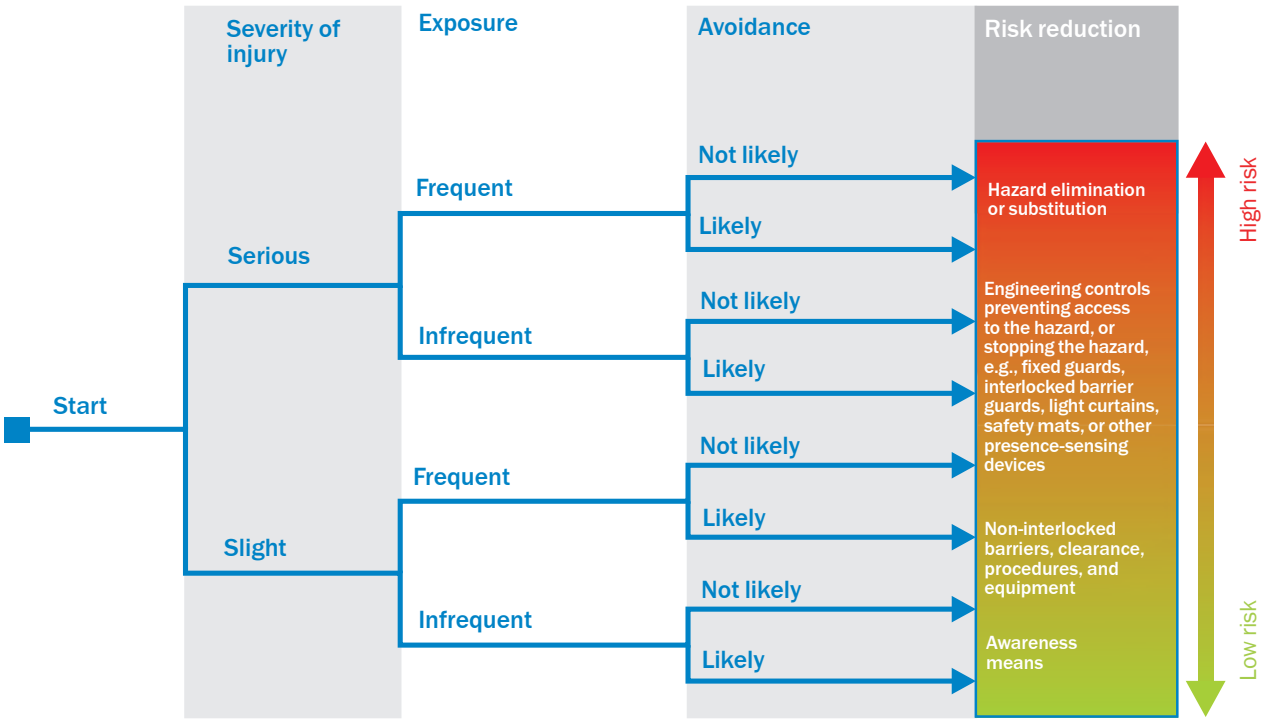
Various risk assessment standards and technical reports utilize different approaches in considering these factors. Based on applicable national, regional and local regulations, please reference one or more of the following standards or technical reports relating to risk assessment and risk reduction categories and associated requirements:

Standard	Description
ANSI / RIA R15.06	Safety Requirements for Robots and Robot Systems
ANSI B11.TR3	Risk Assessment and Risk Reduction - A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine Tools
CAN / CSA Z434	Safety Requirements for Robots and Robot Systems
ISO 14121	Safety of Machinery - Principles for Risk Assessment
ISO 12100	Safety of Machinery - Basic concepts - General principles of design

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

- information about the machine such as specifications, limits, correct use, etc.
- important assumptions that have been made, such as loads, strengths, safety coefficients
- hazards and hazardous situations identified and hazardous events considered
- data used and their sources as well as the accident histories and experience related 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 related to the machine
- list of documents used during the risk assessment
- various tools are available for the estimation of risks, e.g., tables, risk graphs, and numeric methods.

A guided tour of a risk assessment tool called Safexpert is available on the Internet. http://www.sick.com/safexpert/

1

Summary: Risk assessment

General

- Perform a risk assessment for all reasonably foreseeable hazards. This iterative process shall take into account all hazards and risks until only acceptable residual risks remain.

Process of risk assessment

- Start the risk assessment with the definition of the functions of the machine.
- During the risk assessment take into account foreseeable misuse and faults.
- Identify the tasks (performed by operators, maintenance personnel, etc.) and associated hazards (mechanical, electrical, thermal, etc.) of the machine. Take into account these hazards in all phases of the service life of the machine.
- Then estimate the risks due to the hazards. These depend on the extent of injury and the probability of occurrence of the injury.

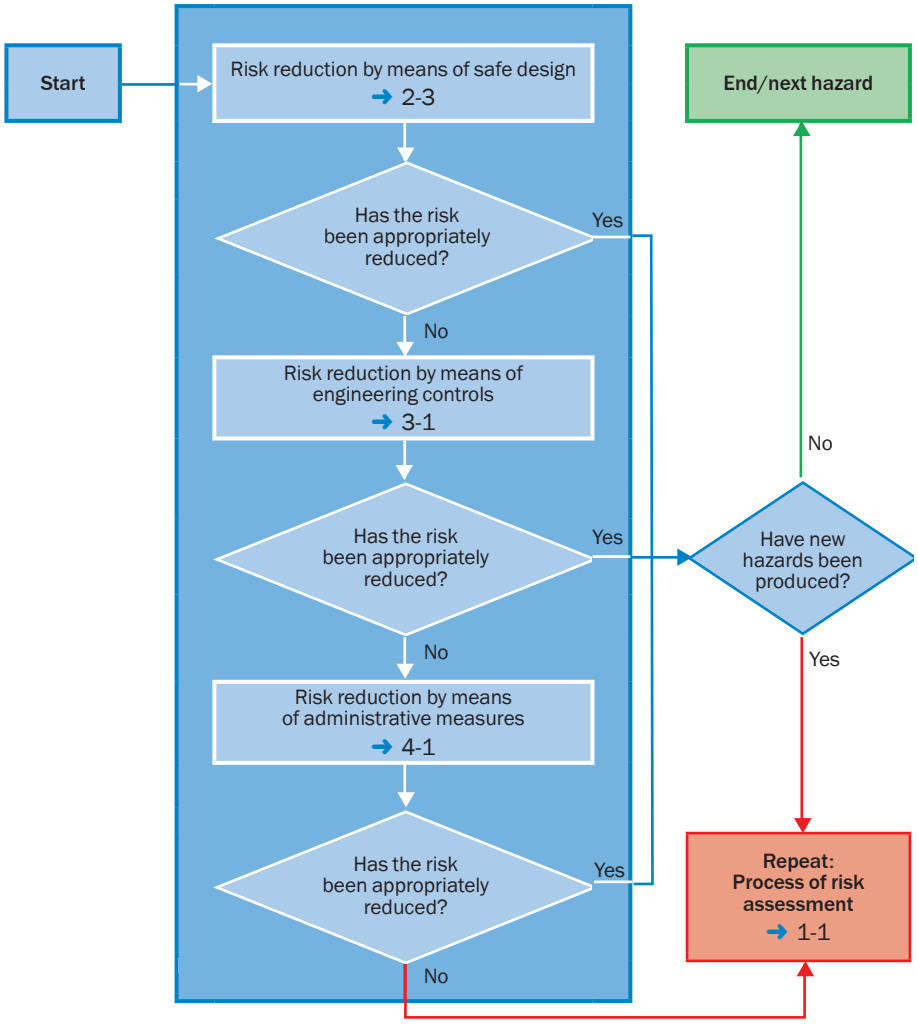
Steps 2 — 4: Risk reduction

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

The 3-step method

The machine manufacturer shall apply the following principles during the selection of the measures, and in the order given:

1. Safe design: elimination of residual risks as far as possible (integration of safety in design and construction of the machine)
2. Protective measures by using engineering controls
3. Administrative measures to inform and warn about the residual risks



→ General principles about the process of risk reduction: ISO 12 100-1, -2, ANSI

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 the least effective solution
5. Personal protective equipment.

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

Table — Hierarchy of safeguarding controls ANSI/RIA R15.06-1999

Risk Reduction Strategy	Examples
1. Elimination or substitution by changes in machine design	• Eliminate human interaction in the process • Eliminate pinch points (increase clearance) • Automated material handling
2. Engineering control (safeguarding technology)	• Mechanical hard stops • Barriers • Interlocks • Presence sensing devices • Two-hand controls
3. Administrative measures	• Lights, beacons and strobes • Computer warnings • Signs • Restricted space painted on floor • Beepers • Horns • Labels
	• Safety job procedures • Safety equipment inspections • Training
	• Safety glasses • Ear plugs • Face shields • Gloves

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 hazards are excluded by design. For this reason, safe design is the most effective.

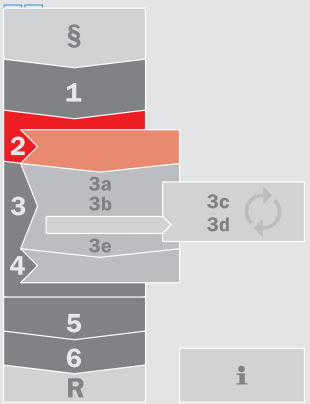
Aspects of safe design relate to the machine itself and the interaction between the person at risk and the machine.

Examples:

- mechanical design
- operating and maintenance concept
- electrical equipment (electrical safety, EMC)
- concepts for stopping in an emergency
- equipment involving fluids
- used materials and lubricants
- machine function and production process

In any case, all components are to be selected, used and adapted such 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 surroundings is also to be taken into consideration.

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

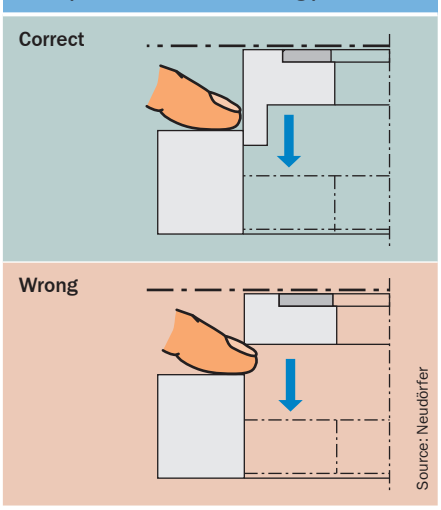


Mechanical design

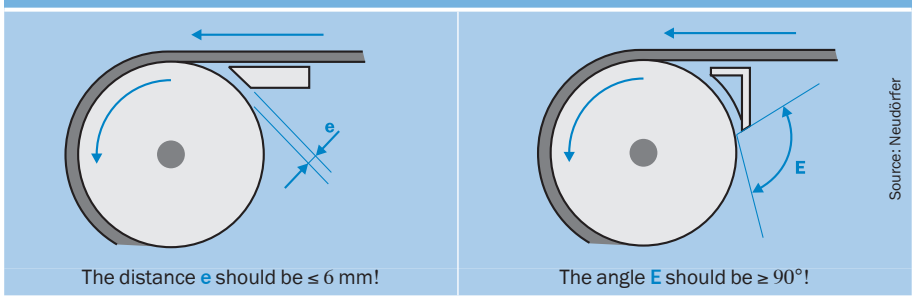
The first objective of every design shall be to prevent the occurrence of hazards in the first place. This objective can be achieved, for example, by means of:

- avoidance of sharp edges, corners and protruding parts
- avoidance of crushing points, shearing points and entanglement points
- limitation of the kinetic energy (mass and velocity)
- consideration of ergonomic principles

Example: Avoidance of shearing points



Examples: Avoidance of entanglement points



The distance e should be ≤ 6 mm!

The angle E should be ≥ 90°!

Operating and maintenance

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

- automatic loading and unloading stations
- maintenance work from the “outside”
- 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.

➜ Color coding convention: NFPA 79 / IEC60204

General meaning of the colors for controls

Color	Meaning	Explanation
White Grey Black	Unspecific	Initiation of functions
Green	Safe/Start/ON	Actuate during safe operation or to establish normal situation
Red	Emergency / Stop / OFF	Actuate in hazardous situation, emergency situations or stop/ off commands
Blue	Instruction	Actuate in situation that requires mandatory action
Yellow	Abnormal	Actuate in abnormal situation

General meaning of the colors for indicators

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

Electrical equipment

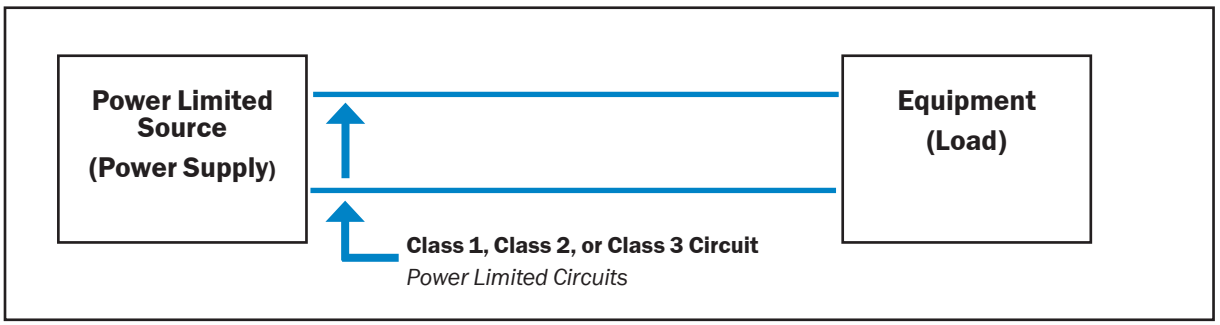
Measures are necessary to exclude electrical hazards on machines. Here a differentiation is made between two types of hazards:

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

➜ In the following sections, and in NFPA 79, NFPA 70, you will find important information on the design of the electrical equipment.

Protection against electric shock

The National Electrical Code (NEC) is the 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 24VDC power supply (the most commonly used Class 2 voltage), the maximum power allowed is 100W. 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

Protection by Enclosures

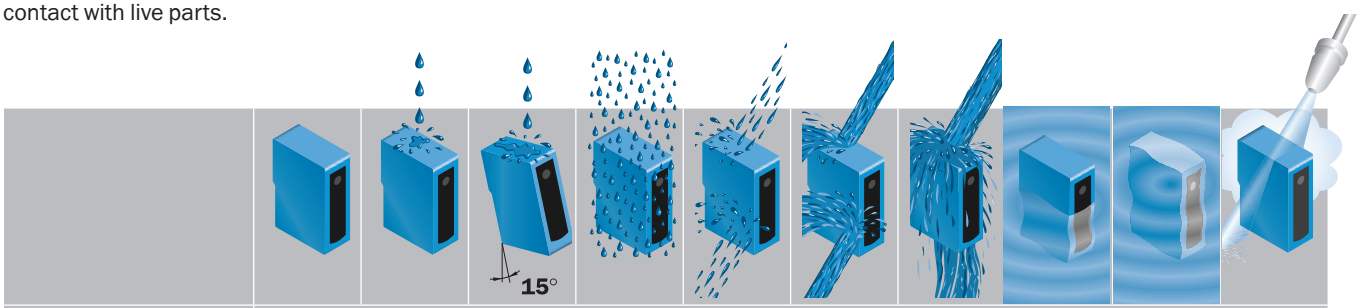
Typically electrical equipment enclosures need to meet the requirement for enclosure ratings. Two widely accepted rating systems are the NEMA types/number and the IP rating code. NEMA, short for National Electric Manufacturers' Association, and their type number system is commonly specified at installations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

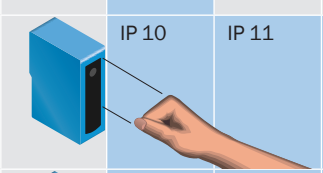
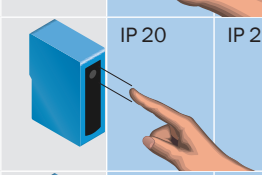
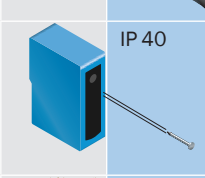
The NEMA classifications are as follows.

Standard NEMA **Suggested Usage**	**NEMA 1** **Inside**	**NEMA 2** **Inside**	**NEMA 3** **Outside**	**NEMA 3S** **Outside**	**NEMA 4** **Inside or Outside**	**NEMA 4X** **Inside or Outside**	**NEMA 6** **Inside or Outside**	**NEMA 6P** **Inside or Outside**	**NEMA 12** **Inside**	**NEMA 13** **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 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		

The enclosure IP ratings describe the protection against the entry of water (not water vapor) and foreign bodies (dust). In addition, they describe the protection against direct physical contact with live parts.

Typically control cabinets should be IP 54.



1st digit: Protection against the entry of foreign bodies		**2nd digit:** Protection against the entry of water (not water vapour, not other liquids!)									
		IP ...0	**IP ...1**	**IP ...2**	**IP ...3**	**IP ...4**	**IP ...5**	**IP ...6**	**IP ...7**	**IP ...8**	**IP ...9K**
		No protection	Dripping water vertical	Dripping water at an angle	Sprayed water	Splashed water	Water jet	Water jet, powerful	Immersion temporary	Immersion permanent	100 bar, 16 l/min., 80 °C
IP 0... No protection		IP 00									
IP 1... Size of the foreign body ≥ 50 mm ∅		IP 10	IP 11	IP 12							
IP 2... Size of the foreign body ≥ 12 mm ∅		IP 20	IP 21	IP 22	IP 23						
IP 3... Size of the foreign body ≥ 2.5 mm ∅		IP 30	IP 31	IP 32	IP 33	IP 34					
IP 4... Size of the foreign body ≥ 1 mm ∅		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-proof		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 power sources on the equipment after they have been shut off and de-energized. Power 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)
- ➜ CSA Standard Z460 Control of hazardous energy (Lock-Out / Tag-Out)

Lock-Out/Tag-Out Checklist (Source NIOSH's web site)

When performing Lock-Out / Tag-Out on circuits and 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 workers 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 normal stop function of a machine, it shall also be possible to stop a machine for safety reasons.

Requirements

- Every machine shall be equipped with a control for shutting down 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 or function-related reasons on the machine.
- A command to shut down the machine shall have a higher priority than the commands for placing the machine in operation.

Stop categories

Safety and function-related aspects in machines result in stop functions in varying categories. Stop categories are not to be mistaken for the safety categories as in ISO 13 849-1.

Stop category 0	Supply of power to the machine actuators is immediately removed (uncontrolled shut down)
Stop category 1	Machine performs a controlled stop, only then the supply of power to the actuators is removed
Stop category 2	Machine performs a controlled stop with power left available to the machine actuators

➜Stop functions: NFPA 79

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

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, 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 for emergency stop devices: ISO 13 850
➜Requirements on emergency stop: NFPA 79

Electromagnetic compatibility (EMC)

The machine and the components used shall be selected and verified such that they are immune to the expected electromagnetic interference. Increased requirements apply to safety components.

Electromagnetic interference can be caused by:

- fast, transient, electrical disturbances (burst)
- surge voltages, e.g., caused by lightning strikes to the grid
- electromagnetic fields
- high-frequency interference (neighboring cables)
- ElectroStatic Discharge (ESD)

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

Typical minimum interference field strengths in the frequency range of 900 to 2000 MHz

Application area	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

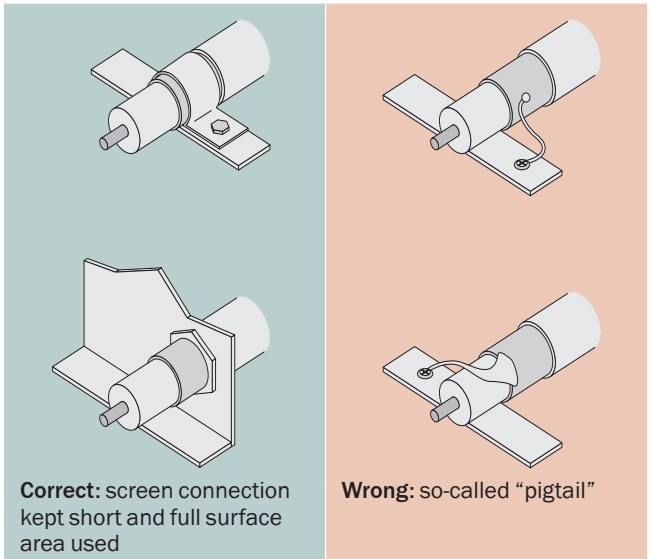
Example: Typical distances from phone systems for different field strengths

Application area	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	Approx. 3 m	Approx. 1 m	≤ 1 cm	Maximum transmission power (900 MHz)

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 (mains supply/ actuator systems/inverters)
- Do not use the screen to carry equipotential bonding currents.
- Keep screens short and use the full surface area.
- Connect any functional earth (FE) provided.
- Connect existing communication cables carefully. Twisted cables are often required to transmit data (fieldbus).

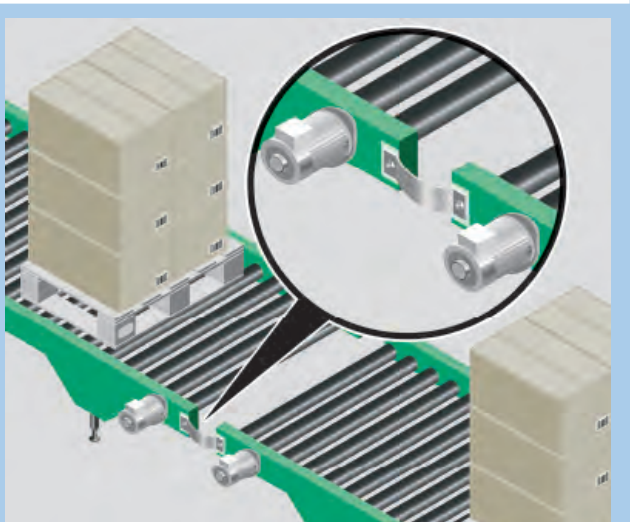
Example: Connecting shield correctly



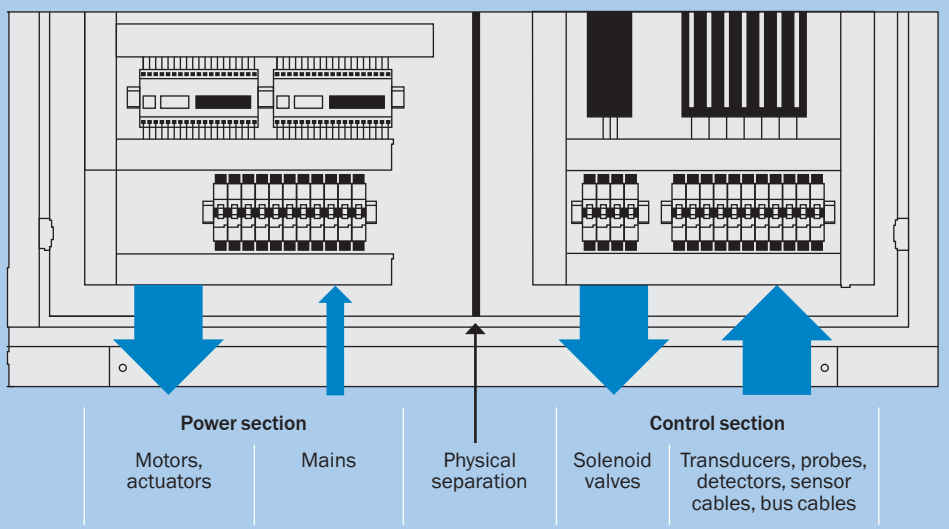
Correct: screen connection kept short and full surface area used

Wrong: so-called “pigtail”

Example: Providing equipotential bonding



Example: Physical separation



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

Fluid technology (Hydraulic and Pneumatics)

Fluid technology is the overall term used for all processes by which energy is transmitted using gases or liquids. The higher level 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.

Sub-systems

Every fluid-related system comprises the sub-systems:

- 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 hydraulics (energy transmission using hydraulic oils) and pneumatics (transmission using compressed air). Oil-based hydraulics require a circuit for the fluid (feed and return), while in pneumatics the waste air is discharged to the surroundings 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 sub-system 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 usage of acoustic attenuators shall not produce any additional hazard, acoustic attenuators shall not cause any damaging back-pressure. Special care must be taken when designing these systems to prevent stored energy from causing additional hazards.

Summary: Safe design

Mechanics, electrics, operation

- Keep to the principle of not allowing hazards to occur in the first place.
- Design such that the operators are exposed to the hazardous area as little as possible.
- Avoid hazards produced directly due to electrical power (direct and indirect contact) or produced indirectly due to faults in the control system.

Actions in an emergency, shutting down

- Plan a control for shutting down the machine in normal operation.
- Establish a hazardous energy control program (Lock-Out / Tag-Out).
- Use an emergency stop to shut down a dangerous process or a dangerous movement.
- Use emergency switching off if sources of power that produce a hazard shall be safely isolated.

EMC

- Be aware of electromagentic compatibility and interference. The components used shall be selected and verified such that ...
  - they do not cause electromagnetic interference that disturbs other devices or systems.
  - they are themselves immune to the interference to be expected.

Step 3: Protective measures by using engineering controls

Engineering controls are realized by means of protective devices (covers, doors, light curtains, two-hand controls) or monitoring units (in position, velocity, etc.), that perform a safety function.

Not all protective devices are integrated into the machine's control system. An example of this situation is a fixed physical guard (barriers, covers), which does not need to be removed frequently. The main task is complete with the correct design of this protective device.

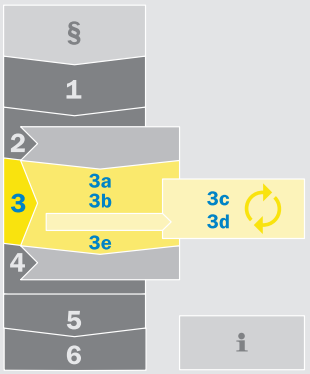
Functional safety

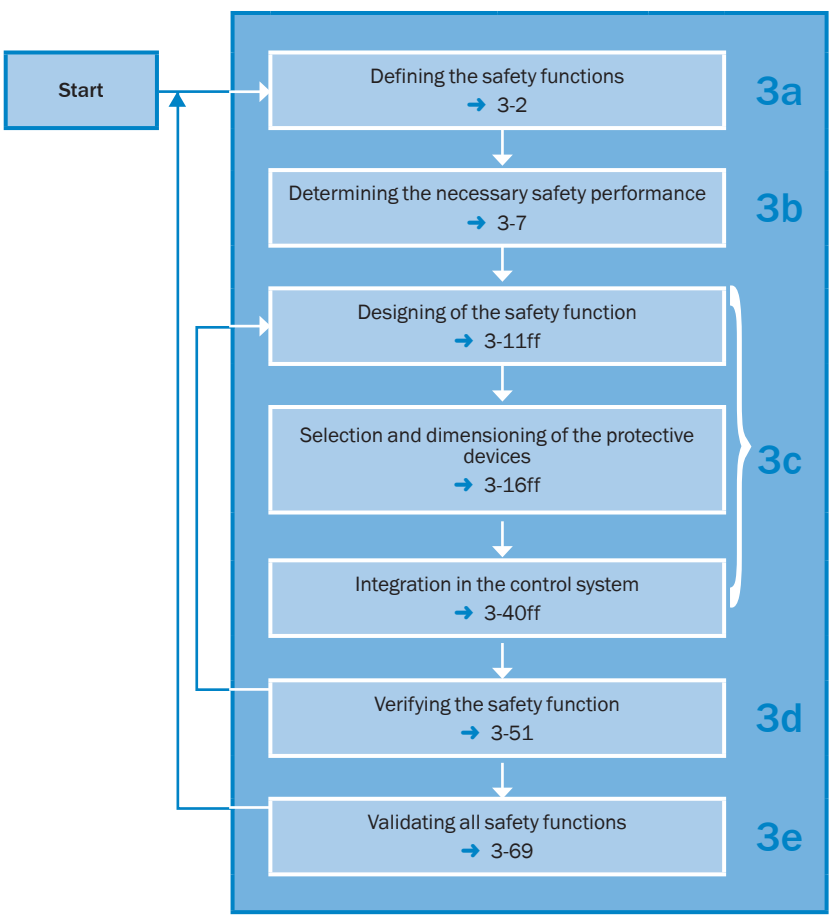
Where the effect of a engineering controls is dependent on the correct function of a control system, the term functional safety is used. To implement functional safety, safety functions and the necessary safety performance shall be defined, then implemented with the correct components, and then verified.

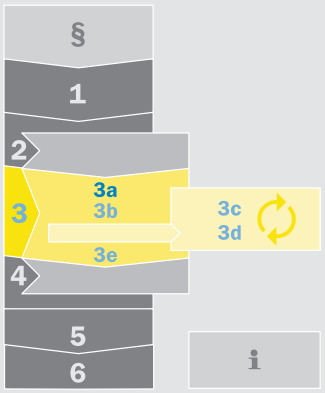
Validation

The validation of all engineering control measures ensures the correct safety functions have a reliable effect.

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





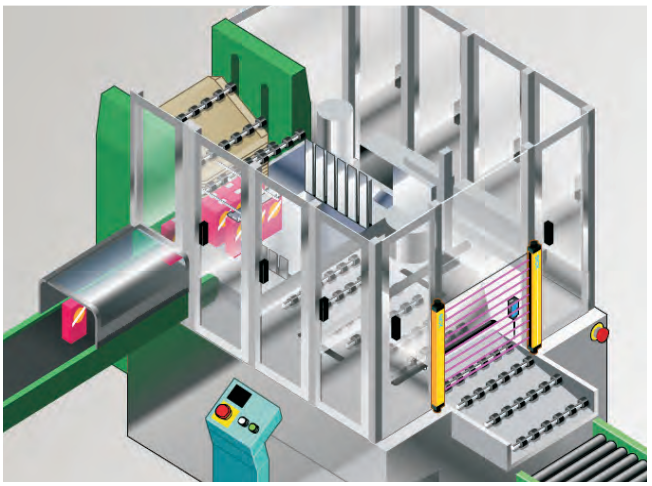


Step 3a: Defining the safety functions

The safety function defines how the risk is to be reduced by engineering controls. A safety function is to be defined for each hazard that has not been eliminated in design. An exact definition of the safety function is necessary to obtain the required safety with a reasonable level of effort. The necessary type and number of components for the function are derived from the definition of the safety function.

Permanently preventing access

Access to a hazardous point is prevented by means of mechanical covers, barriers or obstacles, so-called physical guards.

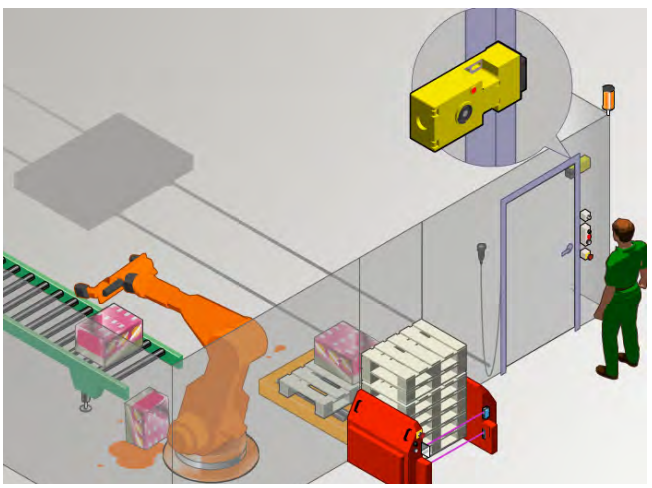


Examples:

- prevention of direct access to hazardous points by means of covers (see illustration)
- using tunnel-shape features that prevent access to the hazardous points and permit the passage of materials or goods (see illustration)
- prevention of physical access to hazardous areas by means of fences

Temporarily preventing access

Access to a hazardous point is prevented until the machine is in a safe state. On request, a machine stop is initiated. When the machine reaches the safe state, access is allowed.



Example:

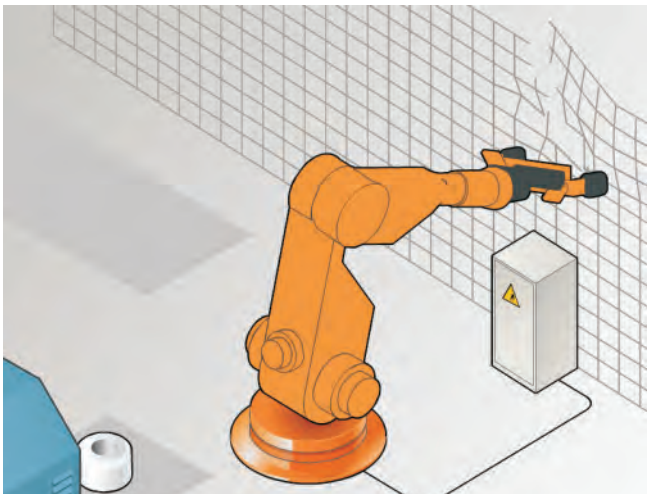
- Physical Guard with locking devices (see illustration)

Retaining parts/substances/radiation

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

Examples:

- safety cover with special viewing window on a lathe for protection from flying chips and parts of workpieces
- fence that can retain a robot arm (see illustration)

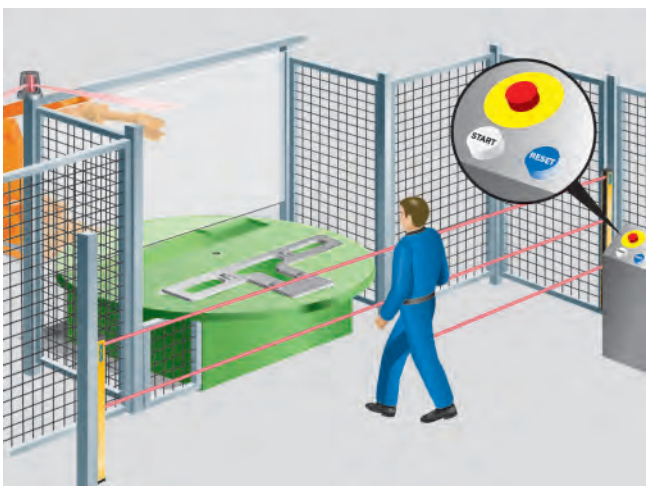


Initiating a stop

A safety-related stop function places the machine in a safe state on demand (e.g., approach of a person). To prevent problems on restarting, it is common to initiate a normal stop before a safety stop (stop category 1). Additional safety functions may be necessary to prevent unintentional restarting.

Examples:

- opening a guard with an interlock, but that has no locking device
- interrupting the light beams on a photoelectric safety switch providing access protection (see illustration)



Avoiding unexpected start-up

After actuating the “Initiating a stop” function or switching-on the machine, specific actions are required to place the machine in operation. These actions include manually resetting a protective device to prepare for restarting the machine.

Examples:

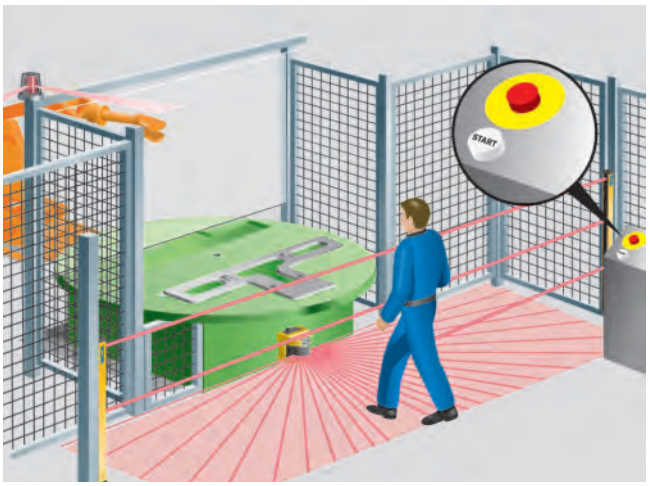
- resetting a photoelectric switch (see illustration “Initiating a stop”: blue “Reset” button)
- resetting the emergency stop device
- restarting the machine when all the necessary safety devices are effective

Preventing start

After “Initiating a stop,” starting or putting back in operation is prevented by technical measures as long as there are people in the hazardous area.

Examples:

- trapped key systems
- detection in the active protective field of a safety laser scanner (see illustration). The “Initiating a stop” function is implemented by the vertical protective field from the photoelectric safety switch.

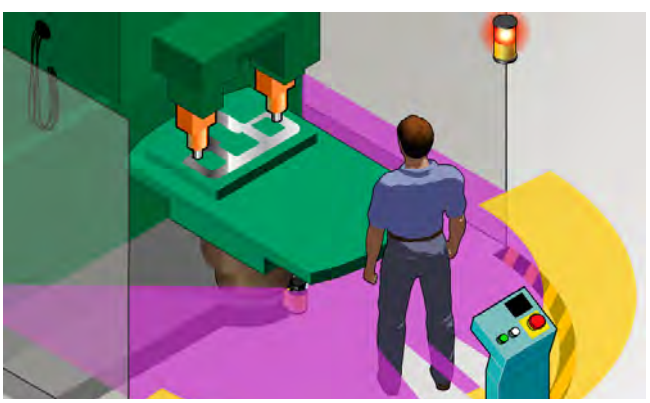


Combination of initiating a stop and preventing start

Renewed starting is prevented using the same protective device that initiates the stop as long as there are people or limbs in the hazardous area.

Examples:

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

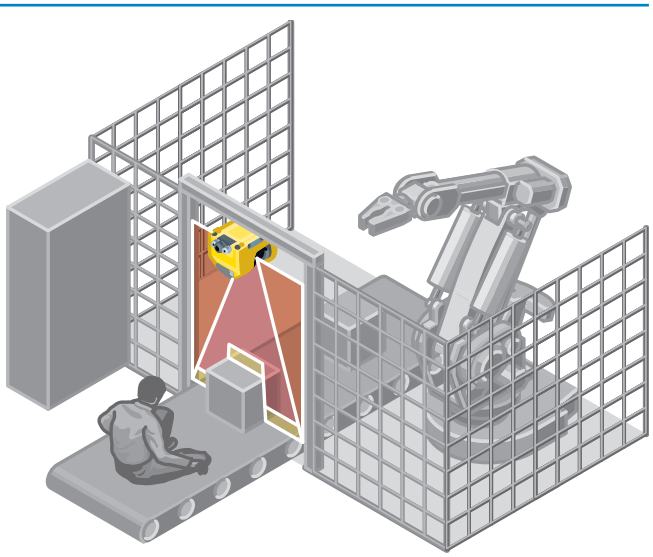


Differentiating between man/material

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

Examples:

- muting of an item by electro-sensitive protective equipment (ESPE)
- horizontal light curtains with integrated algorithm for man-material differentiation
- protective field switching on a safety laser scanner (see illustration)

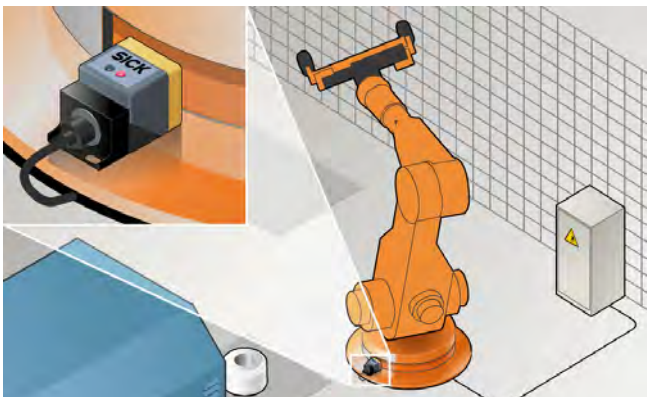


Monitoring machine parameters

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 velocity, temperature or pressure
- position monitoring (see illustration)



Disabling safety functions manually and for a limited time

If safety functions need to be temporarily disabled for setup work or process monitoring, there shall be additional measures for risk reduction. The function shall be disabled manually.

Examples:

- limiting the movement velocity or movement power
- limiting the duration of movement (inching)
- hand-held control unit with enabling switch and +/– buttons (see illustration)

3
a

Combining or changing safety functions

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

Examples:

- after an operating mode change between setup and normal operation, the machine is stopped. A renewed manual start command is necessary.
- disabling the stop command from a safety light curtain during the hazard-free return stroke of a press
- adjustment of the area monitored by a laser scanner to the velocity of the vehicle

Shutting down in an emergency

Shutting down in an emergency (emergency stop) is an additional protective measure and not a primary means of risk reduction. For this reason, this function is not actually considered a safety function.

Depending on the risk assessment for the machine, it is nevertheless recommended to implement this function with the same safety performance as the primary protective measures.

➜ Requirements for emergency stop: NFPA 79

Other functions

Other functions can also be performed by safety-related devices, even if these are not used to protect people. The actual safety functions are not impaired in this way.

Examples:

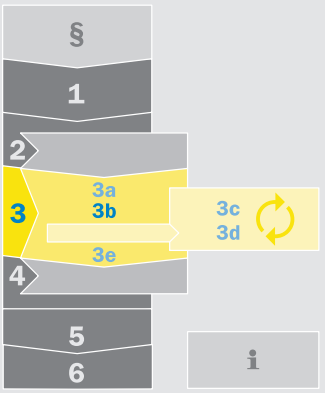
- tool/machine protection
- PSDI mode (cyclic triggering)
- state of the protective device is also used for automation tasks (e.g., navigation)
- transmission of the state of the protective devices over a bus system to a central control room

Summary: Defining the safety functions

Define which safety functions are necessary for risk reduction:

- permanently preventing access
- temporarily preventing access
- retaining parts/substances/radiation
- initiating a stop
- preventing start
- avoiding unexpected start-up
- combination of initiating a stop and preventing start
- differentiating between man/material
- monitoring machine parameters
- disabling safety functions manually and for a limited time
- combining or changing safety functions

Step 3b: Determining the necessary safety performance



The design and performance of the safety function shall be commensurate with the risk. Often machine specific standards define the required safety performance.

If this is not the case, the necessary safety performance is to be defined individually for each safety function and applies to all devices involved, e.g. ...

- the sensor/the protective device
- the evaluating logic unit
- the actuator(s)

Examples of standards determining safety performance:

→ ANSI RIA 15.06, CSA Z434, ANSI B11.19, CSA Z432, ISO 13849-1, ISO 13849-2, IEC 62061, IEC 61508

Helpful technical reports are:

→ ANSI B11.TR3, ANSI B11.TR4, ANSI B11.TR6

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

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

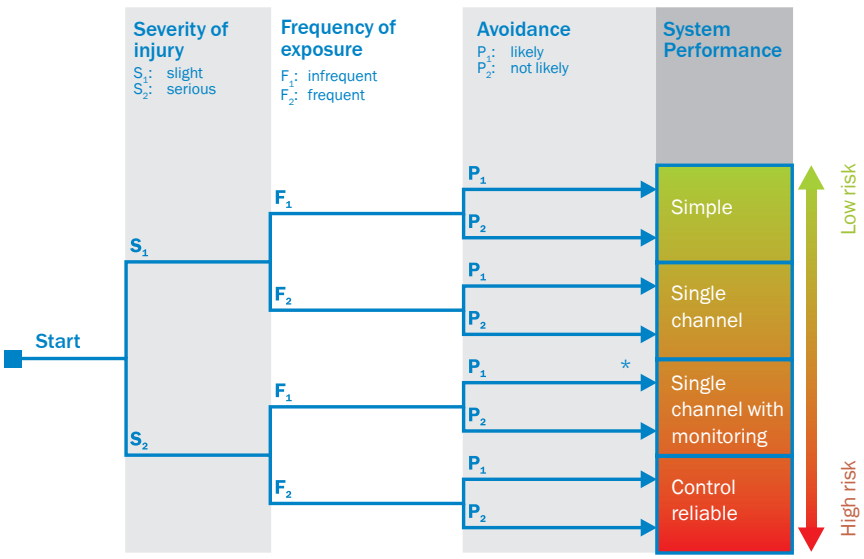
- the severity of the possible injury/harm to the health
- the frequency and/or the duration of the exposure to the hazard
- the possibility of avoiding the hazard

The combination of the parameters determines the required safety performance.

During the application of the procedures described in these standards for the determination of the safety performance, the machine is considered without protective devices.

System performance out of ANSI / CSA

Many North American standards require the safety performance to be “control reliable.“ ANSI B11.2008 / ANSI RIA 15.06 / CSA Z434 suggest also the usage of a risk graph, which ends up in various circuit performance requirements:



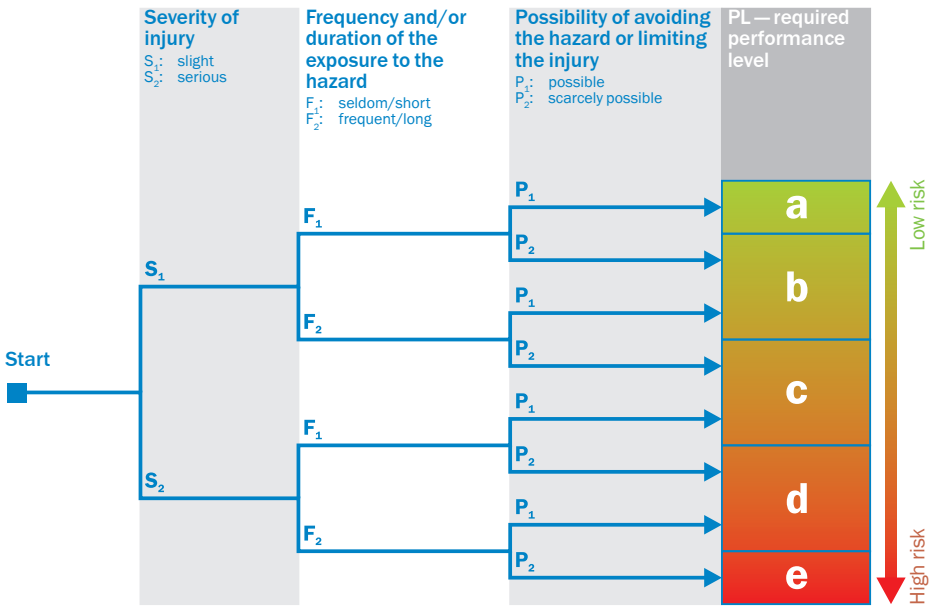
* The Canadian standard CSA Z434 requires the system performance of S2, F1, P2 to be control reliable

Both EN ISO 13 849-1 and IEC 62 061 define requirements for the design and realization of safety-related parts of the control systems. The user can select the relevant standard to suit the technology used in accordance with the information in the table on the right:

Technology	EN ISO 13 849-1	IEC 62 061
Hydraulic	Applicable	Not applicable
Pneumatic	Applicable	Not applicable
Mechanical	Applicable	Not applicable
Electrical	Applicable	Applicable
Electronics	Applicable	Applicable
Programmable electronics	Applicable	Applicable

Performance level as per EN ISO 13 849-1

This standard also uses a risk graph to determine the necessary safety performance. The same parameters **S**, **F** and **P** are used in the older version of ISO 13849-1, which defines safety categories (B,1,2,3,4). However, in the newer version, the result of the procedure is a “required performance level” (PLr: required performance level).



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 failures, as well as the resistance to multiple common cause failures in multiple channel control systems. In addition, further measures to avoid design faults are required.

Safety integrity level as per IEC 62 061

The procedure used here is a numerical procedure. The extent of injury, the frequency/amount of time in the hazardous area and the possibility of avoiding are evaluated. In addition, the probability of occurrence of the hazardous event is taken into consideration. The result is a safety integrity level (SIL).

Effects	Extent of injury S	Class K = F + W + P				
		3-4	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		Probability of occurrence of the hazardous event W		Possibility of avoiding the hazardous event P	
F ≥ 1× per hour	5	Frequent	5		
1× per hour > F ≥ 1× per day	5	Probable	4		
1× per day > F ≥ 1× in 2 weeks	4	Possible	3	Impossible	5
1× in 2 weeks > F ≥ 1× per year	3	Seldom	2	Possible	3
1× per year > F	2	Negligible	1	Probable	1

1) Applies for durations > 10 min

The SIL is determined as follows:

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

SIL is defined in three discrete levels. It depends on the structure of the control system, the reliability of the components used, the ability to detect failures, as well as the resistance to multiple common cause failures in multiple channel control systems. In addition, further measures to avoid design faults are required.

Summary: Determining the necessary safety performance

General

- Define the necessary safety performance for each safety function.
- The “Severity of the possible injury,” “Frequency and duration of the exposure to the hazard” and “Possibility of avoidance” determine the required safety performance.

Standards which can be used

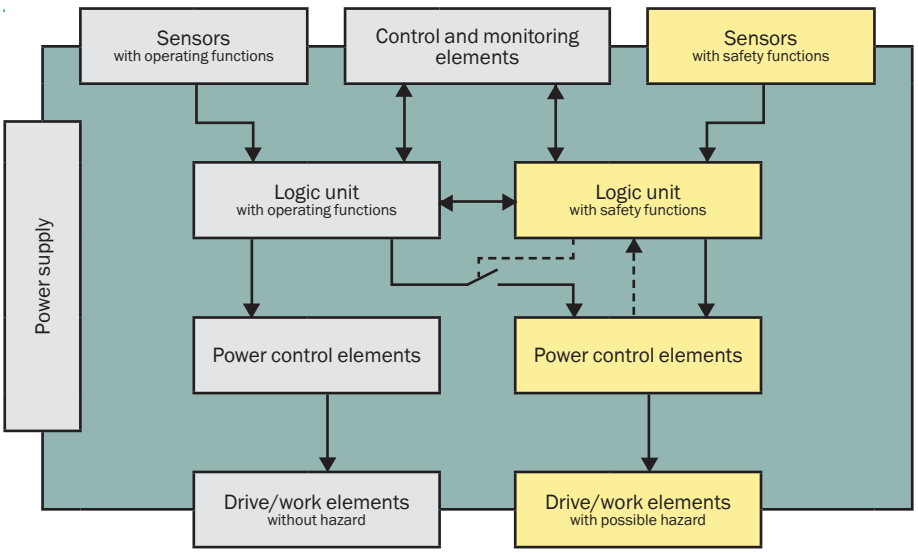
- Many North American standards require the system performance to be control reliable.
- ISO 13 849-1 uses a risk graph to determine the necessary safety performance. The result of the procedure is a “required performance level” (PLr).
- ISO 13 849-1 is also applicable to hydraulics, pneumatics and mechanical systems.
- IEC 62 061 uses a numerical procedure. The result is a safety integrity level (SIL).

Step 3c: Designing the safety function

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

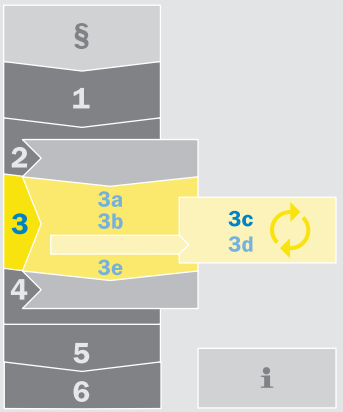
During this process, it needs to be repeatedly checked whether the selection of the technology will provide enough safety and is also technically feasible, or whether other risks or additional risks are produced by the use of a specific technology.

A machine or system comprises various components that interact and ensure the function of a machine or system. Here a differentiation is to be made between components that are purely for operation and those that have safety-related functions.



The safety-related parts of control systems are to be selected to suit the safety functions and the necessary safety performance e.g. sensors, logic units, power control elements 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.



General considerations

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
- Selection of protective devices ➜ (3-16)

Depending on these features it shall be defined which protective devices are to be integrated.

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 physical guards or deflecting guards.)
- ability to stop the dangerous movement without additional hazards (If not possible, select different design/protective device.)
- possibility of hazard due to parts thrown out (If yes, use physical guards.)
- stopping times (Knowledge of the 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 interference/radiated interference
- vibration/shock
- ambient light/light interfering with sensors/welding sparks/ reflective surfaces
- contamination (mist, chips)
- temperature range
- humidity/weather

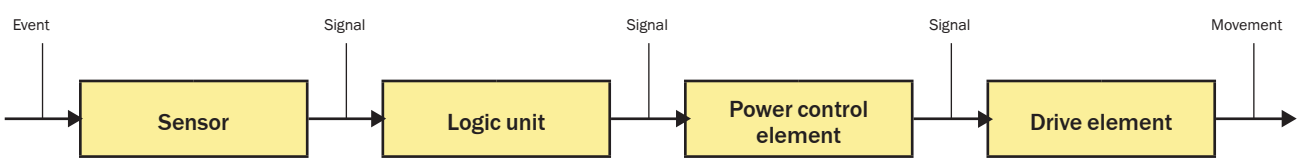
Human aspects

The following human aspects should be taken into account:
- expected qualifications of the machine's operator
- expected number of people in the area
- approach speed (K)
- possibility of bypassing the protective device
- 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 the subsequent verification. A safety function is performed by several sub-systems.

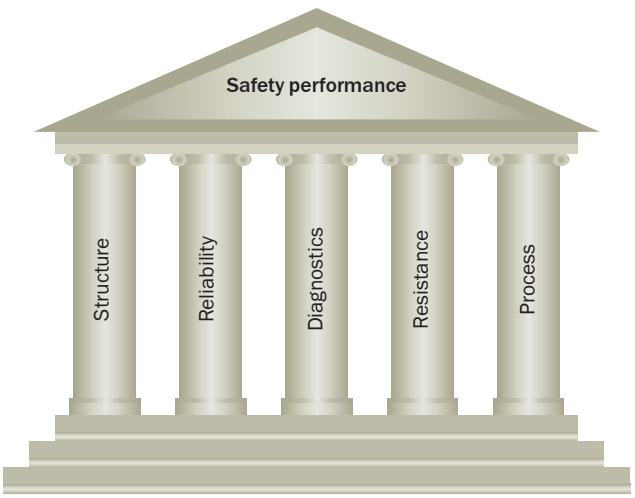
It is often not possible to implement a sub-system using only certified safety components that already provide the safety performance(PL/SIL). Indeed, often the sub-system shall be assembled from several discrete elements. In this case, the safety performance is dependent on various parameters.



Safety-related parameters for sub-systems

The safety performance of a sub-system is dependent on the various safety-related parameters, such as:

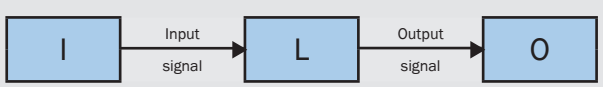
- Structure of the safety system
- Reliability of the components/devices
- Diagnostics for detecting failures
- Resistance to common cause failures
- Process of the system design and testing



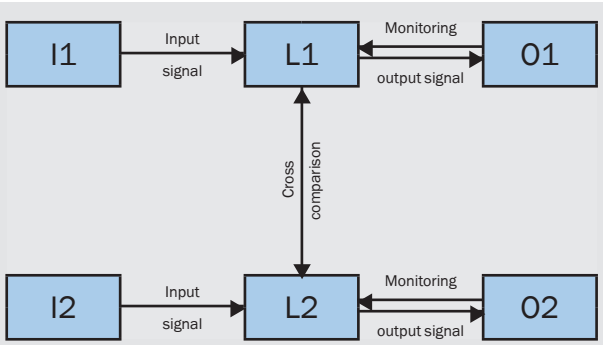
Structure

To reduce the susceptibility of a safety component to failure by means of a better structure, the safety-related functions can be performed in parallel on several channels. Dual-channel safety components are common in the machine safety market (see illustration below). Each channel can stop the dangerous state. The two channels can be of diverse design (one channel uses electromechanical components, the other electronics). Instead of a second equivalent channel, the second channel can also have a pure monitoring function.

Single-channel safety components



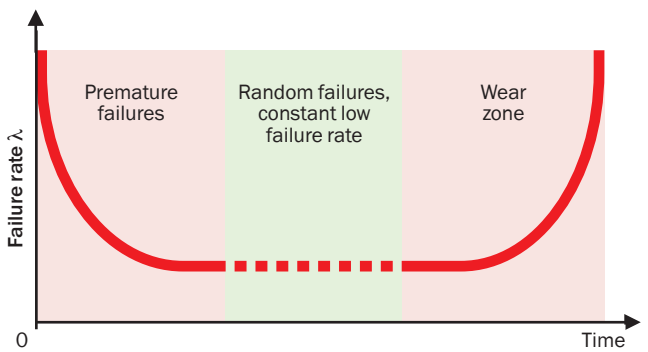
Dual-channel safety components



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. With increasing reliability, a dangerous accident is also less probable. Reliability data are a measure of random failures during service life and are normally stated as follows:

- For electromagnetic or pneumatic components: **B_{10} figures.** Here the service life is dependent on the switching frequency. B_{10} defines the number of switching cycles after which 10 % of the components will have failed.
- For electronic components: **Failure rate** λ (lambda figure). Often the failure rate is stated in FIT (Failures In Time). One FIT is one failure per 10^9 hours.

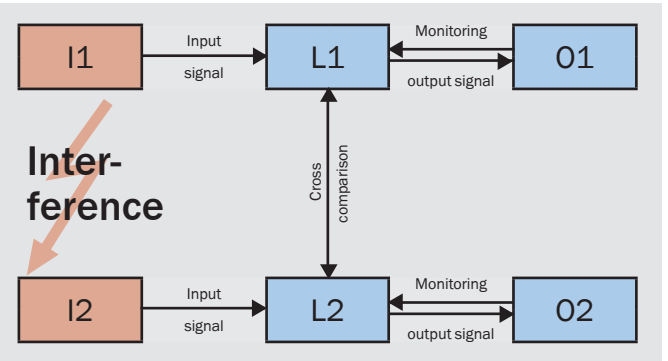


Diagnostics for detecting failures

Certain failures can be detected by diagnostic measures. These include plausibility monitoring, current and voltage monitoring, watchdog functionality, brief function test, etc. Not all faults can be detected, for this reason the degree of fault detection is to be determined. For this purpose, a Failure Mode and Effects Analysis (FMEA) can be performed. For complex designs, measures and data from experience in standards will provide assistance.

Resistance to common cause failures

The term common cause failure is used to refer, for example, to both channels failing simultaneously due to interference. Here appropriate measures are to be taken, e.g., separate cable routing, spark suppression circuits, diversity of components, etc.



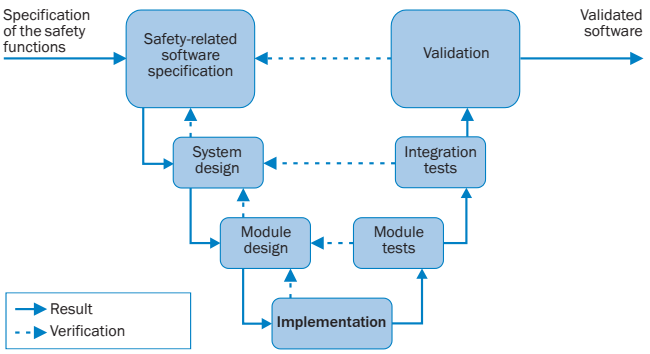
3 C

Process

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

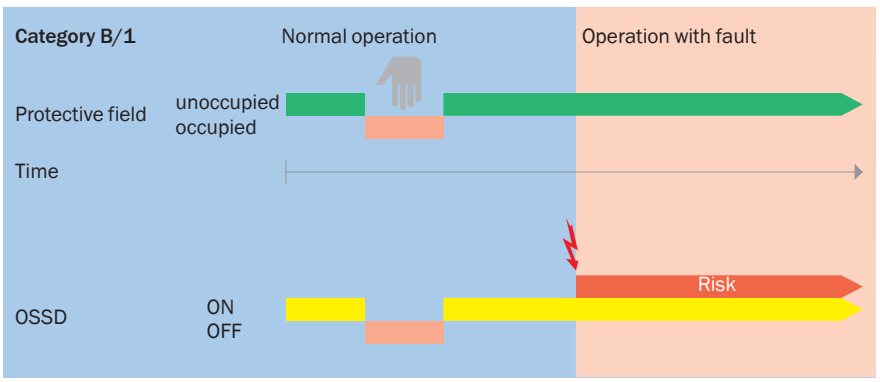
- Organization and competence
- Rules for design (e.g., specification templates, coding guidelines)
- Test concept and test criteria
- Documentation and configuration management

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



Architecture of safety systems

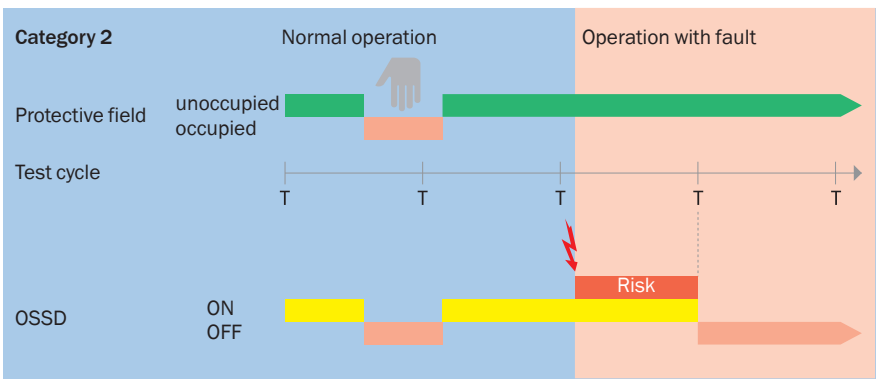
In ISO 13849-1, the safety-related architecture is interpreted with the aid of the categories. These basic principles are also retained in North American standards through the description of the system performance.



Simple / single channel

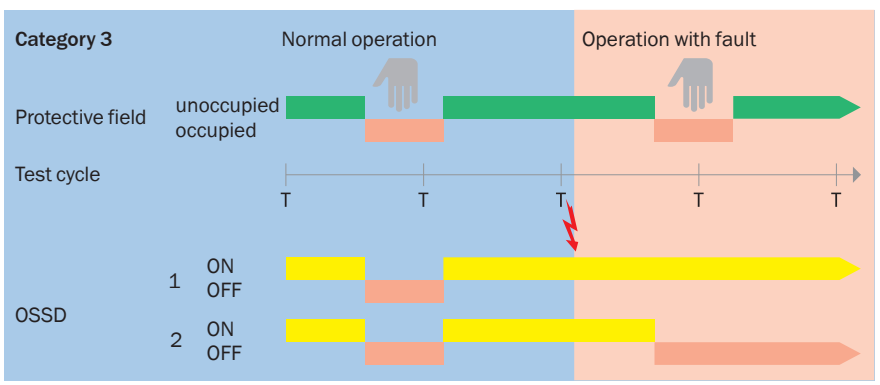
No failure detection. A failure will result in a risk.

The risk can be reduced by using reliable and proven components (Category 1).



Single channel with monitoring

Failures are detected by a test. In the period between the occurrence of the failure and the next test there is a risk.

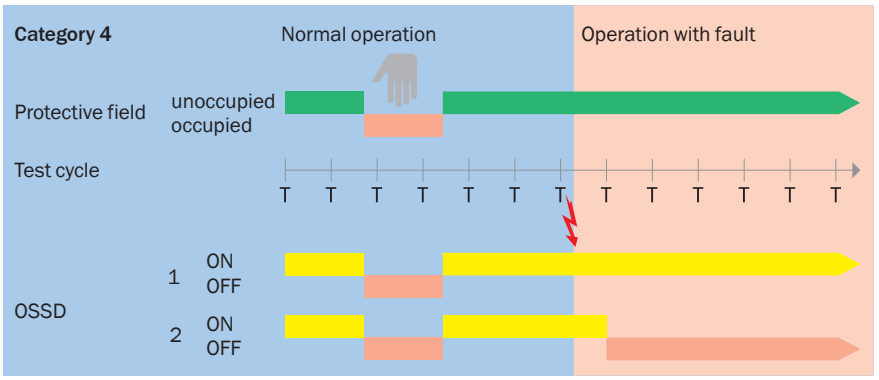


Double channel with monitoring (Control reliable)

The safety function is retained in case of a failure.

The failure is either detected when the safety function is used, or by the next test. An accumulation of failures will result in a risk.

This safety performance can meet the control reliable requirements



Double channel with multiple fault monitoring /Control reliable

The safety function is retained despite a failure.

Unlike Category 3, subsequent failures will not result in the loss of the safety function if the first failure is not detected.

Selection of the protective devices

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

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

* (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 Booklet on Safeguarding OSHA 3170

Electro-sensitive protective equipment (ESPE)

The most widespread electro-sensitive protective equipment are opto-electronic devices. For example:

- light curtains and photoelectric switches (also called AOPD — active opto-electronic protective device)
- laser scanners (also called AOPDDR — active opto-electronic protective device responsive to diffuse reflection)
- cameras

Why opto-electronic protective devices?

If the operator has to reach into a machine, and is therefore exposed to a hazard, the use of opto-electronic protective devices instead of mechanical guards (fixed guard, two-hand control, fences, etc.) is recommended. This will reduce the access time (the operator does not need to wait for the protective device to open), increase productivity (time saving when loading the machine) and improve the ergonomics of the workplace. In addition, operators and other people are equally protected.

3
C

An opto-electronic protective device can be used if the operator is not exposed to any risk of injury due to parts thrown out (e.g., due to splashes of molten material).

Selection of a suitable ESPE

Criteria can be:

- Requirements from ANSI, CSA or international standards
- The space available in front of the hazardous area
- Ergonomic criteria, e.g. cyclic insertion tasks
- Resolution
- Response time of the ESPE

Which safety function is the ESPE to perform?

- Initiating a stop (➜ 3-3)
- Avoiding unexpected start-up (➜ 3-3)
- Preventing start (➜ 3-4)
- Combination of initiating a stop and preventing start (➜ 3-4)
- Differentiating between man/material (muting) (➜ 3-4)
- Monitoring machine parameters (➜ 3-5)
- Other functions, e.g. PSDI mode, blanking, protective field switching, etc. (➜ 3-6)

Safety ratings

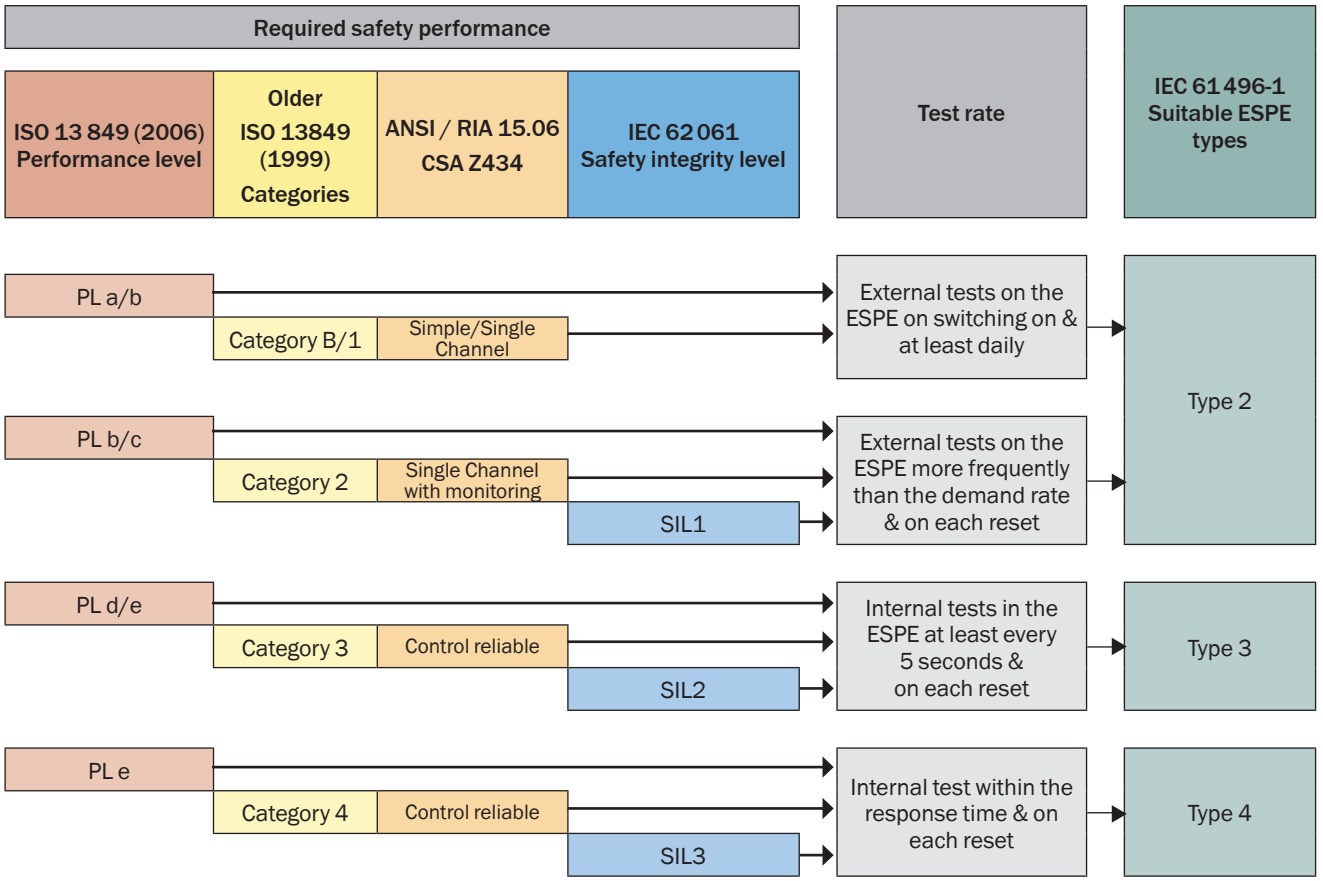
The safety-related parameters for ESPE are implemented in the type classification (type 2, type 3, type 4).

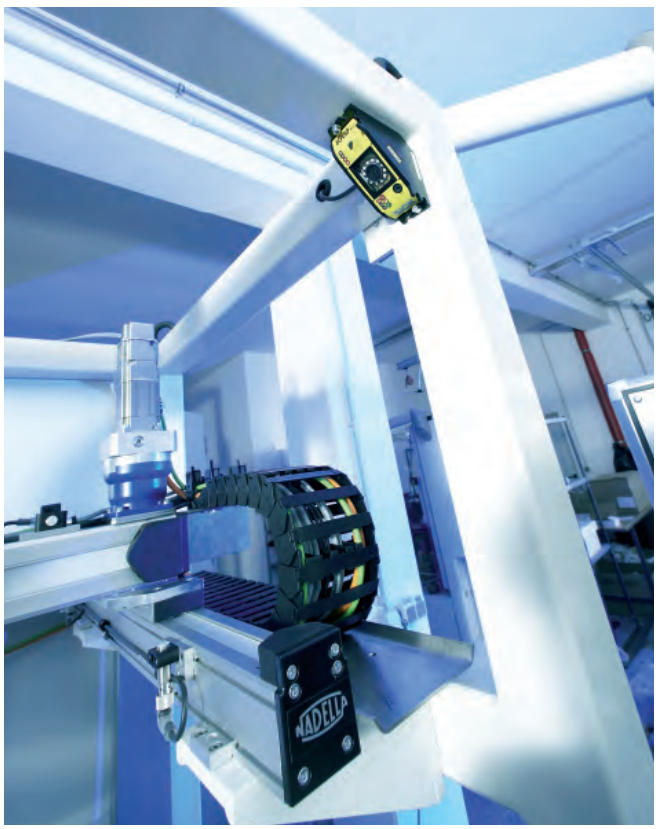
Along with structural aspects, similar to the familiar categories in ISO 13849-1, requirements to be met in relation to electromagnetic compatibility (EMC), ambient conditions and the optical system are defined in the type classification. These include, in particular, the behavior in relation to sources of interference (sun, lights, devices of similar design, etc.) and also the field of view of the optics on the safety light curtains or photoelectric safety switches (the requirements on a type-4 AOPD are higher than on a type-2 AOPD).

The field of view is crucial for determining the minimum distance from reflective surfaces.

➜ Requirements for ESPE IEC 61496 Parts 1, 2 and 3. ANSI B11.19

Selecting suitable ESPE types as a function of the necessary safety performance



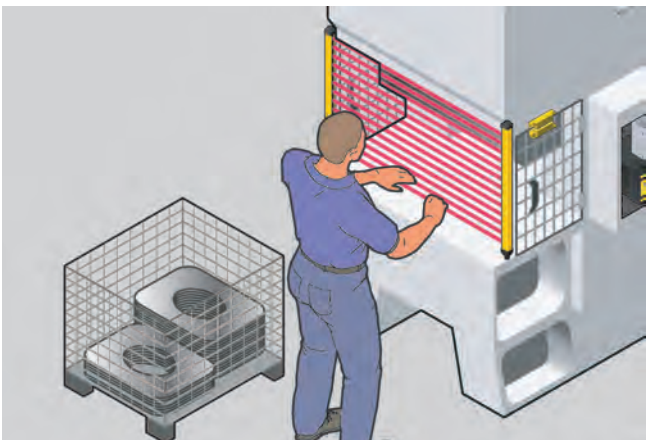


What is to be detected by the ESPE?

Point-of-operation protection: Finger or hand detection

In the case of hazardous point protection, the approach is detected very close to the hazardous point.

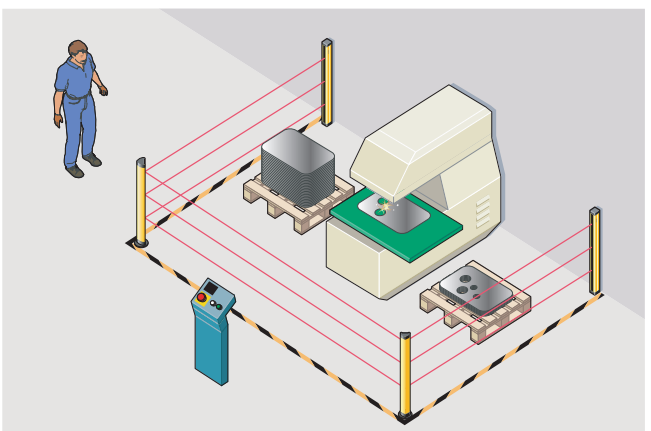
This type of protective device is advantageous because a shorter safety distance is possible and the operator can work more ergonomically (e.g., during loading work on a press).



Access protection (Perimeter guarding):
Detection of a person upon access to the hazardous area

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

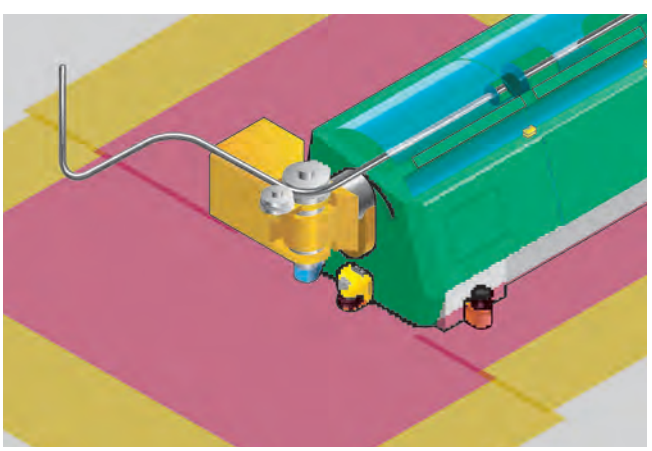
This type of protective device is used to protect the access to a hazardous area. A stop signal is initiated if the hazardous area is entered. A person who is standing behind the protective device will not be detected by the ESPE!



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

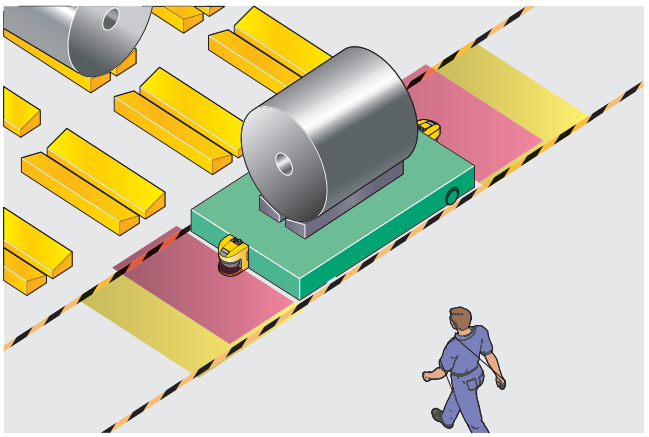
In the case of hazardous area protection, the approach of the person is detected by detecting the person's presence in an area.

This type of protective device is suitable for machines on which, e.g., a hazardous area cannot be seen completely from the reset button. If the hazardous area is entered, a stop signal is initiated and starting prevented.



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

Hazardous area protection is suitable for AGS (automated guided systems), cranes and stackers, to protect the operator and/or third persons during movement of the vehicles or while docking these vehicles to a fixed station.



Possible additional function: Differentiating between man/ material

A special application for an ESPE is the safety function for differentiating between man and material. This safety function is useful on machines on which all work on the pallet loading is automated, i.e. is performed by the machine only (e.g., packing machines, palletizers and depalletizers).

There are two possible types:

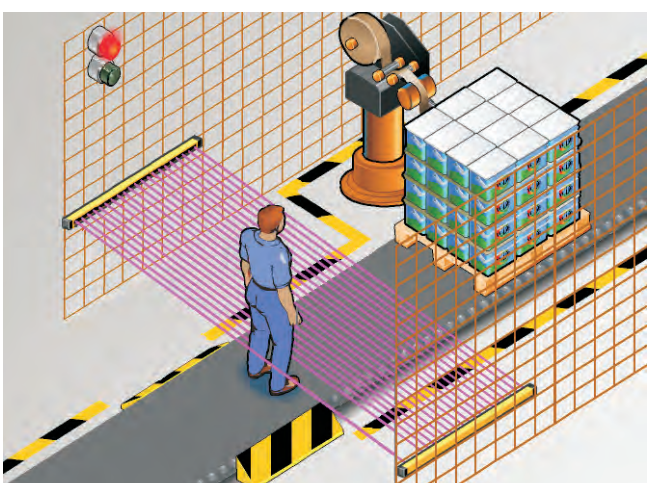
With integrated pattern recognition:

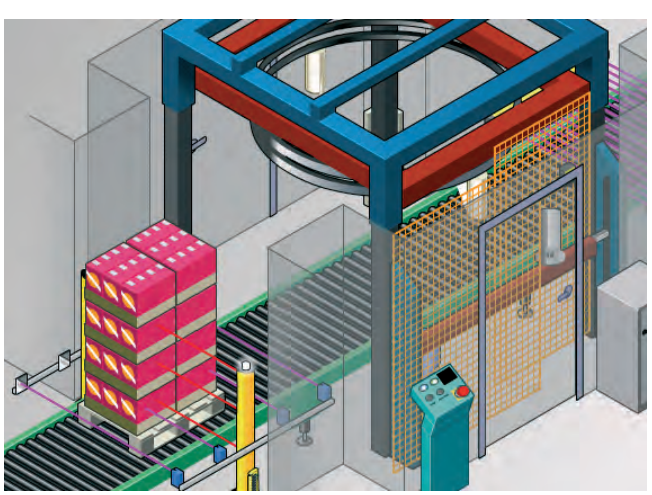
Modern sensors differentiate between man and material using special evaluation algorithms. Here no additional sensors are necessary, and complex installation and maintenance effort are not required.

Using muting:

With muting, protective devices shall be temporarily muted. Here it is necessary to mute the ESPE for the period when the pallet passes through. The muting system shall therefore be able to differentiate between man and material. Various standards on this safety function state, in summary, that ...

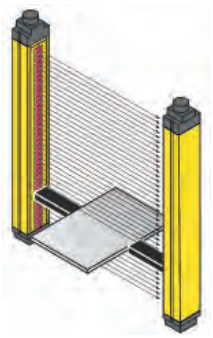
- during muting a safe state shall be ensured by other means, i.e., it shall not be possible to access the hazardous area.
- muting shall be automatic.
- muting shall not be dependent on a single electrical signal.
- muting shall not be entirely dependent on software signals.
- muting signals occurring during an invalid combination shall not permit any muting state, and it shall be ensured that the protective function is retained.
- the muting state is lifted immediately after the system is clear and thus the protective device is reactivated.
- muting is only allowed to be activated during the period of time in the working cycle when the loaded pallet blocks access to the hazardous area.





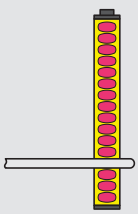
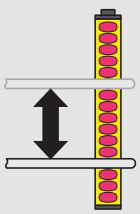
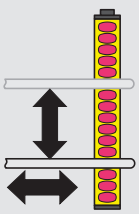
→ Practical application of ESPE: IEC/TS 62 046

Possible additional function: Blanking



Using this function, objects that are in the ESPE's protective field for process-related reasons can be blanked so that no stop is initiated.

A blanked area is in principle a hole in the protective field. Take this situation into account when calculating the safety distance.

Fixed blanking	Floating blanking	
	with object	with or without object
		

Possible additional function: PSDI mode

This operating mode is advantageous if parts are manually inserted or removed periodically. In this mode, the machine cycle is automatically re-initiated after the protective field becomes clear again after one or two interruptions.

It is necessary to reset the ESPE in the following conditions:
- on machine start
- on restart if the ESPE is interrupted during a dangerous movement
- if a PSDI has not been triggered within the PSDI time specified

It is necessary to check that the operator cannot be placed at risk during the working process. This situation limits the use of this operating mode to small machines on which the hazardous area cannot be entered and there is presence detection or mechanical protection. All other sides of the machine shall also be protected using suitable measures.

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

In the USA, at the time of printing, PSDI is not allowed on mechanical power presses.

Please check your local authority for applicability of PSDI.

In Canada, the only reference to PSDI is in Z434-03 for Robots and Robot Systems and it states that initiation is not allowed by a presence sensing device.

3 C

Physical guards

Physical guards are mechanical protective devices that prevent or avoid the operator reaching the hazardous point directly. They can be fixed or movable. Covers, fences, barriers, flaps, doors, etc. are physical guards.
Covers and lids prevent access from all sides. Fences are generally used to prevent full height access. Conversely, barriers can only prevent unintentional/unconscious access to the hazardous point.
The safety function is essential for the design of physical guards. Is the physical guard, e.g., only to prevent access, and/or also to retain parts/materials and radiation?

Examples of materials thrown out:
- fracturing/bursting tools (grinding wheels, drills)
- materials produced (dust, chips, slivers, particles)
- escaping materials (hydraulic oil, compressed air, lubricant, materials)
- parts thrown out 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)

To retain radiation or materials, the mechanical requirements on the physical guards are generally higher than on physical guards to prevent the access of personnel.
Damage (fracture or deformation) to a physical guard is allowed in cases in which the risk assessment defines that no hazards will be produced as a result.

Basic requirements on physical guards

- Physical 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 physical guards shall be retained during the entire period of use of the machines.
- They shall not cause any additional hazards.
- It shall not be possible to easily bypass the physical guards or render them ineffective.
- Physical guards shall not restrict observation of the working process more than necessary, insofar that observation is necessary.
- Physical guards shall be firmly held in place.
- They shall be retained either by systems that can only be opened with tools, or they shall be interlocked to the dangerous movement.

➜ Physical guards: ANSI B11.19, ANSI RIA R 15.06, CSA Z 434, ISO 14120

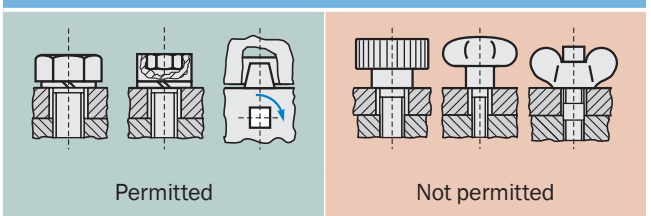
Fastening of physical guards

Physical 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 such that they can only be undone with tools (e.g. spanner, key). Removing them shall involve a task for which tools are required. As best as possible, they should not remain in the protective position if the fastening is undone.

Fastening elements should be designed such 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 physical guard is interlocked.

Example: Types of fastening for physical guards



Adjustable physical guards

Adjustable guards provide a means of adapting the guard to the specific work piece or stock being introduced into the work-space. 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 physical guards

Movable guards that have to be opened frequently or regularly without tools (e.g., for setup work), shall be functionally linked to the dangerous movement (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 the guard is opened (e.g., very long overrun), locking devices are required.

Ergonomic requirements on movable physical guards

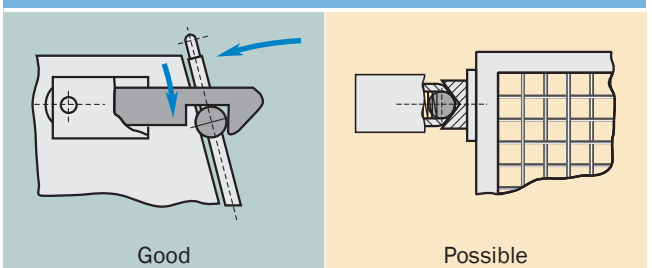
Ergonomic aspects are also significant during the design of physical guards. Physical guards will only be accepted by employees if they do not hinder setup, maintenance and other similar activities any more than necessary. Movable physical guards shall meet the following ergonomic criteria:

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

Mechanical arresting of movable physical guards

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

Example: Arresting device



Interlocking of physical guards

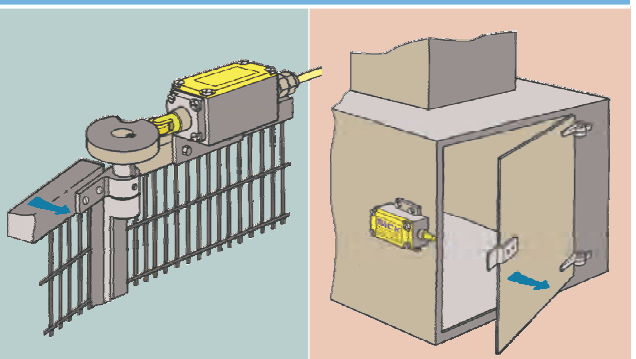
Physical guards shall be interlocked if they:
- are cyclically actuated or opened regularly (doors, flaps)
- can be removed without tools or
- easily protect against a potentially serious hazard

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

An important requirement about interlocking devices is the positive drive.

With positive drive, the moving mechanical parts of the interlock (safety switch) are forcibly moved by the mechanical parts of the physical guard (e.g., door), either by means of direct contact or by rigid parts.

Example: Positive driven design



Safe: Opening the door moves forcibly the mechanical plunger on the safety switch. As a result the safety circuit is opened.

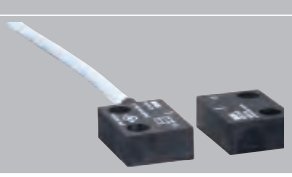
Flawed design: The safety switch will not always open the safety circuit, e.g. if encrusted deposits or lubricating oil residue make the plunger stick.

Source: BG Feinmechanik und Elektrotechnik, BGI 575

Safety switches

The interlocking of a guard by safety switches should meet the following functions:
- The dangerous machine functions cannot be run with the open (missing) guard (preventing starting).
- The dangerous machine function is stopped when the guard is opened (removed) (initiating a stop).

Safety switch designs

Design		Typical applications
	Safety switches with separate actuator	■ Advantageous for sliding and hinged doors and removable covers ■ Interlocking can be implemented using a locking device
	Position switches with direct actuator	■ Safety limit switches ■ Protection of hinged doors and flaps
	Non-contact safety switch	■ Machines in harsh ambient conditions ■ Systems with high requirements for hygiene

Principle of positive opening

Mechanical safety switches feature switch contacts that are opened positively (if necessary to the point of destruction) and the safety function can therefore still be performed even if the contacts are welded together or there are other electrical faults. On safety switches with multiple contacts, the contact elements based on the principle of positive opening (IEC 60 947-5-1: direct opening action) are to be integrated in the safety function.

Marking of contacts that are positive opening as per IEC 60 947

3 C

Mechanical attachment

Reliable mechanical attachment of the safety switches is crucial for their effectiveness.

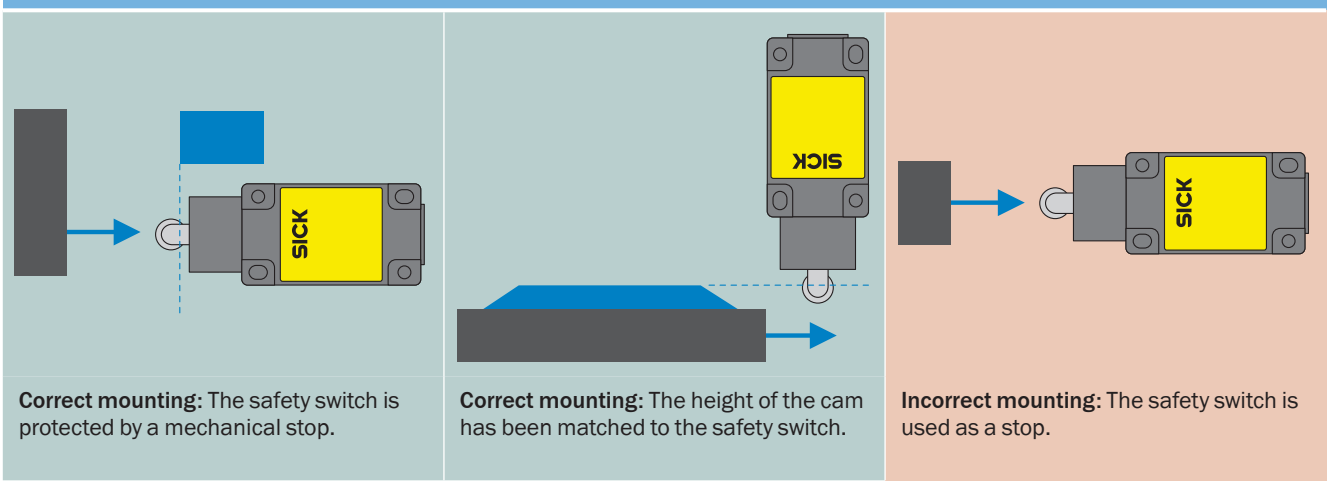
Safety switches ...

- Shall be fitted such that they are protected against damage due to foreseeable external effects.
- Shall not be used as a mechanical stop.
- Their placement and design shall protect them against inadvertent operation, changes in position and damage: The switch and the control cam can be secured by shape (not force), e.g. using round holes, pins, stops.
- To prevent manipulation it shall not be possible to tamper with them using simple means. Simple means includes screws, nails, pieces of metal, coins, bent wire, and the like.
- They shall be protected by their actuation method, or their integration in the control shall be such that they cannot be easily bypassed. (For this reason, the position switches shall have normally closed contacts [de-energize to trip principle]).
- It shall be possible to check the switches for correct operation and, if possible, they shall be easily accessible for inspection.

For position switches the following also applies:

- The actuation stroke shall be set to suit the positive opening travel in accordance with the manufacturer's instructions. The minimum plunger travel defined by the manufacturer shall be observed in order to provide the necessary switching distance for positive opening.

Example: Mechanical attachment of safety switches



Correct mounting: The safety switch is protected by a mechanical stop.

Correct mounting: The height of the cam has been matched to the safety switch.

Incorrect mounting: The safety switch is used as a stop.

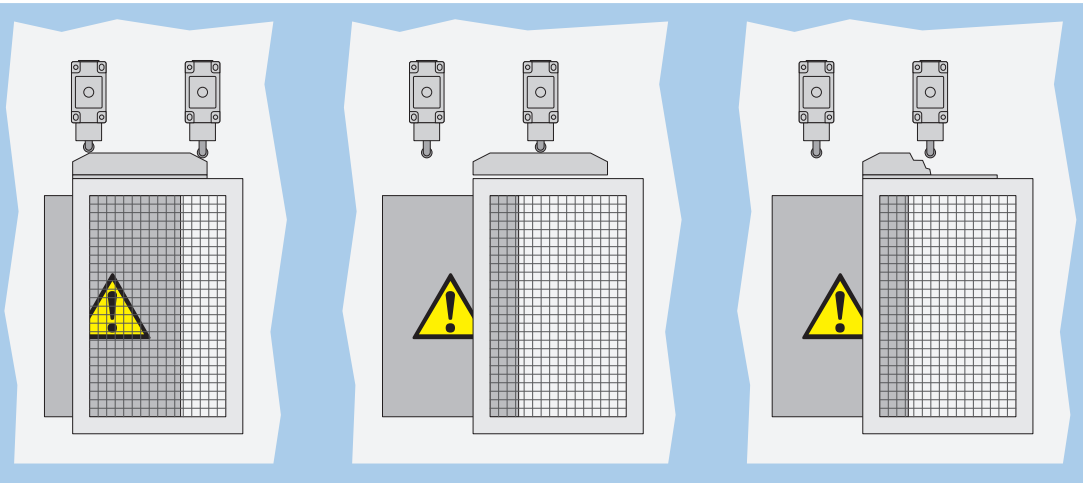
Redundant design

A critical failure of a single safety switch may be caused by manipulation, mechanical failure in the actuation unit or receptacle (example: aging) or due to the effect of extreme ambient conditions (example: contamination with flour jams roller plunger).

In particular, at high levels of safety it is necessary, along with the safety switch, to use an additional switch, e.g., with the opposite function and to monitor both in the control system.

Example: A plastic injection moulding machine with doors that provide protection against a serious hazard and are actuated cyclically. Here the usage of several mechanical switches per door and monitoring logic may be required.

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



Non-contact version

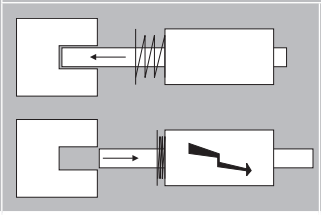
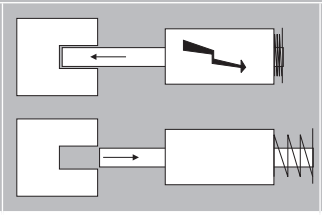
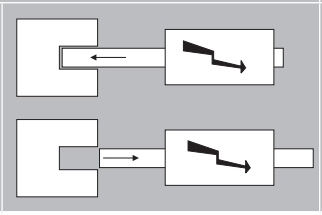
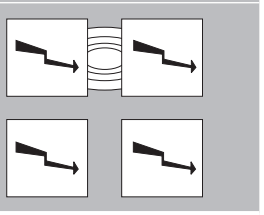
Non-contact safety switches are of redundant internal design or use special principles such as magnetic coding, inductive coupling, transponders with codes.

- ➜ Requirements for safety switches/interlocking devices: ISO 14119, ANSI B11.19
- ➜ Principle of positive opening: IEC 60 947-5-1
- ➜ Plastic/rubber injection moulding machine: ANSI 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:

	Shape			Force
Principle				
Principle of operation	Spring actuated and unlocked using power	Power actuated and unlocked using spring force	Power actuated and unlocked using power	Power actuated and unlocked using power
Term	Mechanical locking device (preferred for personnel protection)	Electrical locking device (preferred for process protection)	Pneumatic/hydraulic locking device	Magnetic locking device

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

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

Mechanical and electrical integration

The same rules generally apply to locking devices as to safety switches. An essential criteria for the selection of the locking device is the force with which the physical guard shall be locked.

In relation to the principle of positive opening, attention is to be paid to which contacts should be positively opened. Door signaling contacts indicate when the actuator has been withdrawn, that the door is open. These contacts can be positive opening, but do not always have to be.

Manual unlocking and emergency unlocking

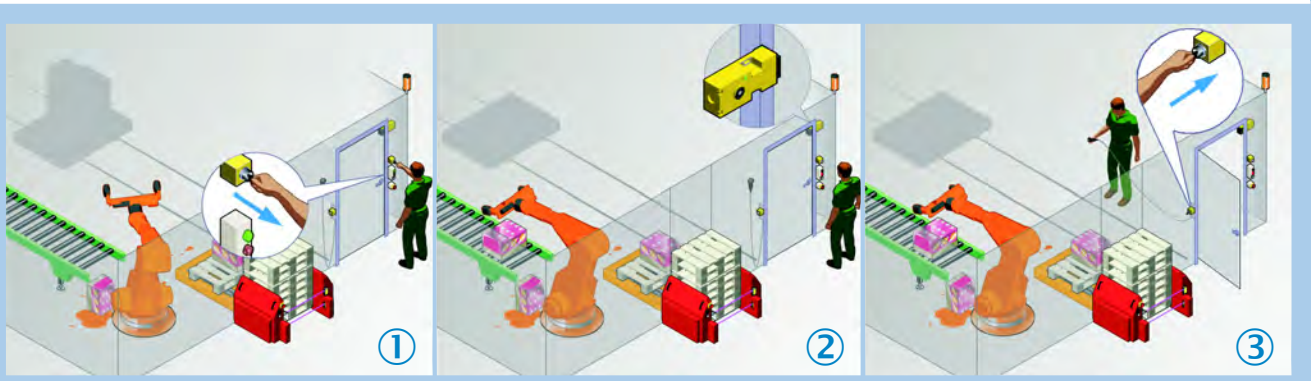
The risk assessment may show that in the case of a failure or in an emergency, measures are required for freeing personnel trapped in the hazardous area. A differentiation is to be made between the concepts of mechanical unlocking (using tools) and emergency or escape unlocking (without tools).

Trapped key systems

Physical guards have the disadvantage that on entry to the hazardous area and subsequent closing of the guard, restarting cannot be effectively prevented. Additional measures are necessary, such as a reset device or the insertion of a carabiner in the safety switch actuator. These organizational measures are dependent, however, on the alertness of the user.

One possible way to prevent an unintentional start is trapped key systems in combination with locking devices. A key inserted outside enables automatic operation and keeps the door locked. When the key is removed (illustration ①) the dangerous state is stopped. In the safe state (e.g. at standstill) the door can be opened (illustration ②). A key inserted in the interior can enable set-up operating modes (illustration ③). Automatic operation is disabled in this situation, even if the door is closed.

Example: Trapped key system



Two-hand control devices

Two-hand control devices are protective devices that force an operator or the operator's limbs to be in a place outside the hazardous area.

A two-hand control always only protects one person! If there are several operators, each person shall actuate a two-hand control. A dangerous movement is only permitted by conscious actuation of the two-hand control and shall stop as soon as a hand releases the control.

The reliability and the safety of the circuitry for two-hand control primarily, but not exclusively, relies on the physical installation and the electrical interfacing of the hand controls (actuating buttons). U.S. standards only refer to Type IIIB and IIIC controls (control reliable).

The following basic principles apply to two-hand controls:

- It shall be ensured both hands are used.
- Releasing one of the two buttons stops the dangerous movement.
- Inadvertent actuation shall be prevented.
- It is not possible to easily bypass the protective feature.
- The two-hand control is not allowed to be taken into the hazardous area.
- It is only allowed to initiate renewed movement after both buttons have been released and activated again.
- It is only allowed to initiate a movement if both buttons have been operated synchronously within 0.5 seconds.

➜ Requirements for two-hand controls: NFPA 79, ANSI B11.19, ISO 13851

Enabling devices

During machine setup, maintenance, and if it is necessary to observe production processes close-up, functions of the protective devices may need to be temporarily suspended. Along with other measures that minimize the risk (reduced force/velocity, etc.), controls are required here that shall be actuated for the entire time the protective devices are suspended. One possible method is to use enabling devices. Enabling devices are physically actuated control switches with which the operator's agreement to machine functions is obtained. As a rule, 3-stage pushbuttons or foot switches are used as enabling devices. Additional start controls for the enabling device are joysticks or inching buttons.

Note: 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, a movement is only permitted as long as the enabling device is actuated.

Principle of operation of the 3-stage enabling device:

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

On changing back from position 3 to position 2, the enabling device function shall not be released.
If enabling devices are equipped with separate contacts in position 3, these contacts should be integrated into the emergency stop circuit.
Protection against tampering is also of major significance on the usage of enabling devices.

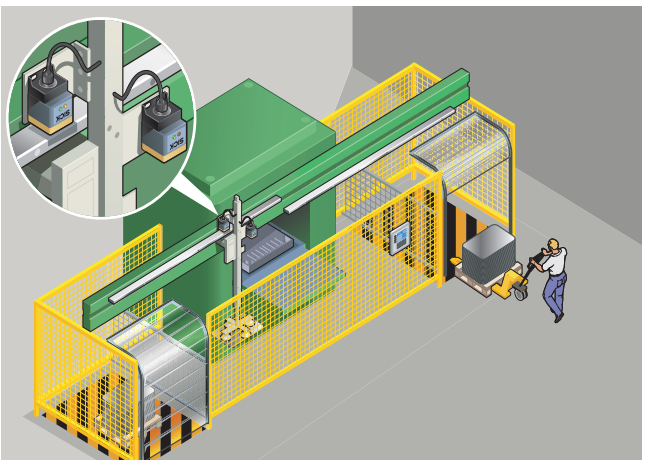
➜ Requirements on enabling devices: ANSI/RIA 15.06 (Industrial Robots), NFPA 79

Sensors for monitoring machine parameters

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

Safe position monitoring

If a machine moves past a specific position, a machine stop is initiated. For this purpose, e.g., safety switches can be used. Electro-sensitive inductive safety switches are particularly suitable for this task. These monitor without the need for a specific mating element, without wear and with a high enclosure rating, a certain part of a robot's axis or a moving part of a machine for presence.

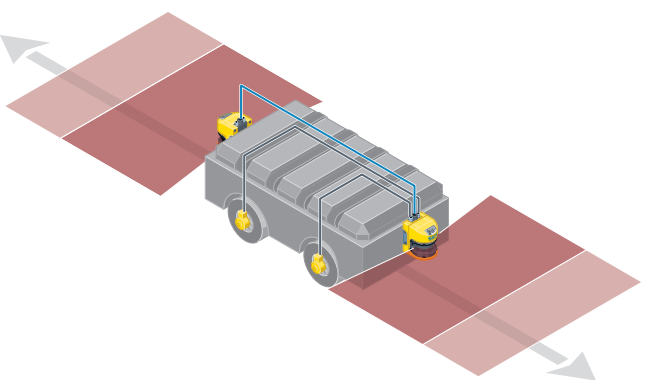


Monitoring of speed/velocity/overrun

Safe encoders or travel measurement systems make it possible to detect and evaluate speed, velocity or overrun.

On automatic transport systems, encoders are often used on the axes. Here an intelligent evaluation algorithm can determine the necessary movement parameters.

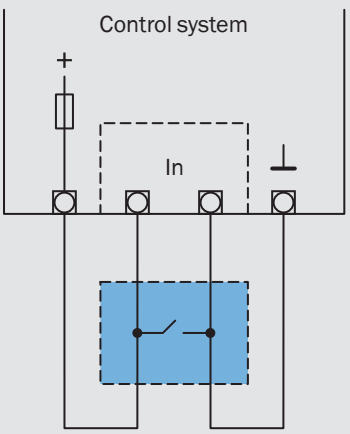
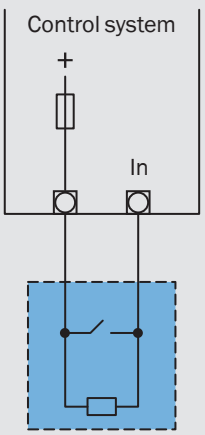
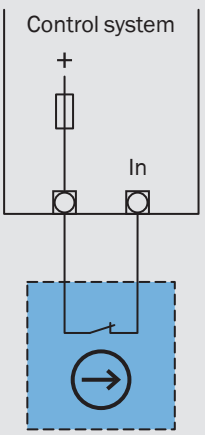
Safe standstill or rotation monitoring modules monitor the movement of drives using sensors or rotary encoders to generate a safe control signal on deviation from set parameters. A further variant can also be to signal the voltage induced by residual magnetism on a motor that is still running down.



Pressure sensitive mats, pressure sensitive strips, bumpers

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 generator (electromechanical or optical) performs 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.

Short-circuit forming designs (energize to trip principle)		Positive opening contact design (de-energize to trip principle)
4-wire variant	Resistance variant	
		
Here a short-circuit is formed on the activation of the protective device. In the case of the 4-wire version, a circuit is short-circuited (a few Ohm). In the case of the resistance variant, a change from a set resistance (in the kOhm range) is detected. These designs require more complex evaluation.		This design is more universal and has advantages. As on a safety switch, a switch contact is opened on the activation of the protective device. A short-circuit is excluded by laying the cables in a special manner.

➜ Performance of pressure sensitive protective devices: ANSI B11.19

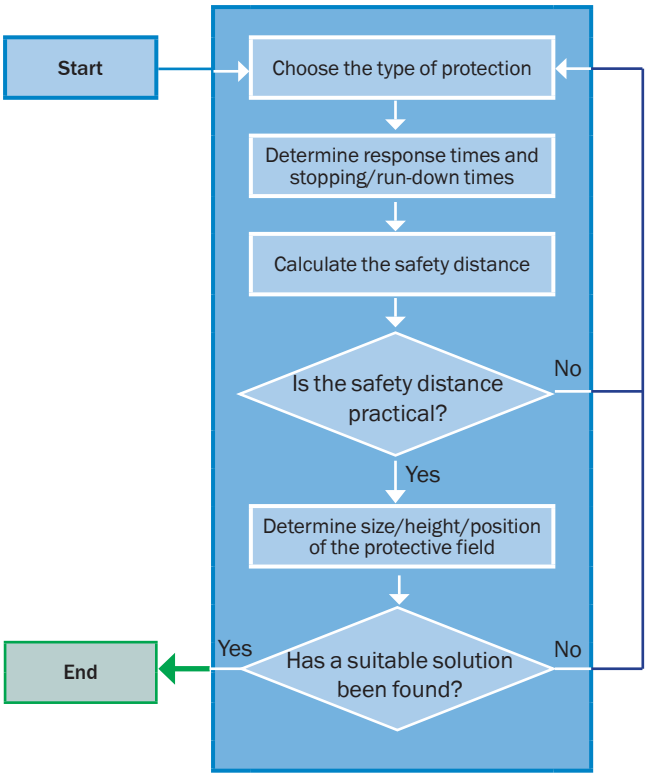
Foot switches

Foot switches are used for switching on and off work processes. Foot switches are only allowed to be used for safety functions on some machines (e.g., on presses, punches, bending and metal working machines) in separate operating modes and only in connection with other engineering controls (e.g. slow velocity). However, they are then to be specially designed:

- with a protective cover against unintentional actuation
- with a 3-stage design similar to the enabling switch principle (see above)
- with the possibility of manual reset (by hand) on the actuation of the actuator beyond the pressure point
- After the dangerous movement has been stopped, renewed switch on using a foot is only allowed after releasing the foot switch and renewed actuation.
- evaluation of at least one normally open contact and one normally closed contact
- in the case of several operators, each person shall actuate a foot switch

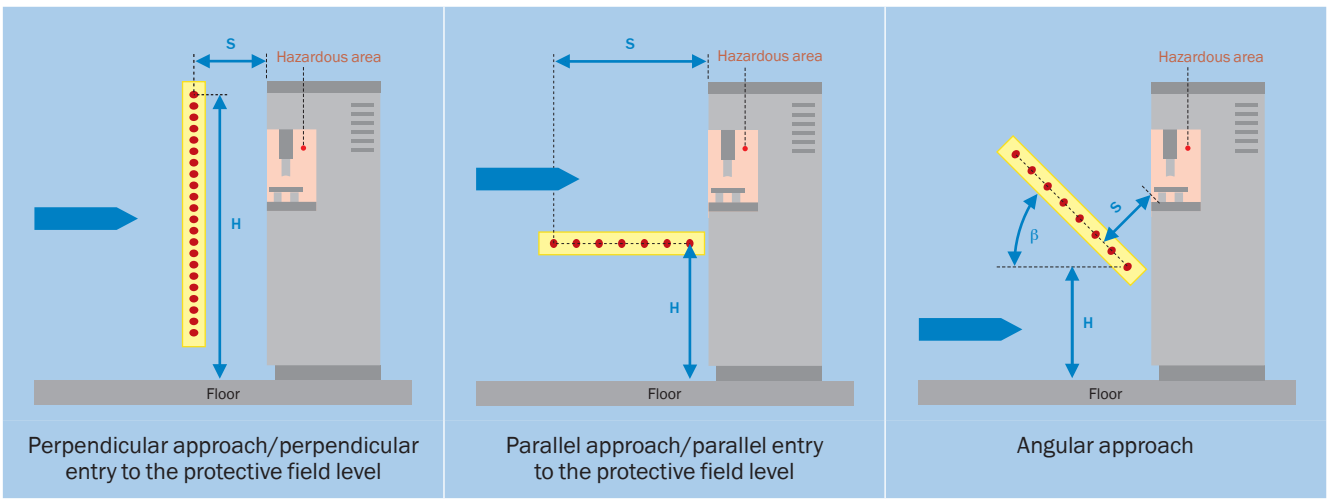
Positioning/dimensioning the protective devices

An essential aspect during the selection of the optimal protective device is the space available. It shall be ensured the dangerous state is eliminated in time prior to reaching the hazard.
The necessary safety distance is dependent on, among other aspects, the size and type of protective device.



Safety distance for ESPE as a function of the approach

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



Perpendicular approach/perpendicular entry to the protective field level

Parallel approach/parallel entry to the protective field level

Angular approach

After the ESPE has been selected, the necessary safety distance between the ESPE's protective field and the nearest hazardous point is to be calculated.

The following parameters are to be taken into account:

- stopping time of the machine
- response time of the safety relevant controller
- response time of the protective device (ESPE)
- supplements as a function of the resolution of the ESPE and/or type of approach

If the minimum distance is too large and unacceptable from an ergonomic point of view, either the total time the machine takes to stop shall be reduced or an ESPE with smaller resolution shall be used. Possible standing behind is to be prevented.

→ The calculation of the safety distance for an ESPE is described in various standards such as in ANSI B11.19, ANSI RIA 15.06, CSA Z434 and ISO 13 855.

General calculation formula

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

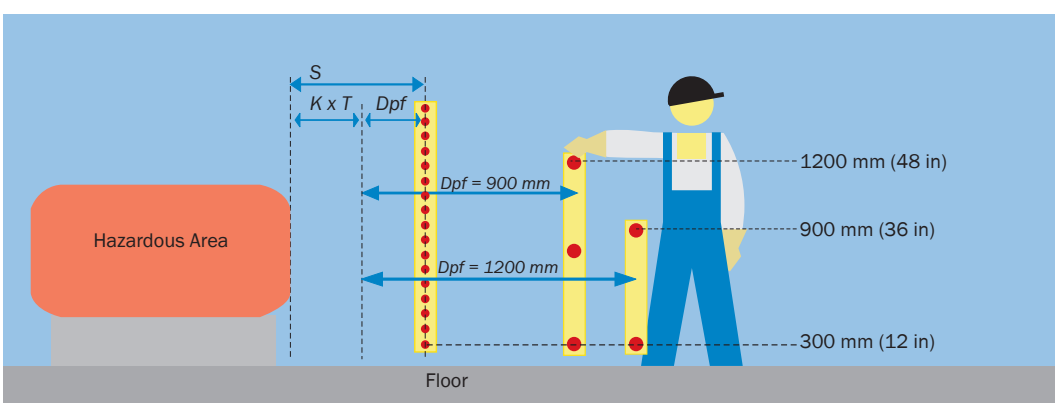
Where ...
- **S** is the minimum distance in millimeters, measured from the nearest hazardous point to the detection point or to the detection line or detection plane of the ESPE.
- **K** is a parameter in mm/s or in/s, derived from data on approach speeds of the body or parts of the body. Often 1600 mm/s (63 in/s) is used.
- **T** is the stopping/run-down time of the entire system in seconds.
- **D_{pf}** is an additional distance in millimeters that defines the entry into the hazardous area before the protective device is triggered (penetration factor).

The following table contains the formula for the calculation of the safety distance S (Per ANSI B11.19 / ANSI RIA 15.06 / CSA Z434). You will find examples on the next page.

Approach	Detection capability (resolution)	Beam height (distance from floor)	Safety Distance
Perpendicular ß = 90° (±5°)	d = < 64 mm (2.5 in)		**$S = K \times \sum T_{total} + D_{pf}$** where D_{pf} is determined by: $D_{pf} = 3.4 \times$ (resolution – 6.875 mm) $D_{pf} = 3.4 \times$ (resolution – 0.275 in)
	64 (2.5 in) ≤ d ≤ 600 mm (24 in)	Height of the bottom beam ≤ 300 mm (12 in) Height of highest beam ≥ 1200 mm (48 in)	D_{pf} = 900 mm (36 in)
	64 (2.5 in) ≤ d ≤ 600 mm (24 in)	Height of the bottom beam ≤ 300 mm (12 in) Height of highest beam ≥ 900 mm (36 in)	D_{pf} = 1200 mm (48 in)
Parallel ß = 0° (±5°)	< 50 mm (2 in) 64 mm (2.5 in) 76 mm (3.0 in) 89 mm (3.5 in) 102 mm (4.0 in) 108 mm (4.25 in) 117 mm (4.6 in) Formula: $d \le \frac{H}{15} + 50$	0 190 mm (7.5 in) 380 mm (15 in) 570 mm (22.5 in) 760 mm (30 in) 860 mm (33.75 in) 990 mm (39 in) If used as a perimeter guard, supplemental safeguarding may be required if height of protective field (lowest beam) is > 300 mm (12 in)	$S = K \times \sum T_{total} + D_{pf}$ where D_{pf} is determined by: D_{pf} = 1200 mm (48 in)
Angular 5° < ß < 85°	If ß ≥ 30°, use the perpendicular approach defined above. If ß < 30°, use the horizontal or parallel approach defined above. The safety distance S is based on the beam closest to the hazardous point.		

S= Safety distance
H = Height
d = Detection capability (resolution)
ß = Angle between detection plane and the direction of entry
T = Time

[1]) Important note:
Under no circumstance shall it be possible to reach the hazard. See page 3-35 for more information



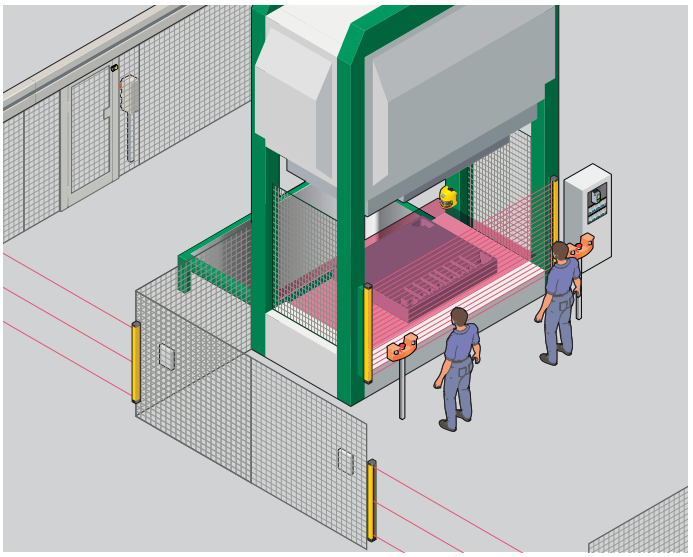
Example of guarding with various detection capabilities for the perpendicular approach

Special cases

ESPE for presence detection

This type of protection is recommended for large systems that are accessible from the floor. In this special case, starting of the machine (safety function: **preventing starting**) shall be prevented while there is an operator inside. This is a secondary protective device.

The safety 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). The secondary protective device (with horizontal protective field) detects the presence of a person in the machine and prevents the machine starting.



Mobile applications on vehicles

If the dangerous state is produced by a vehicle, then the vehicle's road speed is generally used to determine the safety distance and not the speed of approach of the personnel.

If the vehicle (and therefore the protective device) and a person are approaching each other, in the normal case it is assumed the person will recognize the hazard and stop or move away. The safety distance therefore "only" needs to be sufficiently large enough to safely stop the vehicle.

Safety supplements may be necessary dependent on the application and the technology used.

Applications with moving ESPE

On some machines, operators are very close to the hazardous area for reasons related to operation. On press brakes, small pieces of plate need to be held very close to the bending edge. Practical protective devices have been proven to be moving systems that form a protective field around the tool openings. Here the hand approach speed is not taken into account, therefore the general formula cannot be applied.

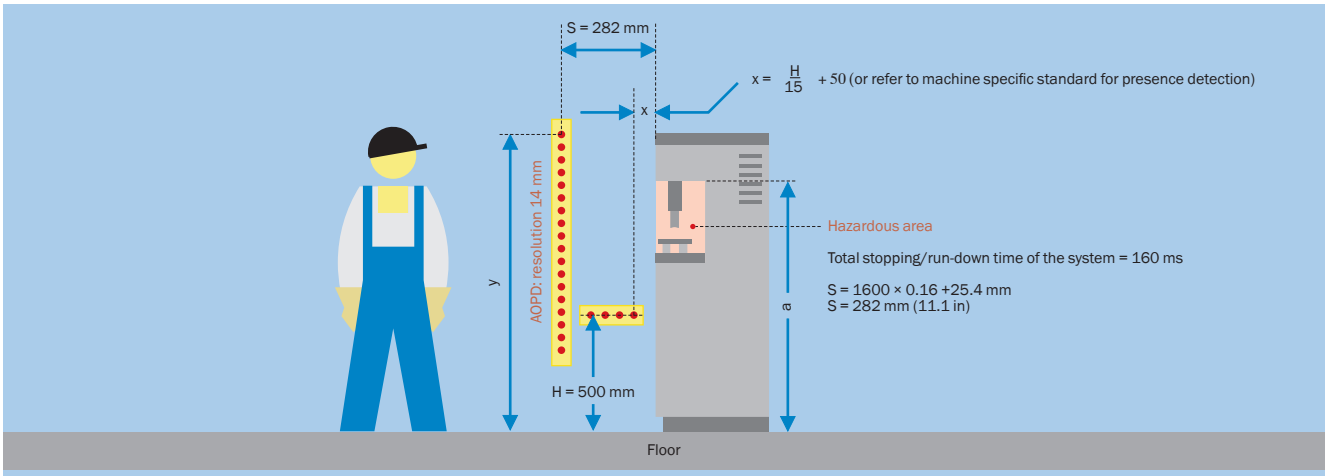
The requirements on the resolution are very high and reflections at the metal surfaces shall be excluded. For this reason focused laser systems with camera-based evaluation are used. In connection with other measures (e.g., 3-stage foot switch, automatic stoptime measurement, requirement to wear gloves, etc.), this type of protection is allowed in particular cases.

Examples for the calculation of the safety distance

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

The calculation, as shown in the diagram, yields a safety distance of S = 282 mm. By using a safety light curtain with the best possible resolution, this is already the optimal safety distance.

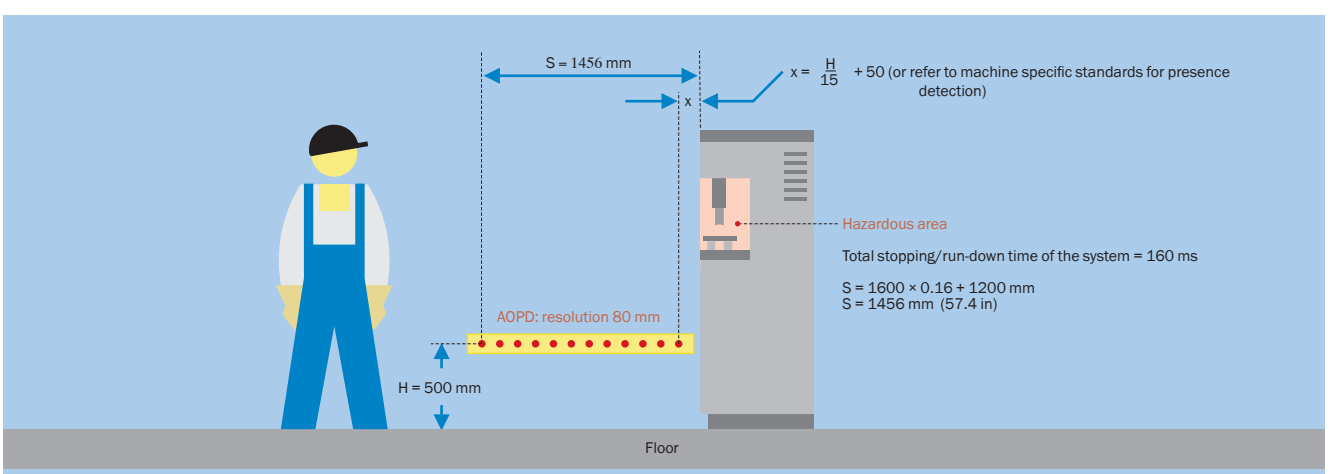
To ensure that the person is detected anywhere in the hazardous area, two AOPDs are used: a vertical AOPD, positioned at the calculated safety distance (perpendicular approach), and a horizontal AOPD, to eliminate the hazard of standing behind the vertical AOPD.



a = Height of the hazardous area
d = Detection capability (resolution of the AOPD)
H = Installation height
S = Safety distance
x = End of the protective field to the machine
y = Height of the top beam, for calculation see “Necessary protective field size/height of the ESPE” on page 3-36

Solution 2: Parallel approach — hazardous area protection

A horizontal AOPD is used. The diagram below shows the calculation of the safety distance S and the positioning of the AOPD. If the installation height of the AOPD is increased to 500 mm, the safety distance is reduced. For this height an AOPD with a resolution less or equal to 80 mm can be used. However, it shall still not be possible to access the hazardous area beneath the AOPD. This type of protection is often implemented using AOPDDR (laser scanners). However, supplements shall be added for these devices for technology-related reasons.

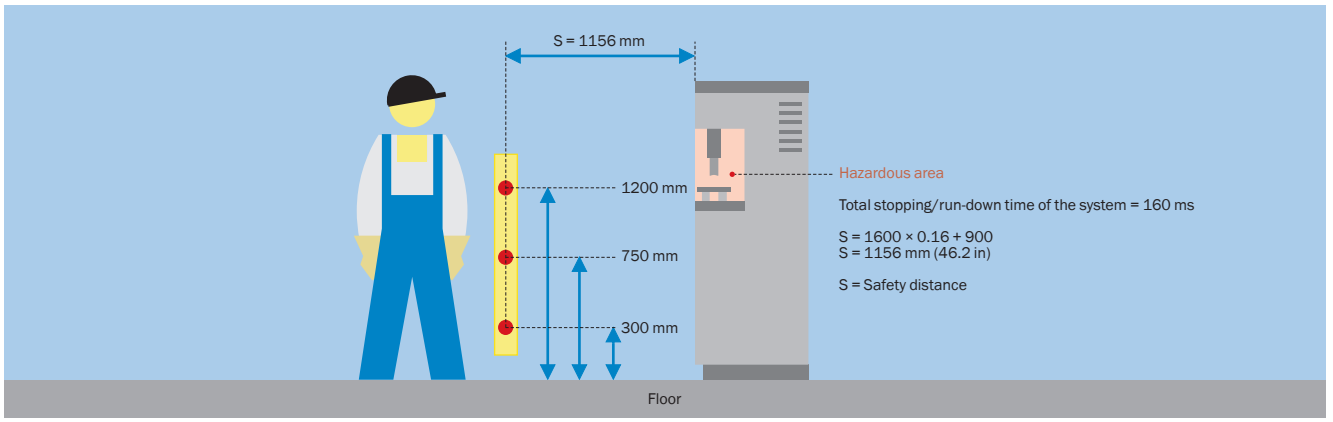


d = Detection capability (resolution of the AOPD)
H = Installation height
S = Safety distance
x = End of the protective field to the machine

3 C

Solution 3: Access protection (Perimeter guarding)

Access protection with 3 beams (at heights of 300 mm, 750 mm and 1200 mm) permits perpendicular approach. This solution permits the operator to stand between the hazardous area and the AOPD without detection. For this reason, additional safety measures shall be taken to reduce this risk. The control mechanism (e.g., reset button) shall be positioned such that the entire hazardous area can be seen. It shall not be possible to reach the button from the hazardous area.



3 c

Overview of the results

The table below shows the results of these solutions. Operative requirements determine which of the solutions is chosen:

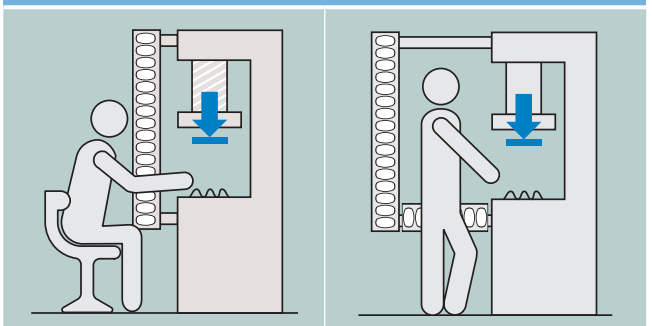
Solution for stopping/run-down time = 160 ms		Advantages	Disadvantages
1	**Hazardous point protection** **S = 282 mm (11.1 in)**	■Increased productivity, as the operator is closer to the work process (short paths) ■Automatic start or PSDI mode possible ■Very little space required	■Higher price for the protective device due to good resolution and presence detection
2	**Hazardous area protection** **S = 1456 mm (57.4 in)**	■Automatic start possible ■Enables the access to be protected independent of the height of the hazardous area	■The operator is much further away (longest distances) ■More space required ■Lower productivity
3	**Access protection** **S = 1156 mm (46.2 in)**	■Most economical solution ■Enables the access to be protected independent of the height of the hazardous area ■Protection on several sides possible using deflector mirrors	■The operator is much further away (long distances) ■Lowest productivity (always necessary to reset the ESPE) ■The risk of standing behind is to be taken into account. Not to be recommended if several people work at the workplace.

Necessary protective field size/height of the ESPE

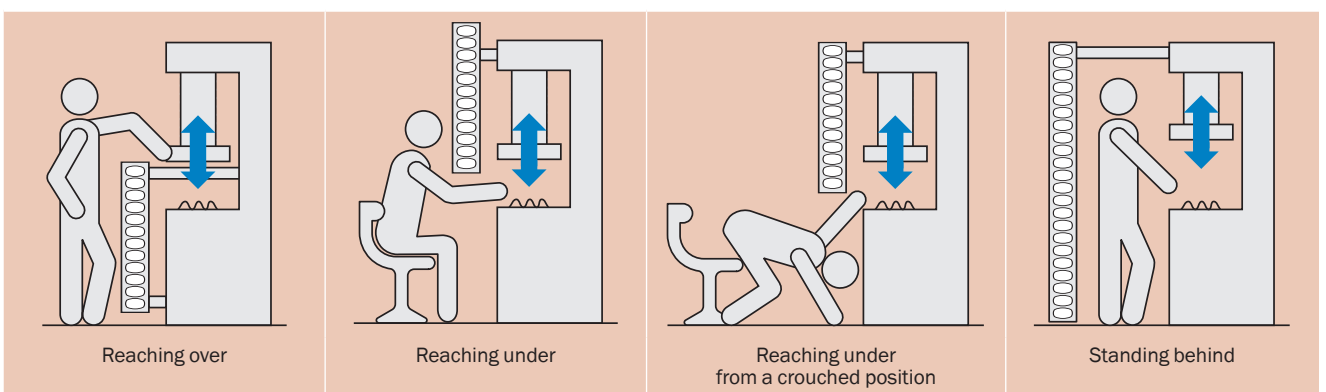
In general, the following errors shall be excluded when mounting protective devices:

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

Examples for correct mounting



Examples for dangerous mounting errors



Once the minimum safety distance between protective field and the nearest hazardous point has been calculated, the protective field height required is to be determined in a further step. In this way it is to be ensured the hazardous point cannot be reached by reaching over.

Necessary protective field height for ESPE as per Draft of ISO 13855 (2009)

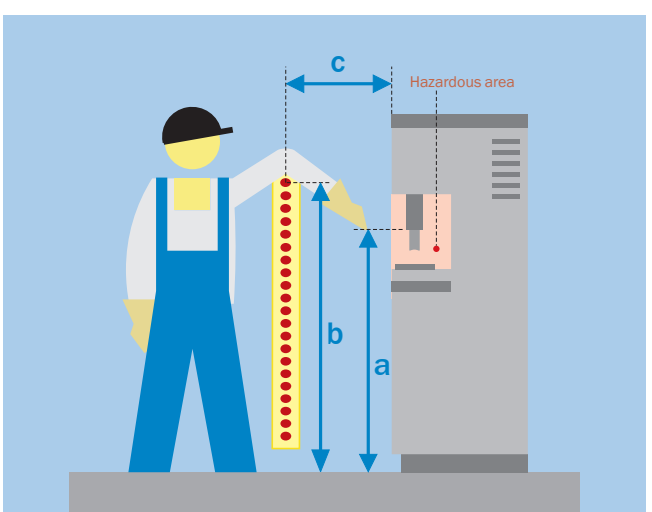
Height a of the hazardous area (mm)	Horizontal distance c to the hazardous area (mm)											
2600	0	0	0	0	0	0	0	0	0	0	0	0
2500	400	400	350	300	300	300	300	300	250	150	100	0
2400	550	550	550	500	450	450	400	400	300	250	100	0
2200	800	750	750	700	650	650	600	550	400	250	0	0
2000	950	950	850	850	800	750	700	550	400	0	0	0
1800	1100	1100	950	950	850	800	750	550	0	0	0	0
1600	1150	1150	1100	1000	900	850	750	450	0	0	0	0
1400	1200	1200	1100	1000	900	850	650	0	0	0	0	0
1200	1200	1200	1100	1000	850	800	0	0	0	0	0	0
1000	1200	1150	1050	950	750	700	0	0	0	0	0	0
800	1150	1050	950	800	500	450	0	0	0	0	0	0
600	1050	950	750	550	0	0	0	0	0	0	0	0
400	900	700	0	0	0	0	0	0	0	0	0	0
200	600	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0
	Resulting height b of the top edge of the protective field (mm)											
	900	1000	1100	1200	1300	1400	1600	1800	2000	2200	2400	2600

Proceed as follows to determine the necessary height for the top edge of the protective field for this safety distance:

1. Determine the height of the hazardous point a and find the value in the column on the left, 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 top edge of the protective field from, e.g. the floor, in the bottom row 1600 mm.

Example

The safety distance calculated between the protective field and the nearest hazardous point is 240 mm.
The top edge of the protective field shall be at 1600 mm in this example so that the hazardous point cannot be reached by reaching over. If the protective field starts, e.g. 700 mm above the reference level, a light curtain with a protective field height of 900 mm is to be used.



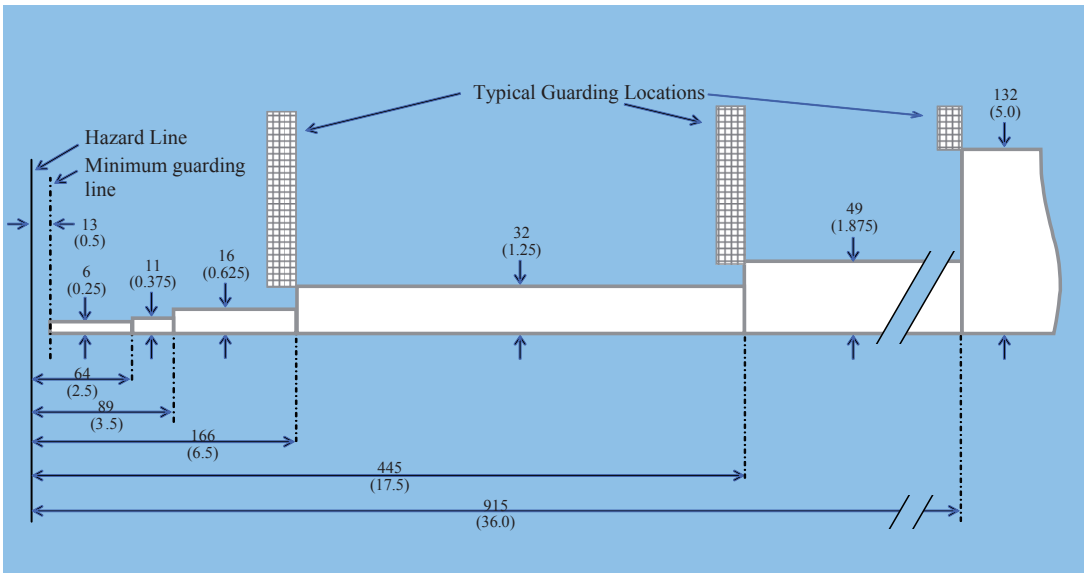
Parameters for determining the necessary protective field height

→ A special table for the necessary protective field height of ESPE was in preparation as in the new Draft of ISO 13 855 at the time of going to press.

Safety distance for physical guards

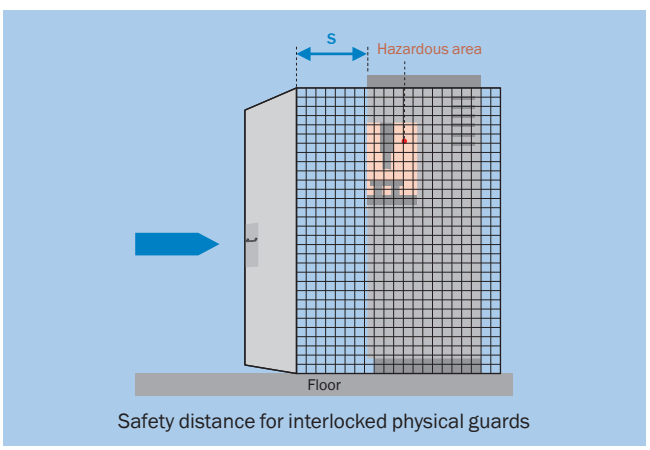
Physical guards shall be at an adequate distance from the hazardous area if they have openings. This requirement also applies to openings between guard and machine frame, clamping plates, etc. There are different distance requirements depending on the type of opening (slotted, square, circle).

Safety distance as a function of the openings on physical guards (for slotted opening)



Safety distance for interlocked physical guards

For interlocked physical guards that initiate a stop, a safety distance shall also be maintained similar to the procedure for the ESPE. As an alternative, interlocks with locking devices can prevent access until there is no longer any hazard.



Safety distance for interlocked physical guards

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

Where ...
- **S** is the minimum distance in millimeters, measured from the nearest hazardous point to the next door opening point.
- **K** is a parameter in millimeters per second, derived from data on approach speeds of the body or parts of the body, as a rule 1600 mm/s (63 in/s).
- **T** is the stopping/run-down time of the entire system in seconds.

➜ Calculation of the safety distance for interlocked physical guards: ANSI B11.19, ISO 13855

3 C

Necessary height of physical guards

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

Note: For Robot applications, American and Canadian standards define minimum horizontal distances and minimum dimension on the guarding.

Necessary height for physical guards in case of high potential hazard.

Height a of the hazardous area (mm)	Horizontal distance c to the hazardous area (mm)									
2700	0	0	0	0	0	0	0	0	0	0
2600	900	800	700	600	600	500	400	300	100	0
2400	1100	1000	900	800	700	600	400	300	100	0
2200	1300	1200	1000	900	800	600	400	300	0	0
2000	1400	1300	1100	900	800	600	400	0	0	0
1800	1500	1400	1100	900	800	600	0	0	0	0
1600	1500	1400	1100	900	800	500	0	0	0	0
1400	1500	1400	1100	900	800	0	0	0	0	0
1200	1500	1400	1100	900	700	0	0	0	0	0
1000	1500	1400	1000	800	0	0	0	0	0	0
800	1500	1300	900	600	0	0	0	0	0	0
600	1400	1300	800	0	0	0	0	0	0	0
400	1400	1200	400	0	0	0	0	0	0	0
200	1200	900	0	0	0	0	0	0	0	0
0	1100	500	0	0	0	0	0	0	0	0
	Resulting height b of the top edge of the protective field (mm)									
	1000	1200	1400	1600	1800	2000	2200	2400	2500	2700

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

1. Determine the height of the hazardous point **a** and find the value in the column on the left, 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 physical guard in the bottom row, e.g. example for high risk 1800 mm.

Example of high potential hazard

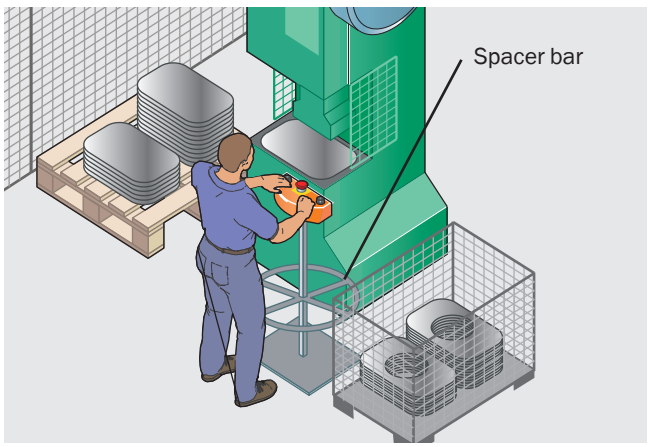
The physical guard shall therefore start 200 mm above the reference level and end at 1800 mm. If the top edge of the guard is to be at 1600 mm, then the safety distance shall be increased to at least 800 mm.

➜ Safety distances and necessary protective field height: ISO 13 857, CSA Z434-04

Safety distance for fixed position protective devices

Example: Safety distance for two-hand control

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



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 data on approach speeds of the body or parts of the body, as a rule 1600 mm/s (63 in/s).
- **T** is the stopping/run-down time of the entire system measured from the release of the control in seconds.

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

➜ Calculation of the safety distance: ANSI B11.19, ISO 13855

Integration of the protective devices in the control system

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

"Control systems are functional assemblies that form part of the information system of a machine and realise logical functions. They co-ordinate 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 by the technology used, i.e. by the information carriers, in fluid, electrical and electronic control systems."

Translation of text from: Alfred Neudörfer, Konstruieren sicherheitsgerechter Produkte, Springer Verlag, Berlin u. a., ISBN 97-3-540-21218-8 (3rd edition 2005).
(English version "The Design of Safe Machines" planned for 2010: ISBN 978-3-540-35791-9)

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 should perform safety functions. For this reason, special requirements are placed on their reliability and their resistance to failures. They are based on principles to control and prevent failures.

Control system			Safety-related aspects	
Principle of operation of the control system		**Typical components**	**Interfering factors**	**Explanations**
Fluid	Pneumatic	■ Multiway valves ■ Vent valves ■ Manual shut-off valves ■ Filters with water trap ■ Hoses	■ Changes in energy levels ■ Purity and water content of the compressed air	Mostly designed as electropneumatic control systems. Service unit necessary for conditioning compressed air.
	Hydraulic	■ Accumulators ■ Pressure limiters ■ Multiway valves ■ Filters ■ Level gauges ■ Temperature gauges ■ Hoses and cables ■ Threaded fittings	■ Purity ■ Viscosity ■ Temperature of the pressurized fluid	Mostly designed as electrohydraulic control systems. Measures necessary to limit the pressure and temperature in the system and to filter the medium.
Electrical	Electro-mechanical	■ Control switches: ▪ Position switches ▪ Selector switches ▪ Push-buttons ■ Switchgear: ▪ Contactors ▪ Relays ▪ Circuit breakers	■ Protection class of the device ■ 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	■ Individual components, e.g.: ▪ Transistors ▪ Resistors ▪ Capacitors ▪ Coils ■ Highly integrated components, e.g. integrated circuits (IC)	As in "Electromechanical" In addition: ■ Temperature fluctuations ■ Electromagnetic interference coupled via cables or fields	Exclusions of failures not possible. Reliable action can only be realized using control system concepts, not by component selection.
	Microprocessor controlled	■ Microprocessors ■ Software	■ Installation fault in the hardware ■ Systematic failures including common mode failures ■ Programming errors ■ Application errors ■ Operating errors ■ Tampering ■ Viruses	■ Measures to prevent failures: ▪ Structured design ▪ Program analysis ▪ Simulation ■ Measures to control failures: ▪ Redundant hardware and software ▪ RAM/ROM test ▪ CPU test

Translation of text from: Alfred Neudörfer, Konstruieren sicherheitsgerechter Produkte, Springer Verlag, Berlin u. a., ISBN 978-3-540-21218-8 (3rd edition 2005)
(English version "The Design of Safe Machines" planned for 2010: ISBN 978-3-540-35791-9)

The safety-related input elements are described in the previous chapter as the safety sensors (protective devices). For this reason only the logic unit and the actuators are described in the following.
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 switches normally to the hazard-free state.)
Fluid control systems are often implemented as electropneumatic or electrohydraulic control systems. In other words,t the electrical signals are converted to fluid energy by valves to move cylinders and other actuators.

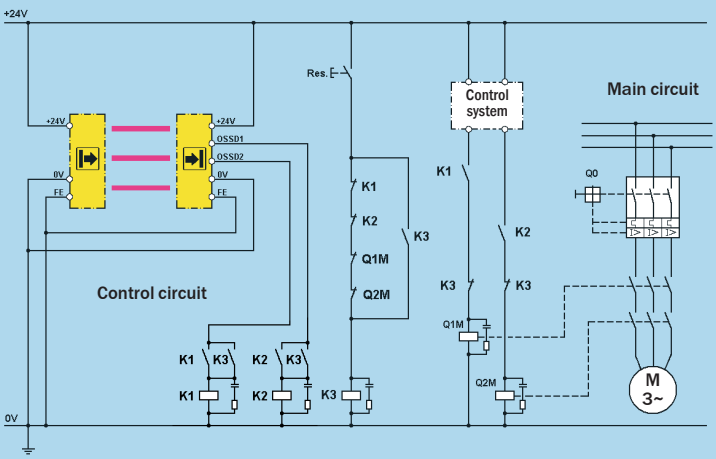
➜ You will find connection diagrams for the integration of protective devices at http://www.sick.com

Logic units

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

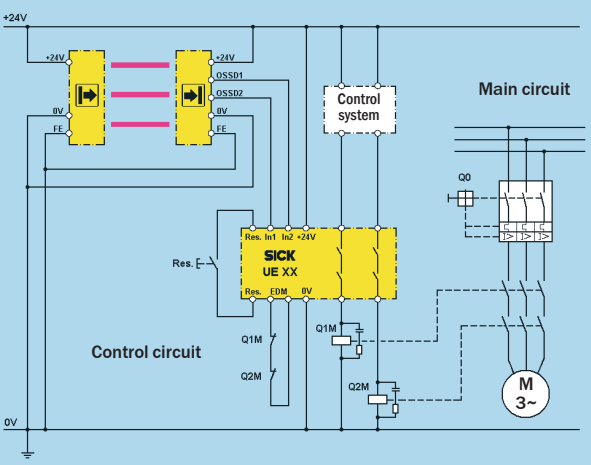
Warning: The signals from the protective devices shall not be processed only by standard control systems (PLC). There shall also be redundant circuits for removing electrical power.

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. The logical operators are implemented using the wiring.
Function: If the contactors K1 and K2 are de-energized, on pressing S1 the K3 contactor is energized and remains energized. If no object is detected in the active protective field, the outputs OSSD1 and OSSD2 are high. The contactors K1 and K2 are energized by the normally open contacts on K3 and latch themselves. K3 is de-energised by releasing the S1 button. 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 with Safety Interface Modules (SIM)



Safety Interface Modules combine one or more safety functions in one housing. They generally have self-monitoring functions. The cut-off paths can be implemented using contacts or semiconductors. They can also have signal contacts.
The implementation of more complex safety applications is simplified. The certified Safety Interface Modules also reduces the effort for the validation of the safety functions.

In Safety Interface Modules, semiconductor elements can perform the task of the electromechanical switching elements instead of relays. Switching techniques such as dynamic signal transmission and multiple channel signal processing with error detection ensure the purely electronic solutions operate reliably.

3 C

Logic unit with software-based components

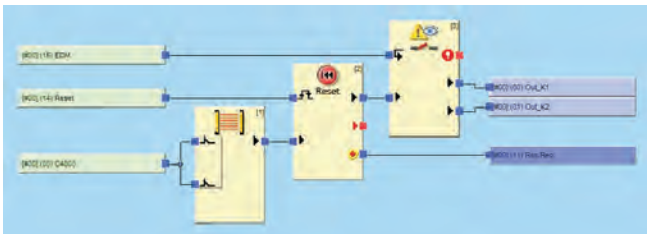
Similar to automation technology, safety technology has developed from hard-wired auxiliary contactors through Safety Interface Modules, to some extent with configurable safety logic for which parameters can be set, to complex safety-rated PLCs. The concept of “proven components” and “proven safety principles” are now available using electrical and programmable electronic systems.
The logical part of the safety function is implemented here in software.
Software is to be differentiated by firmware — developed and certified by the manufacturer of the control system — and the actual safety application. This application is developed by the machine manufacturer using the language supported by the firmware.

Parameterization

Selection of properties from a defined pool of functionality by selector switch or software settings at the time of commissioning,
typical features: binary functions, such as AND/OR logic, small number of I/O devices.

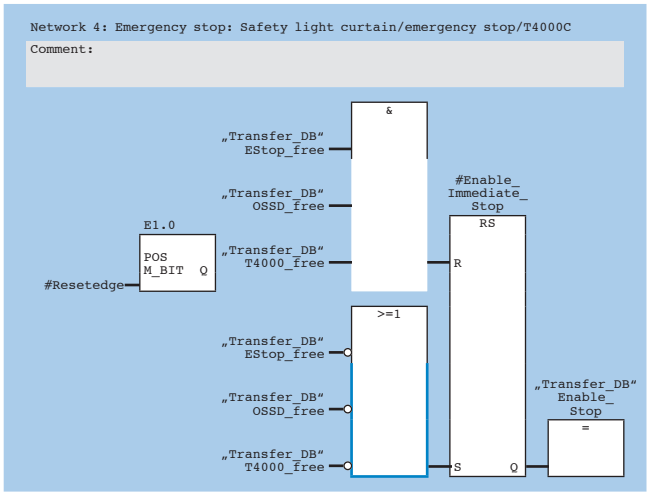
Configuration

Flexible connection of defined function blocks in certified logic with a programming interface, for example, input type selection, discrepancy time settingand configuration of the inputs/outputs on the control system,
typical features: complex binary logic, multiple safety zones



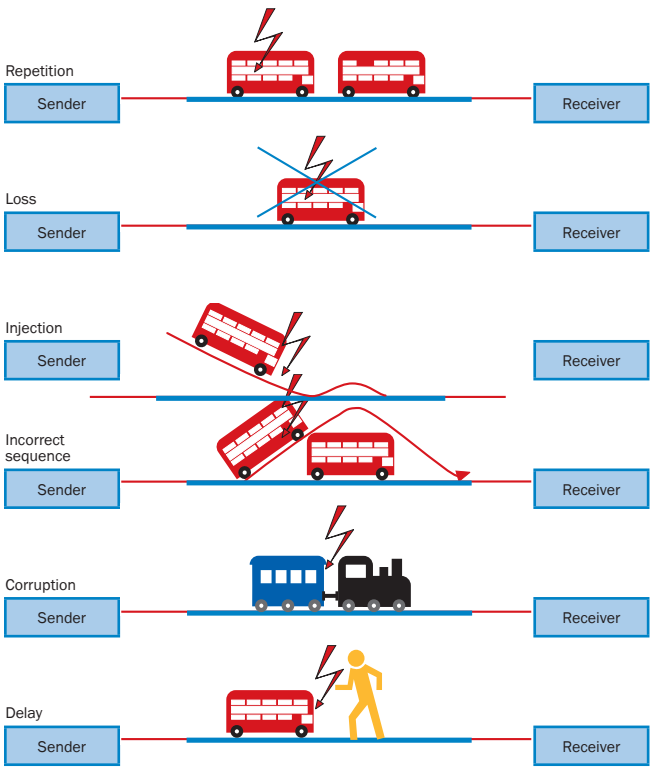
Programming

Design of the logic as required using the functionality defined by the pre-defined programming language, mostly using certified function blocks,
typical 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 responsible for the transmission of states between different parts of control systems. A bus system eases the wiring and as a result reduces the possible mistakes. Several use bus systems already are available for safety-related applications.
A detailed study of different faults and errors in hardware, transmission media, and software has shown that such faults fall into six categories:



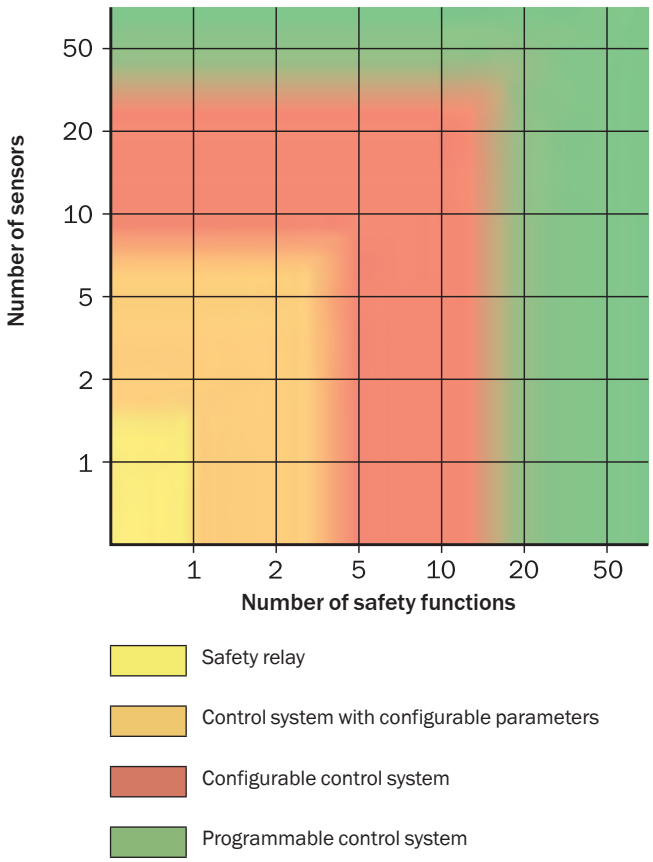
Source: Sicherheitsgerechtes Konstruieren von Druck- und Papierverarbeitungsmaschinen — Elektrische Ausrüstung und Steuerungen; BG Druck- und Papierverarbeitung; edition 06/2004; page 79

Numerous measures can be taken in the higher level control system against the transmission errors mentioned above, such as sequential numbering of the safety-related messages or defined times for incoming messages with acknowledgement. Protocol extensions based on the fieldbus used include such measures. In the ISO/OSI layer model, they act above the transport layer and therefore utilise the fieldbus with all its components as a “black channel,” without modification. The following bus systems are certified for safety applications:

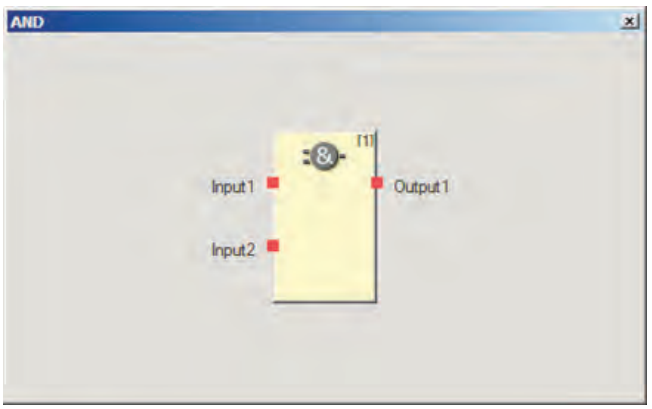
- AS-i Safety at Work
- DeviceNet Safety
- PROFIsafe

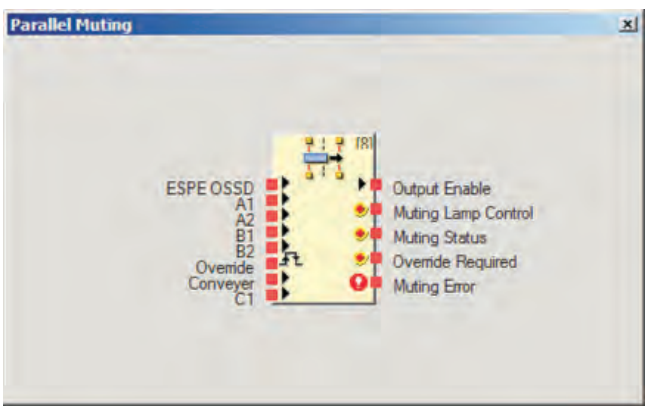
Selection criteria

The criteria for the selection of a control system family are initially the number of safety functions to be used 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.





Software specification

To prevent the occurrence of a dangerous state, software-based logic units in particular shall be so designed that failures in the logic are reliably prevented. To detect systematic failures, a thorough systematic check should be made by someone other than the software program developer.

The safety functions should be implemented in the software-based solution based on a detailed functional specification. This specification should be complete, free of contradictions, possible to read and expand. A review with all those involved in the project is advised.

With poorly documented and unstructured programs, errors will be produced during later modifications, in particular there is a risk of unknown dependencies, so-called side effects. Good specifications and program documentation have a powerful error-prevention effect particularly if the software is developed externally.

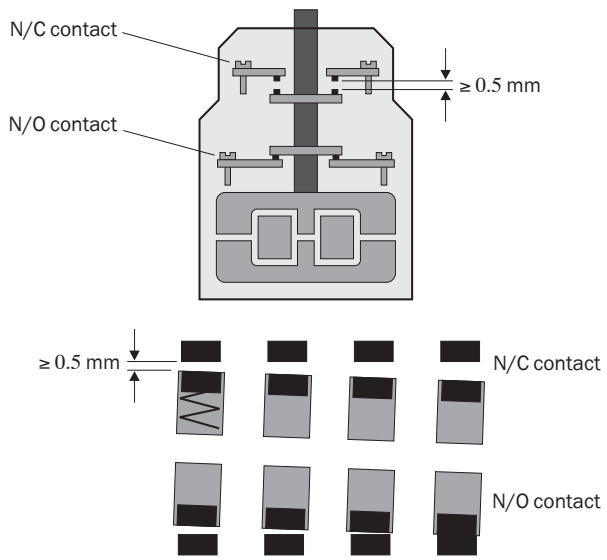
Power control elements

The safety function triggered by the protective devices and the logic unit shall stop a dangerous movement. For this purpose, the actuator elements/work elements are switched off by power control elements.

➜ Principle of switch off/power shutdown: ISO 13849-2

Contactors

The type of power control elements used most frequently are electromechanical contactors. One or more contactors can form a safety function sub-system by means of special selection criteria, wiring and 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. This requirement can be met by using a contactor with positively guided contacts. The contacts are positively guided when the contacts in a set of contacts are mechanically linked such that normally open contacts and normally closed contacts can never be closed simultaneously during the entire service life.
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 shall be ensured even in the event of a fault (welded contact). As on circuit breakers with small 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” on small circuit breakers.



Source: Moeller AG

On larger contactors, so-called “mirror contacts” are often the only option: While any main contact on a contactor is closed, no mirror contact (auxiliary normally closed contact) is allowed to be closed.

Suppressor

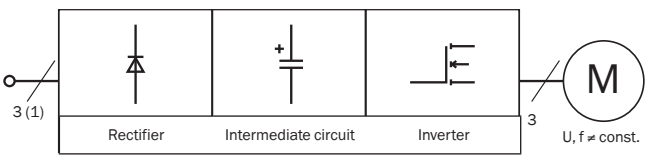
Inductances such as coils on valves or contactors shall be equipped with a suppressor to limit transient voltage spikes on switch off. In this way, the switching element is protected against overload, in particular against overvoltage at particularly sensitive semiconductors. As a rule, such circuits have an effect on the release (OFF) delay. A simple diode for arc-suppression can result in a response time up to 14-times longer. Take this into account for the safety distance calculation.

Suppressor (across inductance)	Diode	Diode combination	Varistor	RC element
			U	
Overvoltage	++	+	o	+
Release delay	– –	o	+	+[1)]

1) It is necessary to exactly determine the element depending on the inductance!

Servo amplifiers and frequency inverters

In drive technology, three-phase drives with frequency inverters have largely replaced DC drives. Here the inverter generates an output voltage of variable frequency and amplitude from the fixed three-phase mains. Depending on the version, regulated rectifiers can feed the energy absorbed by the intermediate circuit during braking back to the mains.
The rectifier stores the power supplied from the mains in 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.



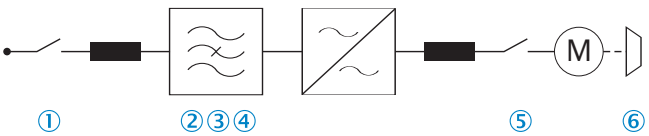
Checklist

- 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/PE using large area connections?
- Commutation choke connected in series for peak current limiting?

To limit transient overvoltages caused by switching loads in DC and AC circuits, interference suppression components should be used.

Safety functionality on servo amplifiers and frequency inverters

Several cut-off paths for the safe isolation of the motor from the voltage supply are possible.



① Mains contactor — poor due to long re-energization time, high wear due to switch on current
② Controller enable
③ Pulse inhibit “safe restart interlock (stop)”
④ Setpoint
⑤ Motor contactor — not allowed on all inverters
⑥ Retaining brake — normally not a service brake

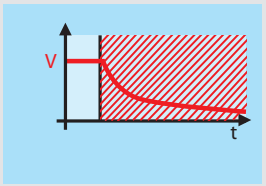
Safety functionality is increasingly integrated into servo drives and frequency inverters.

The function to be found most frequently, STO, shuts down the pulse controlling stage of the inverter for safety reasons using a single-channel or dual-channels, depending on the design.
In the case of single-channel operation, additional measures shall be taken to ensure safety is maintained in the event of an internal failure in the inverter. For this purpose a feedback signal is to be evaluated in the control system.

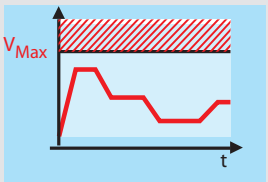
Other examples are shown in the following table.

➜ Functional safety of power drives IEC 61800-5-2

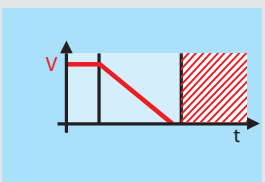
Safety functions of servo drives



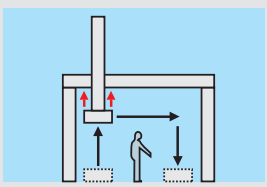
Safe Torque Off (STO)
Safe Torque Off
Stop category 0 in accordance with IEC 60204-1:
Safe drive torque cut off



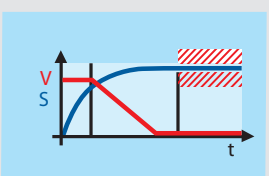
Safe Maximum Speed (SMS)
The maximum speed is safely monitored irrespective of the mode of operation



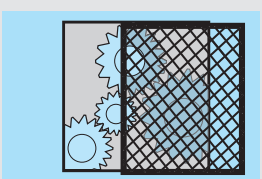
Safe Stop and Safe Drive Interlock (SS1)
Safe Stop 1
Stop category 1 in accordance with IEC 60204-1:
Safely monitored stop, control or drive controlled with safe drive torque cut off



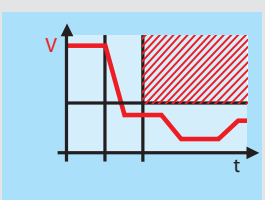
Safe Braking And Holding System (SBS)
The safe braking and holding system controls and monitors two independent brakes



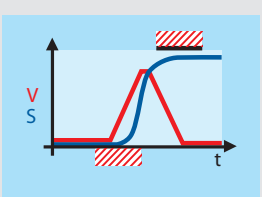
Safe Operating Stop (SS2, SOS)
Safe Stop 2, Safe Operating Stop
Stop category 2 in accordance with IEC 60204-1:
Safely monitored stop with safely monitored standstill at controlled torque



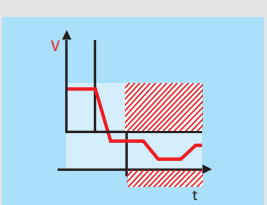
Safe Door Locking (SDL)
When all the drives in one protection zone are in safe status, the safety door lock is released



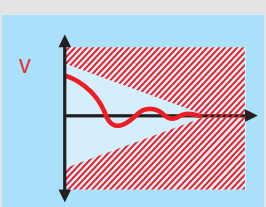
Safely Limited Speed (SLS)
If enable signal is given a safely limited speed is monitored in special operating mode



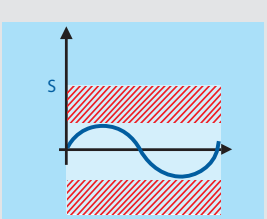
Safely Limited Increment (SLI)
If enable signal is given a safely limited increment is monitored in special operating mode



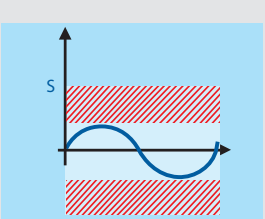
Safely Monitored Direction (SDI)
A safe direction (clockwise, counter-clockwise) is also monitored in addition to safe motion



Safely Monitored Deceleration (SMD)
Safely monitored deceleration ramp when stopping



Safely Limited Position (SLP)
A safely limited position range is also monitored in addition to safe motion



Safely Limited Position Switch (SPS)
Monitoring of safe software limit switches

Source: Bosch Rexroth AG

Fluid control systems

Valves

All valves require cylindrical guides on the moving components. The most frequent cause for the failure of valves are:

- failure of return spring
- contamination of the fluid

The usage of a “spring proven for safety-related applications” is considered a proven safety principle.

An important differentiating factor between the valves is the design of the moving valve body inside the valve.

Seat valves mate with a corresponding seat in the housing when the valve is closed and come to a stop in a fixed position. Using ground surfaces it is possible to achieve complete sealing of the flow path.

On piston valves, the valve body closes or opens the flow path by moving past a bore/groove. The closing edges that determine the overlap on the transition from one switching position to the other are termed control edges. The gap between piston and housing bore necessary for the function results in leakage from the side with the higher pressure to the side with the lower pressure.

Safety-related design principles

For safety-related usage 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 valve body
- analog travel measurement on the moving valve body
- pressure measurement after the valve

In the case of electromagnetically actuated valves, a suppressor is necessary similar to a contactor.

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, mould sand, fibers from cloths, basic contamination)
- contamination that occurs during operation = operating contamination (e.g., ambient contamination, component abrasion)

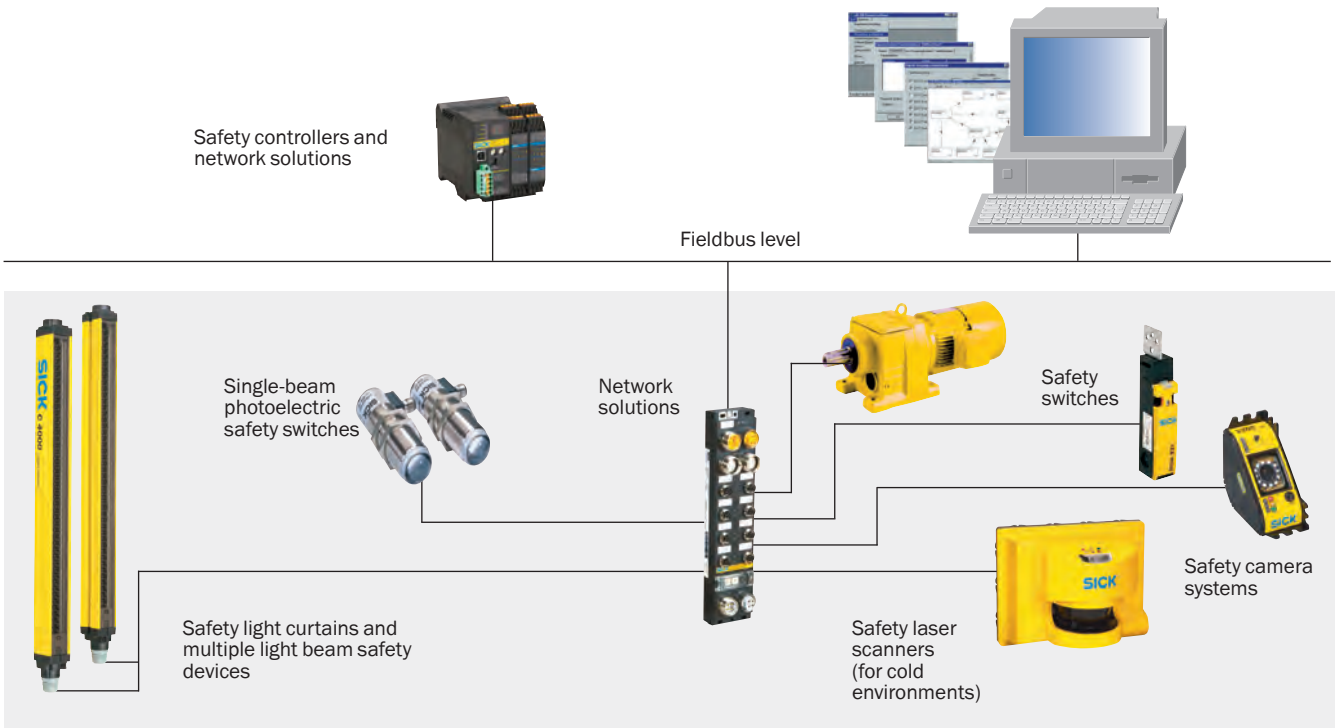
This contamination shall be reduced to an acceptable degree with the aid of filters.

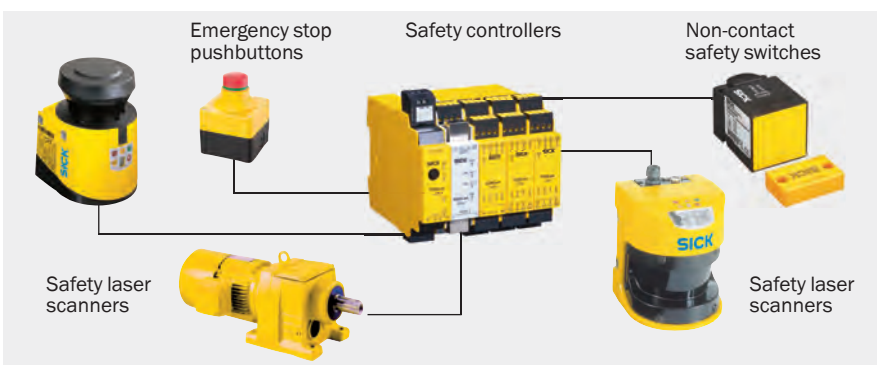
A filter concept refers to the suitable selection of a filter principle for the task required as well as the arrangement of the filter in an appropriate location. The filter concept shall be designed such that it is able to retain in the filter the contamination added to the entire system so that the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

➜ Proven safety principles: ISO 13849-2

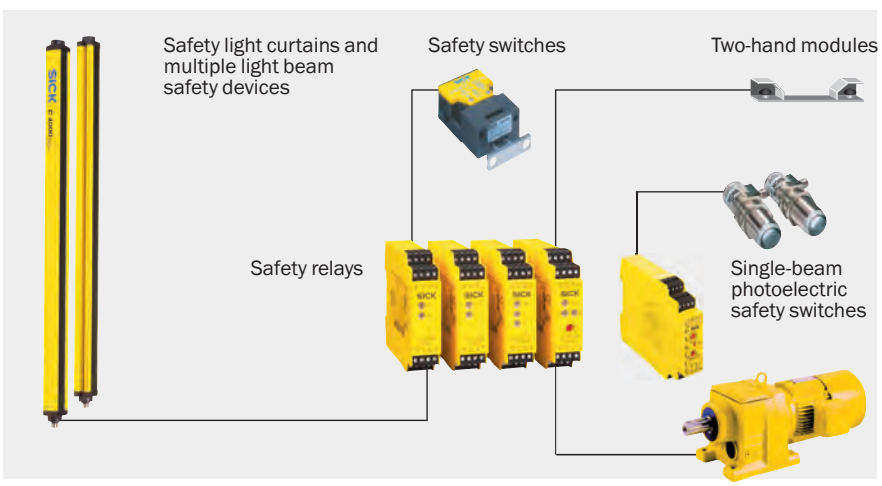
➜ Aging process on hydraulic valves: BIA-Report 6/2004

Product selection





Configuration and diagnostics software



➜ You will find all products online in the product finder at http://www.sickusa.com

Summary: Designing the safety function

Basics

- Develop a safety concept. During this process take into account the features of the machine, the features of the surroundings, the human aspects, the features of the design and the features of protective devices.
- Safety functions are generally formed by the sub-systems sensor, logic and actuator. The safety performance for each sub-system can be determined from the following safety-related parameters: structure, reliability, diagnostics, resistance and process.

Properties and application of protective devices

- Determine the necessary properties for your protective device. Do you need, e.g., one or more items of electro-sensitive protective equipment (ESPE), physical guards, movable physical guards or fixed position protective devices?
- Determine the correct positioning and dimensions for each protective device, in particular the safety distance and the necessary protective field size/height for the related protective device.
- Integrate the protective devices as stated in the operating instructions and as necessary for the level of safety.

Logic units

- Choose the correct logic unit as a function of 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: Verifying the safety function

During verification, it is established by analysis and/or testing that the safety function meets all aspects of the objectives and requirements of the specification.

Verification essentially involves two parts:

- verification of the mechanical safety
- verification of the functional safety

Verifying the mechanical design of the protective device

In the case of mechanical protective devices, it is to be checked whether requirements in relation to the separation or distancing from the hazardous point and, if necessary the requirements on retaining of parts thrown out or radiation are met. In particular attention should be paid to compliance with the ergonomic requirements.

Separating and/or distancing effect

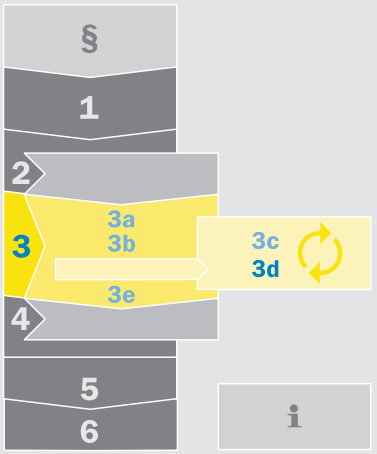
- adequate safety distance and dimensioning (reaching over, reaching under, etc.)
- suitable mesh size or grille spacing on fence elements
- adequate strength and suitable mounting
- selection of suitable materials
- safe design
- resistance to ageing
- design of the protective device such that it is not possible to climb on the protective device

Retaining of parts thrown out and/or of radiation

- adequate strength/resistance to impact and fracture (retaining capacity)
- adequate retaining capacity for the related type of radiation, in particular in the event of thermal hazards (heat, cold)
- suitable mesh size or grille spacing on fence elements
- adequate strength and suitable mounting
- selection of suitable materials
- safe design
- resistance to ageing

Ergonomic requirements

- translucency or transparency (monitoring the operation of the machine)
- design, color, aesthetics
- handling (weight, actuation, etc.)



3 d

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

Example: Checklist for the manufacturer/installer for the installation of protective devices (e.g. an item of ESPE)		
1 Is access to the hazardous area/from the hazardous point adequately prevented and only possible through protected areas (ESPE/physical guards with interlocking device)?	Yes ☐	No ☐
2 Have appropriate measures been taken to prevent (mechanical protection) or monitor unprotected presence in the hazardous area when protecting a hazardous area/hazardous point and have these been secured against removal?	Yes ☐	No ☐
3 Has the maximum stopping and/or stopping/run-down time of the machine been measured and has it been entered and documented (at the machine and/or in the machine documentation)?	Yes ☐	No ☐
4 Has the protective device been mounted such that the required safety distance from the nearest hazardous point has been achieved?	Yes ☐	No ☐
5 Is reaching under/reaching over, climbing under/climbing over or reaching around the protective device effectively prevented?	Yes ☐	No ☐
6 Are the devices/switches mounted correctly and secured against manipulation after adjustment?	Yes ☐	No ☐
7 Are the required protective measures against electric shock in effect (protection class)?	Yes ☐	No ☐
8 Is the control switch for resetting the protective device or restarting the machine present and correctly installed?	Yes ☐	No ☐
9 Are the components used for the protective devices integrated in accordance with the manufacturer's instructions?	Yes ☐	No ☐
10 Are the given protective functions effective at every setting of the operating mode selector switch?	Yes ☐	No ☐
11 Is the protective device effective over the entire period of the dangerous state?	Yes ☐	No ☐
12 Once initiated, will a dangerous state be stopped when switching the protective devices off or when changing the operating mode, or when switching to another protective device?	Yes ☐	No ☐
13 Are the notes included with the protective device attached so they are clearly visible for the operator?	Yes ☐	No ☐

Verifying the functional safety

The safety function shall be checked to verify that the required safety performance matches the actual safety performance. The verification of the safety function should contain the following elements:

- selection of the verification strategy (a verification plan);
- management and execution of verification activities (test specifications, testing procedures, analysis procedures);
- documentation (auditable reports of all verification activities and decisions).

Verification by analysis

The safety performance analysis is to determine its ability to resist or detect safety related faults.
Principally, the following methods are applicable:

- a theoretical check and behavior analysis based on circuit diagrams and the equipment data;
- practical tests on the actual circuit, and fault simulation on actual components, particularly in areas of doubt, of behavior identified during the theoretical check and analysis;
- a simulation of safety circuit behavior, e.g., by means of hardware and/or software models.

In some applications in which multiple safety components are connected in a complex manner, it is usually necessary to divide the parts into several functional groups (sub-systems) and to exclusively submit the interfaces to fault-simulation tests.

Examples of analysis tools include: fault lists, fault tree analysis, failure mode and effects analysis, check lists for systematic faults.

It is impracticable to assess an analysis without assuming that certain faults can be excluded. The faults, which can be excluded, are a compromise between the technical requirements for safety and the theoretical possibilities of occurrence. The analysis shall declare, justify and list all fault exclusions.

Fault exclusion can be based on:

- the improbability of occurrence of certain fault(s);
- generally accepted technical experience which can be applied independently of the application under consideration;
- technical requirements deriving from the application and the specific risk under consideration.

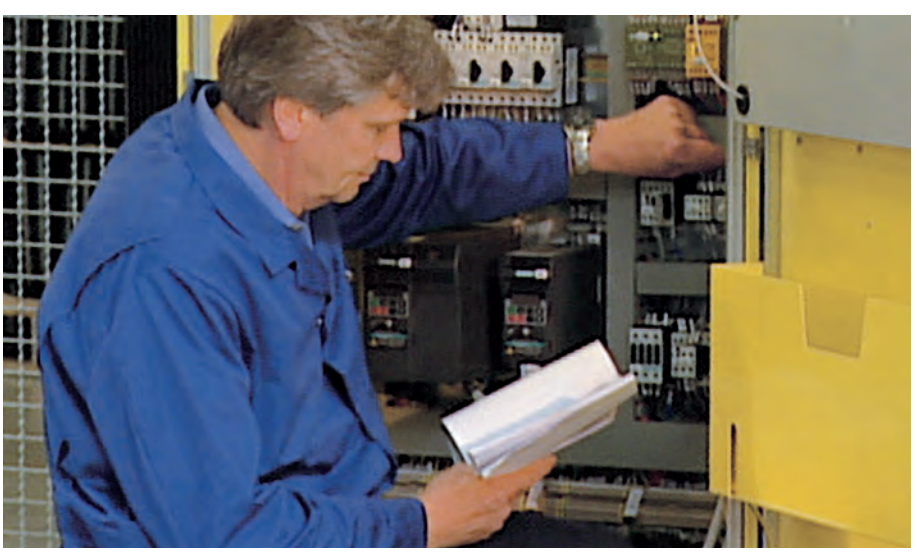
Verification by testing

One step is the testing of the safety functions for complete compliance with their specified characteristics.
Another test shall demonstrate that the specified design performance is achieved during all specified operating mode and all specified environmental conditions. The tests should include, e.g., tests for expected mechanical structure, electrical ratings, temperature, humidity, vibration, shock loading, electromagnetic compatibility, influence of processed materials.

➜ For further information about verification, validation and fault exclusion: ISO 13849-2

Following are three methods used to verify functional safety.

- Determining the system performance achieved based on ANSI RIA 15.06 / CSA Z 434 or using the prescribed method “Control Reliability”
- Determining the performance level (PL) achieved as per ISO 13849-1
- Determining the safety integrity level (SIL) as per IEC 62061



Determining the system performance achieved based on ANSi B11.2008/ ANSI RIA 15.06 / CSA Z 434 or using the prescribed method “Control Reliability“

Some North American standards require the safety performance to be control reliable. “Control reliability” has been defined and implemented based on a variety of definitions. In the definitions presented below, the word “shall” denotes a mandatory requirement for compliance with a regulation or standard. The words “should” and “may” are intended to reflect recommendations and good work practices.

For example, OSHA 1910.211 defines “control reliability” as: A control system designed and constructed so that a failure within the system does not prevent normal stopping action from being applied when required, but does prevent initiation of a successive cycle until the failure is corrected. The failure shall be detectable by means of a simple test or indicated by the control system.

The American National Standards Institute (ANSI) defines “control reliability” in Standard B11.19-2003 (3.14) as: The capability of the machine control system, the protective device, other control components and related interfacing to achieve a safe state in the event of a failure within their safety related functions.

3 d

ANSI B11.19-2003 (E.6.1) further states: “control reliability”:

- Cannot prevent a repeat cycle in the event of a major mechanical failure or in the presence of multiple simultaneous component failures
- Is not provided by simple redundancy. There must be monitoring to assure that redundancy is maintained.

ANSI B11.20-2004 (Annex C) further clarifies the requirements of control reliability by stating the following:
Control reliability is not provided by simple redundancy. There must be monitoring to assure that redundancy is maintained.
Control reliability uses monitoring and checking to determine that a discernable component, module, device or system has failed and that the hazardous motion (or situation) is stopped, or prevented from starting or restarting. Control reliability ensures that a failure of the control system or device will not result in the loss of the safety-related function.

NOTE - Because some failures cannot be detected until the completion of a cycle or a portion of the cycle, loss of safety related functions may occur for a portion of the machine cycle.Control reliability of electrical, electronic, pneumatic, or hydraulic systems or devices frequently consists of monitored, multiple and independent parallel or series components, modules, devices or systems. Control reliability of machine control systems or devices can be achieved by the use of, but not limited to, one or both of the following:

- The use of two or more dissimilar components, modules, devices or systems, with the proper operation of each being verified (monitored) by the other(s) to ensure the performance of the safety function(s).
- The use of two or more identical components, modules, devices or systems, with the proper operation of each being verified (monitored) by the other(s) to ensure the performance of the safety function(s).

These methods require that the protective device, its interface to the control system (or directly to the actuator control) and actuator control meet the above requirements.

Based on these definitions, it is important to take control reliability into account in the development of safety-related electrical, electronic and pneumatic systems. Control reliable circuits include monitoring at the system level. ANSI/RIA R15.06-1999 (4.5.4) provides a practical guide to implementing “control reliability” by requiring the following components:

a. The monitoring shall generate a stop signal if a failure is detected. A warning shall be provided if a hazard remains after cessation of motion
b. Following detection of a failure, a safe state shall be maintained until the fault is cleared
c. Failures with a common cause (e.g., overvoltage) must be taken into account if the probability is high that such a failure may occur
d. The single failure should be detected at time of failure. If not practical, the failure should be detected at the next demand upon the safety function.

In addition, the canadian standards CSA Z432-04 /434-03 state:
Control reliable safety control systems shall be dual channel with monitoring and shall be designed, constructed, and applied such that any single component failure, including monitoring, shall not prevent the stopping action of the robot.

These safety control systems shall be independent of the normal program control (function) and shall be designed to be not easily defeated or not easily bypassed without detection.

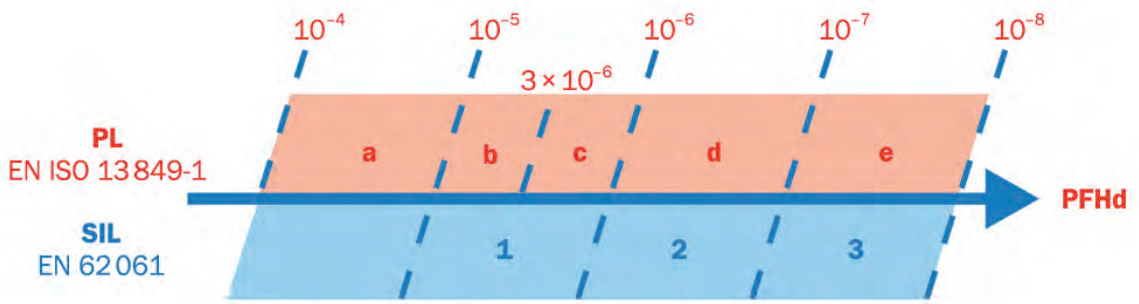
The table below summarizes the expected safety performance and fault tolerance for safety circuits.

OSHA (1910.217) & ANSI B11	ANSI/RIA R15.06	Categories out of ISO13849-1	Interpretation of system performance
N/A	Simple	Category B	Control as per basic specifications.
N/A	Single Channel	Category 1	Use of well-tried and tested components and principles.
N/A	Single Channel with monitoring	Category 2	Safety function shall be tested / checked at suitable intervals. Single fault may cause the loss of the safety function.
Control Reliable	Control Reliable	Category 3	A single fault shall not cause the loss of the safety function. The fault should be detected whenever reasonably practicable. An accumulation of faults may cause the loss of the safety function.
		Category 4	A single fault shall not cause the loss of the safety function. The fault shall be detected at or before the next demand of the safety function. An accumulation of faults shall not cause the loss of the safety function.

Example: Determination of the system performance for a safety function

Safety Function	When the light curtain is interrupted the safety interface module removes power from the hazardous portion of the machine. The hazardous portion of the machine must stop before the user can reach the hazard.
Faults to Consider:	The light curtain and safety interface module (SIM) need to detect internal failures and faults on the wiring. The functional reliability and installation of the contactor that could result in: ■ Stuck armature in one of the contactors, ■ Welded contacts of contactor
Fault Exclusion:	Short circuit from power to the output of the SIM, between the two contactors or any other terminal of the contactor if all the elements are located in the same control panel, wiring meets NFPA 79, shorts validated during commission or other equivalent measures are used.
Safety Principles:	In order to be control reliable monitoring of the contactors is necessary. This monitoring must include a normally closed feedback contact that can accurately reflect the status of the contactor. Typically, the contactor must have a mechanically linked design . This ensures that their normally open contacts used for controlling hazardous motion, has a positive relationship with the normally closed monitoring contacts which can be monitored by the safety interface module. If both contactor elements are put in series to switch off power to hazardous motion, proper overcurrent protection must avoid the common cause failure of both contacts welding at the same time.

The ANSI/CSA method is a deterministic approach, focusing on the structure and the diagnostic capabilities of the safety function. In addition the ISO/IEC methods also check whether the remaining residual risk is acceptable (probabilistic approach). The PFHd figure is determined here as the quantitative parameter for the ISO/IEC methods.



- PL performance level: ability of safety-related parts to perform a safety-related parts to perform a safety function in foreseeable conditions to provide the expected risk reduction
- PFHd: probability of dangerous failure per hour
- SILCL: SIL claim limit (suitability). Discrete level for defining the integrity of the safety function.

3 d

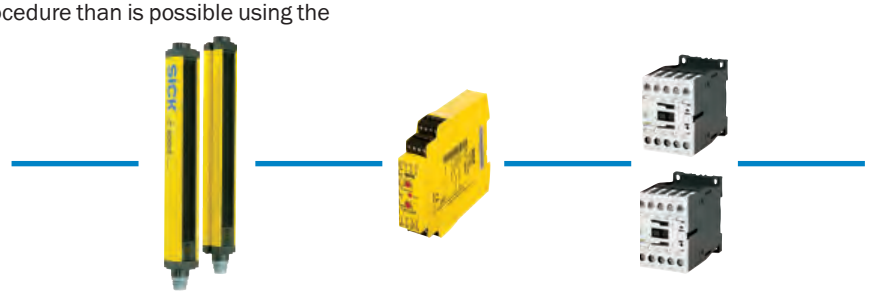
Determining the performance level (PL) achieved as per ISO 13849-1

ISO 13849-1 includes two procedures for determining the performance level:

Simplified procedure
Tabular determination of the performance level based on the performance levels of the sub-systems

Detailed procedure
Calculation of the performance levels based on the PFHd figures for the sub-systems. (This procedure is only described indirectly in the standard.)
More realistic performance levels can often be calculated using the detailed procedure than is possible using the simplified procedure. For both procedures additional structural and systematic aspects for achieving the performance level are to be taken into account.

Sub-systems
A safety function that is realized with the aid of protective measures generally comprises a sensor, logic and actuator. Such a chain can include, on the one hand, discrete elements such as physical guard interlocks or valves and complex safety controllers. As a rule, it is therefore necessary to divide a safety function into sub-systems.



In practice, most often already certified sub-systems are used for certain safety functions. These sub-systems can be, e.g., light curtains, but also safety controllers for which “pre-calculated” PL or PFHd figures are supplied by the manufacturer of the components. These values only apply for a mission time to be stated by the manufacturer. Along with quantifiable aspects, it is also necessary to verify the measures against systematic failures.

→ Further information in relation to the validation: ISO 13849-2
→ You will find a large amount of information on verification using ISO 13849-1 at www.dguv.de/bgia/13849.

Simplified procedure

This procedure makes it possible to estimate the total PL to a sufficiently accurate degree even without knowledge of the individual PFHd figures. If the PL of all sub-systems is known, the total PL achieved for the safety function can be determined with the aid of the table below.

Procedure

- Determine the PL for the sub-system/the sub-systems with the lowest PL in a safety function: **PL (low)**
- Determine the number of sub-systems with this PL (low): **n (low)**

Example 1:

- Three sub-systems achieve PL “e,” the lowest PL (low) is therefore “e.”
- The number of sub-systems with this PL is 3 (so ≤ 3). For this reason the total PL achieved is “e.”
- Adding a further sub-system with the PL “e” would reduce the total PL using this method to “d.”

Example 2:

- One sub-system achieves the PL “d”, two achieve the PL “c”. The lowest PL (low) is therefore “c.”
- The number of sub-systems with this PL is 2 (so ≤ 2). For this reason the total PL achieved is “c.”

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 sub-systems, their PL can be determined as per section “Determining the safety performance for a sub-system as per ISO 13 849-1” further below.

Detailed procedure

An essential, but not exclusive criteria for the determination of the PL is the “probability of dangerous failure per hour (PFHd)” of the safety components. In the detailed procedure, the resulting PFHd value comprises the sum of the individual PFHd values.

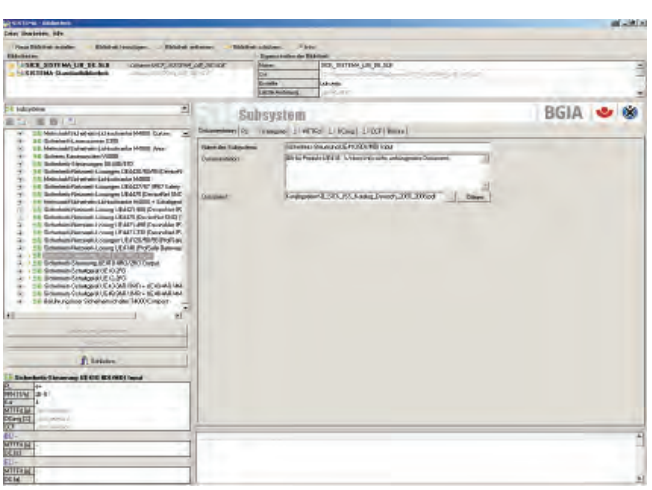
The resulting PFHd value forms the final PL as shown in the illustration on 3-56. (i.e a PFHd value between 10-7 and 10-8 means a PL “e“).
Additional structural restrictions may be taken by the manufacturer of a safety component that shall also be taken into account during the overall assessment.

→ If the PFHd figure is not know for all sub-systems, their safety performance can be determined. See “Determining the safety performance for a sub-system as per ISO 13849-1” further below.

Helpful assistance

The verification methods described required know-how and experience in the usage of performance levels (PL). SICK offers related services (→ “How SICK supports you” on page i-1). A suitable software tool can provide assistance with a systematic procedure.
An effective method for the calculation of the performance level is provided by the SISTEMA software wizard developed by BGIA, a notified body in Germany, and is available free of charge online. SICK offers a library of certified safety components for this application.
In addition, our seminars offer you practical “know-how” for your day-to-day work.

→ You will find information on SISTEMA and all the components data at http://www.sick.com/.



Determining the safety performance for a **sub-system** as per ISO 13849-1

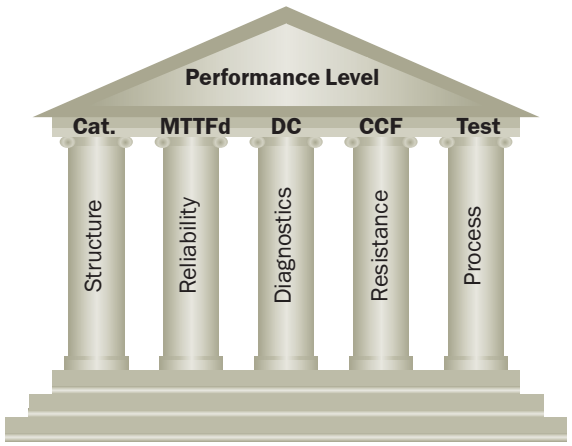
A safety-related sub-system can be formed by numerous individual components, also from different manufacturers. Examples of such components are:

- input side: two safety switches on a physical guard
- output side: a contactor and a frequency inverter for stopping a dangerous movement

In these cases, the PL for this sub-system shall be determined independently.

The performance level achieved for a sub-system comprises the following parameters:

- structure as well as behavior of the safety function under
- fault conditions (category, ➔ 3-58)
- MTTFd figures for individual components (➔ 3-59)
- diagnostic coverage (DC, ➔ 3-60)
- common cause failure (CCF, ➔ 3-60)
- safety-related software aspects
- systematic failures



3 d

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

Sub-systems are generally of single-channel or dual-channel design. Without further measures, single-channel systems react to faults with a dangerous failure. Faults can be detected by using additional testing components or dual-channel systems that mutually test each other. The structure is classified in ISO 13849-1 using categories.

Category	Concise list of the requirements	System behavior	Principles for achieving safety
B	The safety-related parts of controls and/or their protective devices as well as their components shall be designed, built, assembled and combined in compliance with the applicable standards such that they can withstand the effects expected.	■ The occurrence of a failure can result in the loss of the safety function.	Predominantly characterized by the selection of components
1	The requirements of category B shall be met. Proven components and proven safety principles shall be used.	■ The occurrence of a failure can result in the loss of the safety function, but the probability of occurrence is less than in category	
2	The requirements of category B shall be met and proven safety principles used. The machine control shall check the safety function at suitable intervals (test rate 100 times higher than the demand rate).	■ The occurrence of a failure can result in the loss of the safety function between checks. ■ The loss of the safety function is detected by the check.	Predominantly characterized by the structure
3	The requirements of category B shall be met and proven safety principles used. Safety-related parts shall be designed such that... ■ a single failure in each of these parts does not result in the loss of the safety function and ■ whenever feasible within reasonable limits,	■ When the single failure occurs, the safety function is always retained. ■ Some, but not all failures are detected. ■ Accumulation of undetected failures may lead to loss of the safety function.	
4	The requirements of category B shall be met and proven safety principles used. Safety-related parts shall be designed such that: ■ a single failure in each of these parts does not result in the loss of the safety function **and** ■ the single failure is detected at or before the next demand on the protective function **or** ■ if this is not possible, an accumulation of failures will not result in the loss of the safety function.	■ The safety function is always retained when failures occur. ■ The failures are detected in a timely manner to prevent the loss of the safety function.	

Mean time to a dangerous failure (MTTFd)

MTTF is the abbreviation for “mean time to failure.” For the assessment as per ISO 13 849-1 only dangerous failures need to be considered (for this reason “d” for “dangerous”). This value represents a theoretical parameter and expresses the probability of a dangerous failure of a component (not the entire sub-system) during the service life of the component. The actual service life of the sub-system is always shorter.

The MTTF figures can be derived from the failure rates. Failure rates are:

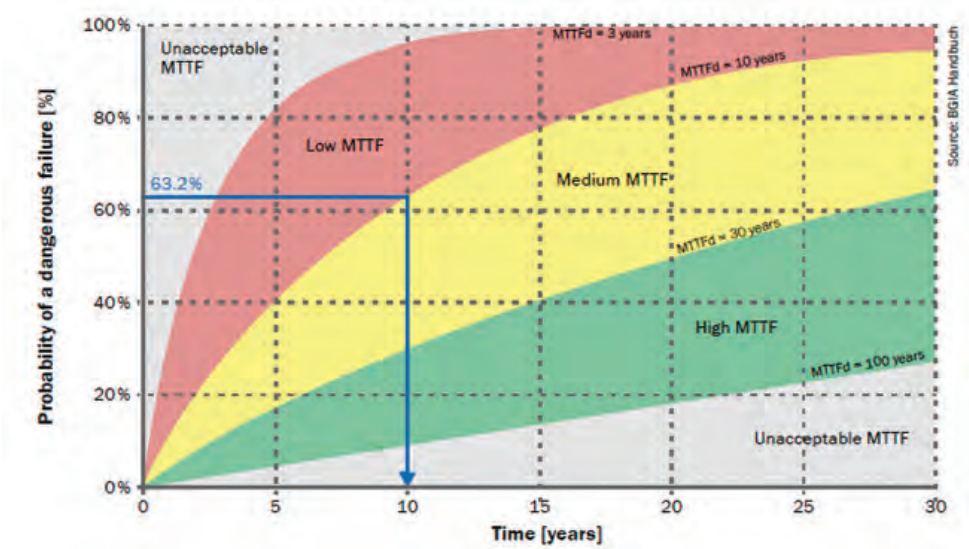
- B10 figures for electromechanical or pneumatic components. Here the service life is dependent on the switching frequency. B10 defines the number of switching cycles at which up to 10 % of the components fail.
- For electronic components: failure rate Lambda figure λ. Often the failure rate is stated in FIT (Failures In Time). One FIT is one failure per 10^9 hours.

ISO 13 849-1 combines the MTTFd figures into ranges:

Designation	Range
Low	3 years ≤ Mean time to a dangerous
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd < 100 years

From the component information, it is possible to calculate the mean time to a dangerous failure in years (MTTFd).

To avoid overvaluing the effect of reliability, the highest useful value for the MTTFd has been limited to 100 years.



3 d

Diagnostic coverage (DC)

The safety performance can be increased if sub-systems are tested internally. The diagnostic coverage (DC) is a measure of the detection of failures. Poor tests only detect a few failures, good tests detect a large number or even all failures.

Instead of detailed analysis (FMEA), ISO 13849-1 proposes measures and quantifies the DC. There is also a sub-division into various ranges here.

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

Common cause failures — resistance

External effects (e.g. voltage level, overtemperature) can render the same components suddenly unusable, irrespective of how infrequently they fail or how well they are tested. (It is not possible to read a newspaper even with two eyes if the light goes out suddenly.) These common cause failures are always to be prevented (CCF — common cause failure).

Here ISO 13 849-1 checks a series of assessments and demands a minimum number of positive implementations.

Requirement		Maximum value
Separation	Separation of signal circuits, separate routing, isolation, air paths, etc.	**15**
Diversity	Different technologies, components, principles of operation, design	**20**
Design, application, experience	Protection against overload, overvoltage, overpressure, etc. (depending on technology)	**15**
	Usage of components and procedures proven over a long period	**5**
Analysis, assessment	Usage of a failure analysis to prevent common cause failures	**5**
Competence/ training	Training of the designers to understand and prevent the causes and consequences of CCF	**5**
Environmental effects	Test the system for susceptibility to EMC	**25**
	Test the system for susceptibility to temperature, shock, vibration, etc.	**10**

Minimum requirement
Total figure ≥ 65

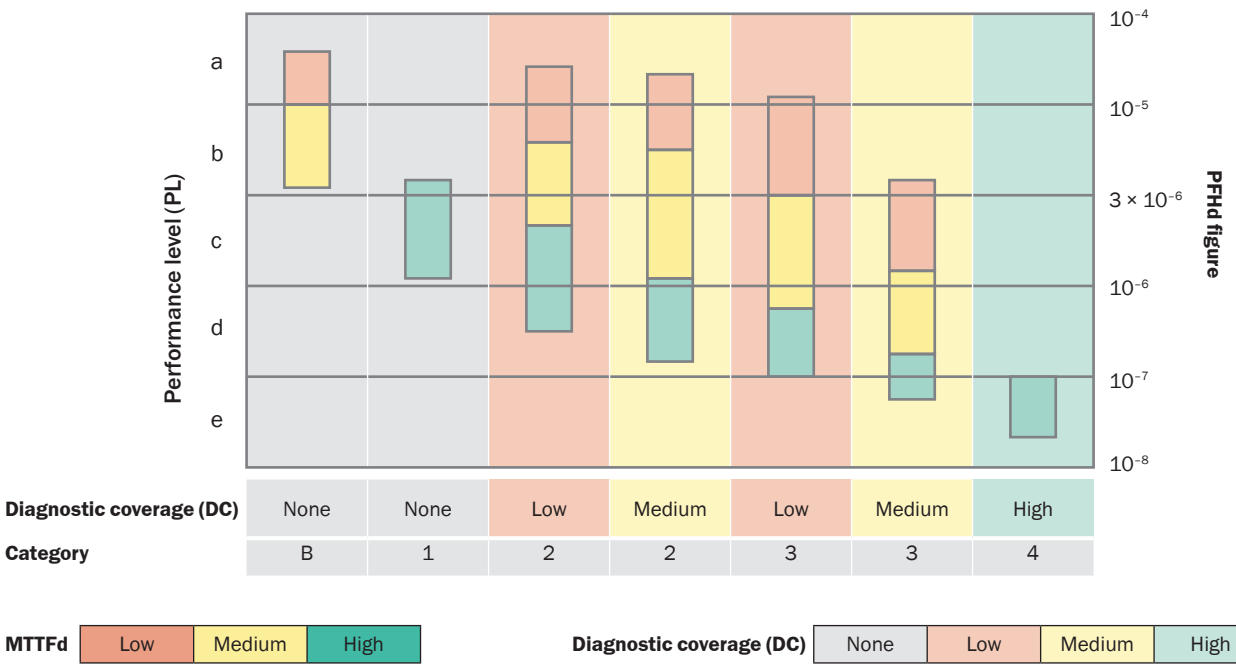
Process

To ensure the aspects above are correctly implemented in the hardware and software, comprehensively checked (principle of counter checking by a second person) and comprehensive documentation provides traceable information on versions and changes, various tools in the standard are to be taken into account.

The process for the correct implementation of safety-related topics is a management task and involves suitable quality management.

Determining the PL of a sub-system

The following illustration shows the relationship between the MTTFd figure (per channel), the DC and the category.



A performance level “d” can, e.g., be realized using a dual-channel control system (category 3). This can be achieved using good quality components (MTTFd = medium) if almost all failures are detected (DC = medium) or it is achieved with very good quality components (MTTFd = high) if a large number of failures are detected (DC = low).

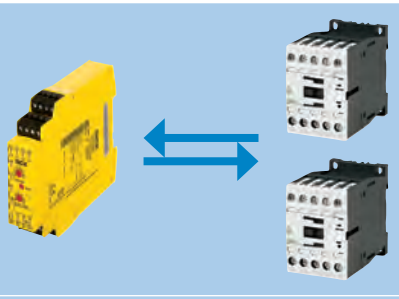
Behind this procedure there is a complex mathematical model of which the user is unaware.
To ensure a pragmatic approach, the parameters category, MTTFd and DC are pre-defined.

3 d

Example: Determination of the PL for the "actuator" sub-system

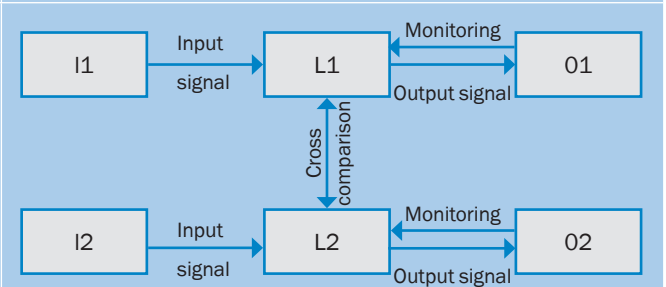
1) Definition of the "actuator" sub-system

The "actuator" sub-system comprises two contactors with "feedback." Due to positive guiding of the contacts on the contactors, it is possible to detect a safety-related failure of the contactors.
The logic unit UE410 is itself not part of the "actuator" sub-system, but it is used for diagnostics purposes.



2) Definition of the category

Single failure safety (with failure detection) results in **suitability for category 3 or 4**.
Note: The final determination of the category is undertaken after the definition of the DC figure.



3) Determination of the MTTFd per channel

As the contacts are subject to wear, it is necessary to determine the MTTFd using the B_{10d} figure and the estimated switching frequency (n_{op}). The formula on the right is available:

$$MTTFd = \frac{B_{10d}}{0.1 \times n_{op}}$$

$$MTTFd = \frac{B_{10d}}{0.1 \times d_{op} \times h_{op} \times C}$$

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]:
Operating data according to manufacturer:

- B_{10d} = 1 300 000
- C = 1/h (assumption)
- d_{op} = 220 d/a
- h_{op} = 16 h/d

Under these conditions the **MTTFd is 3693 years** per channel, which is interpreted as "high."

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

4) Determination of the DC

Due to the positively guided contacts, based on the table of measures in ISO 13 849-1 a **high DC (99 %)** can be derived.

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

3 d

Example: Determination of the PL for the "actuator" sub-system

5) Evaluation of the measures to prevent common cause failures

Measures to prevent common cause failures are implemented in multiple channel systems. The evaluation of the measures produces **75 points**. The minimum requirement is therefore met.

Requirement	Value	Minimum requirement
Separation	15	Total figure 75 ≥ 65
Diversity	20	
Design, application, experience	20	
Analysis, assessment	5	
Competence/training	5	
Environmental effects	35	
	75	

6) Evaluation of the process measures

Systematic aspects for the prevention and control of failures shall also be taken into account. For example:

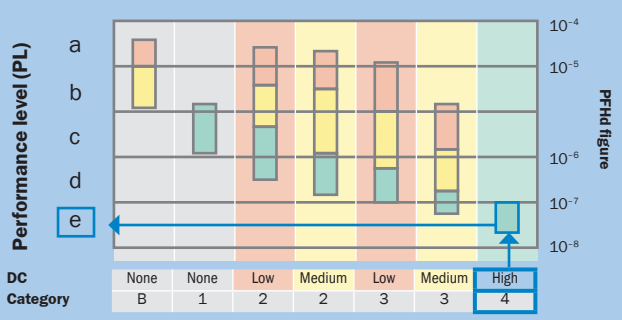
- organization and competence
- rules for design (e.g. specification templates, coding guidelines)
- test concept and test criteria
- documentation and configuration management

✔

7) Result

From the illustration for the determination of the PL for the sub-system (➜ 3-56) the PL for the sub-system can be determined. Due to the high DC, the dual-channel structure meets the requirements for Category 4. The MTTFd is high so in this case the PL "e" is achieved.

The resulting **PFHd figure of 2.47 × 10^{-8}** for this sub-system can be taken from a detailed table in ISO 13849-1.



➜ With the resulting data for the sub-system, it is now possible to determine the performance level of the entire safety function achieved (see "Determining the performance level (PL) achieved as per ISO 13849-1" on page 3-51).

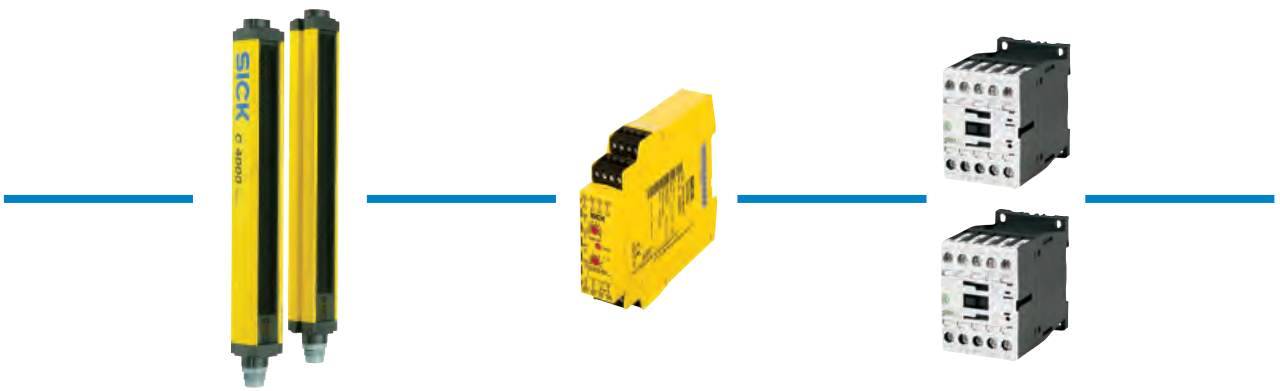
3 d

Alternative: Determination of the safety integrity level (SIL) as per IEC 62061

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

- the safety integrity of the hardware
  - structural limitations (SILCL)
  - probability of random dangerous hardware failures (PFHd)
- the requirements for systematic safety integrity
  - prevention of failures
  - control of systematic failures

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



Safety integrity of the hardware

During the assessment of the overall safety function, the safety integrity of the hardware is determined such that ...

- the lowest SILCL for a sub-system limits the maximum achievable SIL for the overall system.
- the PFHd for the overall control system from the sum of the individual PFHd does not exceed the figures in the illustration on page 3-56.

Example

In the example above, all sub-systems meet SILCL3. The addition of the PFHd figures is less than 1×10^{-7}. The relevant measures for the systematic safety integrity are implemented. For this reason the safety function meets SIL3.

Systematic safety integrity

If different sub-systems are connected together to a control system, additional measures for the systematic safety integrity shall be taken.

The measures for the prevention of systematic hardware failures include

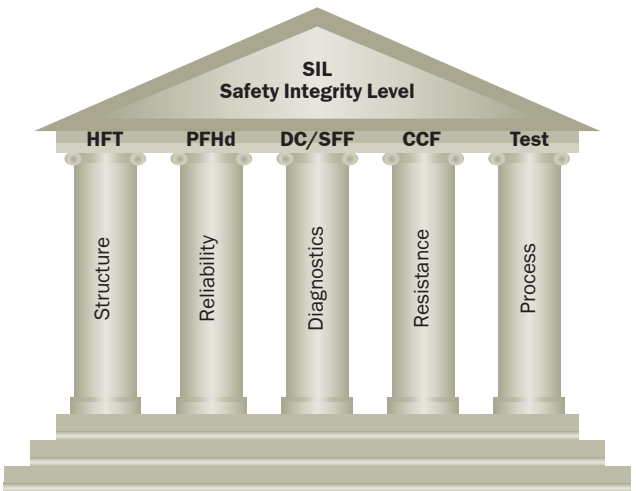
- design in accordance with the plan for functional safety
- correct selection, combination, placement, assembly and installation of sub-systems, including cabling, wiring and other connections
- usage within the manufacturer's specification
- paying attention to the manufacturer's application notes, e.g. catalog information, installation instructions and application of proven design practice
- taking into account the requirements in relation to the electrical equipment as per NFPA 79 / IEC 60204

In addition, to control systematic failures the following shall be taken into account, for example:

- usage of power shutdown to initiate a safe state
- measures for controlling the effects of failures and other effects related to a data communication process, including transmission errors, repetitions, loss, injection, incorrect sequence, corruption, delay etc.

Determining the safety performance for a **sub-system** as per IEC 62 061

The safety performance of sub-systems made of individual components can also be determined in IEC 62 061.

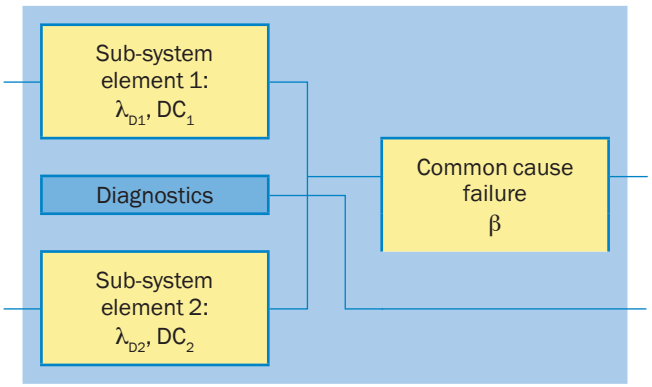


The safety integrity level (SIL) achieved for a sub-system comprises the following parameters:

- hardware fault tolerance (HFT)
- PFHd figure
- safe failure fraction (SFF)
- common cause failure (CCF)
- safety-related software aspects
- systematic failures

Hardware fault tolerance (HFT)

In IEC 62 061 the structure is determined by sub-system types and the 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 with a single failure in the hardware the safety function is retained (dual-channel systems).



Probability of random dangerous hardware failures (PFHd)

Along with the structural limitations, for each sub-system it is also necessary to take into account the "probability of random dangerous hardware failures." Based on a mathematical model, there is a formula for each sub-system type for determining the PFHd figure; the following parameters are used in the calculation:

- diagnostic coverage
- mission time
- diagnostic test interval
- failure rate of the components (λ_D)
- common cause failure (common cause factor β)

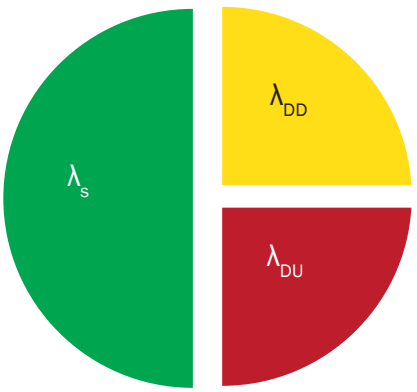
HFT = 1
Diagnostics with DC_1 and DC_2

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

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

Safe failure fraction (DC/SFF)

DC = 50%
SFF = 75%



Safe failure fraction (DC/SFF)

The "safe failure fraction", SFF, is given by the diagnostic coverage DC ($\lambda_{DD}/\lambda_{DU}$) and the fraction of "safe failures" (λ_s).

$$SFF = \frac{\Sigma \lambda_s + \Sigma \lambda_{DD}}{\Sigma \lambda_s + \Sigma \lambda_D}$$

3 d

Common cause failure (CCF) — resistance

IEC 62 061 also requires a series of assessments in relation to the resistance to common cause failures. There is a common cause factor (β) as a function of the number of positive implementations.

Requirement		Maximum value
Separation	Separation of signal circuits, separate routing, isolation, air paths, etc.	**15**
Diversity	Different technologies, components, principles of operation, design	**20**
Design, application, experience	Protection against overload, overvoltage, overpressure, etc. (depending on technology)	**15**
	Usage of components and procedures proven over a long	**5**
Analysis, assessment	Usage of a failure analysis to prevent common cause failures	**5**
Competence/ training	Training of the designers to understand and prevent the causes and consequences of CCF	**5**
Environmental effects	Test the system for susceptibility to EMC	**25**
	Test the system for susceptibility to temperature, shock, vibration, etc.	**10**

Value	CCF factor (β)
< 35	10 %
35 to < 65	5 %
65 to < 85	2 %
≥ 85	1 %

Process

As IEC 62 061 is heavily based on programmable electrical systems it includes — in addition to the aspects described above (V model, quality management, etc.) — also numerous detailed notes and requirements on the correct procedure during the software development of safety-related systems.

Result — determination of the SIL for the sub-system

For each sub-system, first the safety integrity is determined separately for the hardware:

If the sub-systems are already developed sub-systems — as is the case, e.g., for safety light curtains — the manufacturer supplies the related characteristic data as part of the technical specification. Such a sub-system is generally adequately described by information on SILCL, PFHd and mission time.

On the other hand, the safety integrity level shall be determined for sub-systems that comprise sub-system elements, e.g., interlocking devices on guards or contactors.

SIL claim limit (SILCL)

After you have defined the hardware fault tolerance (architecture), the maximum achievable SIL (SIL claim limit) can be determined for the sub-system.

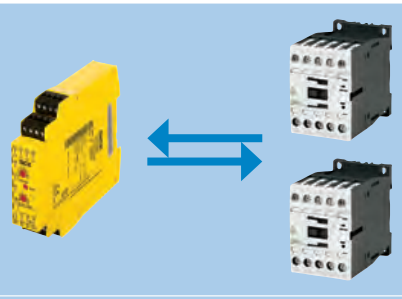
Safe failure fraction (SFF)	Hardware fault tolerance	
	0	1
< 60 %	–	SIL1
60 to < 90 %	SIL1	SIL2
90 to < 99 %	SIL2	SIL3
≥ 99 %	SIL3	SIL3

A dual-channel system with HFT 1 can claim SILCL3 with an SFF of 90%.

Example: Determination of SILCL and PFHd for the "actuator" sub-system

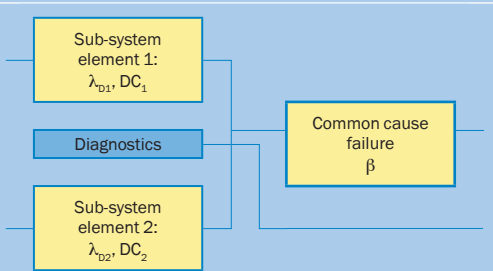
1) Definition of the "actuator" sub-system

The "actuator" sub-system comprises two contactors with "feedback". Due to positive guiding of the contacts on the contactors, it is possible to detect safety-related failure of the contactors.
The logic unit UE410 is itself not part of the "actuator" sub-system, but it is used for diagnostics purposes.



2) Definition of the hardware fault tolerance:

Due to the single failure safety (with failure detection), the hardware fault tolerance is **HFT = 1**.



3) Determination of the PFHd

a) Based on the failure rate λ_D

As the contacts are subject to wear, it is necessary to determine the estimated switching frequency per hour [C] using the B_{10d} figure.
Secondary conditions according to manufacturer:

- B_{10d} = 1 300 000
- C = 1/h (assumption)

These secondary conditions then yield a λ_D **of 7.7 × 10^{-8}** .

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

b) Based on the CCF factor (β)

Measures to prevent common cause failures are necessary in multiple channel systems. The effect is determined based on measures as per the requirements of IEC 62 061. In the example the β factor is 5 % (see below: "5) Evaluation of the measures to prevent common cause failures")
PFHd ≈ 1.9×10^{-9}.

Value	CCF factor (β)
< 35	10 %
35 to < 65	5 %
65 to < 85	2 %
≥ 85	1 %

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

$$\approx \beta \times 0.5 \times \lambda_{Contactor}$$

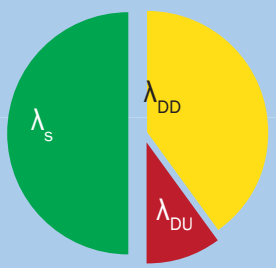
$$\approx 0.05 \times 0.5 \times 0.1 \times \frac{C}{B_{10}}$$

PFHd ≈ 1.9×10^{-9}

4) Determination of the SFF via DC

Due to the positively guided contacts, a "high" DC (99 %) is derived, i.e., of 50 % dangerous failures λ_D, 99 % will be detected. Consequently **SFF = 50 % + 49.5 % = 99.5 %**.

DC = 99%
SFF = 99.5%



5) Evaluation of the measures to prevent common cause failures

Measures to prevent common cause failures are necessary in multiple channel systems. The evaluation of the measures as per IEC 62 061 yields in this example a **CCF-factor (β) of 5 %**.

Value	CCF factor (β)
< 35	10 %
35 to < 65	5 %
65 to < 85	2 %
≥ 85	1 %

3 d

Example: Determination of SILCL and PFHd for the "actuator" sub-system

6) Evaluation of the process measures

Systematic aspects for the prevention and control of failures shall also be taken into account. For example:

- organization and competence
- rules for design (e.g., specification templates, coding guidelines)
- test concept and test criteria
- documentation and configuration management

✔

Result

In the last step the structural limitations are to be taken into account. Due to the existing redundancy (hardware fault tolerance 1) and the SFF > 99 % for this sub-system the **SIL claim limit 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 $\approx 1.9 \times 10^{-9}$

→ With the resulting SILCL data and the PFHd figure for the sub-system, the SIL achieved for the entire safety function can be determined as described above (see "Safety integrity of the hardware" on page 3-59).

3 d

Summary: Verifying the safety function

Basics

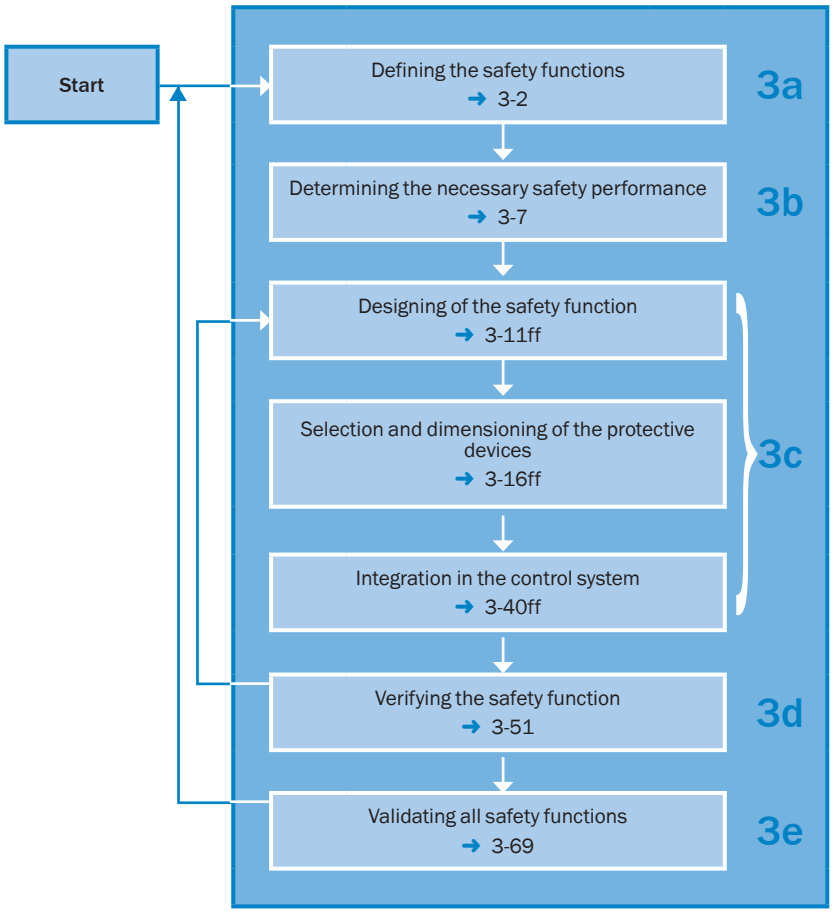
- Verify whether the planned safety functions meet the necessary safety performance. For this purpose verify the mechanical and functional safety.

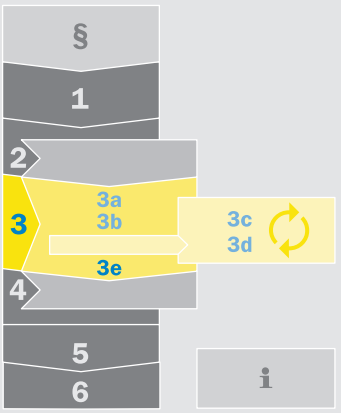
Methods

- Determine the resulting system performance according to the North American standards.
- Determine the resulting level of safety as per ISO 13 849-1 (PL).
  - The simplified procedure (based on the PL)
  - and the detailed procedure (based on the PFHd figures) are available.
- If no PL and no PFHd figure are known for a sub-system (e.g. for the actuator), determine the performance level of the sub-system from the parameters structure, reliability, diagnostics, resistance and process.
- Alternatively, determine the resulting safety performance as per IEC 62 061 (SIL). Here it is also possible to determine the SIL of an un-certified sub-system yourself.

Step 3e: Validating all safety functions

Validation is the thorough checking of a thesis, a plan or a solution in relation to a problem to be solved. Unlike verification — during which only the correct implementation of a solution as per the specification is evaluated — validation is the final evaluation as to whether the solutions are generally suitable for the necessary risk reduction.





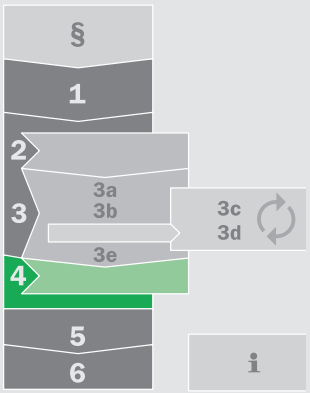
3 e

The purpose of the validation process is to check the specification and the conformity of the design of the components on the machine involved in the safety function.
The validation shall show that safety-related parts of the control function meet the requirements of appropriate safety standards, in particular the requirements for the defined safety performance.
The validation should, if sensible, be performed by people who were not involved in the design of the safety-related parts of the control systems. In Canada, this is part of the Pre Start and Health and Safety Review (PSR).
During the validation process it is important to check for mistakes and particularly for omissions in the safety design.
The critical part of the design of a safety-related control function is generally the specification.
An example on this issue: access to a manufacturing cell is to be protected using a light curtain. The safety function is therefore specified as follows:

"On the interruption of the protective field from a light curtain all dangerous movements shall be stopped as quickly as possible."
In addition, the designer should have also taken into account the restart when the protective field becomes clear again, particularly if it is possible to stand behind the protective field. The validation process shall uncover such defects.
During a validation process, in general several procedures are used that supplement each other.
These procedures include:

- thorough technical check on the positioning and effectiveness of the protective device
- practical check on the reaction to failures in relation to the expected results using simulations
- validation of the ambient requirements using function tests:
  - adequate protection against environment-related aspects such as temperature, humidity, shock, vibration behaviour, etc.
  - adequate immunity to electromagnetic effects

Step 4: Administrative measures



In general, there is an industry agreement that a risk reduction strategy should utilize a hierarchical approach. The most effective solution is safe design followed by engineering controls. The least effective way to minimize the risk are administrative measures.

Administrative measures are acceptable only when guards or safeguarding devices (that prevent you 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:
First:

- Awareness means (like signs, lights, horns, beebers, restriced space painted on floor) and then,
- Training and procedures (like safe work procedures, Lock-Out/ Tag-Out procedures, training of personnel), followed by the least effective solution
- Personal protective equipment (like safety glasses, gloves, ear plugs)

➜ Hierarchical approach for risk reduction: ANSI RIA 15.06 / CSA Z434

4

Step 5: Overall validation

As the functional safety is only part of the risk reduction, it is necessary to evaluate all measures — that is design, technical and organizational — together in an overall validation.

It is therefore possible in practice that, although risk reduction is not achieved with a single technical measure, an adequate result can be achieved in the overall assessment.

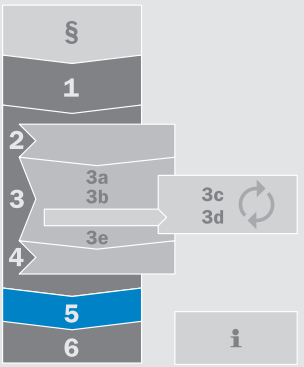
Adequate risk reduction can be considered achieved if all the following questions can be answered in the affirmative:

- Have all operating conditions in all phases of the life of the machine been taken into consideration?
- Has the 3-step method been applied?
- Have the hazards been eliminated or the risks associated with the hazards reduced as far practically feasible?
- Is it ensured the measures implemented will not result in new hazards?
- Have the users been sufficiently informed and warned about the residual risks?
- Is it ensured the operators' working conditions are not impaired by the protective measures taken?
- Are the protective measures implemented compatible?
- Have the consequences that could result from the usage of the machine in the non-commercial/non-industrial sector been adequately taken into account?
- Is it ensured the measures implemented do not excessively impair the correct function of the machine?
- Has the risk been appropriately reduced?

Special requirements for Canada: PSR Legislation, Section 7 of the Occupational Health and Safety Act.

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

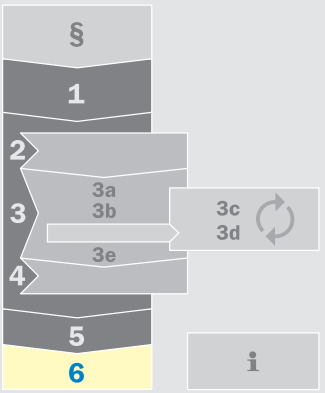
This report is called a Pre-Start Health and Safety Review (PSR). Users must complete or implement the recommendations in the review so that equipment is compliant to the current applicable standards before it is used.



Responsibility of the operating organization

The employer is responsible for the safety of the employees. Machines shall be operated ergonomically and to suit the qualifications of the operator; they shall also be safe at the same time.

Along with safety acceptances and inspections during delivery, the correct specification of the safety-related requirements is to be taken into account as early as procurement.



How should machinery be procured?

A successful project to set up or modernize a production facility starts with the procurement process. Here decisions are made for the different options.

- Clarify in advance the scope of supplier safeguarding implementation provided.
- Define contractually which additional documentation is to be supplied (e.g., risk assessment, ...).
- Define, as far as possible, which consensus standards apply, and how they will be implemented.

Safety inspections

Experience shows that machine safety is only limited in practice. Often protective devices are tampered with to be able to work without hindrance. Other sources of mistakes are the incorrect positioning of protective devices as well as incorrect integration in the control system.

During the operation and maintenance of the machine, the user 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 supplier information for operation and maintenance.

The user shall 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 information for operation and maintenance.

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

See ANSI B11 - GSR 2008 for additional information.

How SICK supports you

SICK makes a contribution to the further development of the safety culture in your organization with the objective ...

- of improving the safety on existing machinery and systems.
- of integral safety during the procurement of new machinery and systems.

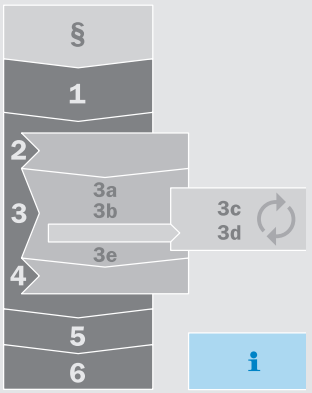
Place high requirements on your partners. Your partner shall:

- have many years of experience
- provide innovative ideas
- be international

By involving SICK experts at an early phase ...

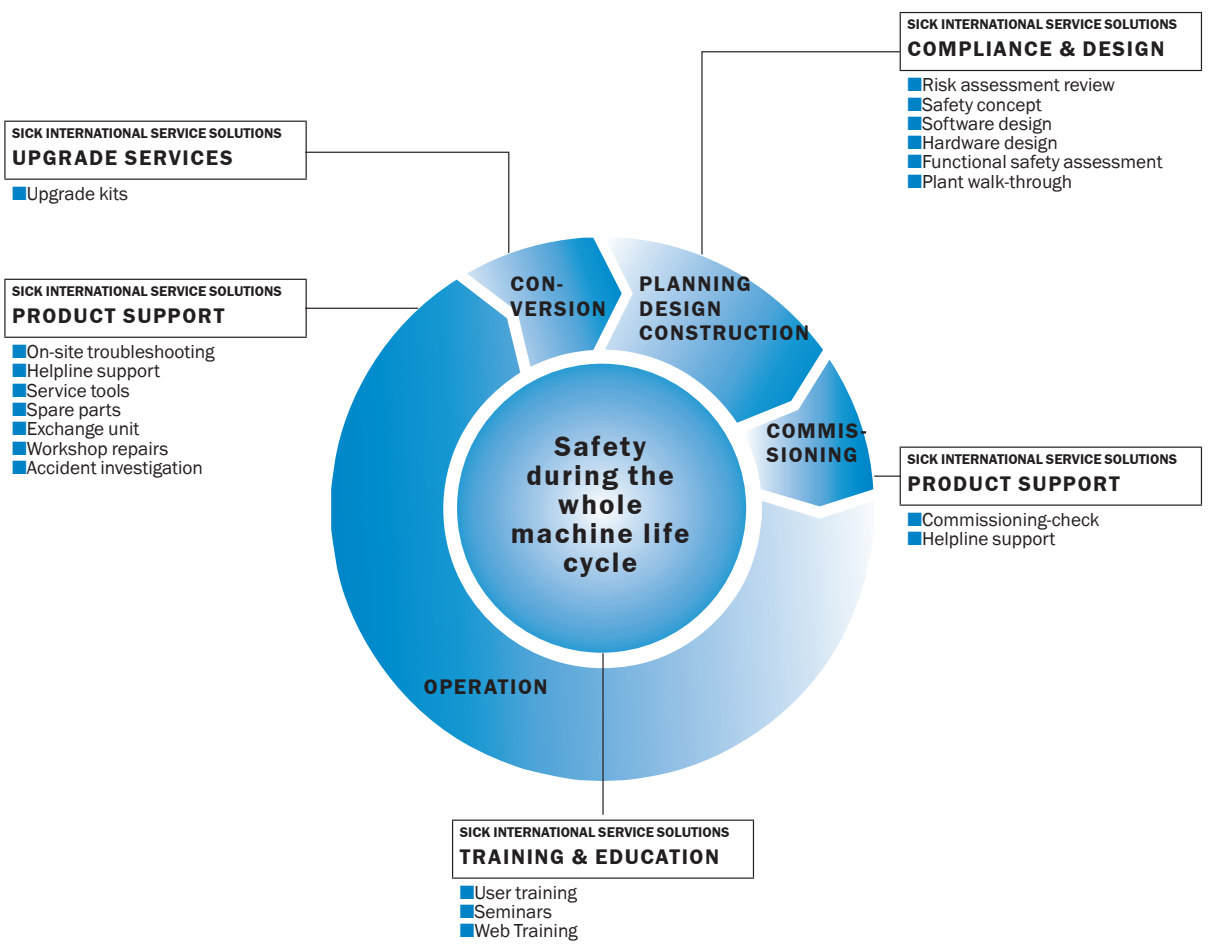
- safety is planned as an integral part of a project.
- potential weak spots are identified at an early stage.
- over-dimensioning is prevented.
- effectiveness and competitiveness are ensured.

SICK provides more safety and added business value.



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

With certified safety products and individual services tailored to cycle your tasks, SICK supports you over the entire life cycle of your machine. From planning through commissioning to maintenance and modernization.



Seminars and user training

User knowledge from practice for practice

The more experience you have, as a rule, the more safely you can tackle an application. To convey experience and as a result optimize applications is an important element of SICK seminars and training courses.

Step ahead with knowledge

Over time, laws and standards change. In addition, changes in technology, starting from the traditional hard-wired technology with relays up to programmable safety modules and even entire networks with bus systems, make it necessary to adapt to these innovations. In our series of seminars on safety principles, we convey the latest knowledge about the following topics:

- selection of suitable protective device as per the standards
- integration of the protective device in the overall control system
- correct assessment of the protective measures based on the applicable standards and regulations

Improving application safety

Our user training is orientated so the safeguarding products can be integrated efficiently and reliably into the planned application. You will receive the information you need on how to use the device and diagnostics features.

The general structure of a user training covers the different phases that arise during the selection and integration of a product:

- selection
  - safety aspects
  - product characteristics and possible applications
- integration
  - integration in the application (mounting) and wiring
  - programming
  - commissioning
- safe operation
  - fault diagnosis and rectification

➜ For Product Training & Support, including courses and schedules, please contact your SICK representative or visit us at http://www.sickusa.com.

On request we will also hold seminars and user training in your premises.

Components (products)

The usage of certified products makes it easier for the machine manufacturer to demonstrate conformity with the requirements of various standards. As a provider of solutions, SICK offers the machine manufacturer a wide range of products from the simple single-beam photoelectric safety switch through safety light curtains, safety laser scanners, camera-based safety sensors and safety switches to modular safety controllers with network support and software solutions for the conformity of machinery.

Advice: Our knowledge — your advantage

SICK has subsidiaries or representatives in all of the major industrialized countries. You will receive expert advice from our technically skilled employees. They will support you not only with product-related knowledge, but also with their knowledge of the market, national laws and standards.

➜ Product selection on page 3-47
➜ You will find all products online in the product finder at www.sickusa.com.
➜ To find out more about the services offered in your country, please contact the SICK representative in your country or visit us at www.sickusa.com.

Summary of important consensus standards and technical reports related to machinery safeguarding in the United States

American National Standards Institute (ANSI)	
ANSI B11.2008	General safety requirements common to ANSI B11 Machines
ANSI B11.1	Mechanical Power Presses — Safety Requirements for Construction, Care and Use
ANSI B11.2	Hydraulic Power Presses — Safety Requirements for Construction, Care and Use
ANSI B11.3	Power Press Brakes — Safety Requirements for Construction, Care and Use
ANSI B11.4	Machine Tools — Shears — Safety Requirements for Construction, Care and Use
ANSI B11.5	Machine Tools — Iron Workers — Safety Requirements for Construction, Care and Use
ANSI B11.6	Lathes — Safety Requirements for Construction, Care and Use
ANSI B11.7	Cold Headers and Cold Formers — Safety Requirements for Construction, Care and Use
ANSI B11.8	Drilling, Milling and Boring Machines — Safety Requirements for Construction, Care and Use
ANSI B11.9	Grinding Machines — Safety Requirements for Construction, Care and Use
ANSI B11.10	Metal Sawing Machines — Safety Requirements for Construction, Care and Use
ANSI B11.11	Gear-Cutting Machines — Safety Requirements for Construction, Care and Use
ANSI B11.12	Machine Tools — Roll-Forming and Roll-Bending Machines — Safety Requirements for Construction, Care and Use
ANSI B11.13	Machine Tools — Single- and Multiple-Spindle Automatic Bar and Chucking Machines — Safety Requirements for Construction, Care and Use
ANSI B11.14	Machine Tools — Coil-Slitting Machines — Safety Requirements for Construction, Care and Use
ANSI B11.15	Pipe, Tube and Shape-Bending Machines — Safety Requirements for Construction, Care and Use
ANSI B11.16	Metal Powder Compacting Presses — Safety Requirements for Construction, Care and Use
ANSI B11.17	Machine Tools — Horizontal Hydraulic Extrusion Presses — Safety Requirements for the Construction, Care and Use
ANSI B11.18	Machine Tools — Machines and Machinery Systems for Processing Strip, Sheet or Plate from Coiled Configuration — Requirements for Construction, Care and Use
ANSI B11.19	Performance Criteria for the Design, Construction, Care and Operation of Safeguarding When Referenced by Other B11 Machine Tool Safety Standards.
ANSI B11.20	Machine Tools — Manufacturing Systems / Cells — Safety Requirements for Construction, Care and Use
ANSI B11.21	Machine Tools using Lasers for Processing Materials — Safety Requirements for Construction, Care and Use
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 TR.1	Ergonomic Guidelines for the Design, Installation and Use of Machine Tools
ANSI B11 TR.3	Risk Assessment
ANSI B11 TR.4	Selection of Programmable Electronic Systems (PES/PLC) for Machine Tools
ANSI B11 TR.6	Safety Control Systems for Machine Tools
ANSI B15.1	Safety Standards for Mechanical Power Transmission Apparatus
ANSI B56.5	Safety Standard for Guided Industrial Vehicles and Automated Functions of Manned Industrial Vehicles
ANSI B65.1	Safety Standards for Printing Press Systems
ANSI B151.1	American National Standard for Plastics Machinery & Horizontal Injection Molding Machines & Safety Requirements for Manufacture, Care, and Use
ANSI B151.27	Safety Requirements for Robots Used with Horizontal Injection Molding Machines
ANSI B155.1	Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery
ANSI RIA R15.06	Safety Requirements for Robots and Robot Systems

National Fire Protection Agency (NFPA)	
NFPA 70E	Electrical Safety Requirements for Employee Workplaces
NFPA 79	Electrical Standard for Industrial Machinery
Underwriters Labs (UL)	
UL508	Industrial Control Equipment

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

CAN/CSA Z142	Code for Punch Press and Brake Press Operation: Health, Safety and Guarding Requirements
CSA Z432	Safeguarding of Machinery
CAN/CSA Z434	Industrial Robot and Robot Systems – General Safety
CSA W117.2	Safety in Welding, Cutting and Allied Processes
CSA Z 460	Control of Hazardous energy / Lock-Out and other methods

Mexican safety standards

NOM-004-STPS	Protection Systems And Safety Devices For Machinery And Equipment Used In The Workplaces
NOM-017-STPS	Personal protective equipment – Selection, use and handling in the work place.
NOM-029-STPS	Maintenance of electrical installations in the workplace - safety conditions
NOM-030-STPS	Preventive Services of Occupational Health and Safety – Organization and operations.

International safety standards

International standard ISO/IEC	Title
ISO 12 100-1 ISO 12 100-2	Safety of machinery — basic concepts, general principles for design
ISO 14 121	Risk assessment
ISO 13 854	Safety of machinery — minimum gaps to avoid crushing of parts of the human body
ISO 13 851	Safety of machinery. Two-hand control devices — functional aspects; Principles for design
ISO 14 120	Safety of machinery. Guards. General requirements
ISO 14 118	Safety of machinery. Prevention of unexpected start-up
ISO 14 119	Safety of machinery. Interlocking devices associated with guards. Principles for design and selection
ISO 13 849-1 ISO 13 849-2	Safety-related parts of control systems ■ Part 1: General principles for design ■ Part 2: Validation
ISO 13 850	Safety of machinery. Emergency stop. Principles for design
ISO 13 855	The positioning of protective equipment with respect to the approach speeds of parts of the human body
ISO 13 857	Safety of machinery — safety distances to prevent hazard zones being reached by the upper and lower limbs
ISO 11161	Safety requirements — integrated manufacturing systems
IEC 60 204-1	Electrical equipment of machines ■ Part 1: General requirements
IEC 61 496-1 IEC 61 496-2 IEC 61 496-3	Safety of machines — electro-sensitive protective equipment (ESPE) ■ Part 1: General requirements and tests ■ Part 2: Particular requirements for equipment using active opto-electronic protective devices ■ Part 3: Particular requirements for Active Opto-electronic Protective Devices responsive to Diffuse Reflection (AOPDDR)
IEC 61 508	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC/TS 62 046	Safety of machinery — Application of protective equipment to detect the presence of persons
IEC 62 061	Functional safety of safety related electrical, electronic and programmable electronic control systems
IEC 61800-5-2	Safety requirements — power drive systems

Useful links

Where do I find ...?			
Information about laws and standards	**United States** US - Osha: ➜ http://www.osha.gov/index.html US - National Fire Protection Association: ➜ http://www.nfpa.org	**Canada** Standards Council Canada: ➜ http://www.scc.ca/en/index.shtml Canada ➜ http://www.ccohs.ca/oshanswers/information/govt.html ➜ http://www.csa.ca Ontario Pre Start Health and Safety reviews ➜ http://www.labour.gov.on.ca/english/hs/guidelines/prestart/index.html Electrical approvals ➜ http://www.labour.gov.on.ca/english/hs/guidelines/liveperformance/gl_live_apx_a.html ➜ http://www.labour.gov.on.ca/ ➜ http://www.iapa.ca	**Mexico** Information about Mexican regulations ➜ http://www.mexicanlaws.com/ ➜ http://www.stps.gob.mx/ENGLISH/index.htm
Order standards	➜ http://web.ansi.org ➜ http://www.global.ihs.com ➜ http://www.nssn.com		
Publishers of standards, international	ISO: ➜ http://www.iso.org/iso/home.htm IEC: ➜ http://www.iec.ch/ For European standards (EN): CEN: ➜ http://www.cen.eu/cenorm/homepage.htm CENELEC: ➜ http://www.cenelec.org/cenelec/Homepage.htm		
Machine related	Manufacturing Technology (B11 Series) ➜ http://www.amtonline.org/ Robotics ➜ http://www.robotics.org/ Packaging ➜ http://www.pmmi.org/		

Glossary

Abbreviation/term		Explanation
λ	**Failure rate per hour**	λ: Failure rate per hour, sum of λ_S and λ_D ■ λ_S: Rate of safe failures ■ λ_D: Rate of dangerous failures, can be divided into: ▪ λ_{DD}: Rate of dangerous failures that are detected by the diagnostic functions ▪ λ_{DU}: Rate of undetected dangerous failures
β factor		Text from IEC 62 061: Is the susceptibility to common cause failures ➜ CCF
A		
AOPD	**Active opto-electronic protective device**	Text from IEC 61 496-2: A device whose sensing function is performed by opto-electronic emitting and receiving elements detecting the interruption of optical radiations generated, within the device, by an opaque object present in the specified detection zone.
AOPDDR	**Active opto-electronic protective device responsive to diffuse reflection**	Text from IEC 61 496-3: Device with a sensor function produced by opto-electronic sender and receiver elements, that detects the diffuse reflection of light, generated by the device, by an object in a defined two-dimensional protective field.
B		
B_{10d}		Number of cycles after which a dangerous failure has occurred on 10 % of the components (for pneumatic and electromechanical components)
C		
Category		Categorization of the safety-related parts of a control system in relation to their resistance to failures and their subsequent behavior in the event of a failure
CCF	**Common cause failure**	Common cause failure: failure of various units due to a single event where these failures are not caused by each other
D		
DC	**Diagnostic coverage**	Diagnostic coverage: measure of the effectiveness of the diagnostics that can be determined as the ratio of the failure rate for the detected dangerous failures to the failure rate for the total dangerous failures
d_{op}		Mean operating time in days per year
E		
EDM	**External device monitoring**	Text from IEC 61 496-1: Means by which the electro-sensitive protective equipment (ESPE) monitors the state of control devices which are external to the ESPE
E/E/PES	**Electrical, electronic & programmable electronic safety-related systems**	Text from IEC 62 061: Electrical, electronic & programmable electronic safety-related systems
EMC	**Electromagnetic compatibility**	Ability of an item of 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
ESPE	**Electro-sensitive protective equipment**	Text from IEC 61 946-1: Assembly of devices and/or components working together for protective tripping or presence-sensing purposes and comprising as a minimum: ■ A sensing device ■ Controlling/monitoring devices ■ Output signal switching devices (OSSD)
F		
FIT	**Failure in time**	Failure rate in 10^{-9} hours. ➜ $\lambda = 1 \times 10^{-9}$ 1/h
FMEA	**Failure mode effects analysis**	Failure mode and effects analysis. Procedure for the analysis of effects (IEC 60 812)
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, on the safety-related systems in other technologies and on the external features for risk reduction
H		
HFT[n]	**Hardware fault tolerance**	Text from IEC 62 061: Ability to continue to perform a required function in the presence of faults or failures
h_{op}	**Operating hours**	Mean operating time in hours per day

Abbreviation/term		Explanation
I		
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.
L		
Lambda figure λ		→ λ
Light curtain		An AOPD with a resolution ≤ 116 mm (A resolution ≤ 40 mm is suitable for finger and hand protection)
LVL	**Limited variability language**	Programming language with limited scope. Type of language that makes it possible to combine pre-defined, user-specific and library functions to implement the specifications for the safety requirements
M		
MTTFd	**Mean time to failure**	Text from ISO 13849-1: Expectation of the mean time to dangerous failure
Muting		Text from IEC 61496-1: Muting. Temporary automatic suspension of one ore more safety function by safety-related parts of the control system
N		
NC	**Normally closed**	Normally closed contact
NO	**Normally open**	Normally open contact
n_{op}	**Numbers of operation per year**	Text from ISO 13849-1: The mean number of annual operations $n_{op} = \frac{d_{op} \times h_{op} \times 3600 \frac{s}{h}}{t_{cycle}}$
O		
OSSD	**Output signal switching device**	The part of the item of 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 correct operation.
P		
PFHd	**Probability of dangerous failure per hour**	Mean probability of a dangerous failure per hour (1/h)
PL	**Performance level**	Text from ISO 13849-1: Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions
Protective field		The area in which the test object specified by the manufacturer is detected by the item of electro-sensitive protective equipment (ESPE)
R		
Resolution/sensor detection capability		The limit for the sensor parameter that causes the item of electro-sensitive protective equipment (ESPE) to trigger. It is defined by the manufacturer.
Response time of an ESPE		The maximum time between the occurrence of the event that caused the triggering of the sensor and the achievement of the off state at the output switching elements (OSSDs).
Restart interlock		Text from IEC 61496-1: Means of preventing automatic restarting of a machine after actuation of the sensing device during a hazardous part of the machine operating cycle, after a change in mode of operation of the machine, and after a change in the means of start control of the machine
S		
SFF	**Safe failure fraction**	Text from IEC 62061: Fraction of the overall failure rate of a subsystem that does not result in a dangerous failure
SIL	**Safety integrity level**	Safety integrity level. Text from IEC 62061: Discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest.
SILCL	**SIL claim limit**	Text from IEC 62061: SIL claim limit (for a subsystem): Maximum SIL that can be claimed for a SRECS subsystem in relation to architectural constraints and systematic safety integrity
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 parts of control system**	Safety-related part of a control system. Text from ISO 13849-1: Part of a control system that responds to safety-related input signals and generates safety-related output signals

Abbreviation/term	Explanation
T	
T_{10d}	Limit for the operating time of a component. Mean time until a dangerous failure has occurred on 10 % of the components. $T_{10d} = \frac{B_{10d}}{n_{op}}$ The MTTFd determined for components subject to wear only applies for this time.
Test rod	Text from IEC 61 496-2: An opaque cylindrical element used to verify the detection capability of the active opto-electronic protective device (AOPD)

Space for your notes

Space for your notes

RANGE OF EXPERTISE

FACTORY AUTOMATION

With its intelligent sensors, safety systems, and auto identification solutions, SICK offers comprehensive solutions for factory automation.

- Non-contact detecting, counting, classifying, and positioning of any type of object
- Accident protection and personal safety using sensors, as well as safety software and services

LOGISTICS AUTOMATION

Solutions from SICK automate material flows and optimize sorting and warehousing processes.

- Automated identification with bar code reading devices for the purpose of sorting and target control in industrial material flow
- Detecting volume, position, and contours of objects and surroundings with laser measurement systems

PROCESS AUTOMATION

Analyzers and process instrumentation from SICK provide the best possible acquisition of environmental and process data.

- Complete system solutions for gas analysis, dust measurement, flow rate measurement, water analysis, liquid analysis, and level measurement as well as other tasks

Worldwide presence with subsidiaries in the following countries:

Australia
Austria
Belgium/Luxembourg
Brazil
China
Czech Republic
Denmark
Finland
France
Germany
Great Britain
India
Italy
Japan
Netherlands
Norway
Poland
Republic of Korea
Republic of Slovenia
Russia
Singapore
Spain
Sweden
Switzerland
Taiwan
Turkey
USA/Canada/Mexico

Please find the detailed addresses and more representatives and agencies in all major industrial nations at **www.sick.com**

7028282.0905 • Subject to change without notice

SICK, Inc. | Minneapolis, MN | USA | phone 800.325.7425 | www.sickusa.com

SICK
Sensor Intelligence.