SIEMENS

Introduction 1

Regulations and standards 2

Terms 3

Attachment 4

Safety Integrated

Introduction and Terminology for Functional Safety of Machines and Systems

Reference Manual

09/2020
E86060-T1813-A101-A6-7600

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

E86060-T1813-A101-A6-7600
Ⓟ 09/2020 Subject to change

Table of contents

1 Introduction 5

1.1 Important notes 5

1.2 General information regarding the Standards 6

1.3 An explanation of how to use this manual 7

2 Regulations and standards 9

2.1 General Information 9

2.2 Regulations and standards in the European Union (EU) 11
2.2.1 Basic principles of the legal requirements in Europe 11
2.2.2 Health and safety at the workplace in the EU 12
2.2.3 Safety of machinery in Europe 12
2.2.4 Functional safety - electrical safety 18
2.2.5 Selecting the devices and basics of the required properties 25

2.3 Structure of the safety function and determining the safety integrity 28
2.3.1 Methodology according to EN 62061 29
2.3.2 Methodology according to EN ISO 13849-1 30
2.3.3 Validation based on the safety plan 31

2.4 Legal requirements and standards regarding safety at work in North America 33
2.4.1 US - general information 33
2.4.2 Machine safety 34
2.4.3 Process industry in the US 38
2.4.4 Occupational safety and health regulations and safety standards in Canada 39

2.5 Safety requirements for machines in Japan 41

2.6 Important addresses 42
2.6.1 Europe 42
2.6.2 America 48

3 Terms 49

4 Attachment 73

4.1 Important type A, B and C standards 73

4.2 Other important documents 75

4.3 Risk assessment according to ISO 12100 76

4.4 Determining the Performance Level 78

4.5 SIL assignment 80

4.6 Drive controls with integrated safety functions 82

4.7 Evaluation of safety functions using the Safety Evaluation in the TIA Selection Tool 84

4.8 Dictionary English - German 89

4.9 Evaluation/feedback 96

Introduction 1

1.1 Important notes

The information in this document is not binding and does not claim to be complete regarding the configuration, equipping and any eventuality. Further, this information does not represent specific customer solutions - but is only intended to provide support when it comes to typical applications. You are responsible in ensuring that the described products are correctly used. This information does not relieve you of your responsibility regarding the safe handling when using, installing, operating and maintaining the equipment. By using this information you agree that Siemens cannot be made liable for possible damage beyond the above mentioned liability clause. We reserve the right to make changes and revisions to this information without prior announcement. When differences occur between the recommendations in this information and other Siemens publications - e.g. catalogs - then the contents of the other documentation have priority.

Date generated: 07/2017

1.2 General information regarding the Standards

pr	project, indicates the draft status of a Standard
EN	European Standard (this applies to all European countries)
DIN EN	Deutsches Institut für Normung (German Institute for Standardization) - the appropriate EN is translated into German; this is also the case for all European countries
ISO	International Organization for Standardization - mainly addresses Standards for electro-mechanical systems
IEC	International Engineering Consortium, electronic/electrical systems, mainly addresses Standards for electronic systems (but also for e.g. contactors)
DIN VDE	National Edition of an IEC
AK (WG)	Working Group in Germany

Example:

prEN ISO 13849-1

This is a draft standard prEN ISO 13849-1, which ISO recommends and advises in the national committees. After it has been passed, it then becomes standard EN ISO 13849-1.

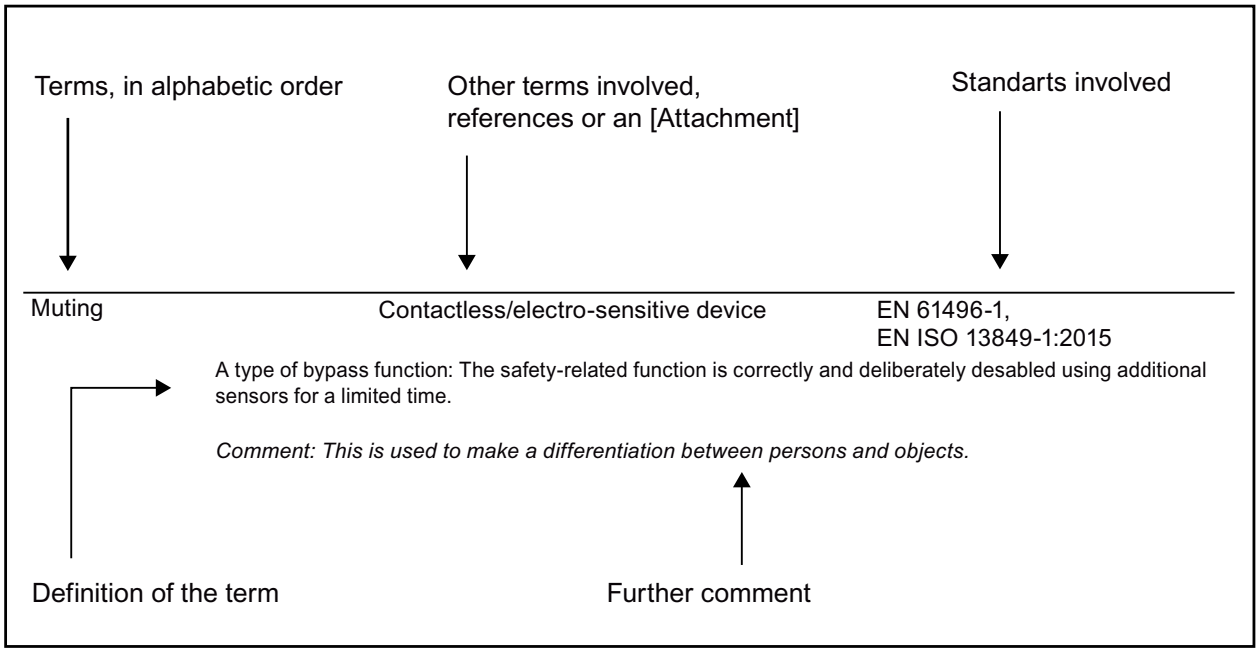
The international edition of a standard is defined using ISO or IEC. If this standard in Europe is applicable under the machinery directive, then this is designated as EN ISO or EN.

Example:

International	**European**
ISO 13849-1	EN ISO 13849-1
IEC 62061	EN 62061

1.3 An explanation of how to use this manual

The third section provides information about the terminology in alphabetical order:



The following appendices are attached in the chapter Attachment (Page 73):

- Appendix 1: Important type A, B and C standards
- Appendix 2: Other important documents
- Appendix 3: Risk assessment according to EN ISO 12100
- Appendix 4: Determining the Performance Level
- Appendix 5: SIL assignment
- Appendix 6: Drive controls with integrated safety functions
- Appendix 7: Evaluation of safety functions using the Safety Evaluation in the TIA Selection Tool
- Appendix 8: English-German dictionary

Regulations and standards 2

2.1 General Information

Objectives of safety systems

The objective of safety systems is to keep potential hazards for both people and the environment as low as possible by using suitable technical equipment, without restricting more than absolutely necessary, industrial production, the use of machines or the production of chemical products. The protection of man and environment has to be put on an equal footing in all countries by applying rules and regulations that have been internationally harmonized. At the same time, this is also intended to avoid different safety requirements in different countries having an impact on the competitive situation - i.e. the intention is to facilitate international trade.

There are different concepts and requirements to guarantee safety in the various regions and countries around the globe. The legal concepts and the requirements as to how proof is to be provided and when, whether adequate safety exists, are just as different as the allocation of responsibilities. For example, in the EU, there are requirements placed both on the manufacturer of a plant or system as well as the operating company, which are regulated using the appropriate European Directives, Laws and Standards. On the other hand, in the US, requirements differ both at a regional and even at a local level.

However, the principle that an employer must ensure safety at the place of work applies throughout the entirety of the US. The product liability laws state that, in the event any damage or injury, the manufacturer can be made liable for such damage or injury that can be attributed to its product. On the other hand, in other countries and regions, other principles apply.

What is important for machinery manufacturers and plant construction companies is that the legislation and rules of the location where the machine or plant is being operated always apply. For instance, the control system of a machine, which is operated and used in the US, must fulfill US requirements, even if the machine manufacturer (i.e. the OEM) is based in Europe. Although the technical concepts with which safety is to be achieved are subject to clear technical principles, it is still important to observe as to whether legislation or specific restrictions apply.

Safety systems and functional safety

From the perspective of the object to be protected, safety cannot be segregated. The causes of danger and also the technical measures to avoid them can vary widely. This is the reason that a differentiation is made between various types of safety, e.g. by specifying the particular cause of a hazard. For instance, the term "electrical safety" is used if protection has to be provided against electrical hazards and the term "functional safety" is used if the safety is dependent on the correct function.

This differentiation is now reflected in the most recent standards, in so much that there are special standards that are involved with functional safety. As far as safety of machinery is concerned, EN ISO 13849 and IEC 62061 contain specific provisions regarding the requirements placed on safety-related control systems, thereby concentrating on functional safety. In the basis safety standard IEC 61508 (also EN 61508 and DIN EN 61508 / VDE 0803) IEC addresses the functional safety of electrical, electronic and programmable electronic systems, independent of any specific application area.

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

To achieve this, specifically qualified technology is required, which fulfills the requirements described in the relevant standards. The requirements to achieve functional safety are based on the following basic goals:

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

The measure for the level of achieved functional safety is the probability of the occurrence of dangerous failures, the fault tolerance and the quality that should be guaranteed by avoiding systematic faults. Various terminology is used to express this in the standards. In IEC 61508: "Safety Integrity Level" (SIL) and EN ISO 13849-1 "Performance Level" (PL) and "Categories".

Standards ensure safety

The demand to make plant, machines and other equipment as safe as possible using state-of-the-art technology comes from the fact that manufacturers and users of equipment and products are responsible for their safety. In the standards, business partners describe state-of-the-art technology relating to all safety-significant aspects. By maintaining and fulfilling these standards, it can be ensured that state-of-the-art technology is achieved - therefore ensuring that a company erecting a plant or a manufacturer producing a machine or a device has fulfilled his responsibility for ensuring safety.

Note

The standards, directives and laws listed in this Reference Manual are just a selection to communicate the essential goals and principles. We do not claim that this list is complete.

2.2 Regulations and standards in the European Union (EU)

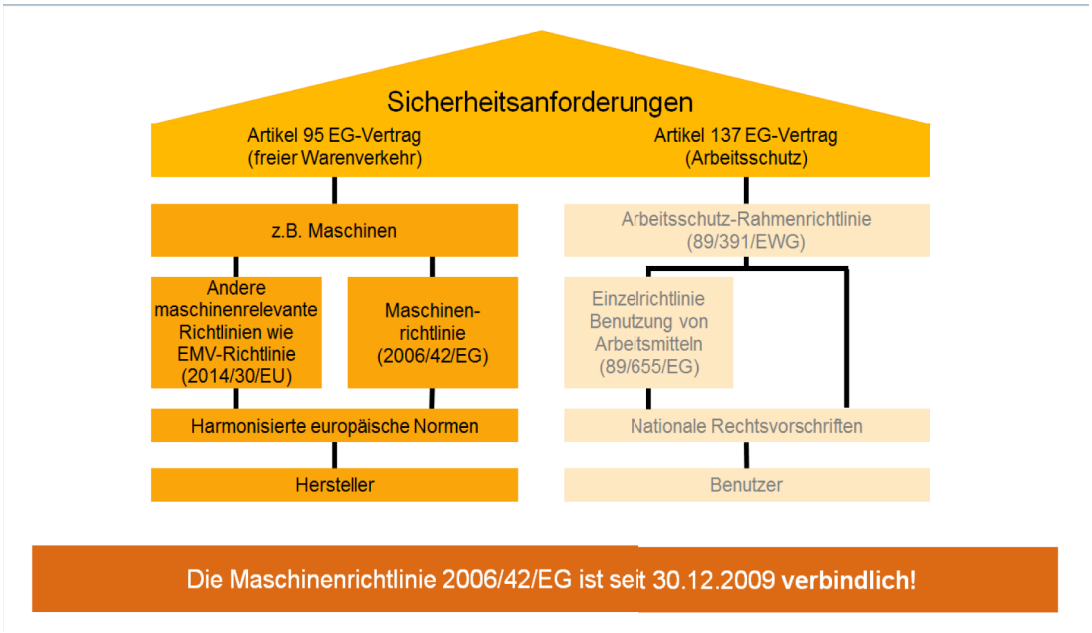


Figure 2-1 Standards and regulations in Europe

2.2.1 Basic principles of the legal requirements in Europe

The EFTA countries have taken on the concept of the EU.

Legislation demands that "the quality of the environment and the health of people are to be protected using preventive measures" Directive 2012/18/EU of the Council "Seveso II".

It also demands "Health and safety at the workplace" (machinery directive, health and safety legislation,...). Legislation demands that this and similar goals are achieved for various areas ("Areas which are legislated") in the (EU) directives. In order to achieve these goals, legislation places demands on the operators and users of plants and the manufacturers of equipment and machines. It also assigns the responsibility for possible injury or damage.

The EU directives

- specify requirements for plants/systems and the operating companies to ensure the health and safety of personnel and the quality of the environment;
- include regulations regarding health and safety at the workplace (minimum requirements);
- define product requirements (e.g. for machines) to ensure the health and safety of the user;
- define different requirements on the implementation of products to ensure the free exchange of goods and requirements on the use of products.

The EU directives, which involve the implementation of products, based on Article 95 of the EU contract that regulates free trade. This is based on a new global concept ("new approach", "global approach"):

- EU directives only contain general safety goals and define basic requirements.
- Standards Associations that have the appropriate mandate of the EU Commission (CEN, CENELEC) can define technical details. These standards are harmonized under a specific directive and are listed in the official EU Journal. When the harmonized standards are fulfilled, then it can be presumed that the associated safety requirements of the directives are also fulfilled. (for more detailed information, refer to "Safety of machinery in Europe").
- Legislation does not specify that specific standards have to be complied with. However, when specific standards are complied with, then it can be "assumed" that the associated safety goals of the EU directives are complied with.
- EU directives specify that Member States must mutually recognize national regulations.

In addition to the directives that are specific to a device type - e.g. the Low-Voltage Directive or Machinery Directive, which will be discussed in more detail in the following, there is also a general "Product Safety Directive". This handles general questions relating to product safety. In Germany, it is implemented in the Product Safety Act (ProdSG).

The EU directives have the same degree of importance, i.e. if several directives apply for a specific piece of equipment or device, then the requirements of all of the relevant directives have to be fulfilled (e.g. for a machine with electrical equipment, the machinery directive and low-voltage directive apply).

Other regulations apply to equipment where the EU directives are not applicable. They include regulations and criteria for voluntary tests and certifications.

The EU directives of the New Approach with the associated lists of the harmonized standards are available in the Internet under: (http://www.newapproach.org/).

2.2.2 Health and safety at the workplace in the EU

The requirements placed on health and safety at the workplace are based on Article 137 (previously 118a) of the EU contract. The master directive "Workplace Health and Safety" (89/391/EEC) specifies minimum requirements for safety at the workplace. The actual requirements are subject to national legislation and can exceed the requirements of these master directives. These requirements involve the operation and use of products (e.g. machines, chemical plants), but not their implementation.

In Germany, the requirements are summarized in the German Health and Safety at Work Regulations (BetrSichV). More detailed information on these regulations can be found on the Bundesanstalt für Arbeitsschutz und Arbeitsmedizin web site(BauA) (http://www.baua.de/en).

2.2.3 Safety of machinery in Europe

Machinery directive (2006/42/EC)

With the introduction of a common European market, a decision was made to harmonize the national standards and regulations of all of the EC Member States, which involve the technical implementation of machines. The consequence of this was that the contents of the machinery

directive had to be implemented in national law as an internal market directive by the individual member states. In Germany, the content of the Machinery Directive was adopted as the Ninth Ordinance to the Equipment and Product Safety Act. For the machinery directive, this was realized with the goal of having unified protective goals and to reduce trade barriers. The area of application of the machinery directive corresponding to its definition "Machinery means an assembly of linked parts or components, at least one of which moves" is extremely comprehensive.

An assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole is also considered to be a "machine".

The application area of the machinery directive thus ranges from an "incomplete" machine up to a complete plant.

Since the 29th of December 2009, the requirements of the new machinery directive 2006/42/EC apply for functional safety.

Risk assessment, requirements placed on the documentation and suitable safety systems, conformity evaluation as well as machine manufacturers outside the European Union have changed in the new machinery directive. Competent appropriately trained personnel must perform the risk assessment of a machine. The risk assessment must be described in the technical documentation of the machine and must be mentioned in the operating instructions.

New processes were defined for the CE conformity evaluation. These apply for machines, which were listed in Annex IV of the machinery directive, as well as for "incomplete machines". Machine manufacturers who wish to import machines into the EU must have the technical documentation of their machine generated in the EU, e.g. by an authorized representative. This simplifies the CE conformity process for the appropriate authorities and gives users a higher degree of safety and security when purchasing and operating a machine.

It is absolutely necessary that the basic health and safety requirements in Annex I of the directive are fulfilled for the safety of machines. The manufacturer must observe the following basics for the integration of safety:

1. "Machinery must be constructed in such a way that it can be operated, set up, and maintained as part of its proper use without endangering personnel." "The measures must ...exclude... the risk of accidents."
2. "In selecting the most appropriate methods, the manufacturer must apply the following basic principles in the order given:
   - Hazards must be eliminated or reduced as far as possible (integration of safety concepts in the development and construction of the machine)
   - The necessary protective measures must be taken in relation to risks that cannot be eliminated
   - Users must be informed about residual hazards due to the incompleteness of these safety measures taken

The protective goals must be responsibly implemented in order to fulfill the requirement relating to conformity with the directive.

The manufacturer of a machine must provide proof that the basic requirements have been complied with. This proof is made easier by applying harmonized standards (e.g. EN ISO 13849-1 or EN 62061).

Standards

To place products in the market or to operate these, then they must fulfill the basic safety requirements of the EU directives. Standards can be extremely helpful when it involves fulfilling these safety requirements. In this case, a differentiation must be made between harmonized European standards and other standards, which although they have been ratified, have still not been harmonized under a specific directive, as well as other technical rules and regulations which are also known as "national standards" in the directives.

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

All standards ratified as European standards must, in principle, be adopted unchanged as national standards of the member states, regardless of whether they have been harmonized under a directive or not. Existing national standards on the same subject must then be revoked. This means that over time, a series of standards (without any conflicting statements) will be created in Europe.

Note

IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" is an important standard that has not been harmonized under an EU directive. It is ratified as EN 61508. There, where EN 61508 is referenced in a harmonized standard, it is a standard that is "also applicable" to the associated harmonized standard.

Harmonized European standards

These are drawn up by two standards organizations CEN (Comité Européen de Normalisation) and CENELEC (Comité Européen de Normalisation Electrotechnique) as a mandate from the EU Commission in order to specify the requirements of the EU directives for a specific product. These standards (EN standards) are published in the official Council Journal of the European Communities and are then accepted in national standards without any changes.

They are used to fulfill the basic health and safety requirements of the protective goals specified in Annex I of the machinery directive.

In Germany, the contact partner for CEN/CENELEC is DIN and the DKE.

By fulfilling such harmonized standards, there is an "automatic presumption of conformity", i.e. the manufacturer can be trusted to have fulfilled all of the safety aspects of the directive as long as they are covered in the particular standard. However, not every European standard is harmonized in this sense. The listing in the European Council Journal is decisive here. The current version of these lists can always be called up in the Internet (http://www.newapproach.org/).

European standards for the safety of machinery are hierarchically structured as follows

- A Standards,
  also known as Basic Standards.
- B Standards,
  also known as Group Standards.
- C Standards,
  also known as Product Standards.

The structure is shown in the following diagram.

<table>
<tr><td>Safety basic standards</td><td>Type-A standards
Basic stipulations for all machines</td><td colspan="5">EN ISO 12100
Safety of machines - basic terminology, general design guidelines
- guidelines for risk assessment</td></tr>
<tr><td rowspan="3">Safety group standards</td><td>Type-B1 standards
Higher-level safety aspects</td><td>Minimum clearance to avoid crushing of parts of the human body

EN 349</td><td>Safety-related parts of controllers

EN 62061
EN ISO 13849-1</td><td>Safety of machinery - Safety distances to prevent hazard zones being reached by upper and lower limbs

DIN EN ISO 13857</td><td>Electrical equipment of machines

EN 60204-1</td><td>Safety of machinery - Interlocking devices associated with guards

EN ISO 14119</td></tr>
<tr><td>Type-B2 standards
Requirements for safety equipment (reference to specific protective equipment)</td><td>Two-hand control
EN 574</td><td colspan="2">EMERGENCY STOP function, functional aspects
- principles for design -
EN ISO 13850</td><td colspan="2">Light barriers, light curtains
EN 61496-1</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Technical standards</td><td>Type-C standards
Technical standards, specific requirements placed on certain types of machinery</td><td>Elevators

EN 81-3</td><td>Injection molding machines

EN 201</td><td>Presses and shearing machines

EN 692
EN 693</td><td>Numerically controlled turning machines

EN ISO 23125</td><td></td></tr>
</table>

Figure 2-2 The European standards for safety of machinery

Type A Standards/Basic Standards

A Standards contain basic terminology and definitions for all machines. This also includes EN ISO 12100 "Safety of machines, basic terminology, general design guidelines."

A Standards primarily address those parties setting B and C Standards. The techniques and methods specified there to minimize risks can also be helpful for manufacturers if there are no applicable C Standards.

Type B Standards/Group Standards

These include all standards with safety-related statements that can address several types of machines.

B Standards also primarily address those parties setting C Standards. However, they can also be helpful to manufacturers when designing and constructing a machine if there are no applicable C Standards.

For B Standards, an additional subdivision has been made, and more precisely in:

Type B1 Standards for higher-level safety aspects, e.g. ergonomic design principles, safety distances from potential sources of danger, minimum clearances to prevent crushing of body parts.

Type B2 Standards for safety equipment are for various machine types, e.g. Emergency Stop equipment, two-hand circuits, interlocking functions, contactless protective equipment and devices, safety-related parts of control systems.

Type C Standards/Product Standards

These involve standards for specific machines - e.g. for machine tools, woodworking machines, elevators, packaging machinery, printing machines and many others.

The European standards are structured so that general statements that are already included in type A or type B Standards are not repeated. As far as possible, references are made to these in type C Standards.

Product Standards include machinery-specific requirements. These requirements, under certain circumstances, deviate from the Basic and Group Standards. Type C Standard/Product Standard has absolutely the higher priority for machine manufacturers (OEMs). The machine manufacturers can then assume that they fulfill the basic requirements of Annex I of the machinery directives (automatic presumption of conformity). If there is no Product Standard for a particular machine, then type B standards can be applied for orientation purposes when designing and constructing a machine.

In order to provide a method to harmonize the basic requirements of the directive, with the mandate of the EC commission, harmonized standards were drawn-up in the technical committees of the CEN and CENELEC for machinery or machinery groups for almost all areas. Drawing-up the standards essentially involves representatives from the manufacturer of the particular machinery, the regulatory bodies, such as Employer's Liability Insurance Associations as well as users. A complete list of all of the listed standards as well as the activities associated with standards - with mandated new standards for the future - are provided in the Internet under: (http://www.newapproach.org/).

Recommendation: Technology is progressing at a tremendous pace, which is also reflected in changes made to machine concepts. For this reason, especially when using type C Standards, they should be checked to ensure that they are up-to-date. It should also be noted that it is not mandatory to apply the standard, but instead, the safety objectives must be achieved.

National standards

If there are no harmonized European standards, or they cannot be applied for specific reasons, then a manufacturer can apply "National Standards". All of the other technical rules fall under this term of the machinery directive, e.g. also the accident prevention regulations and standards, which are not listed in the European Council Journal (also IEC or ISO standards, which were ratified as EN). By applying ratified standards, the manufacturer can prove that recognized state-of-the-art technology was fulfilled. However, when such standards are applied, this does not automatically represent a presumption of conformity as for a harmonized standard.

Risk assessment

As a result of their design and functionality, machinery and plants represent potential risks. Therefore, the machinery directive requires a risk assessment for every machine and, if relevant, risk reduction, so that the remaining risk is less than the tolerable risk.

The following standards should be applied for the techniques to evaluate and assess these risks:

- EN ISO 12100 "Safety of machinery - General principles for design - Risk assessment and risk reduction"
  EN ISO 12100 predominantly describes the risks to be considered and the design principles for risk reduction as well as the iterative process with risk assessment and risk reduction in order to achieve safety.
- ANSI B11.0 - 2015, Safety of Machinery; General Requirements and Risk Assessment (for USA only)
  This standard applies to new, modified or rebuilt power-driven machines, not portable by hand, used to shape and/or form metal by cutting, impact, pressure, electrical or other processing techniques, or a combination of these processes.
  Includes the standards documents ANSI B 11.19 - 2010 (R2008) and ANSI B11.TR3.

Risk assessment process

Risk assessment is a sequence of steps that allows hazards, which are caused by machines, to be systematically investigated. Where necessary, the risk assessment phase is followed by risk reduction. The iterative process is obtained by repeating this procedure (see Fig. 2/4). Using this process, hazards, as far as possible, can be eliminated and the appropriate protective measures can be applied.

Risk assessment encompasses the following

- Risk analysis
  - Determining the limits of the machine (EN ISO 12100)
  - Identifying the hazards (EN ISO 12100)
- Risk evaluation (EN ISO 12100:2010-03 Section 5.6)

After the risks have been estimated, a risk evaluation is made as part of an iterative process to achieve safety. In this case, a decision has to be made whether it is necessary to reduce a risk. If a risk is to be further reduced, suitable protective measures must be selected and applied. The risk assessment should then be repeated.

Risk elements are defined as a support tool to evaluate risks. The following diagram clearly shows the interrelationship between these risk elements.

The risk elements (S, F and W) serve as input quantities for both standards. These risk elements are evaluated in different ways. According to EN 62061, a demanded Safety Integrity Level (SIL) is determined, according to EN ISO 13849-1, a Performance Level (PL).

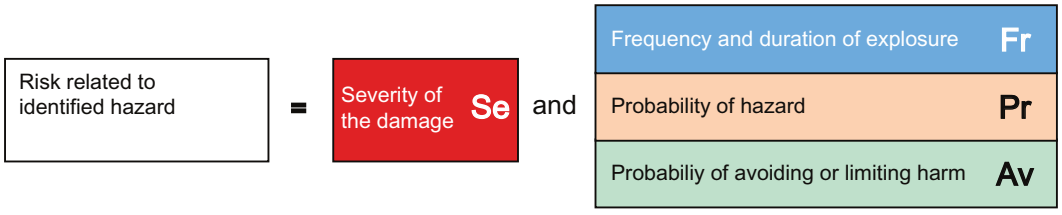


Figure 2-3 Risk elements

If the required degree of safety has still not been achieved, measures are required to further reduce the risk.

The risk must be reduced by suitably designing and implementing the machine. For instance, using suitable control or protective measures for the safety functions.

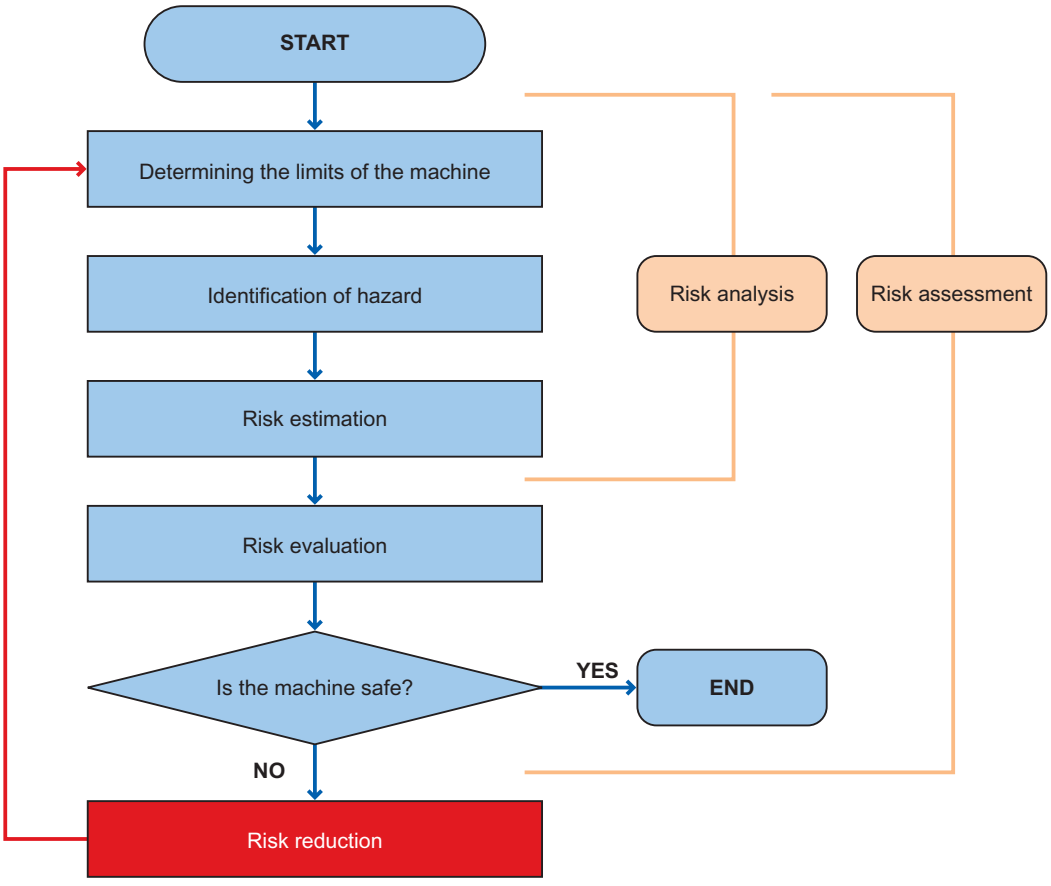


Figure 2-4 Interactive process to achieve safety according to EN ISO 12100

Residual risk (EN ISO 12100)

Safety is a relative term in our technical environment. Unfortunately, it is not possible to implement the so-called "zero risk guarantee" where nothing can happen under any circumstance. The residual risk is defined as: Risk that remains after the protective measures have been implemented. In this case, protective measures represent all of the measures to reduced risk.

2.2.4 Functional safety - electrical safety

Risk reduction

In addition to applying structural measures, risk reduction for a machine can also be realized using safety-relevant control functions. Specific requirements must be observed when implementing these control functions, graduated according to the magnitude of the risk. These are defined in EN ISO 13849-1 and, for electrical control systems, especially with programmable electronics, in IEC 61508.

The requirements placed on safety relevant parts of control systems are classified into categories, according to the level of risk and the necessary risk reduction. With EN ISO 13849-1, a new risk diagram has been introduced; instead of categories, hierarchically graduated Performance Levels (PL) are defined (see Appendix 4.4.).

EN 62061 uses the "Safety Integrity Level" (SIL) to classify risks (see Appendix 4.5.). This is a quantified measure for the safety-related performance of a safety function. The required SIL is also determined based on the risk evaluation principle according to EN ISO 12100. Annex A of the standard describes a method for determining the required Safety Integrity Level.

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

Note

The load circuits of the drives and motors also belong to a machine control system.

When designing and implementing the control, it is necessary to check whether the requirements of the selected PL or SIL are fulfilled.

New aspects must be observed in the standards, so that

- random hardware failures are controlled,
- systematic faults/errors in the hardware and software are avoided, and
- systematic faults/errors in the hardware and software are controlled.

Validation

Validation means that the safety functionality to be achieved is checked and evaluated. The purpose of validation is to confirm the definitions and the level of the conformity of the safety-related parts of the control within the overall definition of the safety requirements of the machine. Further, validation must indicate that each and every safety-related part fulfills the requirements of the relevant standard.

The following aspects are described:

- Fault lists
- Validation of safety functions
- Validation of the specified and the achieved safety performance (Category, Safety Integrity Level or Performance Level)
- Validation of the environmental/ambient requirements
- Validation of the service & maintenance requirements

The requirements for performing validation for the defined safety functions must be described in a validation plan.

Safety Integrated

The measures, which are required to make a complex control adequately and functionally safe for safety tasks, are extremely extensive and involve the concept and the complete development and production processes. This is the reason that devices such as these were specifically designed for safety functions. Examples of such devices are SIMATIC S7-1500 and S7-1200 with

Safety Integrated and SINUMERIK "Safety Integrated" as well as the communication systems PROFIsafe and ASIsafe, the PROFIBUS and AS-Interface for transmitting safety-related data.

Safety-related functions

Safety-related functions include, in addition to conventional functions

- Stopping
- Procedures in an emergency situation
- Preventing undesirable starting

In the meantime, also more complex functions such as:

- State-dependent interlocks
- Velocity limiting
- Position limiting
- Controlled shutdown
- Controlled stopping etc.

The classic functions are also defined in EN 60204-1 and, up until now, were generally implemented using electromechanical components. Electronic programmable systems can also be used to implement more complex functions if they fulfill the relevant standards. Complex functions, e.g. which involve the behavior of variable-speed drives are described in EN 61800-5-2.

Stopping

Stop categories according to EN 60204-1

Three stop categories are defined in EN 60204-1 (VDE 0113 Part 1), which define the control sequence for shutdown, independent of an emergency situation.

Stop category 0	Uncontrolled stop by immediately removing the power feed to the machine drive elements.
Stop category 1	Controlled stop; the power is not disconnected until standstill has been reached.
Stop category 2	Controlled stop where the power feed is still maintained even at standstill. **Note:** Switching off only interrupts the energy feed that can cause the movement. However, the plant/system is not brought into a general no voltage condition.

Procedure in an emergency situation

Procedures in an emergency situation (EN 60204-1) can be described as follows:

- Stopping in an emergency (Emergency Stop)
- Starting in an emergency (Emergency Start)
- Switching-off in an emergency (Emergency Off)
- Switching-on in an emergency (Emergency On)

According to EN 60204-1 and EN ISO 13850, these functions are exclusively initiated by a conscious, operator action. In the following text, only "Switching-off in an emergency" and "Stopping in an emergency" will be discussed.

Note

In Germany, for "Stopping in an emergency", in addition to the term Emergency Stop, frequently Emergency Off is used, even if only stopping is meant.

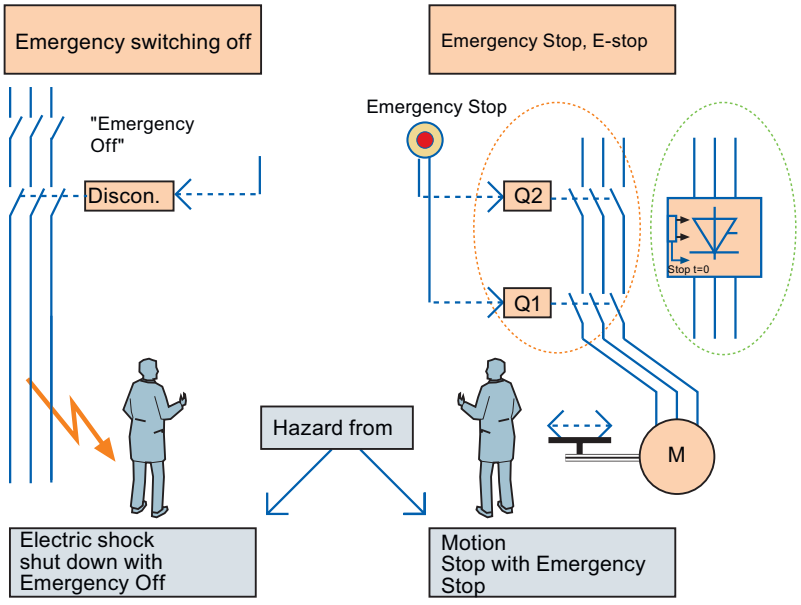


Figure 2-5 Difference between Emergency Off and Emergency Stop

Emergency Off

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

Functional aspects for switching off in an emergency are defined in IEC 60204-1.

Switching-off in an emergency should be implemented, where

- Protection against direct contact (e.g. with contact wires, contact assemblies, switching devices in rooms accommodating electrical equipment) can only be achieved by providing the appropriate clearance or the appropriate barriers.
- there is a possibility of other hazards or damage caused by electrical energy.

Emergency Stop

An action in an emergency that is intended to stop a process or motion that would result in a hazard (from EN 60204-1).

In addition to the requirements for stop, the following requirements apply in case of stopping in an emergency:

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

Devices for Emergency Off and Emergency Stop

Devices that are used to stop equipment and machinery in an emergency must be provided at every operator control location and also at other locations where it may be necessary to initiate a stop in an emergency (exception: operator control stations that are not connected through cables - i.e through a wireless connection).

In order to fulfill the protective goals specified in EN 60204-1 as well as in EN ISO 13850, the following requirements apply to both functions:

- When the contacts switch, even when briefly actuated, the command device must latch positively.
- It must be impossible for the machine to be restarted from a remote main control desk before the danger has been removed. The emergency stop device must be released locally in the form of a conscious operated action.

Wireless operator control stations must have their own function, which can also be clearly identified, to initiate a machine stop. The operator control station that initiates this stop function may neither be marked nor labeled as a device for emergency stopping.

Human – Machine (color coding for operator control devices and displays)

In order to simplify the interaction between man and machine, standards EN 60073 and DIN EN 60204-1 specify the appropriate marking and coding.

Switches, pushbuttons and indicator lights are the main machine components that are used as the interface between man and machine. These operator control elements are clearly identified and coded in a standard fashion using colors that are assigned a very specific significance. This guarantees that the degree of safety for operating personnel is increased and it is also simpler to operate and service the equipment/systems.

The colors of pushbuttons, the significance of these colors, explanations and application examples are shown in the following tables.

The colors for indicator lights, their significance with reference to the state of the machine as well as handling and application examples are listed in the table "Colors for indicator lights and their significance according to EN 60204-1 (VDE 0113 Part 1)".

The following two tables also apply to illuminated pushbuttons.

Color	Description	Explanation	Application examples
RED	Emergency	Actuate in the event of a hazardous condition or emergency	EMERGENCY OFF, Initiation of EMERGENCY OFF functions, conditionally for STOP/OFF
YELLOW	Abnormal	Actuate in the event of an abnormal state	Intervention to suppress an abnormal state, Intervention to restart an interrupted automatic cycle
GREEN	Normal	Actuate to initiate normal states	START/ON however, WHITE should be preferably used
BLUE	Mandatory	Actuate for a condition requiring mandatory action	Reset function
WHITE	No specific meaning assigned (neutral)	For general initiation of functions, except for EMERGENCY OFF (also refer to the note)	START/ON (preferred), STOP/OFF
GRAY			START/ON, STOP/OFF
BLACK			START/ON, STOP/OFF (preferred)
Note: Where a supplemental means of coding (e.g. shape, position, texture) is used to identify pushbutton actuators, then the same colors WHITE, GRAY or BLACK may be used for various functions, e.g. WHITE for START/ON and STOP/OFF actuators.			

Colors for pushbuttons and their significance according to EN 60204-1 (VDE 0113 Part 1)

Color	Description	Explanation	Action by the operator	Application examples
RED	Emergency	Hazardous state	Immediate action to respond to a hazardous state (e.g. by pressing EMERGENCY OFF)	Pressure/temperature outside safe limits, voltage drop, voltage interruption, passing a stop position
YELLOW	Abnormal	Abnormal state Pending critical state	Monitoring and/or intervening (e.g. by establishing the intended function)	Pressure/temperature exceeds the normal ranges, a protective device trips
GREEN	Normal	Normal state	Optional	Pressure/temperature within normal ranges, permissive condition to continue
BLUE	Mandatory	Indicates a condition that requires operator action	Mandatory action	Prompt to enter specified values
WHITE	Neutral	Other states: May be used whenever doubt exists about the use of RED, YELLOW, GREEN or BLUE	Monitoring	General information

Colors for indicator lights and their significance according to EN 60204-1 (VDE 0113 Part 1)

Marking cables

The color coding of switches, pushbuttons and indicator lights has been discussed in the previous chapter. EN 60204-1 permits a higher degree of flexibility when it comes to marking and coding cables. It stipulates that "... it shall be possible to identify conductors at each termination in accordance with the information provided in the technical documentation..."

The numbering of terminals matching the circuit diagram is sufficient if it is possible to visually and easily trace the cable. For complex controls, we recommend that the internal cables used for wiring as well as the outgoing cables are coded so that after the cable has been disconnected from the terminal, it can be easily reconnected to the same terminal. This is also recommended for terminal locations that have to be disconnected when the equipment is transported.

With its formulation in IEC 60204-1 2016, Section 13.2 Identification of conductors, the standards committee wanted to express the following points:

1. Each individual conductor must be able to be identified, however with absolute certainty only in conjunction with the documentation. It is not stipulated that every cable must be able to be identified without the appropriate documentation.
2. The manufacturer and operating company should agree on the type of coding/marking and therefore also on the identification techniques used.

It is not the intention of the standard to specify a certain coding type that must be applied worldwide. For instance, for safety reasons, factory-internal specifications may have a higher priority in order to avoid confusion in areas that are handled by the same personnel. These definitions cannot be generalized due to the wide application range of the particular standard - from small individual machines (higher unit volume standard products) up to large, complex plants (with unique equipment and systems).

Primarily, appropriate testing should be used to avoid installation/assembly errors.

A standard color coding for the cables should be used. We recommend the following color assignment:

- Black for AC and DC main circuits
- Red for AC control circuits
- Blue for DC control circuits
- Orange for interlock circuits, which are supplied from an external power source.

The above color assignment is recommended if a decision is made to just use color coding. The only mandatory specification is the color coding of the protective conductor and the neutral conductor. For all other cabling and wiring, one of the methods listed in section 14.2.4 of the IEC 60204 standard can be selected (color, numbers or letters; or a combination of colors and numbers or colors and letters).

Protective conductor coding/marking

The protective conductor must be able to be uniquely identified as a result of its shape, location, marking or color. If it is only identified as a result of its color, then a two color combination of green/yellow must be used along the whole length of the cable. The green/yellow color combination may only be used for protective conductors.

Neutral conductor coding/marking

If a circuit has a color-coded neutral conductor, then light blue must be used. Light blue may not be used to code other cables if there is a danger of accidentally interchanging them.

If a neutral conductor is not used, a light blue conductor may be used for other purposes, but not as protective conductor.

2.2.5 Selecting the devices and basics of the required properties

Safety function

Risk reduction by means of process engineering is implemented by defining functions for each possible hazardous event or each possible dangerous state of the plant or system that prevent the dangerous event occurring. These so-called "safety functions" are used to ensure that the plant/system remains in a safe state or a safe state is re-established if there is a threat of a hazardous event due to a fault or a disturbance in the plant or system. The safety function can also be used to reduce the extent of any damage due to a hazardous event.

The definition of a safety function always includes the specification of the function itself (e.g. shutting-off the feed to a tank if the level has reached its maximum level) and the "Safe Integrity Level (SIL)" derived from the risk analysis.

Safety Integrity Level	High demand or continuous mode of operation (probability of a dangerous failure per hour)	Low demand mode of operation (average probability of failure to perform its design function on demand)
4	$\geq 10^{-9} \ldots < 10^{-8}$	$\geq 10^{-5} \ldots < 10^{-4}$
3	$\geq 10^{-8} \ldots < 10^{-7}$	$\geq 10^{-4} \ldots < 10^{-3}$
2	$\geq 10^{-7} \ldots < 10^{-6}$	$\geq 10^{-3} \ldots < 10^{-2}$
1	$\geq 10^{-6} \ldots < 10^{-5}$	$\geq 10^{-2} \ldots < 10^{-1}$

Safety Integrity Level according to IEC 61508: Target measure for the failure of a safety function, allocated to a safety-related system

Implementing safety functions

Every safety function always encompasses the entire chain - from information acquisition to information evaluation up to executing the intended action.

The equipment involved, for example, fail-safe PLCs, sensors and actuators etc. must fulfill, as a whole, the SIL determined in the risk assessment. If a device is used for various safety functions at the same time, then it must fulfill the highest SIL of the individual functions.

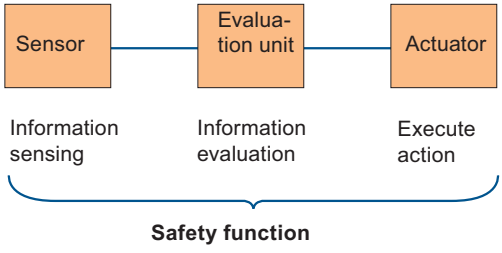


Figure 2-6 Evaluation unit, e.g. safety PLC

Device properties

If PLCs are used to process information, then as "Safety PLC" (SPLC), these must fulfill the requirements of the relevant standards (e.g. IEC 61508) corresponding to the specified SIL. Further, they should be certified by an independent testing organization. The essential characteristics and features of a fail-safe PLC that are specified in a graduated scope in the standards, include:

- In the development, manufacture and service & maintenance, certain measures and techniques must be used, therefore avoiding systematic faults.
- The PLC must be able to control systematic faults that occur in operation.
- The PLC must be able to detect and control random hardware failures in operation.
- Fault control means that when the system detects a fault, it must reliably execute the safety function defined for this particular case (e.g. shut down the plant or system).

Similar requirements also apply to complex field devices. Details on the this are described in IEC 61511.

Application

When using a fail-safe PLC, the conditions defined in the associated safety manual and any additional requirements associated with the certificate must be carefully complied with.

For the peripheral devices to be connected (e.g. sensors and actuators), in addition, the requirements listed in standards (IEC 61508 or IEC 61511) must be carefully observed regarding the following aspects:

- Avoiding systematic faults such as e.g. configuring/engineering, installation and handling faults.
- Detecting and controlling random faults (failures).
- Necessary fault tolerance. This depends on the percentage of failures that fail in the safe direction.
- Required service and maintenance (tests and checks that are repeated).

IEC 61511 states three options for creating a PCS safety instrumented system (SIS):

- According to IEC 61511 Section 11.4.4 to 11.4.9 or
- According to IEC 61508-2:2010 Section 7.4.4.2 (Route 1H) or
- According to IEC 61508-2:2010 Section 7.4.4.3 (Route 2H)

If the option according to IEC 61511 is chosen, a hardware fault tolerance in accordance with the following table shall be fulfilled.

SIL	Minimum HFT
1 (every operating mode)	0
2 (low demand mode)	0
3 (high or continuous demand mode)	1
4 (every operating mode)	1
5 (every operating mode)	2

Furthermore, the devices used shall be chosen in accordance with IEC 61511 Section 11.5. Different measures are required depending on the complexity of the devices used and the required SIL.

- SIL1,2 + FPL → IEC 61508 or prior use
- SIL3 + FPL → IEC 61508 or prior use with additional requirements
- SIL1 + LVL → IEC 61508 or prior use with additional requirements
- SIL2 + LVL → IEC 61508 or prior use with additional assessment
- SIL3 + LVL → IEC 61508
- SIL1,2,3 + FVL → IEC 61508

(FPL = fixed programmable language; LVL =limited variable language; FVL = full variable language)

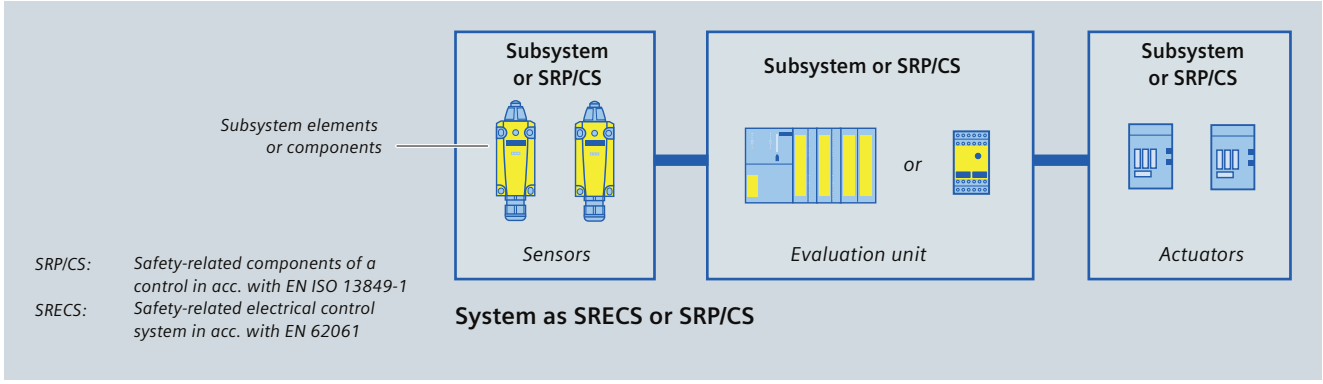
With respect to the process control system, it shall be ensured that each PCS safety instrumented function (SIF) is realized in a PCS safety instrumented system (SIS) and is in accordance with the relevant standards (IEC 61508 or IEC 61511).

2.3 Structure of the safety function and determining the safety integrity

Although the two safety standards EN 62061 and EN ISO 13849-1 use different evaluation methods for a safety function, the results can be transferred between them. Both standards use similar terms and definitions.

The approach of both standards to the entire safety chain is comparable:
A safety function is described as a system.

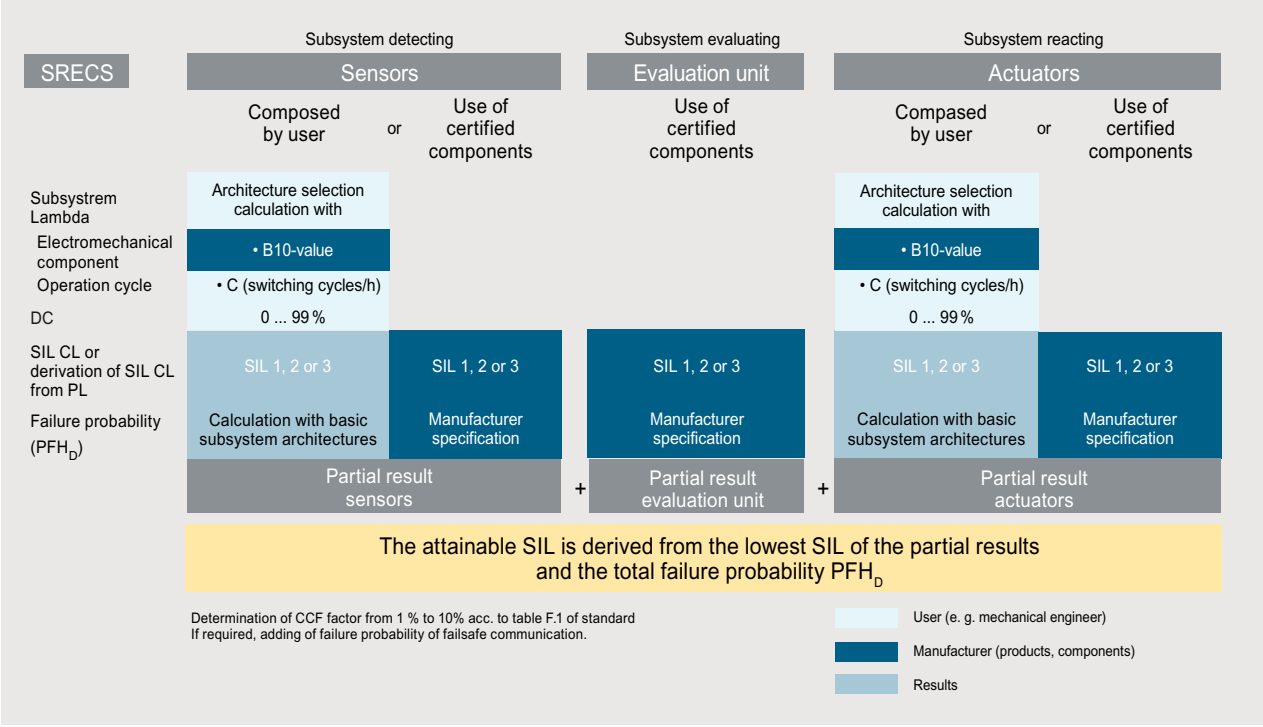
Structure of a safety function



Joint and simplified procedure

1. Evaluate every subsystem or SRP/CS and obtain "partial results". There are two options here:
   - Use certified components with the manufacturers data (e.g. SIL CL, PFH_D or PL).
   - Based on the selected architecture (single or two-channel) the failure rates of the subsystem elements or components are calculated. The failure probability of the subsystem or that of the SRP/CS is then calculated.
2. The partial results concerning the structural requirements (SIL CL or PL) have to be assessed and the probability of failure/PFH_D added.

2.3.1 Methodology according to EN 62061



Note:
The procedure to be followed for the determination of the safety integrity is described in detail in the functional example for EN 62061. See also: (http://support.automation.siemens.com/WW/view/en/23996473)

Subsystem "Detecting" – sensors

For certified components, the manufacturer provides the required values (SIL CL and PFH). When using electromechanical components in a draft user design, SIL CL and PFH values can be determined.

Determining the SIL CL

SIL CL3 can be assumed for the example as the PL x architecture used complies with ISO 13849-1 and the appropriate diagnostics are available.

Calculating the rates of failure λ of the subsystem elements "position switch"

Based on the B10 value and the switching cycles C, the total rate of failure λ of an electromechanical component can be calculated using a formula according to Section 6.7.8.2.1 of EN 62061.

The rate of failure λ comprises safe (λ_S) and hazardous (λ_D) components.

Calculating the probability of dangerous failures per hour PFH_D according to the architecture used

EN 62061 defines four architectures for subsystems (basic subsystem architectures A to D). To determine the probability of failure PFH_D the standard provides calculation formulas for each architecture.

Subsystem "Evaluating" - evaluation unit

For certified components, the manufacturer provides the required values.

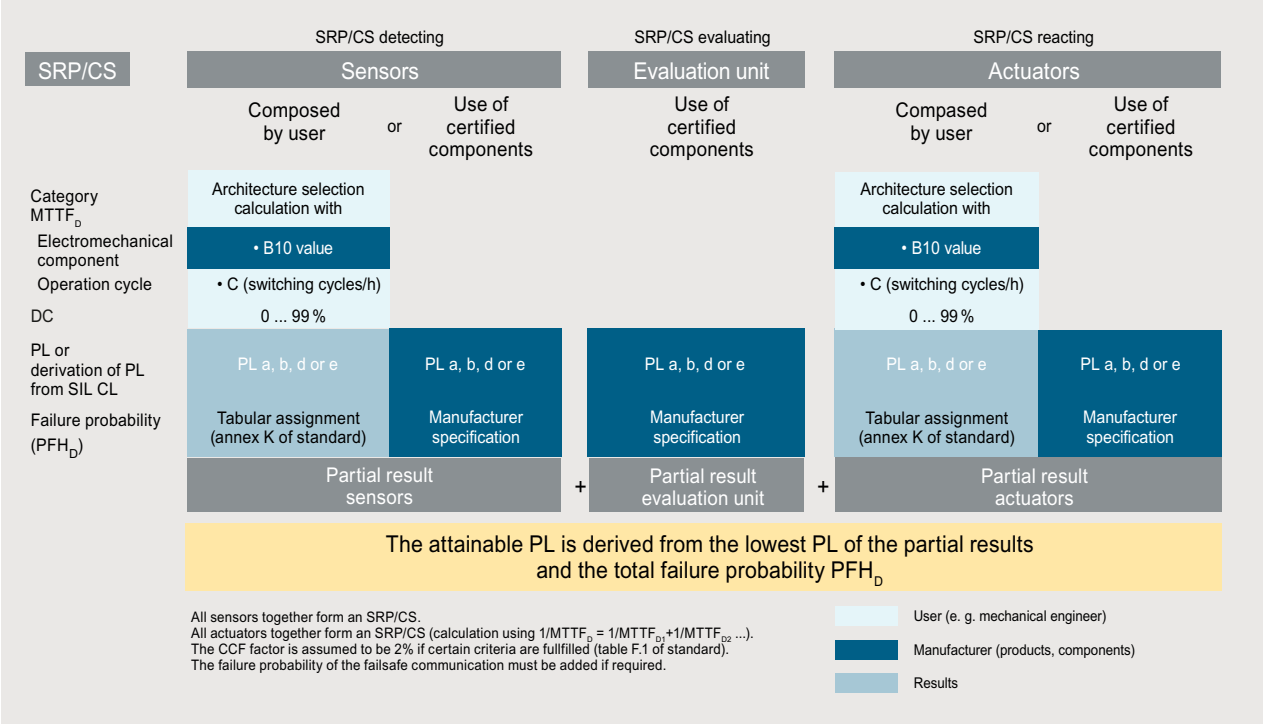
Subsystem "reacting" – actuators

For certified components, the manufacturer provides the required values:
If the "reacting" subsystem is designed by the user, the same procedure is applied as for the "detecting" subsystem.

Determining the safety integrity of the safety function

The minimum SIL limit (SIL CL) of all subsystems of the safety-related control function (SRCF) must be determined.

2.3.2 Methodology according to EN ISO 13849-1



SRP/CS "Detecting" – sensors

For certified components, the manufacturer provides the required values (PL, SIL CL or PFH)$_D$). SIL CL and the PL can be mutually transferred on the basis of probability of failure, refer to the point, implementation of SIL and PL.

When using electromechanical components in a draft user design, PL and PFH$_D$ values can be determined as follows.

Calculating the rates of failure of SRP/CS elements

On the basis of the B10 value and the switching cycle n_{op}, the rate of failure $MTTF_D$ of an electromechanical component can be determined by the user, e.g.:

$MTTF_D = B10_D/(0.1 * n_{op}) = 0.2 * 10^8$ hours = 2 300 years corresponds to $MTTF_D$ = high
with n_{op} = actuations per year (provided by user)
$n_{op} = (d_{op} * h_{op} * 3\,600\ s/h) / t_{cycle}$

With the following assumptions regarding the usage of the component:

- h_{op} is the average operating time in hours per day
- d_{op} is the average operating time in days per year
- t_{cycle} is the average time between the start of two successive cycles of the components (e.g. valve actuation) in seconds per cycle

SRP/CS "Evaluating" - evaluation unit

For certified components, the manufacturer provides the required values.

SRP/CS "reacting" – actuators

For certified components, the manufacturer provides the required values.

When the user designs SRP/CS "reacting" he applies the same procedure as for SRP/CS "detecting".

Determining the safety integrity of the safety function

The lowest PL of all SRP/CS of the safety-related control function (SRCF) must be determined.

2.3.3 Validation based on the safety plan

The validation serves to check whether the safety system (SRECS) meets the requirements defined in the "Specification of the SRCF". The safety plan is the basis for this validation.

The following validation procedure must be followed:

- Definition and documentation of the various responsibilities
- Documentation of all tests
- Validation of each SRCF on the basis of tests and/or analyses
- Validation of the systematic safety integrity of the SRECS

Planning

The safety plan must be drawn-up. Validation is performed using this document.

Testing/checking

All safety functions must be tested in accordance with the specification.

Documentation

The documentation is a basic and essential component of the evaluation procedure in the case of damage.

The content of the documentation list is specified by the machinery directive.
Basically, the following documents are involved:

- Hazard analysis
- Hazard evaluation
- Specification of the safety functions
- Hardware components, certificates etc.
- Circuit diagrams
- Test results
- Software documentation including signatures, certificates etc.
- Information on usage, including safety instructions and restrictions for the operator

After successful validation, the CE Declaration of Conformity for the risk-minimizing protective measure can be issued.

2.4 Legal requirements and standards regarding safety at work in North America

Note: The following description is intended to provide an overview of the principles and basic requirements. It should not be considered as a complete description of the situation. The reader of this document must additionally inform himself about the precise requirements as well as the domestic and local regulations for his particular application.

For legislation regarding occupational safety and health there is a significant difference between the North America and Europe. In America, there is no standard legislation that applies across all of the US States that defines and specifies the responsibility of the manufacturer/supplier. In the US, there is a general requirement that employers must ensure safety at work.

2.4.1 US - general information

The Occupational Safety and Health Act (OSHA) from 1971 regulates the requirement that employers must offer a safe place of work.

The core requirements of the OSH Act are administered through the Occupational Safety and Health Administration (also known as OSHA). OSHA deploys regional inspectors to check whether workplaces comply with the valid rules and regulations.

The rules and regulations of OSHA - relevant for safety at the workplace - are defined in OSHA 29 CFR 1910.xxx ("OSHA Regulations (29 CFR) PART 1910 Occupational Safety and Health") (CFR: Code of Federal Regulations), Subpart O - Machinery and Machine Guarding.

Additional information can be found in the Internet (www.osha.gov).

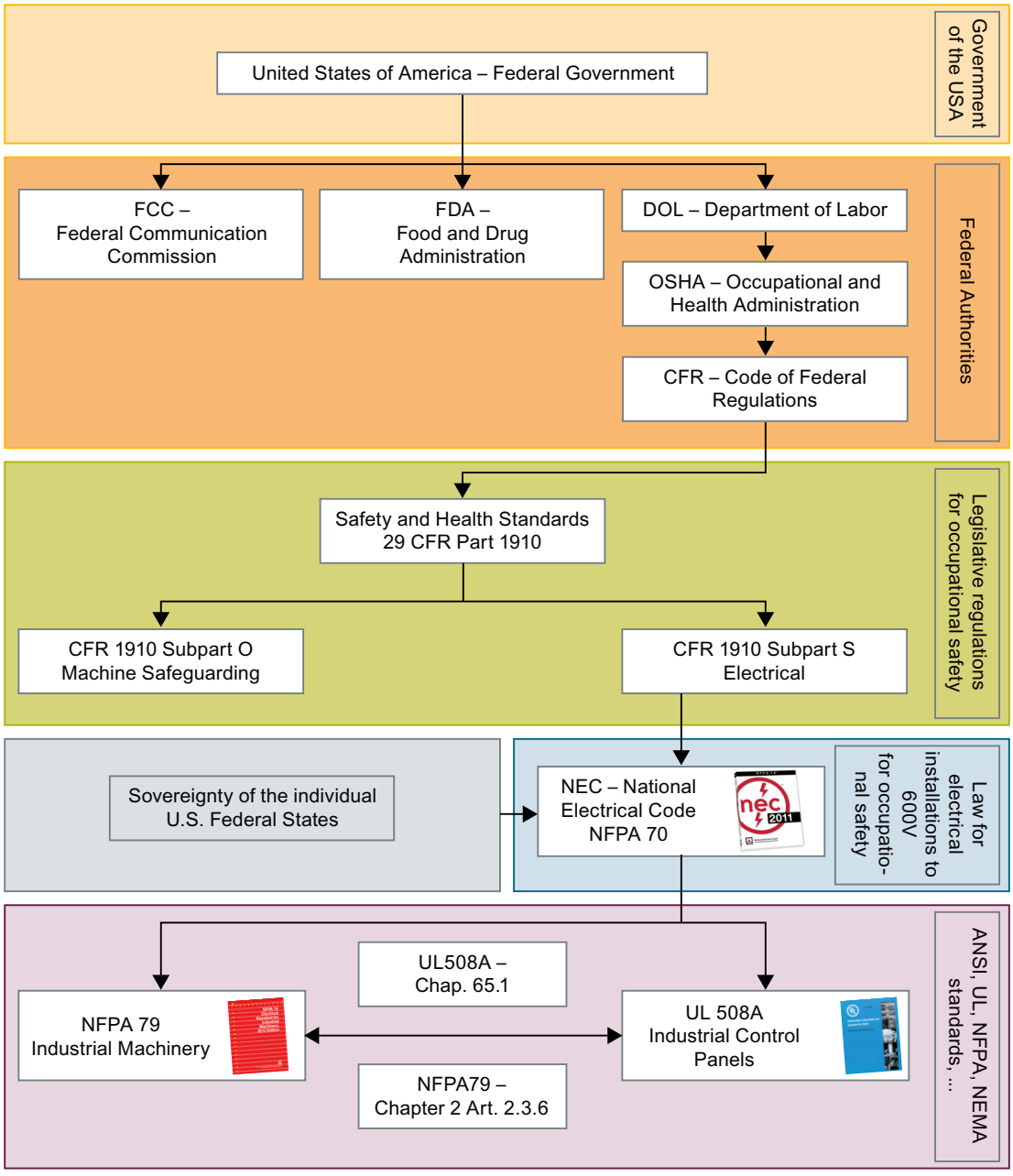


Figure 2-7 Statutory requirements and standards in the USA

2.4.2 Machine safety

Minimum requirements of the OSHA

The OSHA Rules under 29 CFR 1910 Subpart O include general requirements for machines (1910.212) and a series of specific requirements for certain machine types.

OSHA regulations define minimum requirements to guarantee safe places of employment. However, they should not prevent employers from applying innovative methods and

techniques, e.g. "state-of-the-art" protective systems in order to maximize the safety of employees.

In conjunction with certain applications, OSHA requires that all electrical equipment and devices that are used to protect workers be authorized by an OSHA-certified Nationally Recognized Testing Laboratory (NRTL) for the specific application..

Application of other standards

In addition to the OSHA regulations, it is important to carefully observe the latest versions of standards released by organizations such as the ANSI, NFPA, and RIA as well as the extensive product liability legislation in the US. As a result of the product liability, it is in the interest of manufacturers and operating companies to carefully observe and maintain the regulations - and they are more or less "forced" to fulfill the state-of-the-art technology requirement.

Third-party insurance contracts generally demand that the parties involved fulfill the applicable standards of the standardization organizations. Companies who are self-insured initially do not have this requirement. However, in the case of an accident, they must prove that they had applied generally recognized safety principles.

NFPA 70 (known as the National Electric Code (NEC)) and NFPA 79 (Electrical Standard for Industrial Machinery) are two particularly important standards regarding safety in industry. Both of these describe the basic requirements placed on the features and the implementation of electrical equipment. The National Electrical Code is prescribed as a benchmark by US law and applies to all electrical installations in the low-voltage range. In Article 670 Industrial Machinery, the NEC makes an informative reference to NFPA 79. Informative means that NFPA 79 can be applied to machinery but is not mandatory. NFPA 79 enjoys widespread acceptance in the USA and is usually applied to machinery. The requirements in NFPA 79 are coordinated with the National Electrical Code and NFPA 70E standard for electrical safety in the workplace.

NFPA 79

This standard applies to electrical equipment on industrial machines with rated voltages up to and including 600 V. (A group of machines that operate together in a coordinated fashion is also considered to be one machine.)

- Original NFPA 79 1997: Restricted machine safety to electromechanical devices.
  9.6.3 Where a Category 0 stop is used for the emergency stop function, it shall have only hardwired electromechanical components. In addition, its operation shall not depend on electronic logic (hardware or software).
- NFPA 79 2002 – Allowed the use of safety PLC in safety-related functions.
  11.3.4 Use in Safety-Related Functions. Software and firmware-based controllers to be used for safety-related functions shall be listed for this use. [Annex to NFPA 79 2002, A.11.3.4 IEC 61508]

- NFPA 79 2007 – Allowed drives as a final switching device.
  9.2.5.4.1.4 Drives or solid-state output devices designed for safety-related functions shall be allowed to be the final switching element, when designed according to relevant safety standards.
- NFPA 79 2015 allows the use of wireless controllers
  9.2.7.1* General. Cableless control (e.g., radio, infrared) techniques for transmitting commands and signals between a machine control system and operator control station(s) shall meet the requirements of 9.2.7.1.1 through 9.2.7.1.4.
  The core requirements placed on programmable electronics and buses include: System requirements (see NFPA 79 2015 9.4.3.4.2)
  Control systems incorporating software- and firmware-based controllers performing safety-related functions shall be self-monitoring and conform to all of the following:
  (1) In the event of any single failure, the failure shall:
  - Not lead to the loss of the safety-related function(s)
  - Lead to the shutdown of the system in a safe state
  - Prevent subsequent operation until the component failure has been corrected
  - Prevent unintended startup of equipment upon correction of the failure

  (2) Provide protection equivalent to that of control systems incorporating hardwired/ hardware components
  (3) Be designed in conformance with an approved standard that provides requirements for such systems.
  The system shall satisfy the requirements for programmable devices (see NFPA 79 2015 9.4.3.1).
  Software and firmware-based controllers to be used in safety-related functions shall be listed for such use. (OSHA states listed as being certified by an NRTL)

Listing files of electronic devices for safety-related functions

UL has defined a special category for "Programmable Safety Controllers" (code NRGF) for implementation of the requirement in NFPA 79: 2007. This category involves control devices that contain software and are intended to be used for safety-related functions. IEC 62061 or EN ISO 13849-1, 2015, should be considered when taking into account functional safety and when using new technologies, e.g. wireless-based suspended operator panels incorporating electronic shutdown devices.

A precise description of the categories as well as a list of the devices that fulfill these requirements are provided in the Internet:

www.ul.com (http://www.ul.com) –> certifications directory –> UL Category code / Guide information –> search for category "NRGF"

In addition to Underwriters Laboratories Inc. (UL), TÜV SÜD Product Services GmbH (TUVPSG) and TUV Rheinland of North America, Inc. (TUV) can also act as an NRTL for such purposes. The products listed there can also be seen on the internet: The description entered in the listing can be accessed from the homepage (http://www.tuv.com) using the "ID" of the device (input of the required "ID" of the device into the search box (Search by ID, certificate, products ...)).

UL Functional Safety Mark Program (UL test symbol for functional safety)

As part of the introduction and further development of standards for functional safety in North America and Europe, UL is now also offering a UL certification mark for functional safety that is

granted to qualified companies already included in the normal UL certification process. More under www.ul.com/functionalsafety (http://www.ul.com/functionalsafety).

Risk analysis according to NFPA 79

When it comes to "machine safety", NFPA 79 make reference to other standards. In the context of risk analysis, for example, Appendix A of NFPA 79 refers to IEC 62061, ISO 13849-1 and 2, and also to ANSI, B11-TR3, and TR4.

ANSI B11

The ANSI B11 standards are common standards, which have been developed by associations - e.g. the Association for Manufacturing Technology (AMT), National Fire Protection Association (NFPA) and the Robotic Industries Association (RIA).

The risk analysis is used to assess the hazards that a machine presents. Risk analysis is an important requirement according to NFPA 79, ANSI/RIA 15.06 1999, ANSI B11.0 2010 and SEMI S10. A suitable safety technology/system can be selected using the documented results of a risk analysis - based on the specified safety class of the particular application.

For further details, refer to http://www.ansi.org (http://www.ansi.org)

2.4.3 Process industry in the US

The basic safety requirements of the OSHA for the process industry are defined in OSHA´s Process Safety Management of Highly Hazardous Chemicals, Explosives and Blasting Agents Standard (PSM), 29 CFR 1910.119 (www.osha.gov).

OSHA provides guidelines on this with: CPL 22.45A "Process Safety Management of Highly Hazardous Chemicals - Compliance Guidelines and Enforcement Procedures."

OSHA specifies that the process instrumentation must be implemented in accordance with generally accepted "good engineering practice". With a letter dated March 2000, OSHA clarified an inquiry from ISA, that ANSI/ISA 84.01 is a standard that is applicable nationwide and which OSHA recognizes as generally accepted "good engineering practice". However, in the same letter OSHA clearly stated that ISA 84.01 is not the only standard that is considered when fulfilling the requirements of 1910.119 (PSM).

CFR 1910.119 does not clearly state whether the requirements refer to the complete instrumentation. Two types of instrumentation are generally used in the process industry. "Safety Instrumented Systems" (SIS) and "Basic Process Control System" (BPCS). ANSI/ISA 91.01 defines that only the SIS is to be handled under OSHA regulations.

IEC 61511 "Functional safety: Safety Instrumented Systems for the process industry sector" is the IEC standard with the same scope as ISA 84.01. It was developed with significant involvement of the ISA and is to be included in the new edition of ISA 84.

A large proportion of processes fall within the scope of ISA 84.01, but does not formally fall under 29 CFR 1910.119 (PSM). Also in this case, the standard should be applied in order not to violate the basic requirements of the "Duties" section of the Occupational Safety and Health Act (OSHA).

2.4.4 Occupational safety and health regulations and safety standards in Canada

The Canada Labour Code

The Canada Labour Code is the legislation that is applicable to all industries in Canada. Part 2 of the Canada Labour Law governs occupational safety and health at the workplace. Under the Canadian Constitution, labor legislation is primarily a provincial responsibility. The Occupational Health and Safety Act (OHSA) defines the rights and duties of all parties in the workplace. Its main purpose is to protect employees against health and safety hazards at the place of work. The OHSA establishes procedures for handling risks at the place of work. It provides for enforcement of the law where compliance has not been voluntarily achieved. Regulations issued under OHSA identify specific requirements that must be complied with, set standards that must be met and prescribe procedures that must be followed to reduce the risk of accidents at the place of work.

Officials appointed by the central, provincial and territorial governments have the power to inspect workplaces. Further, they can enforce the law by applying all of the necessary legal resources. This addresses both employers and employees. This can include orders to cease work, fines and prosecution. These include, for example the Ministry of Labour (MoL) in Ontario or the Commission for Health and Safety at Work (CSST) in Quebec. The officials work closely with its agencies, safe workplace associations (SWAs), worker training centers and clinics and the Canadian Center for Health and Safety. Some of these key organizations include the Industrial Accident Prevention Association (IAPA) in Ontario and the Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail (IRSST) in Quebec. Insurance boards also play a key role when it comes to workplace safety. For example, the Workplace Safety and Insurance Board (WSIB) oversees the workplace safety education and training system, provides disability benefits within the scope of the accident insurance program, monitors the quality of healthcare through financial measures etc.

Links:

- Government of Canada, Occupational Health and Safety in Canada (www.hrsdc.gc.ca)
- Ministry of Labour (www.gov.on.ca/lab/)
- Commission de la santé et de la sécurité du travail (www.csst.qc.ca)
- Industrial Accident Prevention Association (www.iapa.on.ca)
- The Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail (www.irsst.qc.ca)
- Workplace Safety and Insurance Board (www.wsib.on.ca)

The Regulation for Industrial Companies according to the OHSA in Ontario, Regulation 528/00 Section 7 (PSHSR - Pre Start Health and Safety Review) has been in force since the 7th October 2000 - whereby the 2nd item in the table is specific to the safety of machinery. The employer is responsible for ensuring that all OHSA requirements and the associated regulations are complied with at the workplace. The regulation is, to a large extent, a performance-based standard. This means that the regulation defines what level of protection is to be provided and the objective to be achieved, but does not state how to achieve the required level protection.

Section 7 or Regulation 528/00 refers to current applicable standards in Canada. In order to fully comply with the requirements of Section 7, it is necessary to refer to other recognized applicable codes and standards, such as the Ontario Fire Code, the National Fire code, the NFPA codes and standards, CSA codes and standards, ANSI standards etc. The table shows and summarizes the applicable standards specific to machine safety issues. These are listed as support in fulfilling Section 7 of the Regulation.

A & B standards are generic safety standards that provide basic concepts and principles for the design and general aspects, or deal with one safety aspect or one type of safety related device that can be used for machines/processes.

C Standards are safety standards that deal with detailed safety requirements for a particular machine or process.

The following are the **most important standards for the safety of machinery in Canada** that accept the use of safety-related software and firmware-based controllers - including the latest revisions:

- CSA Z432-04 "Safeguarding of Machinery" accepts the use of programmable safety controls according to Section 8.3. This standard applies to protecting persons from the hazards arising from the use of mobile or stationary machinery. It specifies the criteria to be observed and the description, selection and application of guards and safety devices. Where a CSA standard exists for a specific type of machinery, then this must be applied together with this standard in order to achieve the best possible degree of protection for this specific situation.

CSA safety standards require safety-related software and firmware-based controllers to be certified by a Nationally Recognized Testing Laboratory (NRTL) or Standards Council of Canada (SCC) accredited testing laboratory according to a recognized standard applicable for safety devices.

2.5 Safety requirements for machines in Japan

To be used in Japan

Up until now, the situation in Japan was different than in Europe and the US. Contrary to Europe and the US, where the employer is responsible for safety at the workplace, in Japan, the employee must take every precaution that nothing happens to him. This is the reason that he may only use appropriately trained personnel on a machine.

Comparable, legal requirements regarding functional safety - as in Europe - therefore do not exist. Further, product liability does not play such a role as in the US. However, in the meantime, it has been recognized that today, this concept is no longer adequate. In Japan, a transition is being made to the basic principle that applies in both Europe and the US.

There is no legal requirement to apply standards. However, an administrative recommendation to apply JIS (Japanese Industrial Standards) exists: Japan bases its approach on the European concept and uses the fundamental standards as national standards.

For machine manufacturers and users that are active globally

Japanese machinery manufacturers that export their machines have a vested interest in complying with the European and American requirements so that their products fulfill the requirements and specifications of target markets. Companies with globally distributed production facilities also align themselves to the European and American requirements in order to have, as far as possible, standard safety concepts in all of their plants.

2.6 Important addresses

2.6.1 Europe

1. CEN members = sources for national editions of EN + prEN

AENOR	Asociación Española de Normalización y Certificación (AENOR) Génova 6 E-28004 Madrid Phone: +34 91 432 59 59 Fax: +34 91 319 27 97 E-mail: info@aenor.es (mailto:info@aenor.es) http://www.en.aenor.es (http://www.en.aenor.es)
AFNOR	Association Française de Normalisation 11 Avenue Francis de Pressensé F93571 Saint-Denis La Plaine Cedex Phone: +33 1 41 62 80 00 Fax: +33 1 49 17 90 00 http://www.afnor.org/en (http://www.afnor.org/en)
AS	Austrian Standard Heinestrasse 38 A-1020 Vienna Phone: +43 1 213 00 0 Fax: +43 1 213 00 355 E-mail: office@austrian-standards.at (mailto:office@austrian-standards.at) http://www.austrian-standards.at/ (http://www.austrian-standards.at/)
BSI	British Standards Institution 389 Chiswick High Road GB-London W4 4AL Phone: +44 208 996 90 01 Fax: +44 208 996 70 01 E-mail: cservices@bsigroup.com (mailto:cservices@bsigroup.com) http://www.bsigroup.com/ (http://www.bsigroup.com/)
CEN	European Committee for Standardization Avenue Marnix 17 B-1000 Brussels Phone: +32 25500811 Fax: +32 25500819 E-mail: infodesk@cenorm.be (mailto:infodesk@cenorm.be) https://www.cen.eu (https://www.cen.eu)
CENELEC	European Committee for Electrotechnical Standardization Avenue Marnix 17 B-1000 Brussels Phone: +32 25196871 Fax: +32 25196919 E-mail: info@cenelec. eu (mailto:info@cenelec.Eu) http://www.cenelec.eu/ (http://www.cenelec.eu/)

DIN	Deutsches Institut für Normung e.V. Burggrafenstr. 6 D-10787 Berlin Phone: +49 30 26 01 0 Fax: +49 30 26 01 12 31 E-mail: postmaster@din.de (mailto:postmaster@din.de) http://www.din.de (http://www.din.de)
DS	Dansk Standard Kollegievej 6 DK-2920 Charlottenlund Phone: +45 39 96 61 01 Fax: +45 39 96 61 02 E-mail: dansk.standard@ds.dk (mailto:dansk.standard@ds.dk) http://www.ds.dk/en/ (http://www.ds.dk/en/)
ELOT	Hellenic Organization for Standardization 50, Kifissou Street GR-121 33 Peristeri Phone: +30 210 21 20 100 Fax: +30 210 21 20 131 E-mail: info@elot.gr (mailto:info@elot.gr) http://www.elot.gr (http://www.elot.gr)
IBN/BIN	Bureau de Normalisation Rue de Birmingham 131 BE-1070 Bruxelles Phone: +32 2 738 01 11 Fax: +32 2 733 42 64 E-mail: info@nbn.be (mailto:info@nbn.be) http://www.nbn.be (http://www.nbn.be)
ILNAS	Institut luxembourgeois de la normalisation B.P. 10 34-40, avenue de la Porte-Neuve L-2010 Luxembourg Phone: +352 46 97 46 1 Fax: +352 22 25 24 E-mail: info@ilnas.public.lu (mailto:info@ilnas.public.lu) http://www.ilnas.public.lu (http://www.ilnas.public.lu)
IPQ	Instituto Portugues da Qualidade Rua Antonio Giao, 2 P-2829-513 Caparica Phone: +351 21 294 81 00 Fax: +351 21 294 81 01 E-mail: ipq@mail.ipq.pt (mailto:ipq@mail.ipq.pt) http://www.ipq.pt (http://www.ipq.pt)
IST	Icelandic Standards Skúlatún 2 IS-105 Reykjavik Phone: +354 520 71 50 Fax: +354 520 71 71 E-mail: stadlar@stadlar.is (mailto:stadlar@stadlar.is) http://www.stadlar.is/english/ (http://www.stadlar.is/english/)

NEN	Nederlands Normalisatie-Instituut Postbus 5059 NL-2600 GB Delft Phone: +31 152 690 390 Fax: +31 152 690 190 E-mail: info@nen.nl (mailto:info@nen.nl) http://www.nen.nl (http://www.nen.nl)
NSAI	National Standards Authority of Ireland Northwood, Stantry, IRL-Dublin 9 Phone: +353 1 807 38 00 Fax: +353 1 807 38 38 E-mail: info@nsai.ie (mailto:info@nsai.ie) http://www.nsai.ie (http://www.nsai.ie)
NSF	Norges Standardiseringsforbund P.O. Box 242 NO-1326 Lysaker Phone: +47 67 83 86 00 Fax: +47 67 83 86 01 E-mail: info@standard.no (mailto:info@standard.no) http://www.standard.no/en/ (http://www.standard.no/en/)
SFS	Suomen Standardisoimisliitto r.y. PO Box 130 Malminkatu 34 FIN-00101 Helsinki Finland Phone: +358 9 149 93 31 Fax: +358 9 146 49 25 E-mail: sfs@sfs.fi (mailto:sfs@sfs.fi) http://www.sfs.fi/en (http://www.sfs.fi/en)
SIS	Standardiseringen i Sverige Sankt Paulsgatan 6 S - 118 80 Stockholm Phone: +46 8 555 520 00 Fax: +46 8 555 520 01 E-mail: info@sis.se (mailto:info@sis.se) http://www.sis.se/en/ (http://www.sis.se/en/)
SNV	Schweizerische Normen-Vereinigung Burglistraße 29 CH-8400 Winterthur Phone: +41 52 224 54 54 Fax: +41 52 224 54 74 E-mail: info@snv.ch (mailto:info@snv.ch) http://www.snv.ch/ (http://www.snv.ch/)

UNI	Ente Nazionale Italiano di Unificazione Via Sannio 2 I-20137 Milano MI Phone: +39 02 70 02 41 Fax: +39 02 70 02 43 75 E-mail: uni@uni.com (mailto:uni@uni.com) http://www.uni.com/ (http://www.uni.com/)
UNMZ	Czech Office for Standards, Metrology and Testing ÚNMZ, Gorazdova 24 CZ-128 01 Praha 2 Phone: +420 224 915 489 Fax: +420 224 915 064 E-mail: posta@unmz.cz (mailto:posta@unmz.cz) http://www.unmz.cz/office/en (http://www.unmz.cz/office/en)

2. DIN – Deutsches Institut für Normung e.V., Leading standards committee regarding machines

NAM	Normenausschuss Maschinenbau (NAM) im DIN Lyoner Str. 8 Postfach 710864 60498 Frankfurt/M. Phone: +49 69 6603-1341 Fax: +49 69 6603-1557 http://www.nam.din.de/ (http://www.nam.din.de/)
NWM	Normenausschuss Werkzeugmaschinen Corneliusstraße 4 60325 Frankfurt Phone: +49 69 75608123 Fax: +49 69 75608111 http://www.nwm.din.de/ (http://www.nwm.din.de/)
AGSA, FNErg, FNFW, FNL, NAL, NALS, NAS, Nasg, NI, NKT, NMP, textile standard	Deutsches Institut für Normung e.V. Burggrafenstr. 6 D-10787 Berlin Phone: +49 30 26 01 0 Fax: +49 30 26 01 12 31 E-mail: postmaster@din.de (mailto:postmaster@din.de) http://www.din.de (http://www.din.de)
FNCA, FNKä, FWS, Naa, NAD, NL, NÖG, NRK, NÜA	DIN Deutsches Institut für Normung e.V. Zweigstelle Köln Kamekestraße 8 50672 Köln Phone: +49 221-57 13-509 Fax: +49 221-57 13-311

NA EBM	Normenausschuss Eisen-, Blech- und Metallwaren Gothaer Str. 27 40880 Ratingen Phone: +49 2102 940810 Fax: +49 2102 940851 http://www.naebm.din.de/ (http://www.naebm.din.de/)
NA FuO	Normenausschuss Feinmechanik und Optik Alexander-Wellendorff-Str. 2 75172 Pforzheim Phone: +49 7231/918827 Fax: +49 7231/918833 http://www.nafuo.din.de/ (http://www.nafuo.din.de/)
FAKAU	Normenausschuss Kautschuktechnik Zeppelinstr. 69 60487 Frankfurt/M. Phone: +49 69 7936-117 Fax: +49 69/7936-175 http://www.fakau.din.de/ (http://www.fakau.din.de/)
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE Stresemannallee 15 60596 Frankfurt/M. Phone: +49 69 6308-0 Fax: +49 69 6308-9863 E-mail: dke@vde.com (mailto:dke@vde.com) http://www.dke.de (http://www.dke.de)

3.Sources for technical regulations in Germany

For EC directives as well as legislation and regulations	Bundesanzeiger-Verlags GmbH Amsterdamer Straße 192 50667 Köln Phone: +49 221 97668-0 E-mail: service@bundesanzeiger.de (mailto:service@bundesanzeiger.de) https://www.bundesanzeiger.de/ (https://www.bundesanzeiger.de/)
For DIN standards and VDM sheets	Beuth Verlag GmbH Burggrafenstraße 6 10787 Berlin Phone: +49 30 2601-2260 Fax: +49 30 2601-1260 http://www.beuth.de/de/ (http://www.beuth.de/de/)

For VDE regulations as well as DKE and IEC standards	VDE-Verlag GmbH Bismarckstraße 33 10625 Berlin Phone: +49 30 38 38 68-21 Fax: +49 30 38 38 68-50 E-mail: kundenservice@vde-verlag.de (mailto:kundenservice@vde-verlag.de) https://www.vde.com/de/ (https://www.vde.com/de/)
For accident prevention regulations and ZH-1 documents from the Employers Liability Insurance Association	Carl Heymanns Verlag KG Luxemburger Straße 449 50939 Köln Phone: +49 221 94373-0 Fax: +49 221 94373-901
Information about standards, regulations, directives	Deutsches Informationszentrum für Technische Regeln (DITR) im DIN (Deutsches Institut für Normung) Burggrafenstraße 6 10787 Berlin Phone: +49 30 2601-0 Fax: +49 30 2628125

2.6.2 America

Additional information on machine safety is available under:

ANSI (American National Standards Institute)	http://www.ansi.org (http://www.ansi.org)
OSHA (Occupational Safety and Health Administration)	http://www.osha.gov (http://www.osha.gov)
NFPA (National Fire Protection Association)	http://www.nfpa.org (http://www.nfpa.org)
TUV Rheinland of N.A. Inc.	http://www.us.tuv.com (http://www.us.tuv.com)
UL (Underwriter Laboratories)	http://www.ul.com (http://www.ul.com)
CSA (Canadian Standards Association)	http://www.csa.ca (http://www.csa.ca)
CCOHS (Canadian Center for Occupational - Health and Safety)	http://www.ccohs.ca (http://www.ccohs.ca)
NIOSH (National Institute of Occupational Health and Safety)	http://www.cdc.gov/niosh/homepage.html (http://www.cdc.gov/niosh/homepage.html)
NSC (National Safety Council)	http://www.nsc.org (http://www.nsc.org)
ASSE (American Society of Safety Engineers)	http://www.asse.org (http://www.asse.org)
RIA (Robotic Industries Association)	http://www.robotics.org (http://www.robotics.org)
TÜV Süd	http://www.tuv-sud.com (http://www.tuv-sud.com)

Terms

3

A

Term	Reference	Relevant Standard
AOPD/AOPDDR	**Safety component, ESPE**	**ISO 12100-1**
	Active **o**ptoelectronic **p**rotection **d**evice responsive to **d**iffuse **r**eflection	
Actuator	**Positively-driven contacts**	
	Actuator, e.g. motor, valve, indicator lights, relays, motor contactors with positively-driven contacts etc.	
Requirement	**SRECS, SRCF**	**IEC 62061**
	(Demand) Event that initiates the SRECS to execute its SRCF.	
Requirement class **Demand rate without guard**	**Categories**	**DIN 19250 (no longer valid)** **IEC 61511-3**
	A set of requirements to implement a protective device that should provide safety-related performance of the equipment corresponding to the particular risk involved. The requirement class is obtained by multiplying the extent of the damage and the probability of occurrence (W, probability of the undesirable event occurring). Also refer to IEC 61511-3, Fig. E.2 (relationship between IEC 61511, DIN V 19250 and VDI/VDE 2180).	
Start inhibit	**EMERGENCY STOP (reset) safety relay**	**ISO 13850**
	The reset of the command shall not restart the machinery but only permit restarting (ISO 13850). The start inhibit prevents the safety device from automatically starting the machinery if the power supply voltage returns after an interruption.	
Test when starting	**Safety relay**	
	A manual or automatic test that is executed in order to test the safety-related control system after the power supply voltage was connected to the safety relay. An example of a test when starting is manually opening and closing a guard after the power supply voltage has been switched-on.	
Control (e.g. a contactor)	**Safety relay** **Redundancy, diversity**	
	Single-channel control (not redundant): The safety relay is controlled via a single signal transmitter contact or output. **Two-channel control (redundant):** The safety relay is controlled via two signal transmitter contacts or outputs. *Comment: For this type of control, the protective safety relay can reach, as a maximum, Category 4 according to ISO 13849-1 if the safety relay has a cross-circuit fault detection function, whereby the two signal transmitters must be part of the protective device (EMERGENCY STOP command device, guard). If a two-channel safety relay is controlled through one channel, then the signal transmitter contact or output must switch both channels of the safety relay (e.g. SIRIUS 3TK28 electronic).*	
ANSI B11	**OSHA, NFPA 79**	
	There are a series of additional Standards regarding industrial safety under ANSI B11; these additional Standards offer further instructions in order to achieve the required level of safety (US).	
ASIsafe	**PROFIsafe**	
	Safety-related communications via the Standard AS-Interface (AS-Interface Safety at Work).	
Non-equivalence	**Positively-driven**	
	Non-equivalence (anti-coincidence): Two different signals, e.g. NC and NO contacts.	

Term	Reference	Relevant Standard
Response time	**Safety relay**	
	The time between issuing the control command and actual execution: e.g. time between issuing the control command (e.g. EMERGENCY STOP) until the contacts of the load switching device open or until the drive comes to a complete standstill.	
Failure	**Failure that causes a dangerous situation**	**ISO 12100**
	A unit or device is no longer capable of fulfilling the requested function.	
Target failure value	**PFH_D**	**IEC 62061**
	(target failure value) intended PFH_D that is to be achieved in order to achieve the requirement(s) regarding safety integrity.	
Powering-down in an emergency	**Stopping in an emergency, procedure in an emergency situation, emergency, stop function, EMERGENCY STOP**	**IEC 60204-1, Annex D (Explanation of emergency operation functions), ISO 12100, ISO 13850**
	This is an operation in an emergency that is intended to disconnect the electrical energy to a complete installation or part of an installation if there is a risk of electric shock or another risk having an electrical cause. It should prevent or minimize impending or existing hazards for persons and damage to the machine, production materials and the environment *Note: Hazards include functional irregularities, incorrect machine functions, unacceptable properties and characteristics of the material being processed and human error.*	
Evaluation unit	**Safety relay, SRECS, SRP/CS**	
	A safety-related evaluation unit generates, dependent on the state of the connected signal transmitter, a safety-related output signal either according to a fixed assignment or according to programmed instructions.	
Automatic start	**Start**	**IEC 60204-1**
	A safety function is automatically restored (without an On button). This is e.g. permissible for moving protective guards that cannot be passed around or passed behind (EN ISO 12100-2) - however, not for an Emergency Stop device. This start type is only permissible after a hazard has been assessed.	
A Standard	**Harmonized Standard**	**ISO 12100**
	These are European Basic Safety Standards (type A) that are listed in the Machinery Directive: principles for design, terms (ISO 12100)/hazard analysis, risk assessment.	

B

Term	Reference	Relevant Standard
Beta β	**PFH_D**	**IEC 62061**
	Common cause failure factor (0.1 – 0.05 – 0.02 – 0.01): Common cause failure factor.	
B10	**Lambda λ, PFH_D**	**IEC 62061**
	The B10 value for devices subject to wear is expressed in the number of switching cycles: This is the number of switching cycles that during a lifetime test, 10% of the test objects have failed (or: Number of operating cycles after which 10% of the devices have failed). The failure rate for electromechanical components can be calculated using the B10 value and the operating cycle. **B10d** B10d = B10 / percentage of failures that cause a dangerous situation	
Basic device	**Basic device, expansion device, safety relay**	**ISO 13849-1**
	Equivalent term for basic unit.	
Command device (EMERGENCY STOP device)	**EMERGENCY STOP**	**ISO 13850**

Term	Reference	Relevant Standard
	A manually actuated control device that can be used to initiate an EMERGENCY STOP function.	
Actuator	**Separate actuator, position switch**	
	Coded, mechanical actuator element that opens the positively-driven contacts when withdrawn from the position switch (head).	
B Standard	**Harmonized Standard**	**ISO 12100**
	These are European Group Standards (type B) that are listed in the Machinery Directive: Type B2 - regarding general safety aspects (e.g. ergonomics, safety clearances EN ISO 13855) Type B1 - regarding systems and protective safety devices/guards (e.g. ISO 13849-1).	
ESPE	**Electro-sensitive protective equipment**	**IEC 61496**
	Control/monitoring function with output signal switching device, also known as OSSD, for example light curtains, light arrays, and laser scanners.	
Contactless position switch	**Position switches**	
	Contactless position switches (e.g. magnetically-operated switches).	

C

Term	Reference	Relevant Standard
C Standard	**Harmonized Standard**	**ISO 12100**
	These are European Product Standards (type C) that are listed in the Machinery Directive: Specialist standards – specific requirements for certain machines (e.g. presses EN 692).	
C	**B10, PFH_D**	**IEC 62061**
	Duty **C**ycle: Operating cycle (per hour) of an electro-mechanical component.	
CCF	**Lambda λ, PFH_D**	**IEC 61508, IEC 62061, ISO 13849-1**
	Common **c**ause **f**ailure: Failure with a common cause (e.g. short-circuit).	
CE	**Machinery Directive, Declaration of Conformity, Marking**	**Machinery Directive Art. 10-12, Annex III (EN ISO 17050)**
	The machine manufacturer (OEM) must provide a CE marking if he wishes to market the machine (Machinery Directive, "Protection against foreseeable misuse"). *Note: CE marking for the Low-Voltage Directive is not comparable with the CE marking for the Machinery Directive.*	
CEN CENELEC		
	Comité **E**uropéen de **N**ormalisation: European Committee for Standardization (European standardization committee). **C**omité **E**uropéen de **N**ormalisation **Elec**trotechnique: European Standards Committee for electrical engineering.	

D

Term	Reference	Relevant Standard
DC	**PL, PFH_D**	**ISO 13849-1, IEC 62061 (IEC 61508-2, Annex C)**
	Diagnostic **C**overage: Diagnostics coverage $\Sigma \lambda_{DD}/\lambda_{Dtotal}$, with • λ_{DD}, the rate of detected dangerous hardware failures • λ_{Dtotal}, the rate of total dangerous hardware failures	
Diagnostic test interval (T2)	**PFH_D, T2**	**IEC 62061**
	Diagnostic test interval (e.g. an EMERGENCY STOP button is possibly pressed every 8 hours). IEC 62061: refer to e.g. "Requirements on the behavior (of the SRECS) when detecting a fault in the SRECS" (safety-related electric control system).	
Discrepancy time Discrepancy time monitoring	**Simultaneity, synchronization time**	
	The discrepancy time monitoring tolerates, within a defined time window, that associated signals are not available at the same time.	
Diversity	**Redundancy**	**IEC 60204-1, IEC 61508**
	For redundant requirements with high reliability when fulfilling the safety task the paths should use different configurations (e.g. speed monitoring using a tachometer and centrifugal-force switch): i.e. different resources to execute the required function.	
Speed monitoring	**Safely-reduced speed**	
	Monitors the speed of a mechanical movement (e.g. drive) in a defined speed window. This can be realized without using sensors (current, frequency) or using encoders (generally incremental encoders).	

E

Term	Reference	Relevant Standard
E/E/PE	**Functional safety**	**IEC 61508**
	electrical and/or **e**lectronic and/or **p**rogrammable **e**lectronic technologies of safety related systems: electrical/electronic/programmable electronic systems	
Single fault tolerance, single fault safety	**Fault tolerance**	
	The demanded safety function is still guaranteed after one fault has occurred (e.g. from Category 3 onwards according to ISO 13849-1, i.e. one fault does not result in the safety function being lost.	
Switch-on time	**Safety relay**	
	The time between connecting the control command (e.g. EMERGENCY STOP, position switch, ON button) until the enable circuit closes.	
Switch-on cycle	**Self-monitoring**	
	The correct functioning of a component is automatically and cyclically monitored using a test routine.	
Occurrence time for multiple faults (CET)	**Requirement class**	**(no longer valid) DIN 19250**
	This is the time interval in which the probability that the occurrence of combined safety-critical multiple faults is sufficiently low for the requirement class involved. The time interval starts with the last instant in time at which the system involved was in a state that can be assumed as being fault-free for the requirement class being considered.	
Ground fault detection	**Cross-circuit fault, short circuit Short and ground fault proof routing**	**IEC 60204-1 DIN VDE 0100, Part 25**

Term	Reference	Relevant Standard
	The detection/identification of ground faults either immediately or as part of a cyclic self-monitoring routine - whereby the piece of equipment/device goes into a safe state after a fault condition has been detected/identified.	
First fault occurrence time	**Requirement class**	
	This is the time interval in which the probability that a safety-critical first fault occurs for the requirement class involved is sufficiently low. Fault-controlling measures are not taken into account. The time interval starts with the last instant in time at which the system involved was in a state that can be assumed as being fault-free for the requirement class being considered.	
Extension unit	**Basic device, safety relay**	
	An expansion device is a safety relay that can only be used in conjunction with a basic device to multiply contacts.	
ESPE	**ESPE, OSSD**	**IEC 61496-1**
	Electro-Sensitive Protective Equipment: electro-sensitive protective equipment.	

F

Term	Reference	Relevant Standard
Spring-actuated locking	**Position switch, tumbler mechanism**	**ISO 12100**
	The interlocking is realized using the closed-circuit principle (the spring interlocks and the magnet (solenoid) releases).	
Fault exclusion	**FMEA**	**ISO 13849-1** **ISO 13849-2**
	The ability to resist faults shall be assessed. In some components, certain faults can be excluded for the period in which the SRP/CS is used. For instance, a short-circuit can be excluded by routing cables in a safety-related fashion. If faults are excluded, a detailed justification shall be given in the documentation!	
Fault tolerance (hardware fault tolerance)	**Single fault tolerance, Category, zero fault tolerance, SIL, SRECS, SRP/CS**	**IEC 62061**
	Ability of an SRECS ("safety related electronic control system") of a sub-system or sub-system element to continue to execute a demanded function with the presence of faults or failures (fault tolerance).	
Fault tolerance time	**Fault tolerance**	
	Characteristic of the process that defines the time interval in which the process can receive incorrect control signals without a hazardous state occurring.	
Fault response times		
	The fault response time is the time required from the occurrence of a fault until the return to a safe state. It consists of the fault detection time plus the system cut-off time.	
FMEA	**Fault exclusion**	**IEC 60812**
	Failure **M**ode **E**ffect **A**nalysis: Failure mode and effect analysis (analysis of the fault effect, analysis of the failure effect). An analytical method to systematically and completely detect potential errors and failures of system components as well as their effects.	
Enable circuit **Enabling current path**	**Safety relay**	
	An enable circuit is used to generate a safety-related output signal. To the outside, enable circuits act as NO contact (from the functional perspective, safety-related opening is always considered). A single enable circuit that is internally redundantly configured in the safety relay (two channel) can be used for Category 3/4 according to ISO 13849-1. *Note:* *Enabling current paths can also be used for signaling purposes (i.e. not safety-relevant).*	

Term	Reference	Relevant Standard
FTA	**FMEA, fault exclusion**	**IEC 60812**
Fault Tree Analysis: Fault tree analysis (FTA). This analysis is used to gain more information about what caused the failure of the system. The analysis uses a deductive top-down method.		
Functional safety	**SRECS**	**IEC 62061, IEC 61508**
Part of the overall safety referred to the machine and the machine control system that depends on the correct function of the SRECS ("safety-relevant electrical control system"), safety-relevant systems that employ a different technology and external devices to minimize risk (taken from IEC 61508-4). *Note: Functional safety involves all aspects where the safety depends on the correct function of the SRECS, safety-relevant systems using another technology and external devices to minimize risk.*		
Function block (FB)	**SRCF**	**IEC 62061**
Smallest element of an SRCF ("safety-relevant control function"), whose failure can result in the failure of the SRCF.		
Function test		**IEC 60204-1**
The function test can either be realized automatically using the control system or manually by monitoring or testing, during operation and at defined time intervals or as combination depending on the requirement.		

G

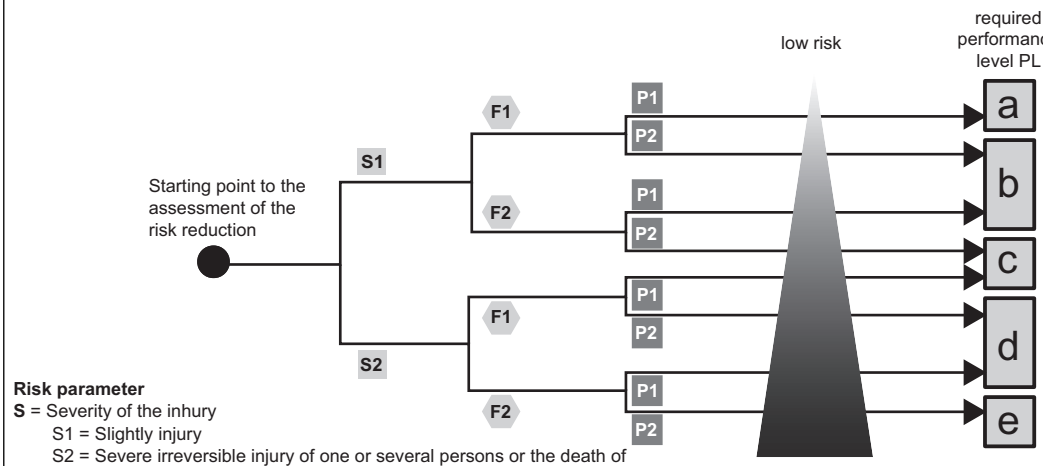
Term	Reference	Relevant Standard
Failure that causes a dangerous situation	**Failure**	**ISO 12100**
Any malfunction in the machinery, or in its power supply, that increases the risk.		
Hazard assessment	**Hazard, risk assessment, MD**	**ISO 12100**
Evaluation of a danger (resulting from a hazard) for the user.		
Hazard	**Hazard assessment, risk assessment, MD**	**ISO 12100**
The hazard (as a result of a specific event) represents danger for the user and can result in injury (potential source of damage).		
Separate actuator	**Position switch, tumbler mechanism**	
Coded, mechanical actuating element that opens positively-opening contacts when it is withdrawn from the position switch (head).		
Simultaneity Simultaneity monitoring	**Discrepancy time, two-hand circuit**	**EN 574**
Signal transmitters are monitored by the safety relay to ensure that they are actuated simultaneously to increase the functional safety of the protective safety device. The monitoring function is realized by checking the signal change of the signal transmitters within the specified time - the synchronous monitoring time. If this time is exceeded, an enable signal is not output. A simultaneous monitoring is specified for several protective safety devices.		
Basic device	**Expansion device, safety relay**	**ISO 13849-1**
This is a safety relay that includes all of the functions that must be available in the particular protective safety device.		

H

Term		Reference	Relevant Standard
Procedures in an emergency situation		**Shutting down in an emergency, stopping in an emergency, Emergency Stop function, EMERGENCY STOP**	**IEC 60204-1, Annex D (Explanation of emergency operation functions), ISO 12100, ISO 13850**
	Refer to switching-off and stopping in an emergency situation: All activities and functions in an emergency situation that are intended to end or resolve the emergency situation.		
Harmonized Standard		**Machinery Directive, A-B-C - Standards**	**ISO 12100**
	Type A (Basic Standards), Type B (Group Standards) and Type C (Product Standards) are listed in the Machinery Directive and therefore allow an assumption to be made that The Machinery Directive is complied with.		

K

Term	Reference	Relevant Standard
Categories (according to ISO 13849-1)	**Harmonized standard (B Standard)** **Risk analysis, risk assessment**	**ISO 13849-1**
	Categories of ISO 13849-1:2015 (B, 1, 2, 3 and 4) allow the performance of the safety-related part of a control to be evaluated when faults occur. **Category B:** The control must be designed so that it can withstand the expected effects System behavior: A fault can result in the loss of the safety function. **Category 1:** The requirements of B shall apply; well-proven safety-related components and principles shall be used. System behavior: The same as the system behavior of B however with a higher safety-related reliability. **Category 2:** The requirements of B must be fulfilled; in addition the safety function shall be checked at suitable intervals. System behavior: The occurrence of a fault can lead to the loss of the safety function between checks. The loss of the safety function will be detected by the test. **Category 3:** The requirements of B must be fulfilled - a single fault may not lead to the loss of the safety function; individual faults must be detected. System behavior: When a single fault occurs, the safety function is always performed. **Category 4:** The requirements of B must be fulfilled; the single fault must be detected when or before the safety function is next requested. System behavior: When faults occur the safety function is always performed; the faults are detected in time. **Connecting sensors in series for Category 3** • **EMERGENCY STOP:** May always be connected in series: It can be excluded that the command device will fail at the same time that it is pressed. • **Monitoring of protective doors:** Position switches may be connected in series if several protective doors are not simultaneously and regularly opened (as otherwise faults cannot be detected). **Connecting sensors in series for Category 4** • **EMERGENCY STOP:** May always be connected in series: It can be excluded that the command device will fail at the same time that it is pressed. • **Monitoring of protective doors:** Position switches must never be connected in series because every hazardous fault must always be detected (independently of the operating personnel).	

Term	Reference	Relevant Standard
	Risk diagram according to ISO 13849-1  **Risk parameter** **S** = Severity of the inhury S1 = Slightly injury S2 = Severe irreversible injury of one or several persons or the death of one person **F** = Frequency and/or exposure time to the hazardous condition F1 = Seldom up to qiute often F2 = Frequent up to continuous **P** = Possibility of avoiding the hazards P1 = Possible under specific conditions P2 = Scarcely possible	
Cascading input	**Safety relay** **Safety-relevant routing**	
	Safety, single-channel input of a safety relay that is internally evaluated just like a sensor signal: Logical AND operation with the other signal transmitter/sensor inputs: If a voltage is not connected, the safety relay safely disables the enable circuits (outputs). *Note: By excluding a fault (short-circuit) in the electrical cabinet, Category 4 according to ISO 13849-1:2015 can be reached; by safely and appropriately routing cables and conductors, this fault can also be excluded outside the cabinet.*	
Designation	**MD, CE, Declaration of Conformity**	**MD, (EN ISO 17050)**
	Certification from the machine manufacturer that the machine complies with all of the relevant Machinery Directive regulations and can therefore be marketed. The user is informed of this with the CE marking.	
Declaration of Conformity	**CE, Machinery Directive,** **Marking**	**MD, (EN ISO 17050)**
	Certification from the machinery construction company (OEM) that the machine fulfills all of the relevant regulations of the Machinery Directive and may therefore be marketed. The user is informed about this with the CE marking. In addition to the Machinery Directive, other directives (e.g. EMC) may also be necessary for correct granting of a CE mark for a machine.	
Short-circuit	**Cross-circuit, testing**	
	A conductive connection - without almost any resistance - between two electrical conductors at a specific voltage.	

L

Term	Reference	Relevant Standard
Lambda **λ**	**PFH, PFH_D** **B10, MTTF**	**IEC 62061**
	Rate of failure: Rate of failure for safe (λ_S) and hazardous (λ_D) faults.	

Term	Reference	Relevant Standard
Laser scanner	**ESPE, AOPD, OSSD**	**IEC 61496-1**
A safety laser scanner provides personnel protection at machines, robots, conveyor systems, vehicles - both when stationary and also for mobile applications. This is an optical scanner that scans areas and operates contactlessly by periodically transmitting pulses of light. An integrated rotating mirror deflects these light pulses into the working zone. Persons or objects that enter the defined protective zone reflect the light pulses, which means that they are detected. The coordinates of the "obstructions" are calculated from the propagation time of the light pulses. The area to be monitored can be freely defined within specific limits using a PC. If the "obstruction" is located in a defined protective field, then the scanner shuts down its safety-related outputs therefore initiating a safety-related stop function.		
Light grid, light curtain	**ESPE, AOPD, OSSD**	**IEC 61496-1**
When one or several light beam(s) is/are interrupted, the device changes its switching state.		
Light barrier	**ESPE, AOPD, OSSD**	**IEC 61496-1**
When a light beam is interrupted, the device changes its switching state.		
Life time	**PFH_D, T1**	**IEC 62061**
The expected lifetime [h] of a component that is required for a safety-related function.		

M

Term	Reference	Relevant Standard
Magnetic field locking	**Position switch, tumbler mechanism**	**ISO 12100**
The interlock is realized using the open-circuit principle (the solenoid locks, the spring releases).		
Magnetically-operated switch	**Contactless position switch, reed contacts**	
This comprises a coded arrangement of several reed contacts whose switching state changes under the influence of the associated magnetic field. Tampering/manipulation is not possible as a result of the coding.		
Manual reset	**Start, restart inhibit**	**ISO 13849-1, IEC 60204-1**
A function to restore one or several safety functions before the machine restarts: After a stop command has been initiated by a protective device, the stop state must be maintained until a manual reset device is actuated and the safe state has been reached for a restart.		
Manual start	**Start, manual reset**	**ISO 13849-1, IEC 60204-1**
The safety function is restored by monitoring a static signal, e.g. pressing an On button. A manual start is only permissible up to Category 3 according to ISO 13849-1, as there is no protection against manipulation. This start type is only permissible after a hazard assessment has been made.		
Machine control	**Categories SRP/CS**	**ISO 13849-1**
Part of the control (automation) that does not necessarily operate in a safety-related fashion, e.g. generates a signal when a fault occurs.		
Machinery	**Machinery Directive**	

Term	Reference	Relevant Standard
	The machine with moving parts represents a possible danger (hazard) for the user. *Note:* *A machine (according to the Machinery Directive) is:* • *an assembly of linked parts or components, at least one of which moves, with the appropriate actuators, control and power circuits, etc., joined together for a specific application, in particular for the processing, treatment, moving or packaging of a material,* • *an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole,* • *interchangeable equipment modifying the function of a machine, which is placed on the market for the purpose of being assembled with a machine or a series of different machines or with a tractor by the operator himself in so far as this equipment is not a spare part or a tool.*	
Machinery directive	**Machine, harmonized standard**	
	DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND THE COMMITTEE from the 17th of May 2006 to harmonize the legal and administrative regulations for the Member States for machinery.	
Multi-fault tolerance, multi-fault safety	**Fault tolerance**	
	The demanded safety function is still guaranteed even after several faults have occurred.	
Signaling circuit **Current signaling path**	**Safety relay**	
	A signaling circuit is used to generate a non safety-related output signal. Signaling circuits can be implemented with either NC or NO contact functionality.	
Minimum actuation time	**Safety relay**	
	This is the shortest time required for the control command to start the device (restart).	
Machinery Directive	**Machinery Directive** **Machine, harmonized standard**	
	Machinery **D**irective	
MTBF	**MTTF, MTTR**	**ISO 13849-1**
	Mean **T**ime **B**etween **F**ailure : Is the sum of **MTTF** (mean time to failure) and **MTTR** (mean time to repair). The Mean Time Between Failure is the average time that expires in normal operation of a device or piece of equipment before a new fault occurs.	
MTTF/MTTF$_D$	**MTBF, MTTR, PL**	**ISO 13849-1**
	Mean **T**ime **T**o **F**ailure/**M**ean **T**ime **T**o **D**angerous **F**ailure: Time up to a failure or dangerous failure. The **MTTF** can be determined for components by analyzing field data or using predictive data. For a constant failure rate, it is the average value for the failure-free operating time **MTTF = 1/λ** , whereby λ is the failure rate of the device (seen from a statistical perspective it can be assumed that 63.2 % of the components involved have failed after the MTTF has expired).	
MTTR	**MTBF, MTTF**	**ISO 13849-1**
	Mean Time To Repair: The MTTR is significantly shorter than the MTTF.	
Muting	**ESPE**	**IEC 61496-1, ISO 13849-1**
	A type of bypass function: The safety-related function is correctly and deliberately disabled using additional sensors for a limited time. (ISO 13849-1: A safety function is temporarily and automatically bypassed) *Note: This is used in the field to make a differentiation between persons and objects.*	

Term	Reference	Relevant Standard
Muting sensors	**Muting, ESPE**	**IEC 61496-1**
	Signal transmitters that are used for muting operation in order to detect a body/object for which an ESPE should not shut down.	

N-type

Term	Reference	Relevant Standard
Proximity switch		
	This can either be inductive, capacitive or optical. It is a switching element that changes its switching state when bodies/objects or liquids approach it (depending on the version). Proximity switches are mainly equipped with semiconductor outputs.	
Line supply failure buffering	**Safety relay, ESPE**	
	Maximum time for which the power supply voltage can be briefly interrupted and this does not result in an incorrect device function or the device being reset.	
NFPA79 (USA)	**NRTL, OSHA**	
	Electrical Standard for Industrial Machinery in the US: This standard applies to electrical equipment of industrial machines with rated voltages less than 600 V. The new Edition NFPA 79-2002 includes basic requirements for programmable electronics and buses if these are used to implement safety-relevant functions. When these requirements are fulfilled, electronic controls and buses may also be used for EMERGENCY STOP functions, stop Categories 0 and 1 (refer to NFPA 79-2002 9.2.5.4.1.4). Contrary to EN 60204-1, NFPA 79 specifies, that for EMERGENCY STOP functions, the electrical energy must be disconnected using an electro-mechanical device.	
Emergency	**Switching off in an emergency** **Stopping in an emergency** **Procedure in an emergency situation**	**IEC 60204-1, Annex D (Explanation of emergency operation functions)** **ISO 12100**
	A dangerous situation that needs to be urgently stopped or a counter-measure urgently found. An emergency can occur: • In normal operation of the machine (e.g. as a result of manual intervention or external influence) • as a consequence of malfunction or a failure of any part of the machine	
EMERGENCY SWITCHING OFF	**Switching off in an emergency** **EMERGENCY STOP**	**ISO 13850** **IEC 60204-1 Annex D**
	A procedure in response to an emergency which is intended to disconnect the supply of electrical energy to either a complete installation or part of an installation if there is a risk of electric shock or another risk as a result of electric energy: The danger should be removed as quickly as possible, e.g. using a "disconnector" in a main supply feeder.	
EMERGENCY STOP	**Stopping in an emergency** **EMERGENCY SWITCHING-OFF**	**ISO 13850** **IEC 60204-1 Annex D**
	This is procedure in response to an emergency that is intended to stop a process or movement that could result in danger (stopping). *Note: The EMERGENCY STOP function is initiated by the single action of a person. According to ISO 13849-1 this must always be available and capable of functioning. The operating mode is not taken into account.*	
EMERGENCY STOP command device	**Mushroom-shaped pushbutton, EMERGENCY STOP, cable-operated switch, positively-opening**	**ISO 13850** **IEC 60204-1**
	Switching device that is actuated in hazardous situations that causes the process, machine or plant to be stopped. This must have positively-opening contacts, should be easy to reach and should be tamper-proof so that it cannot be manipulated.	

Term	Reference	Relevant Standard
EMERGENCY STOP device	**EMERGENCY STOP**	**ISO 13850, IEC 60204-1**
	An EMERGENCY STOP device is a protective device for initiating the appropriate procedure in an emergency situation.	
NRGF **NIPF** **NIPM**	**NRTL, NFPA79**	
	"Categories" for UL 508 (the basis standard for the NRTL listing): NRGF: Programmable Safety Controllers NIPF: Active Opto-electronic Protective Devices NIPM: Active Opto-electronic Protective Devices Responsive to Diffuse Reflection	
NRTL	**NFPA79, OSHA,** **NRGF, NIPF, NIPM**	
	Nationally **R**ecognized **T**esting **L**aboratory: Here, products can be listed so that they may be used and applied in the US (according to NFPA79). An NRTL listing corresponds to a certification. Use for Safety Products: The requirement "listed for such use" should be understood as follows. The basis standard for the listing is UL 508. An NRTL (e.g. UL) confirms that the equipment/device involved is in compliance with UL 508 by entering it into a "list".	
Zero fault tolerance	**Fault tolerance**	
	After fault occurs, the demanded safety function is no longer guaranteed.	

O

Term	Reference	Relevant Standard
OSHA	**NRTL**	
	Occupational **S**afety and **H**ealth **A**ct (www.osha.gov) For legislation regarding occupational safety and health there is a significant difference between the US and Europe. In the US, there is no standard legislation that applies across all of the US States that defines and specifies the responsibility of the manufacturer/supplier. In the US, there is a general requirement that employers must ensure safety at work. The OSHA Rules under 29 CFR 1910 include general requirements for machines (1910.121) and a series of specific requirements for certain machine types. The requirements listed are extremely specific but detailed technical information is not provided. In addition to the OSHA regulations, it is important to carefully observe the up-to-date standards of organizations such as NFPA and ANSI as well as the extensive product liability legislation in the US.	
OSSD	**ESPE**	**IEC 61496-1**
	Output **S**ignal **S**witching **D**evice - this is part of the ESPE that goes into the OFF state if the safety light barrier, light curtain, light grid or the monitoring device responds.	

P

Term	Reference	Relevant Standard
Parts count method	**Lambda λ, MTTF**	**IEC 61709**
	IEC 61709 "Electric components - Reliability - Reference conditions for failure rates and stress models for conversion" (IEC 61709:2017) describes a method and conversion models for calculating failure rates but does not contain failure rates of its own.	

Term	Reference	Relevant Standard
PL **Performance Level**		**ISO 13849-1**
	Capability of safety-relevant parts to execute a safety function under predictable conditions (that should be taken into account) to fulfill the expected risk minimization: from **PL** a (highest failure probability) to **PL** e (lowest failure probability). Beyond this, the Siemens factory standard SN 29500, in addition to the above mentioned methods and models, also provides standard failure rates for electronics and electromechanical components.	
PDF **PFD**		**IEC 61508, IEC 62061**
	Probability of **d**angerous **f**ailure: Probability of dangerous failures. **P**robability of **f**ailure on **d**emand: Probability of failure when a safety function is initiated/ demanded.	
PFH **PFH_D**	**B10, C, CCF, Lambda λ**	**IEC 62061**
	Probability of **f**ailure per **h**our: Probability of dangerous failure per hour to determine "random integrity". **P**robability of **d**angerous **f**ailure per **h**our: Probability of a dangerous failure per hour.	
Mushroom pushbutton	**EMERGENCY STOP command device**	**ISO 13850, IEC 60204-1,** **EN / IEC 60947-5-5**
	EMERGENCY STOP command device that has the shape of a mushroom.	
Bounce time	**Position switches**	
	This is the time between the first and last closing or opening of a contact (for standard position switches, with snap-action contacts, approx. 2 to 4 ms).	
Proof test **Proof test interval**	**PFH_D, T1**	**IEC 62061**
	Proof test: Repeated test that is executed to detect faults in an SRECS so that - if necessary - the system can be brought into an "as new state", or as close as is practically possible to an "as new state" (taken from IEC 61508-4).	
PROFIsafe	**ASIsafe**	
	Safety-related communications via the Standard PROFIBUS (black channel).	
Position switches	**Standard position switch, tumbler mechanism, separate actuator, positively-opening**	**EN 50041, EN 50047, EN ISO 14119,** **EN / IEC 60947-5-1 Annex K**
	Part of the interlocking mechanism of a protective guard that changes its switching state as a function of the control command that is mechanically issued. There are position switches with and without tumbler mechanism, with and without separate actuator. There are different types of position switch that can be used to establish interlocking mechanisms. For type-1 interlocking devices: • Position switch with integrated actuator (e.g. with roller lever) • Hinge switches • Standard position switches (design in accordance with EN 50041 or EN 50047) For type-2 interlocking devices: • Position switch with separate actuator • Position switch with separate actuator with tumbler	

Q

Term	Reference	Relevant Standard
Cross-circuit fault	**Categories, short-circuit, testing**	**ISO 13849-1**
This can only occur for multi-channel control circuits for equipment/devices and is a short-circuit between channels (e.g. in a two-channel sensor circuit).		
Cross-circuit fault detection	**Categories (especially 3/4) Testing**	**ISO 13849-1**
This is the ability of a safety relay to detect cross-circuit faults - either immediately or as part of a cyclic monitoring routine: The device goes into a safe condition after the fault has been detected.		

R

Term	Reference	Relevant Standard
Redundancy		
The use of more than one device or system is intended to ensure that when the functions of one device or system fails, then another device is available to execute this function. *Note: With redundancy (e.g. multi-channel structure), the tolerance with respect to faults is increased. This can be used to increase the level of safety and/or availability.*		
Reed contact	**Contactless position switch, magnetically-operated switch**	
Reed contacts are closed by magnets and open again as soon as the magnet has been withdrawn: This means that they respond to magnetic fields.		
Series circuit	**Categories**	**ISO 13849-1**
Sensors, e.g. EMERGENCY STOP command devices, are connected in series and evaluated by means of a safety relay.		
Reset	**Start, safety relay**	
Switch-on function (ON) that represents a restart inhibit function.		
Reset button	**Start, safety relay**	
The ON button represents a restart inhibit in a safety relay that is only withdrawn after it has been actuated.		
Risk (risk elements)	**Risk assessment, danger**	**ISO 12100**
The combination of probability that damage will occur and the extent of the damage.		
Risk analysis Risk assessment	**Risk, danger**	**ISO 12100**
The standard ISO 12100 lists techniques that are required and necessary to carry out a risk assessment. The risk assessment initially involves a risk analysis followed by a risk evaluation.		
Release time	**Safety relay**	
The time from the control command or the supply voltage being removed until the enable circuit is opened.		

Term	Reference	Relevant Standard
Feedback circuit	**Safety relay**	**ISO 13849-1**
	This is used to monitor controlled actuators (e.g. relays or load contactors with positively-driven contacts). The evaluation unit can only be activated when the feedback circuit is closed. *Note: The NC contacts (these are positively-driven contacts) of the load contactors to be monitored are connected in series and integrated into the feedback circuit of the safety relay. If a contact welds in the enable circuit, then it is no longer possible to re-activate the safety relay because the feedback circuit remains open* *The (dynamic) monitoring of the feedback circuit does not have to be safety-related because it is only used for fault detection: The ON button is generally switched using the positively-driven contacts of the actuator in series (fault detection when starting).*	

S

Term	Reference	Relevant Standard
Pressure sensitive mats, safety switching strips, switching edges, switching buffer elements	**Safety-related component**	EN ISO 13856-1
	These are signal transmitters whose signal state changes when they are stepped-on (pressure sensitive mat) or are de-formed (safety switching strips, switching edges). Pressure sensitive mats generate a cross-circuit fault when they are stepped on.	
Protective door monitor	**Safety relay**	**ISO 13849-1**
	This is an evaluation unit that monitors the position of position switches at a protective guard. It generates a safety-related output signal if this protective door is closed. Today, conventional safety relays handle this function (e.g. 3TK28).	
Cable-operated switch	**Command device, EMERGENCY STOP command device**	**ISO 13850, EN 60204-1, EN / IEC 60947-5-5**
	This is mainly used in EMERGENCY STOP protective safety devices and is a signal transmitter whose switching state changes if a cable/line - connected to the switch - is pulled or the line/cable breaks. This device is used to monitor long system lengths (e.g. conveyor belts).	
Self-monitoring	**Diagnostic test interval, T2**	**IEC 62061**
	The correct functioning of a component is automatically and cyclically monitored using a test routine.	
Sensitive protection equipment (SPE)		**ISO 12100**
	Sensitive **p**rotection **e**quipment: Equipment operating on a mechanical principle (neither contactless nor electro-sensitive).	
SFF	**DC, PFH_D**	**IEC 62061**
	Safe failure fraction Component of the total failure rate of a subsystem that does not result in a dangerous failure. *Note: The component of safe failures (SFF) can be calculated using the following equation:* *$(\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$,* *whereby λ_S is the rate of non-dangerous failures,* *λ_{DD} the rate of dangerous failures that are detected by the diagnostic functions and λ_D the rate of dangerous failures.*	
Safely-reduced speed		**IEC 60204-1, IEC 61800**

Term	Reference	Relevant Standard
	The function allows an axis or spindle to be monitored for a specified speed. When setting-up, e.g. the speed limits should be applied corresponding to the valid C Standard - e.g. 2 m/min for axes. In many machines, the safely-monitored speed is also used during automatic processing and machining. In order to prevent damage to the machine or to the production materials, it is possible to safely prevent maximum speeds and velocities from being exceeded. The drive manufacturer must provide the appropriate protective measures that permit only the machinery construction company (OEM) to change the speed/velocity limit values. Further, each time that the speed/velocity limit values are re-set or modified, an acceptance test must be carried-out. During this acceptance test, the commissioning (start-up) engineer must accelerate the drive up to the speed/velocity limit value and document that the safety-related response operates perfectly. This must be documented in a form provided by the drive manufacturer. *Note: Can also be used to detect an "overspeed" condition.*	
Safety clearance	**ESPE**	**DIN EN ISO 13855**
	Defines the necessary clearances and velocities of a person that are used as input parameter to assess a hazard (e.g. for light curtains, laser scanners, ...).	
Safe operational stop	**Safe stopping process**	**IEC 60204-1, IEC 61800-5-2**
	Contrary to safe standstill, for a safe operating stop, the drives remain completely in the closed-loop control mode. The higher-level two-channel safety-related control is permanently supplied with the position values and initiates a safety-related response if the drive moves away from the standstill position. The safe operating stop function is always used where frequent interventions must be made in the process, where it is not practical to isolate the power supply using hardware - or is not possible for technological reasons. Application Examples include setting-up operation and running-in CNC programs.	
Safe Torque Off (Safe standstill)	**Safe stopping process**	**IEC 60204-1, IEC 61800-5-2**
	For Safe Torque Off, the energy feed to the drive is safely interrupted. It is not permissible that the drive generates a torque and therefore cannot make any hazardous movement. It is not necessary to monitor the standstill function. The energy feed to the drive can be disconnected using contacts but this measure does not have to be used. **External control:** Several drive systems allow the Safe Torque Off to be externally controlled using terminals. In this case, using the manufacturer's documentation a check should be made as to whether it is necessary to process the feedback contact in the machine control. Further, it cannot be completely excluded that a safety relay does not jam or does not pull-in. A safety-related circuit is only obtained when the positively-driven feedback contact is processed in a safely-related fashion. When the safe standstill is functioning perfectly, the relays that can be controlled axis by axis bypass the enable circuit of the relay combination for the protective doors. If the relay fails, then the higher-level line contactor is de-energized. **Internal control:** If the Safe Torque Off is internally controlled - e.g. using the redundant computer system of the drive control - then the drive manufacturer must ensure that the relay is safely read back. Examples for an internal control include, for example, shutdown (trip) after a fault response. This can occur, for instance after speed or position limit values have been exceeded or when carrying-out the forced checking procedure of the shutdown path (test stop).	
Safe separation • **of circuits**	**safe routing, position switch**	**IEC 61140** **(EN 50178)**
	The objective is operational safety, protection against voltage transfer, for different voltages in a cable or piece of equipment that must be isolated for the highest voltage (protection against electric shock).	
Safe stopping process **Stopping in an emergency**	**EMERGENCY STOP**	**IEC 60204-1, ISO 13850**

Term	Reference	Relevant Standard
	For the safe stopping process the drive is stopped corresponding to the hazardous situation. In so doing, the electrical, electronic and electro-mechanical equipment and devices that are necessary to decelerate the drive must be incorporated in the safety analysis - taking into account additional protective measures. The following are suitable, for example: • Controlled stopping with a safely monitored deceleration time • Controlled stopping where the braking ramp is safely monitored • Uncontrolled stopping using mechanical brakes Application examples include, for example: Enabling switches, electrical interlocking of moving protective devices and guards or response after faults are detected.	
Safety-related component	**Machinery Directive**	**Machinery Directive Annex V**
	These are listed in Annex V of the Machinery Directive, e.g.: • Sensor-controlled protective devices for personnel (light curtains, pressure-sensitive mats, electromagnetic detectors) • Automatically moving protective devices and equipment at machines according to the letter A, numbers 9, 10 and 11 • Two-hand circuits • Rollover protection structure • Protection against falling objects *Note: In the Machinery Directive Article 1 (2c), a safety component is a component,* *— that is used to guarantee a safety function,* *— that is brought onto the market separately,* *— the failure and/or malfunction of which endangers the safety of persons, and* *— that is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function.*	
Protective device	**Machinery**	**Machinery Directive**
	These are required wherever hazards can occur for man, machine and the environment.	
Safety combination	**Evaluation unit, safety relay**	
	This is an old term for a safety switching device or evaluation unit.	
Safety relay	**Evaluation unit, SRECS, SRP/CS**	
	This is another term for a safety combination or evaluation unit. A safety-related evaluation unit generates, dependent on the state of the connected signal transmitter, a safety-related output signal either according to a fixed assignment or according to instructions that have been programmed/parameterized.	
Safety-related routing	**Protective separation (of circuits)**	**IEC 61140** **(protection against electric shock)**
	Cables with basic isolation may not be routed along sharp edges or should be routed in steel pipes and ducts (protection Class 2): Is used to exclude faults (highest insulation).	
SIL, Safety Integrity Level **SIL CL, SIL claim limit**	**PFD, PFH_D, SRECS**	**IEC 61508** **IEC 62061**

Term	Reference	Relevant Standard
	One of three possibilities to define safety integrity specifications of the safety function that can be assigned to SRECS. Safety integrity level 3 is the highest possible level, level 1 the lowest. SIL claim limit (EN 62061): The Safety Integrity Level (SIL) that can be claimed for the SRECS must be less than or equal to the lowest value of the SIL claim limit for the safety integrity of the hardware, systematic integrity and the structural restrictions of one of the subsystems. *Note: The target measure to determine the performance of a safety function (functional safety) – this term was introduced into the English Edition of IEC 61508: A SIL (PFH_D) is determined in IEC 62061 for failure probability and a PL is determined in ISO 13849-1.*	
Mirror contact	**Positively-driven contacts**	**EN IEC 60947-4-1**
	A typical application of mirror contacts is to provide highly reliable monitoring of the switching state in control circuits of machinery.	
SRCF	**Functional safety, SRECS**	**IEC 62061**
	(**S**afety-**R**elated **C**ontrol **F**unction) Safety-relevant control function executed by the SRECS with a defined level of integrity is intended to maintain the safe state of the machine or to prevent a direct increase in the risks.	
SRECS	**Functional safety, SRP/CS safety relay, evaluation unit**	**IEC 62061**
	(**S**afety-**R**elated **E**lectrical **C**ontrol **S**ystems) Safety-related electrical control system of a machine whose failure results in an immediate increase in the risks.	
SRP/CS	**Machine control, evaluation unit, safety relay**	**ISO 13849-1**
	(**S**afety-**R**elated **P**arts of **C**ontrol **S**ystems). Safety-related part of a control that responds to the safety-related input signals and generates safety-related output signals.	
Start (automatic, manual or monitored)	**Pushbutton monitoring, manual reset**	**ISO 13850, IEC 60204-1, ISO 13849-1**
	A safety relay can either be manually or automatically started as well as a monitored start. For a manual or monitored start, an enable signal is generated after pressing the On button after the input image has been checked and after a positive test of the safety relay. This function is also known as steady-state operation and is specified e.g. for Emergency Stop protective devices (IEC 60204-1, conscious action). Contrary to the manual start, the monitored start evaluates a signal change of the On button. This means that the On button cannot be manipulated/tampered with (misuse). The manual start is permissible up to Category 3 according to ISO 13849-1 - however, a monitored start must be used for Category 4 according to ISO 13849-1. With an automatic start, an enable signal is generated without manual agreement after the input image has been checked and a positive test of the safety relay completed. This function is also known as dynamic operation and is not permissible for Emergency Stop protective devices. Guards that are not possible to walk behind can operate with the automatic start. This start type is only permissible after a hazard has been assessed.	
Standard position switch	**Tumbler mechanism, separate actuator**	**EN 50041, EN 50047**
	The designs (enclosure types) of standard position switches are sub-divided into small (EN 50047) and large (EN 50041) enclosure types.	
Position monitoring	**Position switches**	
	Using the positioning monitoring function, the position of a guard is monitored - e.g. a protective door - using a suitable signal transmitter and safety relays.	

Term	Reference	Relevant Standard
Stopping in an emergency	**Stopping in an emergency, procedure in an emergency situation, emergency stop function, EMERGENCY STOP**	**IEC 60204-1, Annex D (Explanation of emergency operation functions)** **ISO 12100** **ISO 13850**
An action in an emergency that is intended to stop a process or motion that would result in a hazard. Stopping in an emergency must be assigned either a stop category 0 or 1. The stop category applicable for stopping in an emergency must be defined using the risk assessment for the particular machine.		
Standstill monitoring	**Stop function, safely reduced speed, safe stopping process**	**ISO 13850** **IEC 60204-1**
A drive function is monitored - either without encoder (sensorless) or with encoder - for a defined speed: This corresponds to a speed monitoring with N = 0 rpm.		
Stop function	**Shutting down in an emergency, stopping in an emergency**	**ISO 13850** **IEC 60204-1**
Stop Category 0 Uncontrolled stopping by immediately disconnecting the energy feed to the machine drive elements. **Stop Category 1** Controlled stopping where the energy feed is only interrupted once standstill has been reached. **Stop Category 2** Controlled stopping where the energy feed is still maintained even at standstill.		
Structural restriction	**SIL, SIL CL, sub-system**	**IEC 62061**
Number of structural requirements that restrict the SIL that can be made applicable for a sub-system.		
Synchronous monitoring time	**Two-hand circuit, discrepancy time**	**EN 574**
This is the time in which both hands must simultaneously actuate the control elements in order to generate a safety-related output signal (this is generally < 0.5 s).		
Systematic safety integrity	**SIL, SIL CL, SRECS, sub-system**	**IEC 61508, IEC 62061**
Part of the safety integrity of an SRECS or its sub-systems regarding its tolerance to systematic failures with dangerous effects.		

T

Term	Reference	Relevant Standard
T1	**PFH_D** **Proof test interval, lifetime**	**IEC 62061**
Shortest value of the proof test interval (repeat test) or lifetime [h] (e.g. T1 = 10^5 [h] corresponds to an expected lifetime of 100,000 hours or approx. 11.4 years). *Note: In EN 62061, this value is required to estimate – using a simplified basis – the probability of dangerous, random hardware failures of subsystems.*		
T2	**PFH_D**	**IEC 62061**
Diagnostic test interval: Diagnostic test interval IEC 62061: Refer to "requirements on the behavior (of the SRECS) when detecting a fault in the SRECS" (safety-related electric control system) *Note: The mean time to recovery, which is considered in the reliability model, needs to take the following facts into account: diagnosis testing- interval, MTTR and every other delay before recovery.*		

Term	Reference	Relevant Standard
Pushbutton monitoring	**Start, monitored start Categories**	**ISO 13849-1**
	The function of the pushbutton (safety-relevant device) is monitored by a dynamic signal change when the pushbutton is actuated. *Note: For example, a plant or system is prevented from being powered-up because of a short-circuited pushbutton (e.g. as a result of manipulation/tampering).*	
Sub-system	**Function block (FB), SRECS**	**IEC 62061**
	Unit of the SRECS design architecture at the uppermost level, whereby a failure in any one sub-system results in a failure of the safety-related control function. *Note: A complete sub-system can comprise a number of identifiable and separate sub-system elements that, if they are combined, can implement function blocks assigned to the sub-system.*	
Sub-system element	**Sub-system, SRECS**	**IEC 62061**
	Part of a sub-system that includes an individual component or a group of components.	
Testing	**Cross-circuit fault**	**ISO 13849-1**
	Test pulse with the appropriate suppression time to detect faults.	
Guard	**Position switches**	**Fixed guards: DIN EN ISO 13857 Safety of machinery - Safety distances to prevent hazard zones being reached by upper and lower limbs, EN 349, EN 811, EN 14120** **Movable guard: EN ISO 14119 Safety of machinery - Interlocking devices associated with guards, DIN EN ISO 13855, DIN EN ISO 13855** **Type A Standard: ISO 12100**
	Guard or a part of the machine that is specifically used to prevent entry and protect against hazards. *Note: Depending on the particular type of construction, this can be implemented using protective grids, protective doors, enclosures, covers, paneling, fences, shield etc.*	

U

Term	Reference	Relevant Standard
Monitored start	**Start, manual reset**	**ISO 13850, IEC 60204-1, ISO 13849-1**
	The safety function is restored by monitoring a dynamic signal change, e.g. using an On pushbutton. This is absolutely mandatory for a Category 4 emergency stop protective device since it provides protection against manipulation. This start type is only permissible after a hazard has been assessed.	

V

Term	Reference	Relevant Standard
Presumption of conformity	**Machinery Directive, type A-B-C Standards**	
	If the listed, harmonized Standards (in the Machinery Directive) are fulfilled then it can be presumed that the Machinery Directive was fulfilled.	
Interlocking equipment and devices	**Protective safety device, position switch, tumbler mechanism**	**ISO 12100 EN ISO 14119 Safety of machinery - Interlocking devices associated with guards**

Term	Reference	Relevant Standard
	This is a mechanical, electrical or another interlocking device that has the function of preventing the operation of a machine element under certain specific conditions (generally as long as a guard is not closed).	
Intended architecture	**Categories, redundancy**	**ISO 13849-1**
	The intended architectures show the logical representation of the system structure for each category. The intended architectures are shown for the compiled SRP/CS starting at the point where the safety-relevant signals are generated and ends at the output of the power transmission element.	

W

Term	Reference	Relevant Standard
Restart inhibit	**Start, monitored start**	**ISO 13850** **IEC 60204-1**
	Using the restart inhibit the evaluation unit is prevented from issuing a release after a shutdown, after the operating mode of the machine was changed or after a change was made to the actuation type. The restart inhibit is only withdrawn using an external command (e.g. ON button). *Note:* *ISO 13849-1 refers to "manual return" – an internal function of the SRP/CS to restore given safety functions before a machine is restarted.*	
Recovery time	**Safety relay**	
	This is the minimum time required in order to re-start the equipment after the control command or the power supply voltage was interrupted.	

Z

Term	Reference	Relevant Standard
Tumbler mechanism	**Position switches**	**EN ISO 14119 Safety of machinery - Interlocking devices associated with guards (ISO 14119)**
	The objective of a tumbler mechanism is to maintain a protective guard in the closed position. Further, it is connected to the control, so that the machine cannot start if the protective guard is not closed and interlocked and so that the protective guard is kept interlocked until there is no risk of injury. *Note: Up to Category 3 according to ISO 13849-1, the tumbler mechanism does not have to be safely controlled; however, for Category 4 according to ISO 13849-1 this must always be controlled in a safety-related fashion.* *From Category 3 according to ISO 13849-1, the position of the interlocking device (solenoid) must be individually monitored and may not be connected in series with the monitoring of the separate actuator (due to poor fault detection).*	
Enabling switch	**Evaluation unit, safety relay**	
	An enabling switch is a manually operated signal transmitter which can be actuated to withdraw the protective effect of protection equipment. It is not possible or permissible to initiate hazardous states using the enabling switch alone - a "second, conscious" start command is required for this.	
Positively-driven contacts	**Actuator, relay**	**EN 50205, IEC 60947**
	For positively-driven contacts of a relay/contactor, the NC contact and NO contact may never be simultaneously closed over the complete lifetime of the device. This also applies if the relay/contactor is in an incorrect state (faulted). Example: If an NO contact is welded, then all of the other NC contacts of the relay/contactor involved remain open no matter whether the relay/contactor is energized or not.	

Term	Reference	Relevant Standard
Positive opening ⊖	**Position switch, EMERGENCY STOP command device**	**IEC 60204-1, IEC 60947-5-1**
For positively-opening contacts, the contacts separate as a direct result of a defined motion of the switch actuator using non-sprung mechanical linkage. For the electrical equipment of machinery, the positively-opening contacts are expressly specified in all safety circuits. *Note: Positively-opening contacts are designated according to IEC 60947-5-1 by the symbol (arrow in a circle) (function to protect persons).*		
Two-hand circuit	**Synchronous monitoring time**	**EN 574, IEC 60204-1**
Is a device, which requires that it is simultaneously actuated by both hands for a minimum time (generally < 0.5 s) in order to initiate and maintain machine operation as long as a hazardous situation is present. This represents a measure that only protects the person who is actuating the device. *Note: In order to initiate the hazardous operation, both operator elements (two-hand buttons) must be simultaneously actuated. The enable signal is withdrawn if one of the two operator elements is released during the potentially hazardous motion. The hazardous operation can only be re-initiated if both operator elements have returned to their initial position and are then actuated again simultaneously.*		
Two-hand operating console	**Synchronous monitoring time, two-hand circuit**	**EN 574**
This is a device to implement a two-hand circuit.		
Two-fault safety	**Category** **SIL**	**ISO 13849-1** **IEC 62061**
This means that after two faults have occurred, the specified, safety-related function is guaranteed.		
Two-channel structure	**Redundancy, categories, intended architecture**	**ISO 13849-1**

Attachment

4

4.1 Important type A, B and C standards

Basic Standards (type A)		
Principles for risk assessment	EN ISO 12100	Principles, list of hazards

Group Standards (type B1) regarding safety aspects		
Fires and explosions	EN 1127-1	Explosion protection, methodology
	EN 13463-1	Use of non-electrical equipment
	EN 13478	Fire protection
	EN 13821	Minimum ignition energy
Ergonomic design principles	EN 614-1	Design principles
	EN 547-3	Human body measurements
	EN 1005-3	Force limits, machine actuation
	EN ISO 14738	Workstations for machinery
Hazardous substances	EN 626-1	Reduction of risks to health
	EN 626-2	Verification procedures
	EN 1093-1	Air pollution; test procedures
Noise	EN ISO 3740	Guidelines, measuring the sound pressure level
	EN ISO 4871	Measuring data, subsequent checking
	EN ISO 11200	Guidelines, measuring the sound pressure level
	EN ISO 11688-1	Low-noise designs
	EN ISO 11689	Comparison of emissions
Hygiene	EN 1672-2	Food & beverage machinery (type C Standard)
Laser	EN 12626	Machinery using lasers
	EN 60825-1	Laser equipment
	EN ISO 11553	Machinery using lasers
Vibration	EN 1299	Vibration isolation
Safety distances	EN ISO 13857	Upper limbs
	EN 349	Avoiding parts of the human body from being crushed
	EN ISO 13857	Lower limbs
	EN 13855	Approach speed
Radiation	EN 12198-1	Assessment, risk minimization
Temperatures	EN 563	Hot surfaces

Group Standards (type B2) for systems and protective devices/guards		
Lighting	EN 1837	Lighting integrated into machinery
Electrical equipment	EN 60204-1	General requirements

Group Standards (type B2) for systems and protective devices/guards		
Fluid power systems	EN 4413	Hydraulics
	EN 983	Pneumatics
Protective devices/guards	EN 14120	Design of protective guards
	EN ISO 14119	Interlocking equipment and devices
	EN 12874	Protection against flashback
	EN 60825-4	Laser protection devices
	EN 61496-1	Electro-sensitive protective equipment
Signals and actuators	EN 457	Auditory danger signals
	EN 842	Visual danger signals
	EN 894-1	Interaction with displays and actuators
	EN 894-2	Design of displays
	EN 894-3	Design of actuators
	EN 981	Auditory/visual systems
	EN 61310-1	Visible, audible, tactile signals
	EN 61310-2	As above, designation
	EN ISO 13850	Emergency Stop devices
Controllers	EN 574	Two-hand circuits
	EN ISO 13849-1	Safety-related categories, design guidelines
	EN ISO 13849-2	Validation
	EN 1037	Unexpected start
	EN 1760-1	Pressure sensitive mats, switching boards
	EN 1760-2	Switching strips, switching bars
	EN 62061	Safety-relevant electrical, electronic and programmable electronic control systems
Access to / into machines	EN 547-1	Whole body access
	EN 547-2	Access openings
	EN 547-3	Human body measurements
	EN ISO 14122-1	Access selection between two levels
	EN ISO 14122-2	Working platforms, walkways
	EN ISO 14122-3	Railings, stairs, ladders
	EN ISO 14122-4	Vertical ladders

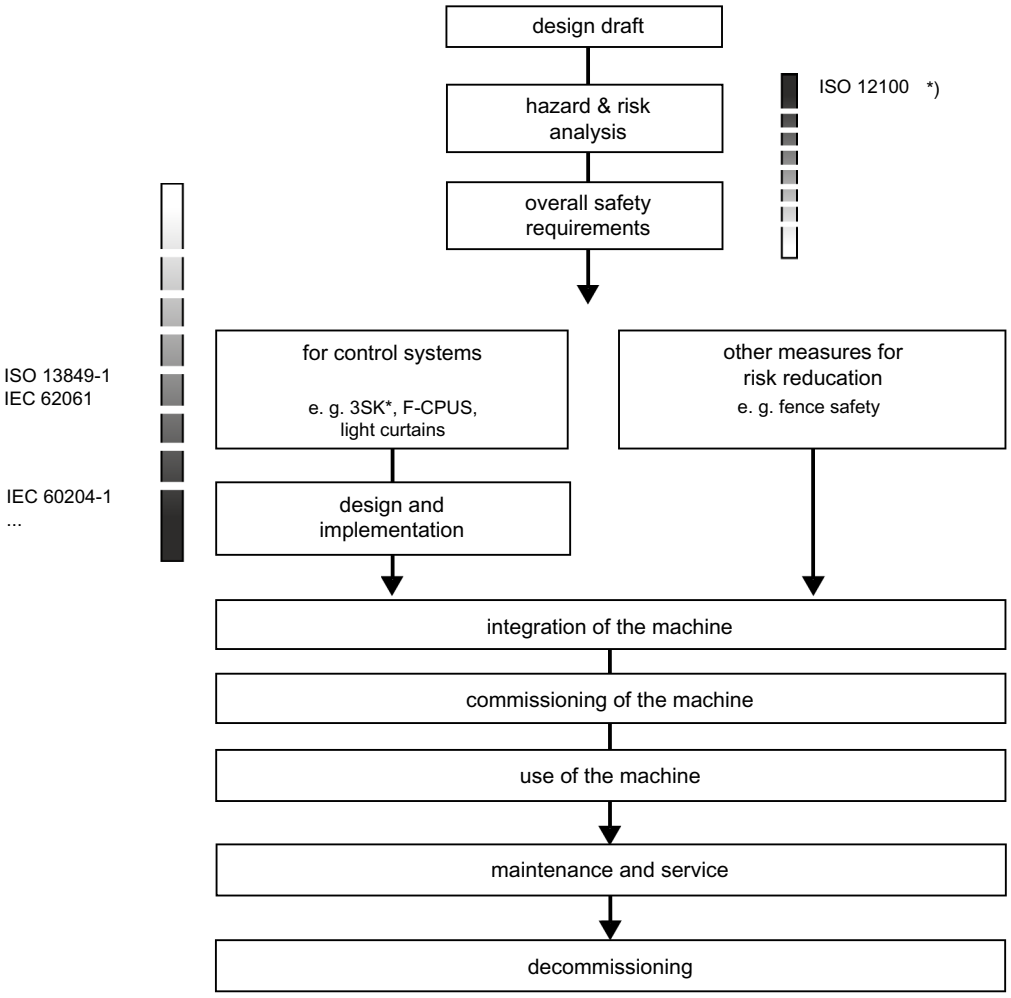
Additional type C standards are listed in the Safety Integrated System Manual.

4.2 Other important documents

- **IEC 61326-3-1**
  EMC and functional safety
- **IEC 61508 (VDE 0803)**
  Functional safety of safety-related electrical, electronic, programmable electronic systems
- **ISO Guide 51**
  Guidelines for the inclusion of safety aspects in Standards
- **Low-Voltage Directive 2014/35/EU**
  Relating to electrical equipment designed for use within certain voltage limits.
  It is the most important regulatory instrument for the safety of electrically-operated devices.

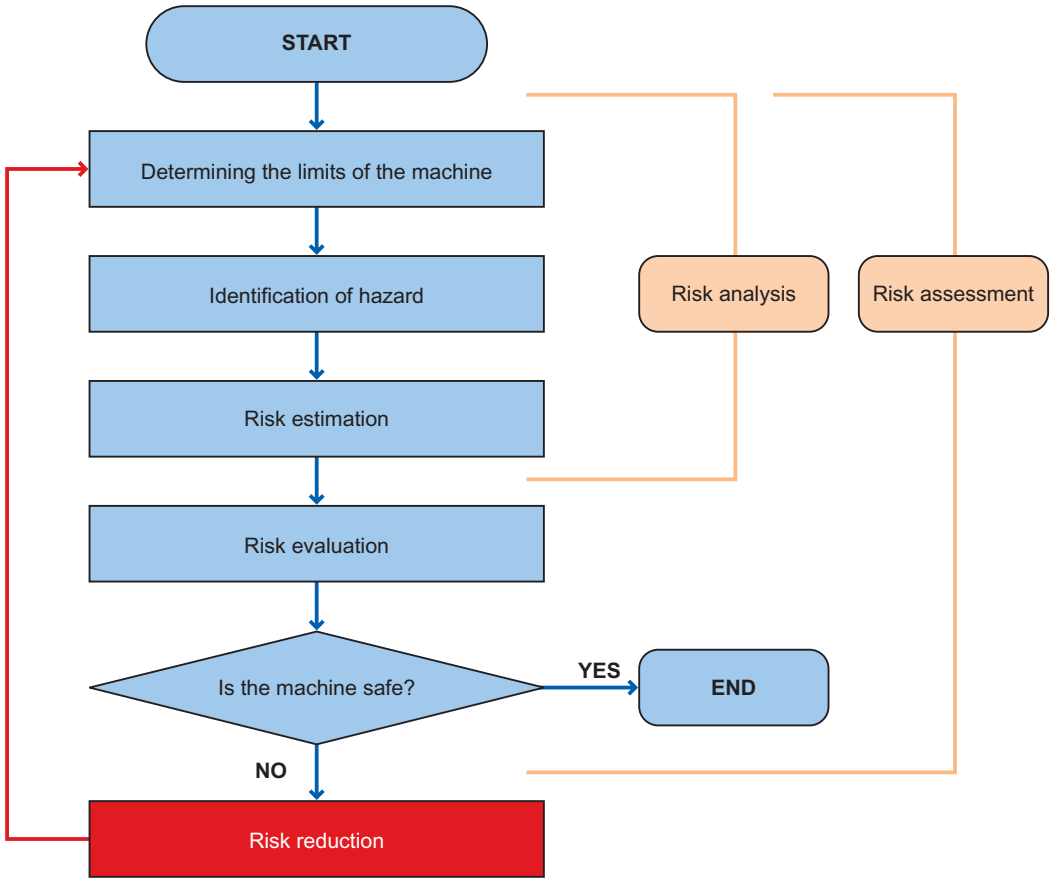
4.3 Risk assessment according to ISO 12100

Lifecycle of a machine



Risk reduction process

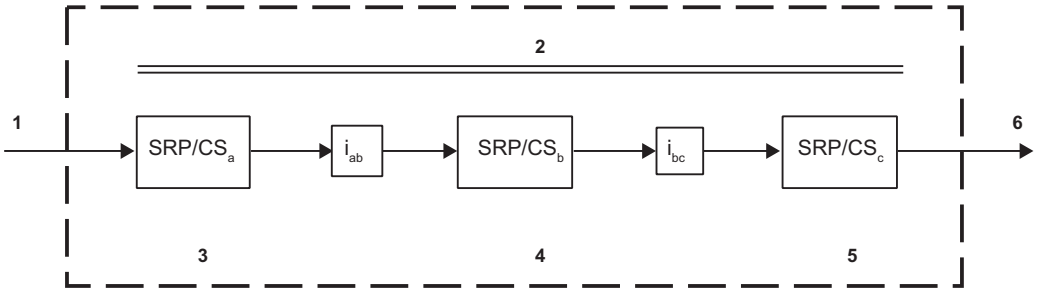
Risk reduction according to ISO 12100



Risk reduction and the selection of appropriate protective measures are not part of the risk assessment. For a further explanation, see Section 5 of EN ISO 12100.

4.4 Determining the Performance Level

Safety function according to ISO 13849-1



1 Initiation means, e.g. manual input
2 Typical safety function (input, logic, output)
3 Input
4 Logic
5 Output
6 Machine actuator, shutdown device, brake(s)
i_{ab} Interface between safety functions a and b
i_{bc} Interface between safety functions b and c

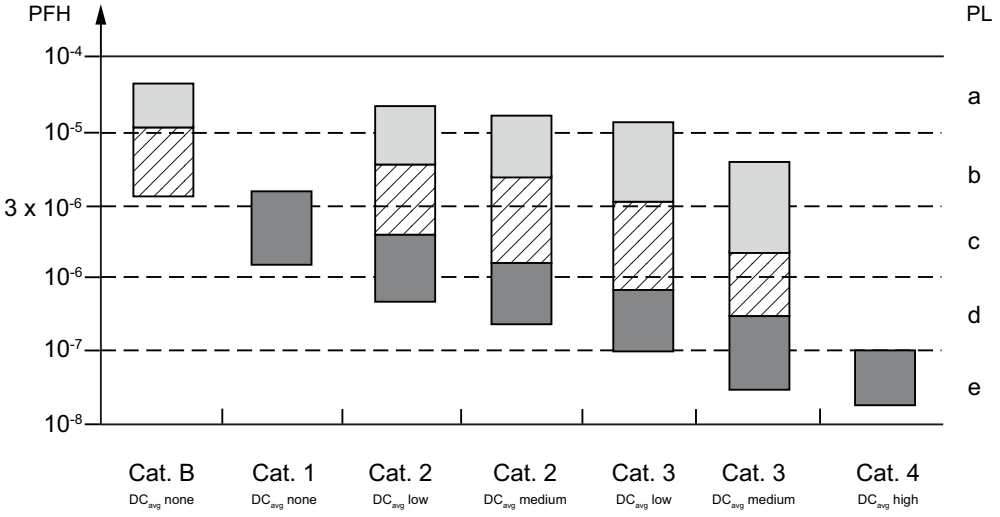
Correlation between the Performance Level (PL) and the Safety Integrity Level (SIL)

Performance Level (PL) according to EN ISO 13849-1	Average probability of a dangerous failure per hour [1/h]	Safety Integrity Level (SIL) according to EN 61508 / IEC 62061
a	$\geq 10^{-5}$ to $< 10^{-4}$	No special safety requirements
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

Note 1:
The magnitude of each hazardous situation in this standard is classified in five levels "a" to "e", whereby the risk reduction contributed by the SRP/CS is low in "a" and high in "e".

Note 2:
It should be noted that performance levels "b" and "c" together cover only one order of magnitude on the PDF (Probability of Dangerous Failure per hour) scale (or one level on the SIL scale).

Assignment of performance level ↔ relation between the categories DC, $MTTF_D$ and PL according to ISO 13849-1



Categories are the basic parameter to reach a special PL. They specify the required behavior of the SRP/CS in terms of fault resistance.

- Category B is the basic category. The occurrence of a fault can result in loss of the safety function.
- In Category 1, the improved resistance to faults is mainly achieved through the selection and application of components.
- In Categories 2, 3, and 4, the improved performance in terms of the specified safety function is mainly achieved by improving the structure of the SRP/CS.

More information can be found in the "Terminology" section under "Categories".

$MTTF_D$ Mean time to dangerous failure

$MTTF_D$ of each channel = low (>10 years)

$MTTF_D$ of each channel = medium (>30 years)

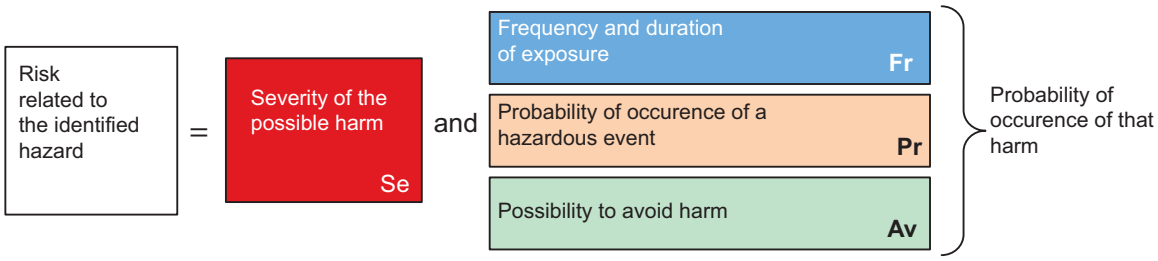
$MTTF_D$ of each channel = high (30 to 100 years)

Table 4-1 Simplified procedure to evaluate the PL achieved by an SRP/CS

Category (Cat.)	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**None**	**None**	**Low**	**Average**	**Low**	**Average**	**High**
$MTTF_D$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Average	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

4.5 SIL assignment

SIL estimate according to IEC 62061



Risk assessment and safety measures

Document No.:
Part of:

Product:
Issued by:
Date:

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Consequences	Severity Se	Class Cl					Frequency and Duration Fr		Probabiliy of occurence of a hazardous event Pr				Avoidance Av	
		3-4	5-7	8-10	11-13	14-15								
Death, loosing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≥ 1 per h	5	Common	5				
Permanent, loosing fingers	3		OM	SIL 1	SIL 2	SIL 3	< 1 per h bis ≥ 1 per day	5	Likely	4				
Reversible, medical attention	2			OM	SIL 1	SIL 2	< 1 per day bis ≥ 1 per 14 days	4	Possible	3			Impossible	5
Reversible, first aid	1				OM	SIL 1	< 1 per 2 week to ≥ 1 per year	3	Rarely	2			Possible	3
							< 1 per year	2	Negligible	1			Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measures	Safe

Comments

OM Other methods

SIL and PFH_D

Safety Integrity Level (SIL)	Probability of a dangerous failure per hour
1	$10^{-6} \leq PFH_D < 10^{-5}$
2	$10^{-7} \leq PFH_D < 10^{-6}$
3	$10^{-8} \leq PFH_D < 10^{-7}$

Probability of failure, electro-mechanical components

Failure rate
$\lambda = 0.1 \cdot C/B10$

$\lambda = 0.1 \cdot 10/10^6 = 10^{-6}$ C: Cycle, actuating cycle per hour B10: Number of actuating cycles after which 10 % of the devices have failed (IEC 61810-2)
Probability of failure (dangerous, in one hour)
$PFH_D = \lambda_D \cdot 1h$
$\lambda = \lambda_s + \lambda_d$ λ_s safe hardware failures λ_d dangerous failures

Architecture A: Zero fault tolerance, without diagnostic function (refer to Category 1)
Zero fault tolerance: One fault results in the loss of the safety function diagnostics: Without fault detection
$\lambda_D = \lambda_{D1} + ... + \lambda_{Dn}$

Architecture B: Single fault tolerance with a diagnostic function
Single fault tolerance: One fault does not result in the loss of the safety function diagnostics: Without fault detection
$\lambda_D = (1 - \beta)^2 \cdot \lambda_{De1} \cdot \lambda_{De2} \cdot T1 + \beta \cdot (\lambda_{De1} + \lambda_{De2})/2$
β: Factor of errors with common cause T_1: Life expectancy

Architecture C: Zero fault tolerance, with diagnostic function (refer to Category 2)
Zero fault tolerance: One fault results in the loss of the safety function diagnostics: With fault detection
$\lambda_D = \lambda_{De1} \cdot (1 - DC_1) + ...+ \lambda_{Den} \cdot (1 - DC_n)$
DC: Diagnostics coverage

Architecture D: Single fault tolerance, with diagnostic function (refer to Category 3/4)
Single fault tolerance: One fault does not result in the loss of the safety function diagnostics: With fault detection
$\lambda_D = (1 - \beta)^2 \cdot \{[\lambda_{De1} \cdot \lambda_{De2} \cdot (DC_1 + DC_2) \cdot T_2/2] + [\lambda_{De1} \cdot \lambda_{De2} \cdot (2 - DC_1 - DC_2) \cdot T_1/2]\} + \beta \cdot (\lambda_{De1} + \lambda_{De2})/2$
T_2: Diagnostic test interval

4.6 Drive controls with integrated safety functions

Definitions of the safety functions in IEC 61800-5-2, Adjustable speed electrical power drive systems, Safety Requirements, Functional.

Abbr.	Name	Functions
STO	Safe Torque Off	This function prevents force-generating energy from being supplied to the motor. This safety sub-function corresponds to an uncontrolled stop according to IEC 60204-1, Stop Category 0
SS1	Safe Stop 1	Motor decelerates, the braking ramp is monitored and STO after zero speed has been reached or STO after a delay time has expired (stop Cat 1 acc. to IEC 60204)
SS1-d	Safe Stop 1 deceleration controlled	Initiate and control the magnitude of motor deceleration within selected limits to stop the motor and execute the STO function when the motor speed falls below a defined limit value.
SS1-r	Safe Stop 1 ramp monitored	Initiate and monitor the magnitude of motor deceleration within selected limits to stop the motor and execute the STO function when the motor speed falls below a defined limit value.
SS1-t	Safe Stop 1 time controlled	Trigger motor deceleration and execute the STO function after an application-specific delay
SS2	Safe Stop 2	Motor decelerates, the braking ramp is monitored and SOS after zero speed has been reached or SOS after a delay time has expired (stop Cat 2 acc. to IEC 60204)
SS2-d	Safe Stop 2 deceleration controlled	Initiate and control the magnitude of motor deceleration within selected limits to stop the motor and execute the SOS function when the motor speed falls below a defined limit value.
SS2-r	Safe Stop 2 ramp monitored	Initiate and monitor the magnitude of motor deceleration within selected limits to stop the motor and execute the SOS function when the motor speed falls below a defined limit value.
SS2-t	Safe Stop 2 time controlled	Trigger motor deceleration and execute the SOS function after an application-specific delay
SOS	Safe Operating Stop	Motor is at zero speed and opposes external forces (i.e. is not moved by external forces)
SLA	Safely-Limited Acceleration	This function prevents the motor from exceeding the defined limit value for acceleration and/or deceleration.
SAR	Safe Acceleration Range	This function maintains motor acceleration and/or deceleration within defined limit values.
SLS	Safely-Limited Speed	The drive is prevented from exceeding a speed limit value
SSR	Safely Speed Range	This function maintains the motor speed within defined limit values.
SLT	Safely-Limited Torque	This function prevents the motor exceeding the defined torque (or when using a linear motor, the defined force).
STR	Safe Torque Range	This function maintains the motor torque (or when using a linear motor, the defined force) within the defined limit values.
SLP	Safely-Limited Position	This function prevents the motor shaft (or the drive unit if a linear motor is being used) from exceeding the defined position limit(s).
SLI	Safely-Limited Increment	This function prevents the motor shaft (or the drive unit if a linear motor is being used) from exceeding the defined limit value of a position increment. NOTE With this function, the PDS(SR) monitors the incremental movements of a motor as follows: – an input signal (e.g. start) triggers an incremental movement with a defined maximum path, whereby safe monitoring is used; – once the path necessary for this incremental movement has been covered, the motor is stopped and remains in this state as appropriate for the application.
SDI	Safe Direction	This function prevents the motor shaft from moving by more than a defined amount in the unintended direction

Abbr.	Name	Functions
SMT	Safe Motor Temperature	This function prevents the motor temperature(s) from exceeding a defined upper limit value/ defined upper limit values
SCA	Safe Cam	This function supplies a safety-related output signal to indicate whether the motor shaft lies within a defined range.
SSM	Safe Speed Monitor	This function supplies a safety-related output signal to indicate whether the motor speed is below a defined limit value.
SBC	Safe Brake Control	This function supplies a safety-related output signal/safety-related output signals to control an external brake/external brakes.

1. Additional safety functions are permissible.
2. No differentiation between safety functions for machines and processes.
3. Response when a limit value is violated:
   Must be individually defined as the optimum response depends on the system architecture and application.
4. Response for a safety function fault:
   Must be individually defined as the optimum response depends on the system architecture and application.

4.7 Evaluation of safety functions using the Safety Evaluation in the TIA Selection Tool

Description of functions

The Safety Evaluation in the TIA Selection Tool offers you valuable support when evaluating safety functions on machines and in plants.

This function in the TIA Selection Tool guides the user step-by-step from the definition of the safety system structure, through the selection of components, all the way to the determination of the achieved safety integrity according to ISO 13849-1 and IEC 62061. The procedure is the same for both standards with regard to handling. The focus is on the fast and simple execution of a safety calculation together with the system configuration.

All Siemens product data are directly available in the TIA Selection Tool through the pre-implemented Siemens VDMA library. It is also possible to integrate and use VDMA libraries from other manufacturers. You will also be supported by extensive Getting started instructions. Users receive the results of the evaluation in the form of a standard-compliant report that can be integrated into the documentation as a verification of safety.

The desktop version always ensures flexible working. Regular updating of the TIA Selection Tool ensures that the calculations are always carried out in accordance with the current standards and that the latest technical data of all safety-relevant components from Siemens are always accessed.

The application of standards and the use of certified products minimizes costs and risk. Siemens Safety Integrated products are certified in accordance with the relevant manufacturer's standards and can be easily called-up in the tool together with the manufacturer's data.

Prerequisites

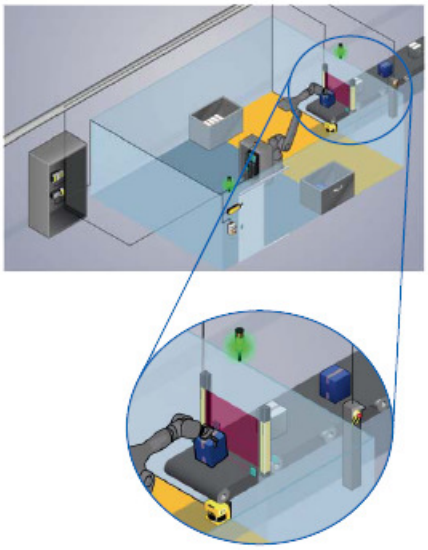
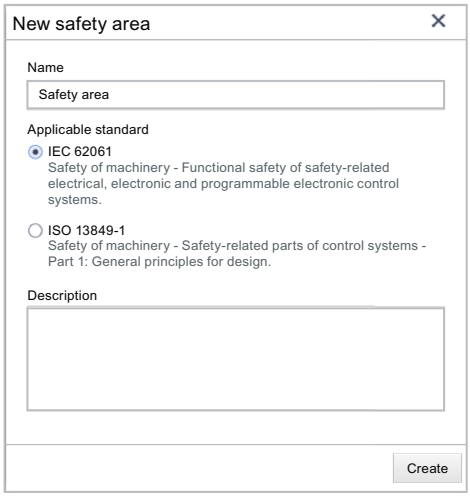
A prerequisite for the use of Safety Evaluation is a previously performed hazard assessment (risk analysis) in which the resulting safety functions are defined. The logical functions with the hardware sub-functions that are already being considered (e.g. detecting, evaluating and reacting) must be selected.

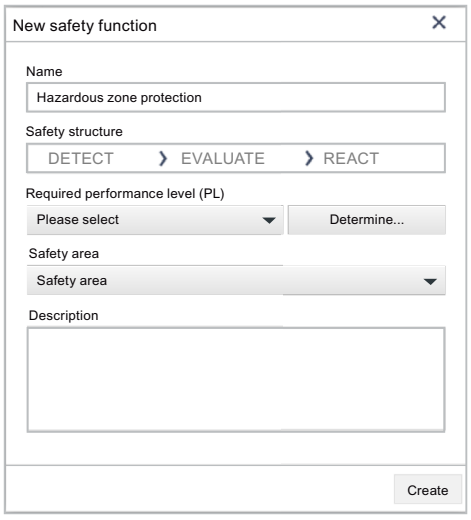
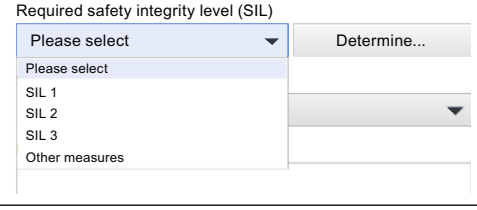
Those responsible (person responsible for the project and project test/check) must also be nominated for the subsequent acceptance tests.

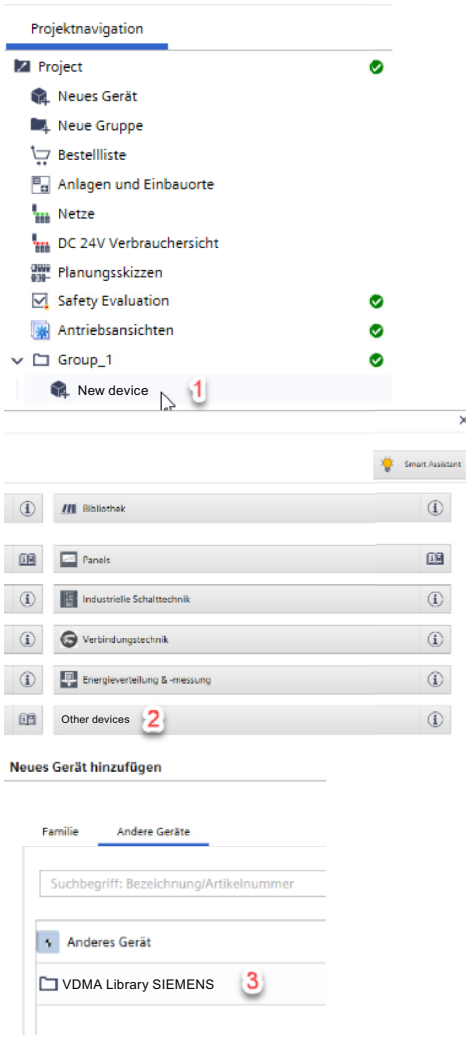
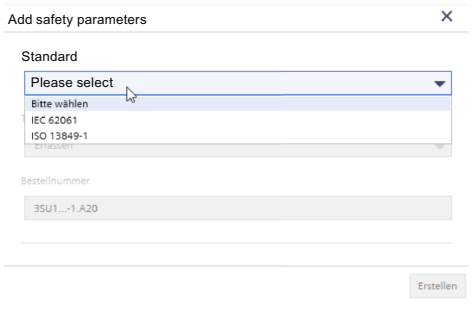
Information on Safety Evaluation in the TIA Selection Tool

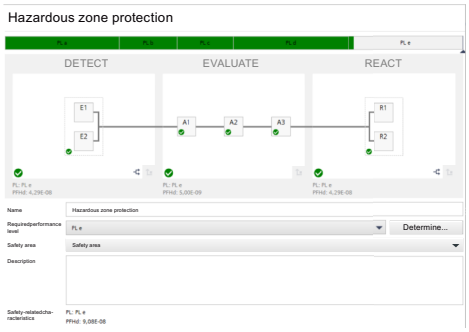
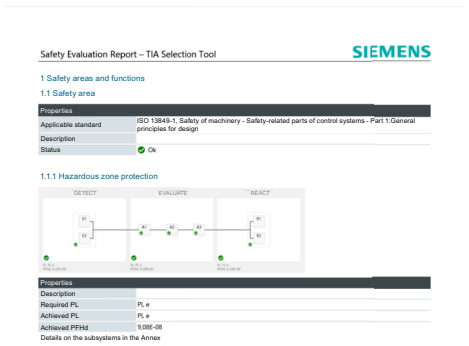
www.siemens.com/safety-evaluation (http://siemens.com/safety-evaluation)

Here you can find and download the Safety Evaluation in the TIA Selection Tool. A Getting Started document and FAQs on Safety Evaluation in the TIA Selection Tool are also available here.

Step 1 **Definition of a safety function** For example, the "hazardous zone protection" safety function • The light curtain is interrupted – The contactors open – Removal stops	
Step 2 **Create a safety area and select the applicable standard** • IEC 62061 or • ISO 13849-1	

Step 3 **Create safety function** The safety function "hazardous zone protection" consists of the following sub-systems • Detection (light curtain) • Evaluation (modular safety system) • Reaction (contactors)	
and enter the required PL or SIL	

Step 4 **Product selection in the TIA Selection Tool by creating a new device** 1. "New device" 2. "Other device" 3. "Selection of the module from the Siemens VDMA library"	
Step 5 **Parameterize module**	

Step 6 **Add devices to subsystems of a safety function**	
Step 7 **Generation of the result report for the machine documentation**	

Safety Evaluation in the TIA Selection Tool – advantages at a glance

- Automatic safety evaluation and documentation according to current standards
- Quick and easy handling of safety calculations
- Cost-efficient configuration of safety functions
- Reliable documentation: standard-compliant report
- Calculation of the safety level according to IEC 62061 and ISO 13849
- Less time to evaluate the safety functions
- Fast access to actual product data
- Helpful selection wizards
- Homogeneous workflow
- Integration of third-party VDMA libraries possible
- Creation of user-defined modules
- User-friendly archiving: TIA Selection Tool projects can be saved and called as needed
- Worldwide service and support
- Flexible working due to the use of an offline version

4.8 Dictionary English - German

English		German
Access to a hazardous zone (to a danger zone)		Access to a danger zone
Access means		Accesses
Access code		Access code
Accessibility		Accessibility
Active opto-electronic protective device		Active opto-electronic protective device
Actuator/manual control		Actuator element
Actuator element		Drive element
Adequate risk reduction		Adequate risk reduction
Adjustable guard		Adjustable guard
Sharp object		Sharp object
Retaining point		Retaining point
Assembly of machines		Assembly of machines
Barrier		Barrier
Burn		Burn
Center of gravity		Center of gravity
Cleaning		Cleaning
Color		Color
Commissioning		Commissioning
Common cause failures		Common cause failures
Common mode failures		Common mode failures
Comparative emission data		Comparative emission data
Complementary protective measures		Complementary protective measures
Construction		Construction
Containment (of materials, etc.)		Containment (of materials, etc.)
Containment (of stored energy)		Containment (of stored energy)
Control		Control
Control device		Control device
Control guard (see also: interlocking guard with a start function)		Control guard (see also: interlocking guard with a start function)
Control mode		Control mode
Control system		Control system
Critical component		Critical component
Crushing hazard		Crushing hazard
Cutting element		Cutting element
Cutting/severing hazard		Cutting/severing hazard
Damage to health		Damage to health
Danger		Danger
Danger zone (see also: hazardous zone)		Danger zone
De-commissioning		De-commissioning
Defeating (a protective device)		Defeating (a protective device)

English		German
Defeating (a warning device)		Defeating (a warning device)
Depressurizing		Depressurizing
Mechanical design (of a machine)		Mechanical design (of a machine)
Design error		Design error
Design engineer		Design engineer
Diagnostic system		Diagnostic system
Direct contact		Direct contact
Display		Display
Disposal (of a machine)		Disposal (of a machine)
Disturbance(s)		Disturbance(s)
Door		Door
Drawing-in/trapping hazard		Drawing-in/trapping hazard
Dust		Dust
Sharp edge		Edge (sharp -)
Electric shock		Electric shock
Electrical equipment		Electrical equipment
Electrical hazard		Electrical hazard
Preventing an electrical hazard		Electrical hazard (preventing -)
Electrical overload		Electrical overload
Electromagnetic compatibility		Electromagnetic Compatibility
Procedure in an emergency situation		Procedure in an emergency situation
Emergency situation		Emergency
Emergency Stop (function)		Emergency Stop (function)
Actuator to stop in an emergency		Actuator to stop in an emergency
Emergency Stop device		Emergency Stop device
Emissions		Emissions
Emission value		Emission value
Enabling/agreement device		Enabling/agreement device
Entanglement hazard		Entanglement hazard
Environment		Environment
Environmental conditions		Environmental conditions
Ergonomic principle		Ergonomic principle
Error (Human)		Error (human -)
Escape and rescue (of a person)		Escape and rescue (of a person)
Explosive atmosphere		Explosive atmosphere
Exposure to a hazard		Exposure to a hazard
Exposure to a hazard (limiting)		Exposure to a hazard (limiting)
Exposure value		Immission value
Failure		Failure
Failure to danger		Dangerous failure
Falling hazard		Falling hazard
Fault		Fault
Fault finding		Fault finding

English		German
Fixed guard		Fixed guard
Foundation		Foundation
Friction/abrasion hazard		Friction/abrasion hazard
Guard		Guard
Guard locking device		Guard locking device
Handling		Handling
Harm		Harm
Hazard		Hazard
Hazard combination		Hazard combination
Hazard identification		Hazard identification
Hazardous substances		Hazardous substances
Hazards generated by materials and substances		Hazards generated by materials and substances
Hazards generated by neglecting ergonomic principles		Hazards generated by neglecting ergonomic principles
Hazards due to noise		Hazards due to noise
Hazards due to radiation		Hazards due to radiation
Hazards due to vibration		Hazards generated by vibration
Hazard zone (see also: danger zone)		Danger zone
Hazardous malfunctioning		Hazardous malfunctioning
Hazardous/dangerous situation		Hazardous/dangerous situation
Heat		Heat
Heat source		Heat source
High pressure fluid ejection hazard		High pressure fluid ejection hazard
Hold-to-run control device (jog switch)		Hold-to-run control device (jog switch)
Human behavior		Human behavior
Hydraulic equipment		Hydraulic equipment
Impact		Shock
Impact hazard		Impact hazard
Impeding device (barrier)		Impeding device (barrier)
Index (of the instruction handbook)		Index (of the operating instructions)
Indirect contact		Indirect contact
Information for use		Information for use
Measure to achieve intrinsically safe design		Measure to achieve intrinsically safe design
Inspection		Inspection
Inspection (frequency of)		Inspection (frequency of)
Installation (of the machine)		Installation (of the machine)
Instruction Manual		Operating Instructions
Instructions		Instructions
Insulation fault		Insulation fault
Intended use of a machine		Intended use of a machine
Interlocking device (interlock)		Interlocking device (interlocking)
Interlocking guard		Interlocking guard
Interlocking guard with guard locking		Interlocking guard with guard locking

English		German
Interlocking guard with a start function (see also: control guard)		Guard with a start function (see also: Control guard)
Energy isolation and energy dissipation		Energy isolation and energy dissipation
Language		Language
Language (of the Instruction Manual)		Language (of the operating instructions)
Lifetime of a machine		Lifetime of a machine
Lifting equipment		Lifting equipment
Lifting gear/crane		Lifting gear/crane
Lighting		Lighting
Limit		Limit
Stepping circuit		Stepping circuit
Limiting device		Limiting device
Live part (of electrical equipment)		Live part (of electrical equipment
Load		Load
Loading (feeding)/unloading (removal) operations		Loading (feeding)/unloading (removal) operations
Lubrication		Lubrication
Machine/machinery		Machinery
Machine-power supply interface		"Machine-power supply" interface
Maintainability (of a machine)		Maintainability (of a machine)
Maintenance		Maintenance
Maintenance point		Maintenance point
Maintenance staff		Maintenance staff
Malfunction (malfunctioning)		Malfunction
Manual control (function)		Manual control
Actuator		Actuator element
Characters		Characters
Markings		Markings
Material		Material
Maximum speed of rotating parts		Maximum speed of rotating parts
Measurement methods		Measurement methods
Mechanical hazard		Mechanical hazard
Mechanical restraint device (form locking)		Mechanical restraint device (form locking)
Mirror Contact		Mirror contact
Mode selector		Mode selector switch
Moisture		Moisture
Movable elements/parts		Movable elements/parts
Movable guard		Movable guard
Noise		Noise
Normal operation		Normal operation
Operating modes		Operating modes
Operation		Operation
Operative part		Operative part

English		German
Operator		Operator
Operator-machine interface		Operator-machine interface
Component with defined behavior on failure		Component with defined behavior on failure
Overload (electrical)		Overload (electrical)
Overload (mechanical)		Overload (mechanical)
Overspeed		Overspeed
Packaging (action)		Packaging (action)
Packaging		Packaging
Pictogram		Pictogram
Platform		Platform
Pneumatic equipment		Pneumatic equipment
Portable control unit (teach pendant)		Portable control unit/mobile control device (operator panel on a swivel arm)
Positive mechanical action		Positive mechanical action
Positive mode (connected)		Positive mode (connected)
Positively Driven Contact		Positively driven contact
Power control element		Power control element
Power supply/energy source		Power supply/energy source
Power transmission element		Power transmission element
Pressure sensitive mat		Pressure sensitive mat
Preventing access		Preventing access
Changeover		Changeover
Programmable electronic control system		Programmable electronic control system
Prohibited usage/application		Prohibited usage/application
Protective device		Protective device
Protective measure		Protective measure
Protruding part		Protruding part
Radiation		Radiation
Range of applications		Field of application
Reasonably foreseeable misuse		Reasonably foreseeable misuse
Rectification (fault)		Rectification (fault)
Reduced speed		Reduced speed
Redundancy		Redundancy
Relevant hazard		Relevant hazard
Reliability (of a machine)		Reliability (of a machine)
Rescue and escape (of a person)		Rescue and escape (of a person)
Residual risk		Residual risk
Restart/restarting		Restart/restarting
Restricting access		Restriction of access
Risk		Risk
Risk analysis		Risk analysis
Risk assessment		Risk assessment
Risk comparison		Risk comparison

English		German
Risk estimation		Risk estimation
Risk evaluation		Risk evaluation
Risk reduction		Risk reduction
Safeguard		Protective device
Safeguarding		Technical protective measures
Safety function (safety critical function)		Safety function (directly acting -)
Scald		Scald
Electrosensitive protective equipment		Electrosensitive protective equipment
Sensor		Sensor
Setting-up/setting		Setting-up/setting
Setting (control mode for)		Setting (control mode for)
Setting-up point/setting point		Setting-up point/setting point
Severing hazard		Severing hazard
Shearing hazard		Shearing hazard
Signal		Signal
Significant hazard		Significant hazard
Siren		Siren
Slipping hazard		Slipping hazard
Software		Software
Software (access to the)		Software (access to the)
Spatial limit		Spatial limit
Speed/velocity		Speed/velocity
Stabbing/puncture hazard		Stabbing/puncture hazard
Stability		Stability
Stairs		Stairs
Static electricity		Static electricity
Stopping		Stopping
Storage (of a machine)		Storage (of a machine)
Stress (human)		Stress
Stress (environmental)		Environmental stress
Stress (mechanical)		Mechanical stress
Symbol		Symbol
Symbol (in the Instruction Manual)		Symbol (in the operating instructions)
Teach pendant (portable control unit)		Operator panel on a swivel arm (portable control unit/mobile control device)
Teaching/programming/instructing		Teaching/programming/instructing
Thermal hazard		Thermal hazard
Training		Training
Shipping		Shipping
Protective device with proximity response		Protective device with proximity response
Trip/tripping hazard		Trip/tripping hazard
Proximity response		Proximity response
Two-hand circuit		Two-hand circuit

English		German
Unexpected/unintended start-up		Unexpected/unintended start-up
Unloading (removal)/loading (feeding) operations		Unloading/loading operation (removal and feeding operation)
User-friendliness (of a machine)		User-friendliness (of a machine)
Use (of a machine)		Use (of a machine)
User		User
Valve		Valve
Vapor (gas)		Steam (gas)
Vibration		Vibration
Walking area		Walking area
Walkways		Walkways
Warning		Warning
Warning device		Warning device
Working environment		Working environment
Working part		Working part
Written warning		Written warning

4.9 Evaluation/feedback

Siemens AG

Technical Assistance

DF CP S&MK TA

D-90327 Fuerth

Fax: +49 (911) 895-5907

E-Mail: technical-assistance@siemens.com

Online-Support: www.siemens.com/automation/support-request

From

Name:

Department:

Location:

email:

Internet:

Evaluation of the Introduction and Terminology for Functional Safety of Machines and Systems

very good ❑ good ❑ poor ❑

Reasons: _____

_____

_____

_____

_____

_____

_____

Should you come across any printing errors when reading this publication, please notify us on this sheet. We would also be grateful for any suggestions and recommendations for improvement