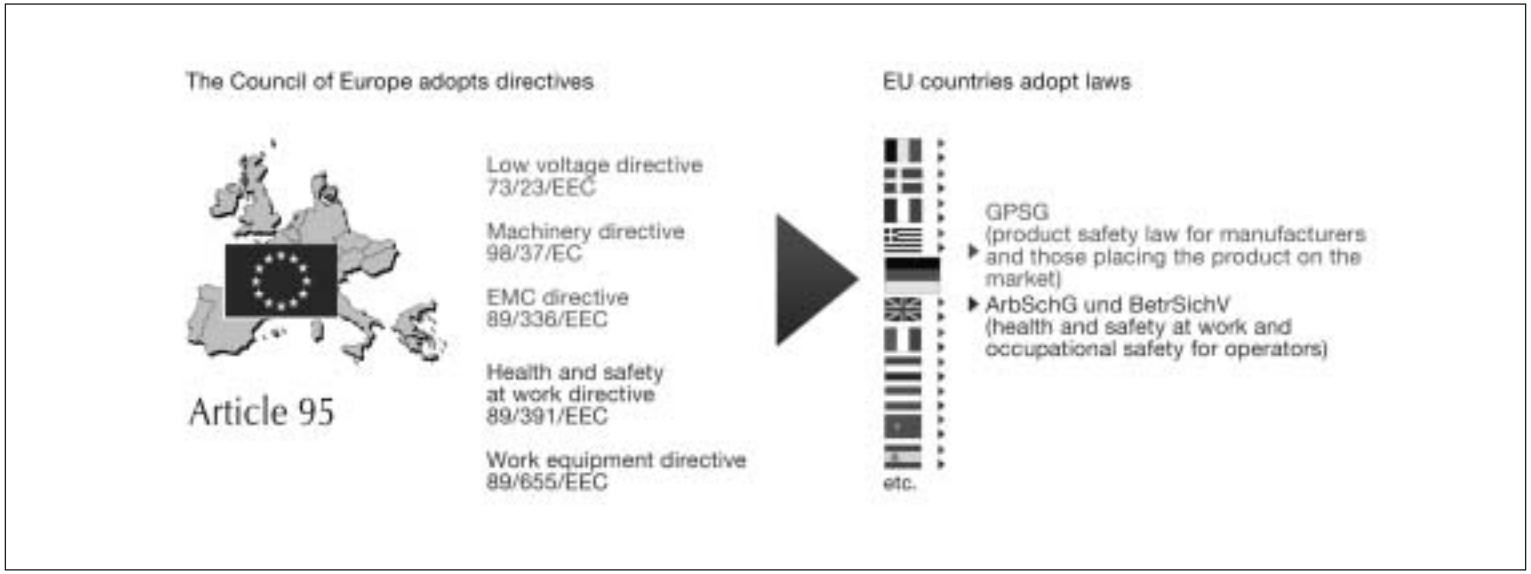
European directives and position of the standards in Europe



Incorporation of the directives into domestic law (using Germany as an example)

European directives

The concept of a single European internal market in terms of the “New Approach” can be traced right back to the start of the 70s: The low voltage directive is the first piece of European legislation to take into account the approach towards harmonisation of a common single market.

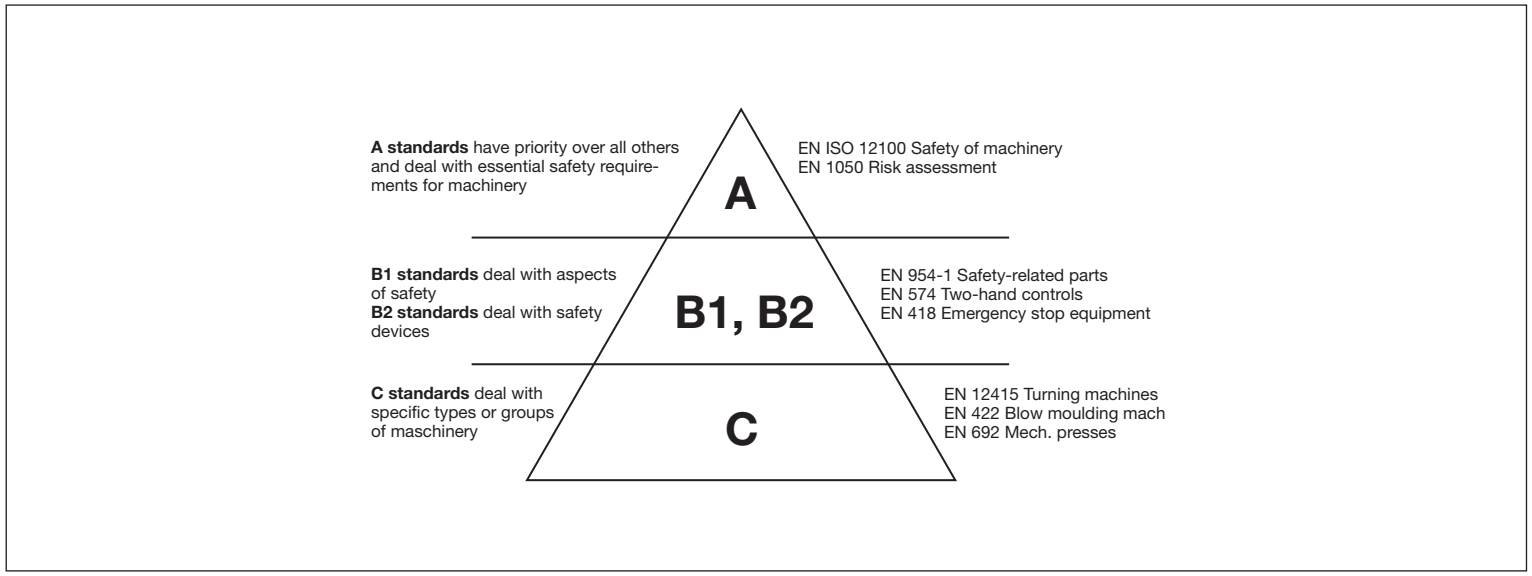
Products that are covered by one or more of the following directives have to apply a CE-mark, i.e. the product must be accompanied by a declar-ation of conformity. With a declaration of conformity the manufacturer confirms that his product meets all the requirements of the European directives that relate to his product. This means he can launch and sell his product within the scope of the EU without consideration of any national regulations.

Key engineering directives:

- General product safety (2001/95/EC)
- Health and safety (89/391/EEC)
- Use of work equipment (89/655/EEC)
- Lifts (95/16/EC)
- Waste electrical and electronic equipment (2002/96/EC)
- Electromagnetic compatibility (EMC) (2004/108/EC)
- Devices for use in potentially explosive areas (ATEX) (94/9/EC)
- Machinery (98/37/EC) / (2006/42/EC)
- Low voltage equipment (2006/95/EC)
- Personal protective equipment (89/686/EEC)
- Cable cars (2000/9/EC)

The directives are addressed to member states, who are obliged to incorporate the European directives into domestic law. In Germany this is normally achieved through the device safety law.

European directives and position of the standards in Europe



Standards pyramid

Position of the standards in Europe

The legal position of standards is discussed again and again. Inside Europe, i.e. within the scope of the European directives that are subject to the CE-marking obligation, a manufacturer is not bound by standards or other specifications. He simply needs to comply with the health and safety require-ments of the directive(s). The associated benefits of a division between standards and legislation are obvious: It is easier for legis-lators to agree on the essential requirements than on technical details. Also, the directives do not regularly have to be adapted to the state of technology; member states can use their own legal system for incorporation and manufacturers are free to select the ways in which they implement the requirements of the directive.

So what are the benefits of applying the standards? With so-called harmonised standards with presumption of conformity, there is a shifting of the burden of proof, i.e. if manufacturers apply these standards, it is presumed that they will also comply with the specific requirements of the European directives. The regulatory authorities would therefore need to prove that a manufacturer did not meet the legal requirements.

However, should a manufacturer deviate from the harmonised standards, he himself must prove how he has met the essential sa-fety require-ments. This is generally done via a hazard analysis. In practice one would en-deavour to apply the harmonised standards, unless the products concerned are highly innovative and no harmonised standards yet exist. The standards for which this “pre-sumption effect” applies can be researched in the Official Journal of the EU (e.g. on the Internet). Standards in Europe are subdivided into what are termed A, B and C standards.

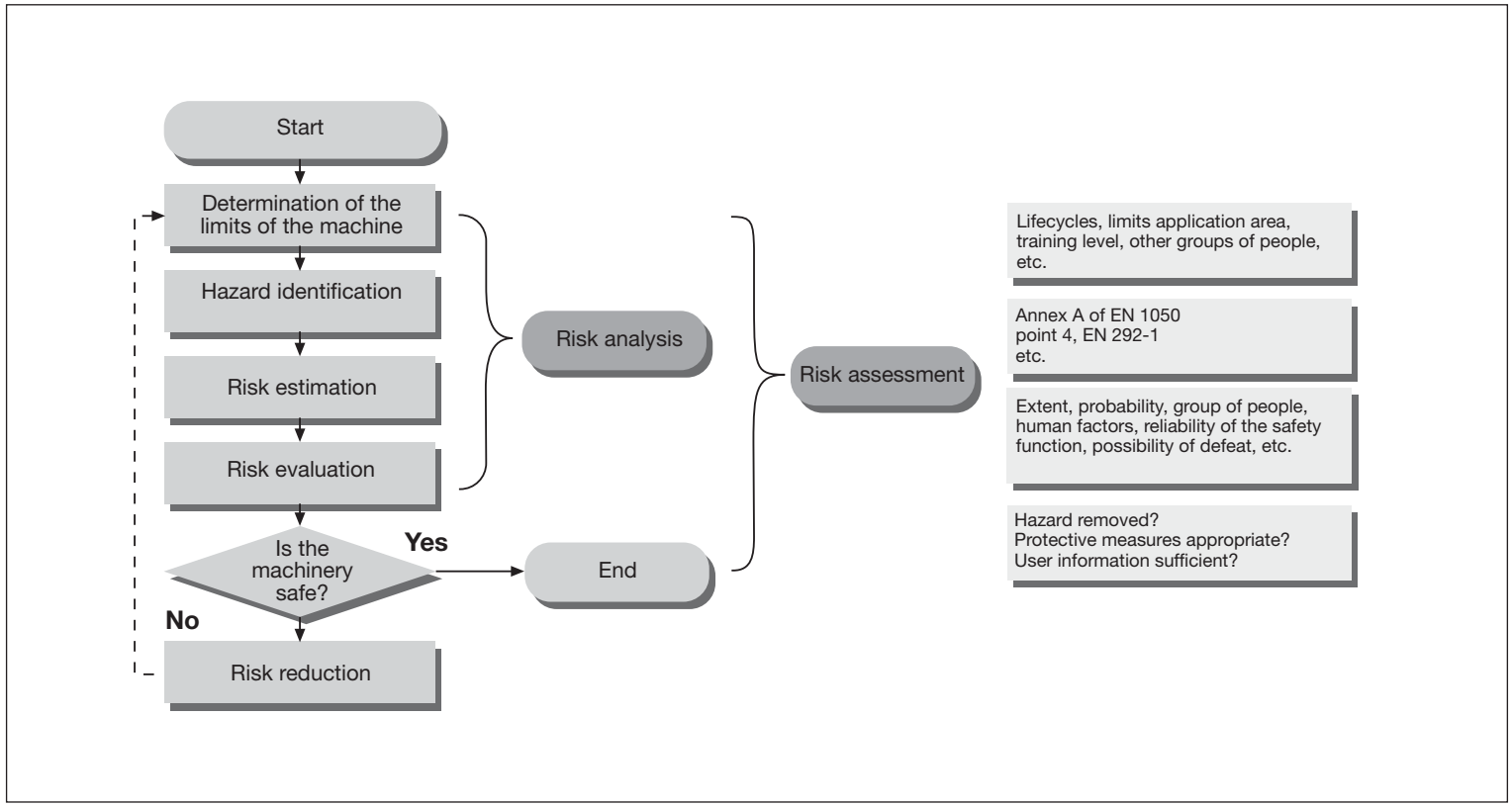
Risk assessment

Risk assessment

Under the terms of the machinery directive, a machine manufacturer must assess the hazards in order to identify all the hazards that apply to his machine. He must then design and construct the machine to take account of his assessment. This requirement also applies to operators who act as manufacturers under the terms of the machinery directive. For example, this may occur with machines that are interlinked or for machinery that has been upgraded and substantially modified.

EN ISO 14121-1 contains “Principles for risk assessment” on machinery. These approaches can be called upon as part of a comprehensive analysis. EN ISO 13849-1 expands on EN ISO 14121-1 with regard to the assessment of safety-related parts of control systems.

The hazards emanating from a machine may be many and varied, so for example, it is necessary to consider not just mechanical hazards through crushing and shearing, but also thermal and electrical hazards and hazards from radiation. Risk reduction is therefore an iterative process, i.e. it is carried out before and during the planning phase and after completion of the plant or machine.



Iterative process in accordance with EN ISO 14121-1

Legal regulations outside Europe and standards for functional safety

Legal regulations outside Europe

The situation is somewhat different in the USA: people there are mainly familiar with two types of standards: ANSI (American National Standards Institute) and OSHA (Occupational Safety and Health Administration).

OSHA standards are published by the state and compliance is mandatory. ANSI standards, on the other hand, are developed by private organisations and their application is generally not absolutely essential. However, ANSI standards can still be found included as part of a contract. Beyond that ANSI standards are being taken over by OSHA. You can also still come across the NFPA (National Fire Protection Association), which developed NFPA 79 as a counterpart to EN 60204-1, for example. The OSHA standards can be compared with the European directives. Unlike the European directives, OSHA standards are more involved with formulating technical specifications than abstract requirements.

The legal basis in the USA can be seen as a mix of product standards, fire codes (NFPA), electrical codes (NEC) and national laws. Local government bodies have the authority to monitor that these codes are being enforced and implemented.

Russia and the CIS states have implemented GOST-R certification for some years now, in other words, technical devices that fall within a specific product area must undergo a certain certification process. Machinery and any corresponding technical accessories undergo a type approval test through a European notified body, for example. This test is generally recognised by a Russian-based approvals body. From the point of view of safety, the same requirements apply as in Europe.

China, on the other hand, has introduced CCC certification. Similar to the position in Russia, technical products are subject to mandatory certification through a national approvals body in China. In addition, production sites are inspected. If a technical device falls with the scope of the product list, which is subdivided into 19 categories, certification is mandatory, otherwise it will be necessary to supply a type of “declaration of no objection” from a national notified body.

Japan is currently in a transition period: The plan is for Japan to adopt the European “new approach” – in other words, to keep standards and legislation separate. At the moment the international ISO and IEC standards are being directly incorporated into national legislation, which is why people are currently confronted with frequent amendments to laws and lengthy implementation periods.

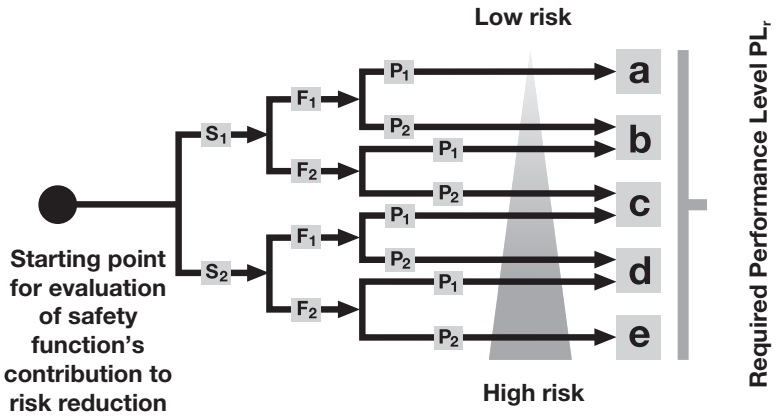
Standards for functional safety

Different standards may be called upon to observe functional safety on control systems, depending on the application. In the area of machine safety, EN ISO 13849-1 is the main standard named for safety-related control systems. Irrespective of the technology, this applies for the whole chain from the sensor to the actuator. The risk graphs and corresponding risk parameters can be used to estimate the potential risk for danger zones on machinery. The category is then established without the use of risk-reducing measures.

Safety-related parts of control systems – General principles for design in accordance with EN ISO 13849-1

Determination of the required Performance Level (PL_r)

- **S – Severity of injury**
  - S_1 = Slight (normally reversible injury)
  - S_2 = Serious (normally irreversible injury, including death)
- **F – Frequency and/or exposure to a hazard**
  - F_1 = Seldom to less often and/or the exposure time is short
  - F_2 = Frequent to continuous and/or the exposure time is long
- **P – Possibility of avoiding the hazard or limiting the harm**
  - P_1 = Possible under specific conditions
  - P_2 = Scarcely possible



Safety-related parts of control systems – General principles for design in accordance with EN ISO 13849-1

As the successor standard to EN 954-1, EN ISO 13849-1 is based on the familiar categories. Equally, it examines complete safety functions, including all the components involved in their design. EN ISO 13849-1 goes beyond the qualitative approach of EN 954-1 to include a quantitative assessment of the safety functions. A performance level (PL) is used for this, building upon the categories.

Components/devices require the following safety parameters:

- Category (structural requirement)
- PL: Performance level
- $MTTF_d$: Mean time to dangerous failure
- DC: Diagnostic coverage
- CCF: Common cause failure

The standard describes how to calculate the performance level (PL) for safety-related parts of control systems, based on designated architectures. EN ISO 13849-1 refers any deviations to IEC 61508.

Risk assessment in accordance with EN ISO 13849-1

Risk assessment is an iterative process, i.e. it will need to be carried out more than once. The risk must be estimated and the performance level defined for each hazard on which the risk is to be reduced through control measures. The risk is estimated through consideration of the severity of injury (S), the frequency and duration of exposure to the hazard (F) and the possibility of avoiding or limiting the harm (P).

Parameters S, F and P are used on the risk graph to determine the required performance level (PLr) for a safety function. The selection of parameters is no different to the procedure used in EN 954-1 (1996). However, the result is no longer a category but a PL.

Safety-related parts of control systems – General principles for design in accordance with EN ISO 13849-1

Performance Levels (PL) in accordance with EN ISO 13849-1	Probability of a dangerous failure per hour [1/h]
a	$10^{-5} < PFH < 10^{-4}$
b	$3 \times 10^{-6} < PFH < 10^{-5}$
c	$10^{-6} < PFH < 3 \times 10^{-6}$
d	$10^{-7} < PFH < 10^{-6}$
e	$10^{-8} < PFH < 10^{-7}$

Performance level

The performance level (PL) classifies 5 levels of probability of failure. The table shows the relationship between PL and the probability of dangerous failure per hour PFH_D).

Once the required PL has been established, the PL achieved by the safety function (SRP/CL) is calcu-lated. To do this the SRP/CL can be divided into logical blocks, such as input, logic solving and output for example.

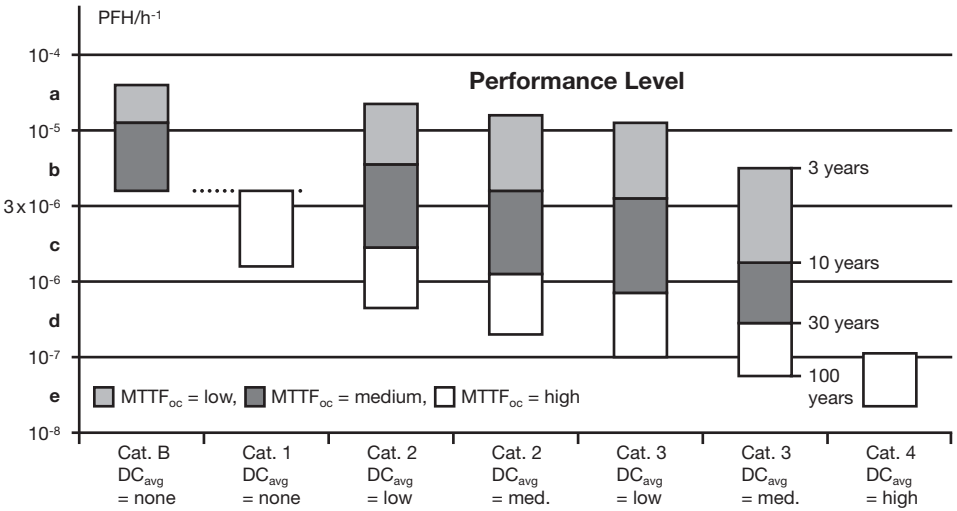
When using a designated architecture or an architecture of similar structure, the achieved PL can be calculated graphically using the bar chart. To do this the architecture of the SRP/CL in divided into categories. $MTTF_D$ and DC_{avg} are also required. From Category 2 onwards, the CCF will also need to be examined. A com-ponent's $MTTF_D$ value is usually provided by the manufacturer. The standard provides tables and check lists for calculating the other values.

It is also possible to calculate the achieved PL of an SRP/CL. The probability of dange-rous failure of all the blocks that combine to form the safety function is added up:

$PFH_{System} = PFH_{Input} + PFH_{Logic} + PFH_{Output}$

The PL achieved by an SRP/CL must be at least as high as the PL required by the safety function.
If this condition is not met, the safety func-tion must be implemented differently.

Relationship between categories DC, $MTTF_d$ and PL



Functional safety and legal position of EN/IEC 61508

Functional safety with EN/IEC 61508?

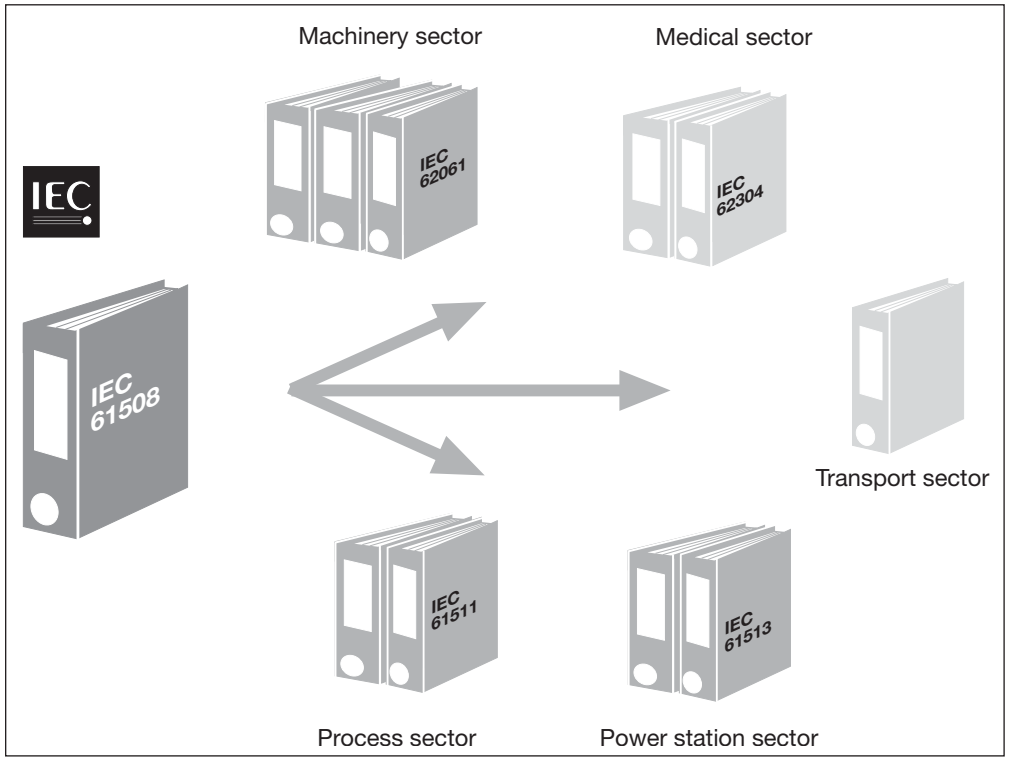
EN/IEC 61508 is regarded as a generic safety standard, which deals with the functional safety of electrical, electronic and programmable electronic systems, irrespective of the application.

One of the main tasks of EN/IEC 61508 is to serve as a basis for the development of application-oriented standards. Standards' committees are currently busy in the areas of machine safety with EN/IEC 62061, and process safety with EN/EC 61511.

These sector-specific standards are intended to continue the principle approaches of EN/IEC 61508 and to implement the requirements for the relevant application area in a suitably practical manner.

What is the legal status of EN/IEC 61508?

As EN/IEC 61508 is not listed in the Official Journal of the European Communities for implementation as a European directive, it lacks the so-called "effect of presumption", so if the standard is used on its own, a control system designer cannot presume that the relevant requirements of the specific European directive have been met.



Sector standards from EN/IEC 61508

Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany, Telephone: +49 711 3409-0, Telefax: +49 711 3409-133, E-Mail: pilz.gmbh@pilz.de

Functional safety in accordance with EN/IEC 62061

Risk assessment and determination of required Safety Integrity Level (SIL)

Consequences	S	Class Cl 3-4	5-7	8-10	11-13	14-15	Frequency and duration	Fr	Probability of hzd. event	Pr	Avoidance	P
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 hour	5	Very high	5		
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1 h – ≤ 1 day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	> 1 day – ≤ 2 wks	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	> 2 wks – ≤ 1 year	3	Rarely	2	Possible	3
							> 1 year	2	Negligible	1	Likely	1

☐ AM = Other measures recommended

Functional safety of safety-related electrical, electronic and programmable electronic control systems in accordance with EN/IEC 62061

EN/IEC 62061 represents a sector-specific standard under EN/IEC 61508. It describes the implementation of safety-related electrical control systems on machinery and examines the overall lifecycle from the concept phase through to decommissioning. Quantitative and qualitative examinations of the safety functions form the basis.

Risk estimation is an iterative process, i.e. it will need to be carried out more than once. The risk must be estimated and the SIL defined for each hazard on which the risk is to be reduced through control measures. The risk is estimated through consideration of the severity of injury (Se), the frequency and duration of exposure to the hazard (Fr), probability of occurrence of a hazardous event (Pr) and the possibility of avoiding or limiting the harm (Av).

The required SIL is assigned using the table above, where Cl = Fr + Pr + Av.

Functional safety in accordance with EN/IEC 62061

Safety Integrity Level (SIL) in accordance with EN IEC 62061	Probability of a dangerous failure per hour [1/h]
No special safety requirement	$10^{-5} < PFH < 10^{-4}$
1 (1 failure in 100 000 h)	$3 \times 10^{-6} < PFH < 10^{-5}$
1 (1 failure in 100 000 h)	$10^{-6} < PFH < 3 \times 10^{-6}$
2 (1 failure in 1 000 000 h)	$10^{-7} < PFH < 10^{-6}$
3 (1 failure in 10 000 000 h)	$10^{-8} < PFH < 10^{-7}$

SIL assignment

The safety integrity level (SIL) classifies three levels of probability of failure. The table shows the relationship between SIL and the probability of dangerous failure per hour (PFH_D).

The SRECS (safety-related electrical control system) is divided into subsystems. The subsystems are assigned to actual devices. The SIL must be defined for each subsystem.

The probability of a dangerous failure is calculated by adding the probabilities of failure of all the subsystems of the SRECS:

$PFH_D = PFH_{D1} + ... + PFH_{Dn}$

The selection or design of the SRECS must always meet the following minimum requirements:

Requirements for hardware safety integrity, comprising

- Architectural constraints for hardware safety integrity
- Requirements for the probability of dangerous random hardware failures

plus requirements for systematic safety integrity, comprising

- Requirements for avoidance of failures and
- Requirements for the control of systematic failures.

The following parameters are required in assessing hardware safety integrity:

λD: Dangerous failure rate
T1: Proof test
T2: Diagnostic test interval
DC: Diagnostic coverage
β: Common cause failure

The calculated probability of failure (PFHD) of each SRECS must be less than the probability of failure required by the safety function. The required probability of failure, depending on the SIL, can be taken from the table. If this condition is not met, the safety function must be implemented differently.

The achieved SIL can only be as high as the lowest SILCL (SIL Claim Limit) of a subsystem involved in performing the safety function.

Safe failure fraction (SFF)	Hardware fault tolerance 0	Hardware fault tolerance 1	Hardware fault tolerance 2
< 60 %	Not allowed	SIL 1	SIL 2
60 % – < 90 %	SIL 1	SIL 2	SIL 3
90 % – < 99 %	SIL 2	SIL 3	SIL 3
99 %	SIL 3	SIL 3	SIL 3

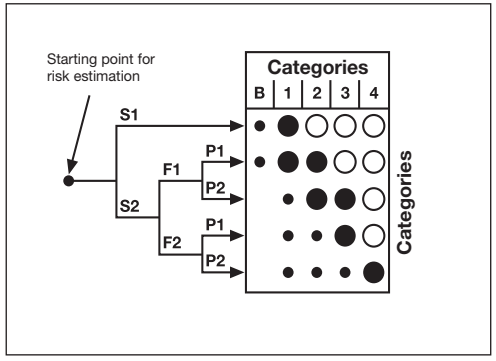
Risk parameters and categories in accordance with EN 954-1/EN ISO 13849-1[1)]

Risk parameters

S = Severity of injury:
1 = Slight (normally reversible) injury
2 = Serious (normally irreversible) injury, including death

F = Frequency and/or exposure to the hazard:
1 = Seldom to quite often and/or exposure time is short
2 = Frequent to continuous and/or exposure time is long

P = Possibility of avoiding the hazard:
1 = Possible under specific conditions
2 = Scarcely possible



Risk graph from EN 954

Categories in accordance with EN 954-1

The control system requirements derived from the risk graph are specified as follows:

Category B

Basic category with no special requirements = "good industrial standard"

Category 1

Safety-related parts must be designed and constructed using well-tried components and well-tried safety principles.

Well-tried means: the components have been widely used in the past with successful results in similar applications, or they have been manufactured using principles that demonstrate its suitability and reliability for safety-related appli-cations.

Example: safety switch with forced-opening contacts.

Well-tried safety principles are circuits that are constructed in such a way that certain faults can be avoided by the appropriate arrangement or layout of components.

Example: avoiding a short circuit through appropriate separation, avoiding component failures that result from overdimensioning, using the failsafe principle (on switching off).

Note: The occurrence of a fault can lead to the loss of the safety function.

Category 2

Safety-related parts of control systems must be designed so that their safety function(s) are checked at suitable intervals by the machine control system. The safety function(s) must be checked: at the machine start-up and prior to the initiation of any hazardous situation; periodically during operation, if the risk assessment and the kind of operation show that it is necessary.

This check may be initiated automatically or manually. Automatically, for example, the check may be initiated by a signal generated from a control system at suitable intervals. The automatic test should be provided by preference. The decision about the type of test depends on the risk assessment and the judgement of the end user or machine builder. If no fault is detected, operation may be approved as a result of the test. If a fault is detected, an output must be generated to initiate appropriate control action. A second, independent shutdown route is required for this.
Notes: In some cases Category 2 is not applicable because the checking of the safety function cannot be applied to all components and devices. Moreover, the cost involved in implementing Category 2 correctly may be considerable, so that it may make better economic sense to implement a different category.
In general Category 2 can be realised with electronic techniques. The system behaviour allows the occurrence of a fault to lead to the loss of the safety function between checks; the loss of the safety function is detected by the check.

Category 3

Safety-related parts of control systems must be designed so that a single fault in any of these parts does not lead to the loss of the safety function.
Whenever reasonably practicable, the single fault shall be detected at or before the next demand upon the safety function.

This does not mean that all faults will be detected. The accumulation of undetected faults can lead to an unintended output signal and a hazardous situation at the machine.

Category 4

Safety-related parts of control systems must be designed so that a single fault in any of these parts does not lead to a loss of the safety function; the single fault must be detected at or before the next demand upon the safety functions (e.g. immediately at switch on, at the end of a machine operating cycle). If this detection is not possible, then an accumulation of faults shall not lead to a loss of the safety function.

[1)] Only applicable until November 2009. Replaced by EN ISO 13849-1