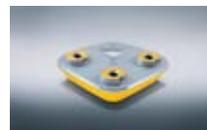
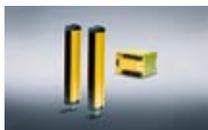




The Safety Compendium

pilz
the spirit of safety

For the application of functional safety standards.



▶ The new Safety Compendium

- 1 Preface
- 2 Standards, directives and laws
- 3 Safeguards
- 4 Safe control technology
- 5 Safe communication
- 6 Safe motion
- 7 Mechanical, pneumatic and hydraulic design
- 8 Appendix



1

Preface

▶ 1 Preface

Chapter	Contents	Page
1	Preface	1-3
1.1	Authors	1-5

▶ 1 Preface

It's now more than five years since Pilz published the first Safety Compendium. It has since established itself on the market and among our customers as one of the standard works in the machinery safety sector. In day-to-day operations it serves as an orientation guide for functional safety and standards and provides comprehensive technical information to a wide range of users – both in the machinery design sector and on the operator side.

As a complete safe automation supplier, our aim is to resolve your automation tasks safely, economically and reliably. To this end we provide innovative products and systems

We also see our role as an advisor in all matters regarding machinery safety. This is expressed through our comprehensive range of services, which demonstrates our competence in consulting, engineering and training. It's for good reason, for example, that our expert CMSE® – Certified Machinery Safety Expert training is also known as the driver's licence for machinery safety.

Our highest priority is to provide specialist knowledge, answer questions on functional safety and supply information about changes and revisions. Our Safety Compendium is a result of this philosophy.

You now have in your hands the 4th revised and expanded edition of the Pilz Safety Compendium.

Practical examples, graphic illustrations of applications and overview tables of the current standards are just some of the many issues covered by this machinery safety reference book.

Besides containing the latest news on standards, it also features information on the mission time of safety functions and on the use of used components, for example. There is also detailed coverage of the subject of interlinking machinery.

We are delighted if this reference work provides some additional technical information and proves to be a valuable resource.

I'm also happy to start a dialogue with you at any time – and not just about the Safety Compendium. We can all benefit from this additional insight.

I wish you some very productive hours with your Safety Compendium.



*Renate Pilz
Managing Partner
Pilz GmbH & Co. KG*

▶ 1.1 Authors



Christian Bittner is acting team leader of the Consulting Services Group within Pilz GmbH & Co. KG. He is in direct contact with customers: His duties include performing risk assessments, producing safety concepts, CE certification and other safety services.



Holger Bode is responsible for international project planning for press upgrades and new installations in Pilz's press working group. Responsibilities include the development of full conversion measures and the production of control concepts, hazard assessments and safety concepts. He is also Quality Manager of the accredited Pilz inspection body.



Arndt Christ is Head of the Customer Support Department at Pilz GmbH & Co. KG. Within the department he is responsible for groups such as Technical Support and the consulting units, as well as system integration and the training team. He is familiar with customers' requirements on all safety-related subjects, and so guarantees a user-friendly implementation in the field of safety technology.



Roland Gaiser is head of the Actuator Systems division in development at Pilz GmbH & Co. KG. He also lectures on system development and simulation at the Faculty of Mechatronics and Electrical Engineering at Esslingen University. He has extensive knowledge in the field of basic development of actuator systems.

▶ 1.1 Authors



Andreas Hahn is head of the Networks, Control Systems and Actuator Technology division in product management at Pilz GmbH & Co. KG. He is also involved in Pilz's internal standards committee, which deals with the interpretation of standards. He has many years' experience in the design of automation solutions.



Jürgen Hasel is a trainer and consultant at Festo Didactic GmbH & Co. KG. His seminars focus on pneumatics, electropneumatics, valve terminals and safety technology. Earlier in his career he worked in the development department at Festo AG. He has been working closely with the training department of Pilz GmbH & Co. KG for some years. At Pilz he teaches the CMSE course (Certified Machinery Safety Expert) certified by TÜV Nord, as part of product-neutral training.



Prof. Dr. Thomas Klindt is a partner at the international law firm NOERR and is also honorary professor for Product and Technology Law at the University of Kassel. He is a member of the chamber's internal product safety & product liability practice group, which oversees national and international product liability processes, product recalls and compensation claims.



Thomas Kramer-Wolf is the standards specialist at Pilz GmbH & Co. KG. He is a member of various standards committees and combines theoretical work with practical interpretation of standards, also as part of Pilz's internal standards committee.

▶ 1.1 Authors



Dr. Alfred Neudörfer is a lecturer in the Faculty of Mechanical Engineering at Darmstadt University of Technology. He is also a guest professor in safety technology at Nagaoka University of Technology in Japan. The subject of many of his lectures, seminars and technical papers is the design of safety-related products.



Andreas Schott is responsible for the Training and Education division within Pilz GmbH & Co. KG. As team leader, he works with his team to produce educational and practically relevant training concepts for both product-neutral and product-specific courses and seminars. His many years of experience as a state-approved electrical engineer and software programmer have familiarised him with the practical requirements of customers when it comes to safety technology.



Eszter Fazakas, LL.M. is a lawyer with the international law firm NOERR. She is also a member of the chamber's internal product safety & product liability practice group, which oversees national and international product liability processes, product recalls and compensation claims.



Gerd Wemmer works as an application engineer in Customer Support at Pilz GmbH & Co. KG. He is responsible for consultancy, project engineering and the preparation of safety concepts for customers, from machine manufacturers to end users. He has many years' practical experience in safety technology.

▶ 1.1 Authors



Matthias Wimmer works in Customer Support at Pilz GmbH & Co. KG. He presents seminars on various subjects, including: “Functional safety standards”, “Machinery Directive 2006/42/EG” and “Safeguards”. As an application engineer he produces risk assessments and safety concepts for machinery. He is also a member of the standards working group ISO/TC 199/WG 8, “Safe control systems”.



Michael Wustlich is team leader of the Software, Application and Tests division at Pilz GmbH & Co. KG. His duties include the development of user-level safety-related software in the form of standardised, certified products. Together with his team he is responsible for the specification and design of systematised application tests across all product groups.



2

Standards, directives and laws

▶ 2 Standards, directives and laws

Chapter	Contents	Page
2	Standards, directives and laws	2-3
2.1	Standards, directives and laws in the European Union (EU)	2-3
2.2	CE marking	2-5
2.2.1	The basis of machine safety: Machinery Directive and CE mark	2-5
2.2.2	Legal principles	2-5
2.2.3	CE marking of machinery	2-6
2.3	Directives	2-16
2.3.1	Machinery Directive	2-17
2.4	Standards	2-18
2.4.1	Publishers and scope	2-18
2.4.2	EN engineering safety standards	2-19
2.4.3	Generic standards and design specifications	2-21
2.4.4	Product standards	2-38
2.4.5	Application standards	2-41
2.5	International comparison of standards, directives and laws	2-42
2.5.1	Directives and laws in America	2-42
2.5.2	Directives and laws in Asia	2-43
2.5.3	Directives and laws in Oceania	2-45
2.5.4	Summary	2-46
2.6	Validation	2-46
2.6.1	Verification of safety functions in accordance with EN ISO 13849-1/2	2-47
2.6.2	Verification of safety functions in accordance with EN 62061	2-47
2.6.3	General information about the validation plan	2-48
2.6.4	Validation by analysis	2-49
2.6.5	Validation by testing	2-49
2.6.6	Verification of safety functions	2-49
2.6.7	Validation of software	2-51
2.6.8	Validation of resistance to environmental requirements	2-52
2.6.9	Production of validation report	2-52
2.6.10	Conclusion	2-52
2.6.11	Appendix	2-53
2.7	Certification and accreditation	2-55
2.7.1	Accreditation: Quality seal for customers	2-55
2.7.2	Accreditation or certification	2-58
2.7.3	Tests in accordance with industrial safety regulations (BetrSichV) and accreditation	2-59
2.7.4	Conclusion	2-60

▶ 2.1 Standards, directives and laws in the European Union (EU)

The European Union is increasingly merging. Machine builders will recognise this in the increasing harmonisation of laws, regulations and provisions. Not that long ago, each country published its own guidelines on the different areas of daily life and the economy, but today you'll find more and more standardised regulations within Europe.

How are European laws, directives and standards connected?

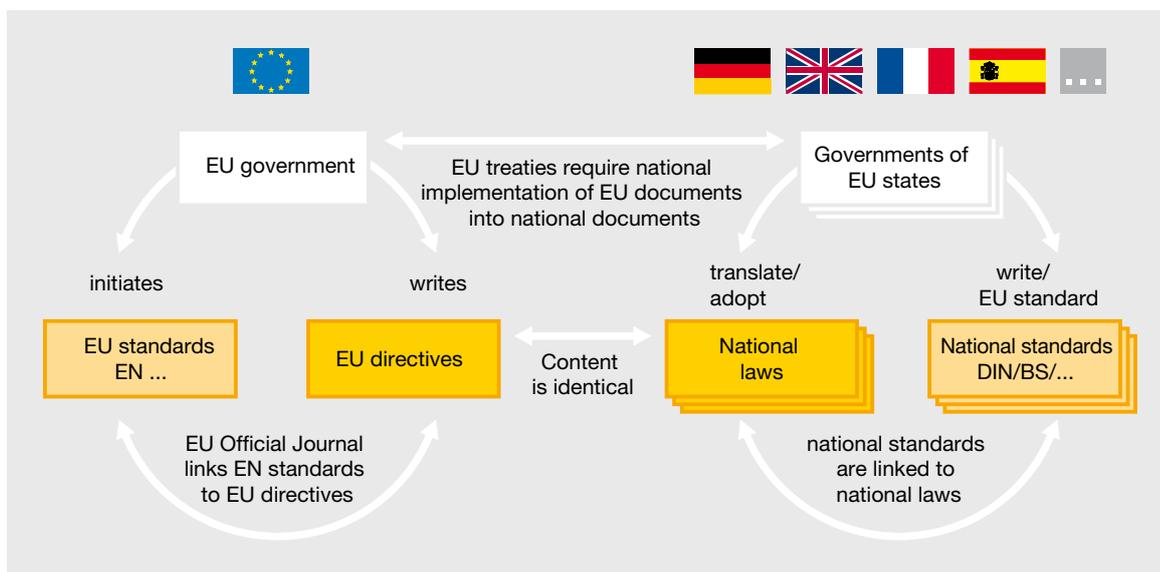
Initially, the EU formulates general safety objectives via directives. These safety objectives need to be specified more precisely; the actual provision is made via standards.

EU directives generally deal with specific issues. The directives themselves have no direct impact on individual citizens or companies. They only come into effect through the agreements of individual countries within the EU, who incorporate these directives into their domestic law. In each EU country, a law or provision refers to the relevant EU directive and thus elevates it to the status of domestic law. Between the time a directive is adopted and the point at which it is incorporated into domestic law

there is inevitably a transition period, during which time the directive awaits incorporation into domestic law in the individual countries. However, for users this is generally unimportant because the directives themselves provide clear indication on the respective validity date. So although the titles of these documents describe them almost harmlessly as directives, in practice they have legal status within the EU.

This explains how laws and directives are connected, but doesn't deal with the issue of the standards.

Although the standards themselves make interesting reading, on their own they have no direct legal relevance until they are published in the Official Journal of the EU or are referenced in domestic laws and provisions. These are the publications by which a standard can acquire "presumption of conformity". Presumption of conformity means that a manufacturer can assume he has met the requirements of the corresponding directive provided he has complied with the specifications in the standard. So presumption of conformity confirms proper conduct, as it were. In a formal, legal context this is called a reversal of the burden of proof. Where the



Relationship between harmonised standards and laws in the EU.

▶ 2.1 Standards, directives and laws in the European Union (EU)

manufacturer applies a harmonised standard, if there is any doubt, misconduct will need to be proven. Where the manufacturer has not applied a harmonised standard, he will need to prove that he has acted in compliance with the directives.

If a manufacturer does not comply with a standard, it does not necessarily mean that he has acted incorrectly. Particularly in innovative industries, relevant standards either may not exist or may be inadequate. The manufacturer must then demonstrate independently that he has taken the necessary care to comply with the safety objectives of the relevant directives. Such a route is usually more complex but, in an innovative industry, it is often unavoidable.

It's important to stress that the EU does not publish every standard in the Official Journal, so many are still not harmonised. Even if such a standard is deemed to have considerable technical relevance, it will still not have presumption of conformity. However, sometimes a standard that has not been listed in the EU Official Journal does achieve a status that's comparable with harmonisation. This is the case, for example, when a harmonised standard makes reference to the respective standard. The standard that is not listed in the EU Official Journal is then harmonised "through the back door", as it were.

▶ 2.2 CE marking

2.2.1 The basis of machine safety: Machinery Directive and CE mark



When the Machinery Directive (MD) was ratified in 1993, the aim was to remove trade barriers and enable a free internal market within Europe. After a two-year transition period, the Machinery Directive has been binding in Europe since 01.01.1995. It describes standardised health and safety requirements for interaction between man and machine and replaces the host of individual state regulations that existed on machinery safety. The new Machinery Directive 2006/42/EC has applied since 29.12.2009.

The CE mark stands for “Communauté Européenne”. A manufacturer uses this mark to document the fact that he has considered all the European internal market directives that are relevant to his product and applied all the appropriate conformity assessment procedures. Products that carry the CE mark may be imported and sold without considering national regulations. That’s why the CE mark is also referred to as the “Passport to Europe”.

Generally speaking, all directives in accordance with the new concept (“new approach”) provide for CE marking. Where a product falls under the scope of several directives which provide for CE marking, the marking indicates that the product is assumed to conform with the provisions of all these directives.

2.2.2 Legal principles

The obligation to affix CE marking extends to all products which fall under the scope of directives providing for such marking and which are destined for the single market. CE marking should therefore be affixed to the following products that fall under the scope of a directive:

- ▶ All new products, irrespective of whether they were manufactured in member states or third-party countries
- ▶ Used products imported from third-party countries and second hand products
- ▶ Products that have been substantially modified and fall under the scope of the directives as new products.

The directives may exclude certain products from CE marking.

The manufacturer uses the declaration of conformity to confirm that his product meets the requirements of the relevant directive(s).

The information that follows is intended to explain CE marking in terms of the Machinery Directive.

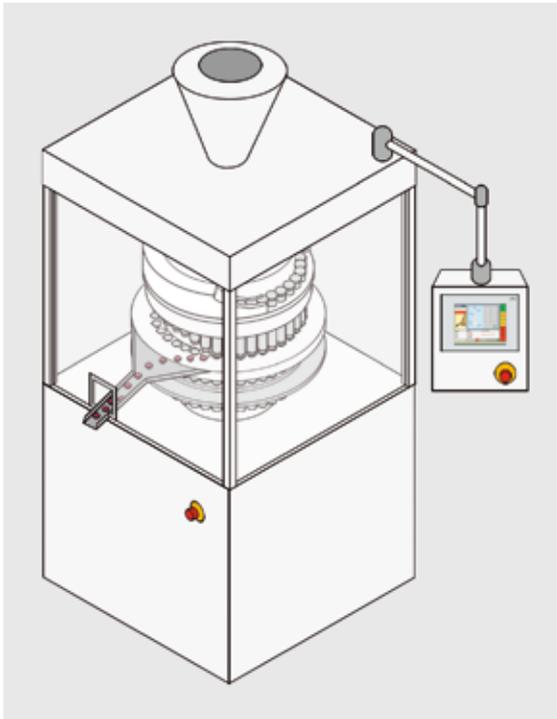
▶ 2.2 CE marking

2.2.3 CE marking of machinery

2.2.3.1 What is a machine?

For the purposes of the Directive, one definition of a machine is:

An assembly of linked parts or components, at least one of which moves, and which are joined together for a specific application. (see Article 2 of the Machinery Directive)



Example of a machine for the purposes of the Directive.

The following are also considered as machines for the purposes of the Machinery Directive:

- ▶ An assembly of machines or complex plants (complex plants include production lines and special purpose machinery made up of several machines)

- ▶ Safety components (The issue of which components to classify as safety components is very controversial. Annex V of the Machinery Directive contains an extremely comprehensive list of safety components.)
- ▶ Interchangeable equipment that can modify the basic functions of a machine.

There is also a list of exceptions where machinery falls under the scope of the Directive by definition, but for which other statutory provisions generally apply.

2.2.3.2 CE-marking of plant and machinery

According to the Machinery Directive, a machine manufacturer is anyone who assembles machines or machine parts of various origins and places them on the market.

A manufacturer may be the actual machine builder or – where a machine is modified – the operator. In the case of assembled machinery, it may be the manufacturer, an assembler, the project manager, an engineering company or the operator himself, who assembles a new installation from various machines, so that the different machine parts constitute a new machine.

However, according to the Machinery Directive, only one manufacturer is responsible for the design and manufacture of the machine. This manufacturer or his authorised representative takes responsibility for implementing the administrative procedures for the entire plant. The manufacturer may appoint an authorised representative, who must be established in the EU, to assume responsibility for the necessary procedures for placing the product on the market:

- ▶ Compiling the plant's technical documentation
- ▶ Complying with the technical annex
- ▶ Providing operating instructions for the plant
- ▶ Affixing the CE mark in a suitable position on the plant and drawing up a declaration of conformity for the entire plant

▶ 2.2 CE marking

It's important that the manufacturer considers the safety aspect early, as the contracts are being formulated or in the components' requirement manual. The documentation shall not be compiled solely from the point of view of machine performance. The manufacturer is responsible for the whole of the technical documentation and must determine the part that each of his suppliers is to undertake in this process.

2.2.3.3 Use of machinery in the European Economic Area

Irrespective of the place and date of manufacture, all machinery used in the European Economic Area for the first time from 01.01.1995 is subject to the EU Machinery Directive and as such must be CE certified.

2.2.3.4 Assembled machinery

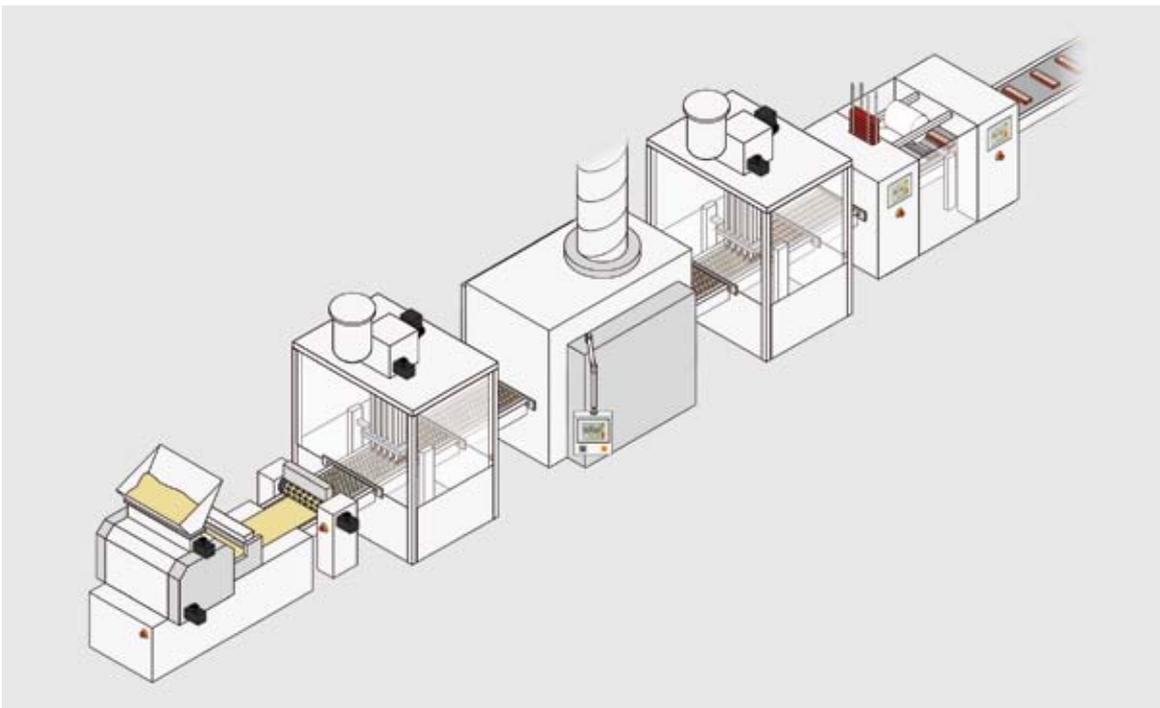
On large production lines a machine may often consist of several individual machines assembled together. Even if each of these bears its own CE mark, the overall plant must still undergo a CE certification process.

2.2.3.5 Importing a machine from a country outside the EU

When a machine is imported from a third country for use within the EU, that machine must comply with the Machinery Directive when it is made available on the EU market. Anyone who places a machine on the market for the first time within the European Economic Area must have the necessary documentation to establish conformity, or have access to such documentation. This applies whether you are dealing with an "old machine" or new machinery.

2.2.3.6 Machinery for own use

The Machinery Directive also obliges users who manufacture machinery for their own use to comply with the Directive. Although there are no problems in terms of free trade - after all, the machine is not to be traded - the Machinery Directive is applied to guarantee that the safety level of the new machine matches that of other machines available on the market.



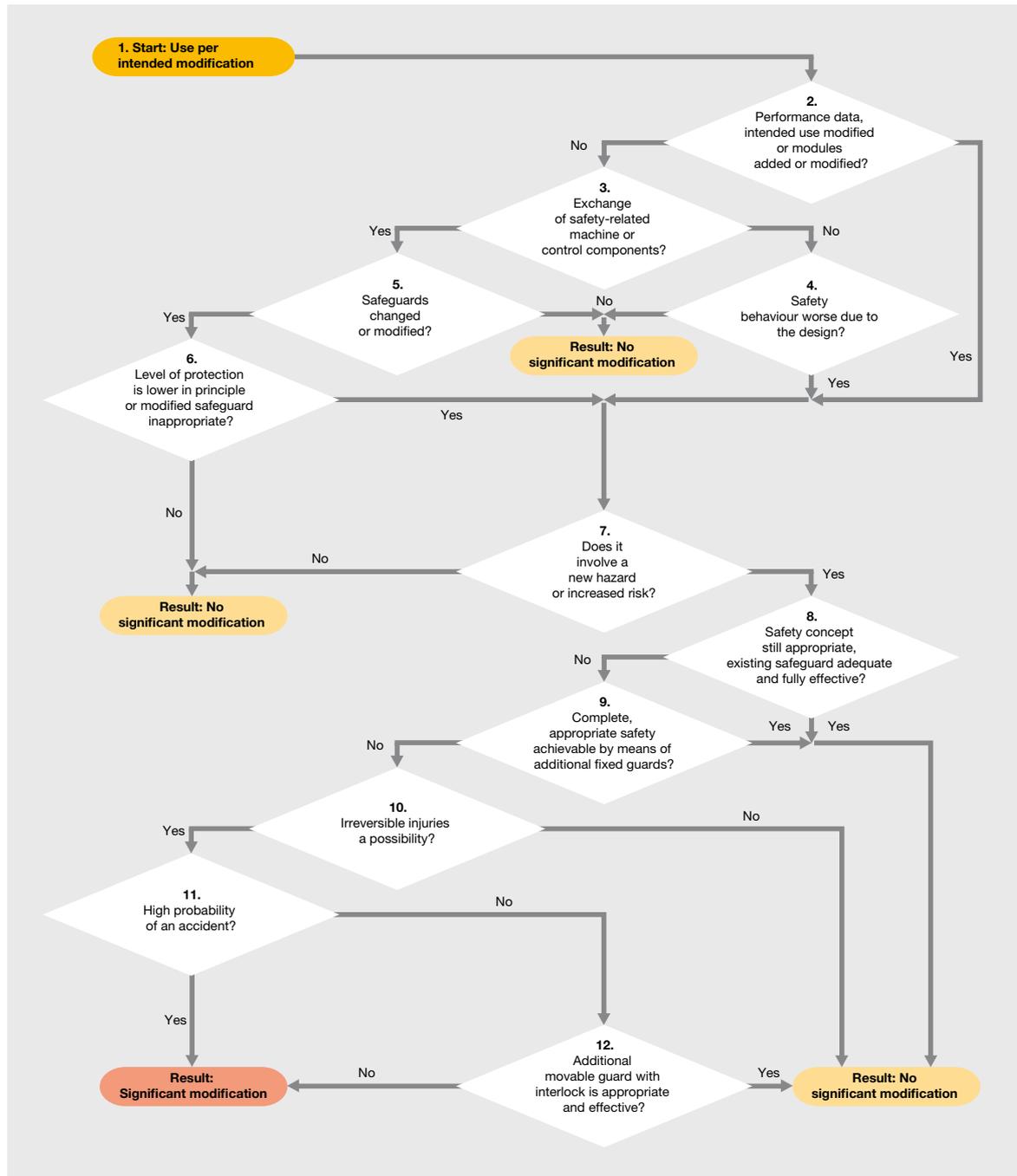
CE certification for individual machines and the overall plant.

▶ 2.2 CE marking

2.2.3.7 Upgrading machinery

Essentially, the Machinery Directive describes the requirements for new machinery. However, if a machine is modified to such an extent that new

hazards are anticipated, an analysis will need to be carried out to determine whether the upgrade constitutes a significant modification. If this is the case, the measures to be taken will be the same as those for new machinery.



“Significant modification” decision tree, as per “Significant modifications to machinery” from the chemical industry trade association BG Chemie.

▶ 2.2 CE marking

2.2.3.8 Interlinked machinery

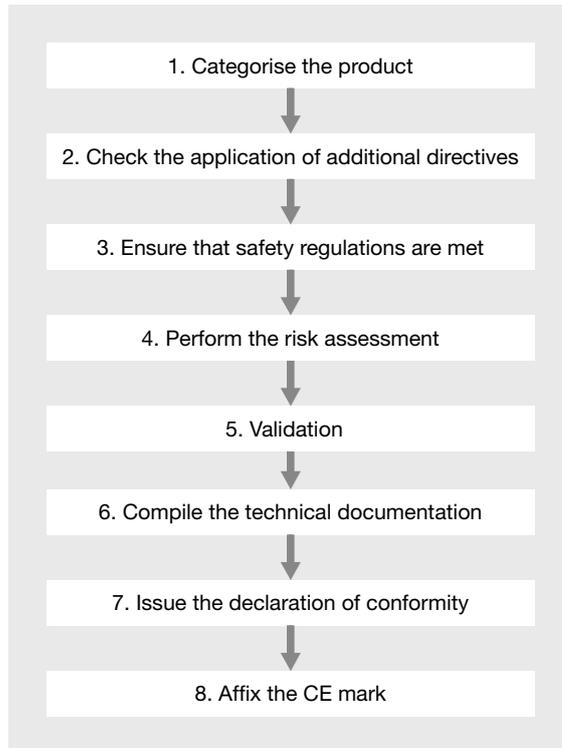
A system can no longer be regarded as a single machine if an event on one machine has a safety-related impact on another machine and this cannot be prevented by appropriate safeguards. The fundamental principle applies: an interlinked plant must comply with the current legal status (particularly with regard to the Machinery Directive) and the conformity assessment procedure must be repeated for the entire plant.

Normally, the newly added machine and the interface between the new and existing machine must first undergo a risk assessment to work out the appropriate safety measures. On this basis a safety concept is developed, along with the safety design (specification of safety requirements) and the system integration. The process is completed with verification of the safety functions, to demonstrate that the safety measures that have been implemented meet all the requirements. And also with interlinked machinery, the process must end with the declaration of conformity for the whole system.

A particular challenge exists if existing machinery is to be linked to new machinery, which has been built with reference to different standards. In particular this is the case if a machine built to EN 954-1 is to be linked to another machine, which has been manufactured to 13849-1. EN 954-1 was valid until 31.12.2011. It included the integration of safety technology, but not the verification of components. The current standard EN ISO 13849-1 requires safety functions to be verified. In this case, the data for the safety functions for both machines is available in different forms, which makes it more difficult to validate the new, interlinked machine. With its extensive experience, Pilz can provide support in such cases. As an authorised representative, Pilz can perform the whole EC conformity assessment procedure for third parties, always taking current standards into account.

▶ 2.2 CE marking

2.2.3.9 Eight steps to a CE mark



Step 1: Categorise the product

The CE marking process starts by categorising the product. The following questions need to be answered:

- ▶ Is the product subject to the Machinery Directive?

Here it's important to note that in the Machinery Directive 2006/42/EC (in contrast to its predecessor), some new products have been introduced (e.g. pressure vessels, steam boilers and funicular railways), while others have been omitted (e.g. electrical household and office equipment).

- ▶ Is the product listed in Annex IV of the Machinery Directive?

Annex IV of the Machinery Directive lists machinery that is considered “particularly hazardous”, such as presses, woodworking machinery, service lifts, etc. In this case, CE marking and the declaration of conformity must meet special requirements.

- ▶ Is the machine a subsystem or partly completed machinery?

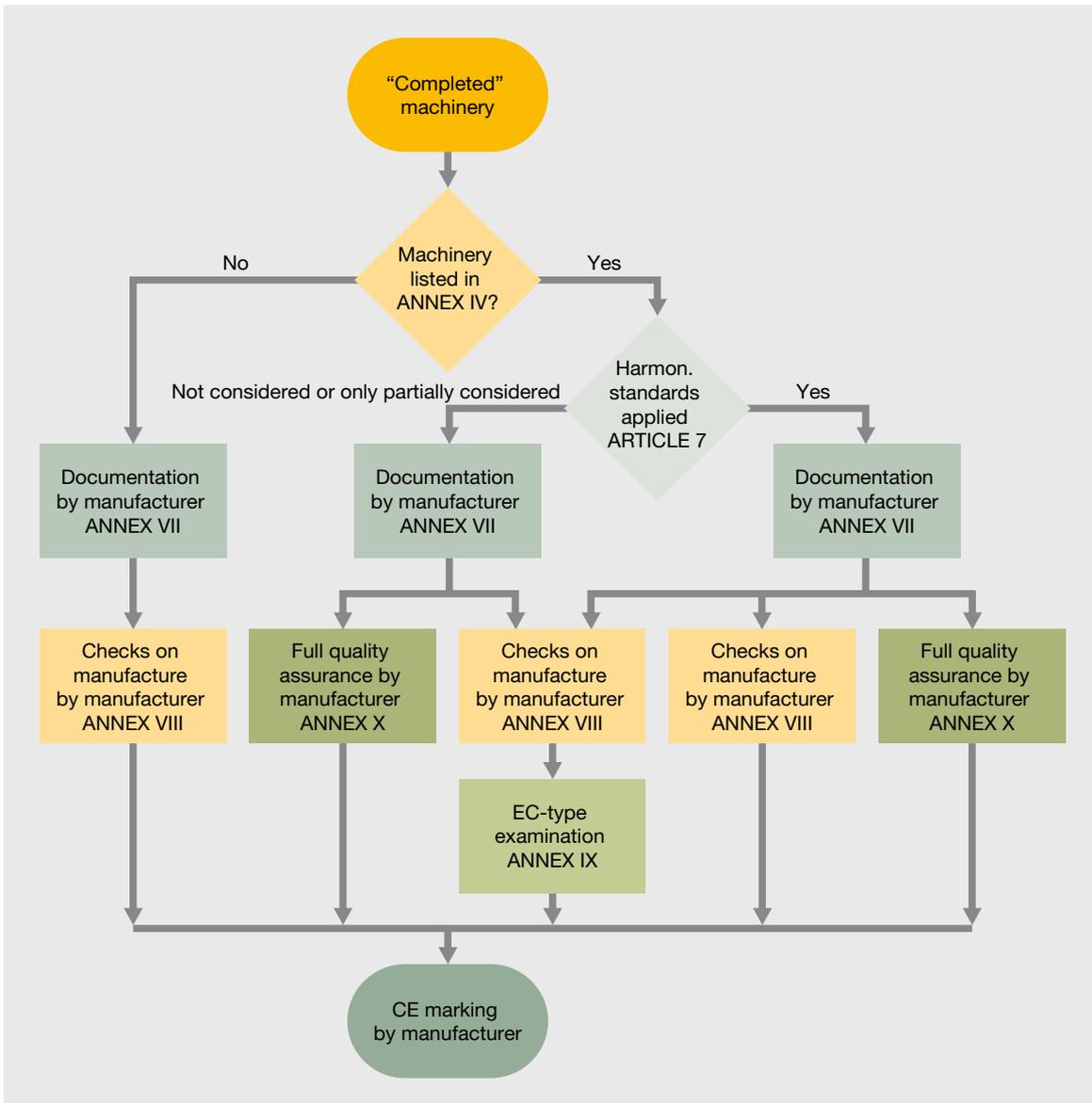
Manufacturers issue an EC declaration of conformity for functional machines that meet the full scope of Annex I of the Machinery Directive. For subsystems, e.g. robots, which cannot yet meet the full scope of Annex I, the manufacturer issues an installation declaration in accordance with Annex II B.

The new Machinery Directive refers to subsystems as “partly completed machinery”. From the moment the new Machinery Directive becomes valid, all partly completed machinery must be accompanied by a declaration of incorporation in accordance with Annex II. At the same time, the manufacturer must perform a risk assessment and provide assembly instructions in accordance with Annex VI. Effectively the manufacturer's declaration or declaration of incorporation bans the subsystem from being put into service, as the machine is incomplete and as such may not be used on its own.

▶ 2.2 CE marking

▶ Is it a safety component?

Under the Machinery Directive 2006/42/EG, safety components are treated as machinery and will therefore be given a CE mark.



Potential assessment procedures in accordance with the new Machinery Directive.

2.2 CE marking

Step 2: Check the application of additional directives

Where machinery is also subject to other EU directives, which cover different aspects but also provide for the affixing of the CE mark, the provisions of these directives must be met before the CE mark is applied. If the machine contains electrical equipment, for example, it will often be subject to the Low Voltage Directive and, possibly, the EMC Directive too.

Step 3: Ensure that safety regulations are met

It is the responsibility of the machine manufacturer to comply with the essential health and safety requirements in accordance with Annex I of the Machinery Directive. The formulation of these requirements is relatively abstract, but specifics are provided through the EU standards.

The EU publishes lists of directives and the related harmonised standards. Application of these standards is voluntary, but compliance does provide presumption of conformity with the regulations. This can substantially reduce the amount of evidence required, and a lot less work is needed to incorporate the risk assessment.

▶ 2.2 CE marking

Step 4: Perform the risk assessment

Hazard identification		Hazard No: 1	
Title:	Distance of safeguard inadequate		
Location:	Press loading area		
Target:	Upper extremities		
Activity:	Normal mode		
Task:	Operation		
Function:	Minor corrections during operation		
Type of hazard:	Mechanical		
Subtype:	Risk of crushing		
Description:	The operator is protected from the tool's hazardous movement by a light curtain. However, the machine is not far enough away. It is possible to reach the danger zone before the tool has come to a standstill.		
Risk estimation and assessment			
Probability of occurrence	2	Frequency of event:	4
Degree of possible harm	8	Number of persons affected:	1
Hazard Rating Number (HRN):	64.0	Overall result:	High risk
Risk reduction		Reference	
Replace light curtain with a tunnel at least 1 m in length. Access will effectively be prevented as a result. The side safety gate is used for access during operation.		EN 1088:1995: EN ISO 13855:2008	
Anticipated residual risk			
Probability of occurrence	0.033	Frequency of event:	4
Degree of possible harm	2	Number of persons affected:	1
Hazard Rating Number (HRN):	0.264	Overall result:	Negligible risk

Extract from a risk assessment.

▶ 2.2 CE marking

The manufacturer is obliged to carry out a risk assessment to determine all the hazards associated with his machine. The result of this assessment must then be considered in the design and construction of that machine. The contents and scope of a hazard analysis are not specified in any directive, but EN ISO 12100 describes the general procedure.

All relevant hazards must be identified, based on the intended use – taking into consideration all the lifecycles once the machine is first made available on the market. All the various groups who come into contact with the machine, such as operating, cleaning or maintenance staff for example, are also considered.

The risk is assessed and evaluated for each hazard. Risk-reducing measures are established in accordance with the state of the art and in compliance with the standards. The residual risk is assessed at the same time: If it is too high, additional measures are required. This iterative process is continued until the necessary safety is achieved.

Step 5: Validation

Validation is now one of the key steps in the conformity assessment procedure. Essentially it proves that a machine complies with safety regulations. All information about validation is available in Chapter 2.6.

Step 6: Compile the technical documentation

In accordance with the Machinery Directive, technical documentation specifically comprises:

- ▶ An overall drawing of the machinery and drawings of the control circuits
- ▶ Full, detailed drawings (accompanied by any calculation notes, test results, etc.) required to check the conformity of the machinery with the essential health and safety requirements
- ▶ A list of the essential requirements of this directive, standards and other technical specifications used in the design of the machinery, a description of the protective measures implemented to eliminate hazards presented by the machinery (generally covered by the risk assessment)
- ▶ Technical reports or certificates; reports or test results showing conformity
- ▶ The machine's operating instructions
- ▶ A general machine description
- ▶ Declaration of conformity or declaration of incorporation plus the assembly instructions
- ▶ Declarations of conformity for the machines or devices incorporated into the machinery

This documentation does not have to be permanently available in material form. However, it must be possible to assemble it and make it available within a period of time commensurate with its importance. It must be retained for at least ten years following the date of manufacture and be available to present to the relevant national authorities. In the case of series manufacture, that period shall start on the date that the last machine is produced.

▶ 2.2 CE marking

Step 7: Issue the declaration of conformity

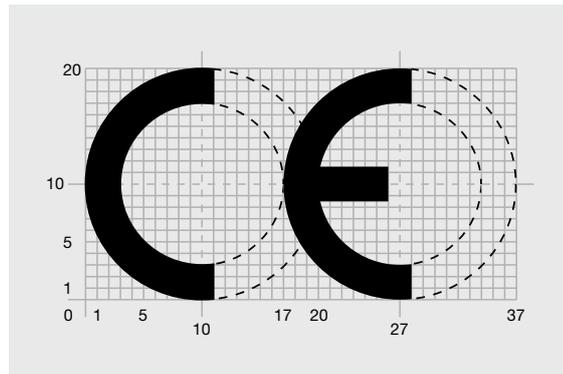
By issuing the EC declaration of conformity, the manufacturer declares that they have considered all the directives that apply to the product. The person signing an EC declaration of conformity must be authorised to represent his company. This means that the signatory is legally entitled to execute a legal transaction, such as signing the EC declaration of conformity, on account of their job function.

When an authorised employee of the company adds their valid signature to an EC declaration of conformity, they trigger the liability of the natural responsible person and, if applicable, the company as a legal entity.

The declaration may also be signed by an authorised representative, who is established in the EU.

The Machinery Directive requires the declaration to name the person authorised to compile the technical documentation. This person must be established in the EU.

Step 8: Affix the CE marking



CE mark characteristics

The CE mark may be affixed once the EC declaration of conformity has been issued.

It's important that CE marking for the complete machine is clearly distinguishable from any other CE markings, e.g. on components. To avoid confusion with any other markings, it is advisable to affix the CE marking for the complete machine to the machine type plate, which should also contain the name and address of the manufacturer.

▶ 2.3 Directives

Of the almost 30 active directives now available, only a small selection is relevant to the typical machine builder. Some directives may have a very long or bureaucratic title in addition to the directive number (e.g. 2006/42/EC). Variations can be seen in the last part of the directive number. This will contain EC, EU, EG, EWG or some other abbreviation, depending on the language area and issue

date. As a result it is generally very difficult to name the directive. These long titles are often abbreviated separately, even though this can also lead to misunderstandings. Here is a list of some of the key directives with both their official title and their usual, though unofficial, abbreviated title:

Directive	Abbreviated title (unofficial)	Official title
2006/42/EC	Machinery Directive	Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)
2001/95/EC	Product Safety Directive	Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety
2004/108/EC	EMC Directive	Directive 2004/108/EC of the European Parliament and of the Council of 15 December 2004 on the approximation of the laws of the Member States relating to electromagnetic compatibility and repealing Directive 89/336/EEC
1999/5/EC	Radio Equipment Directive	Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity
2003/10/EC	Noise Directive	Directive 2003/10/EC of the European Parliament and of the Council of 6 February 2003 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (noise)
2006/95/EC	Low Voltage Directive	Directive 2006/95/EC of the European Parliament and of the Council of 12 December 2006 on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits
89/686/EEC	Personal Protective Equipment Directive	Council Directive on the approximation of the laws of the Member States relating to personal protective equipment

The aim of the directives is to guarantee freedom of movement within the EU. The full texts of the directives <http://eur-lex.europa.eu/de/legis/index.htm> are available from the EU. Of all these directives, only the Machinery Directive will be examined here in any further detail. However, the list of relevant standards will naturally refer to standards that relate to other directives.

▶ 2.3 Directives

2.3.1 Machinery Directive

2006/42/EC has special significance in terms of the functional safety of machinery. This directive, generally known as the “Machinery Directive”, is concerned with the standardisation of European safety requirements on machinery.

2.3.1.1 Content

The Machinery Directive covers the key aspects of machine safety. The contents of the Machinery Directive are as follows:

- ▶ Scope, placing on the market, freedom of movement
- ▶ Conformity assessment procedures
- ▶ CE marking
- ▶ Essential health and safety requirements
- ▶ Categories of machinery and the applicable conformity assessment procedures
- ▶ EC declaration of conformity and type-examination
- ▶ Requirements of notified bodies

2.3.1.2 Validity

The Machinery Directive 2006/42/EC replaced the previous version 98/37/EC with effect from 29.12.2009. There was no transition period.

2.3.1.3 Standards relating to the Machinery Directive

At this point, it makes no sense to name all the standards that are listed under the Machinery Directive and are therefore considered as harmonised. As of Autumn 2013, there were more than 760 standards listed directly. To then add all the standards that are relevant indirectly via the standards that are listed directly, would go far beyond the scope of this compendium. The following chapters will therefore concentrate on those standards for the Machinery Directive which are of general significance.

▶ 2.4 Standards

2.4.1 Publishers and scope

At European level, harmonisation of the legislation also triggered harmonisation of the standards. Traditionally, almost every country has one or more of its own standards institutes. There are also some international co-operations. This means that the same standard is published at different levels under different names. In most if not all cases, the generic name of the standard is continued and recognisable as part of the national standard name. More about that below.

2.4.1.1 International standards

At international level, the most important publishers of engineering standards are probably the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO), both of which are based in Geneva. While the IEC is primarily concerned with electrical and electronic issues, ISO deals mainly with mechanical issues. Well over 100 countries are currently members of the two organisations, which gives considerable weight to those standards developed by IEC and ISO.

The EN standards are applied at European level. EN standards are normally developed through CEN and CENELEC as an EU initiative. As with IEC and ISO, CEN and CENELEC divide up the standards. CENELEC is responsible for electrical issues.

Today, many standards are developed almost in a package as an IEC or ISO standard in co-operation with the EU via CEN and CENELEC. EN IEC or EN ISO standards are the result of these efforts.

2.4.1.2 National standards

The diversity of national standards and standards institutes is almost unmanageable. In the EU at least, the aim is to produce the majority of standards directly as an EN standard, which is then reflected at national level, i.e. the EN standard is declared a national standard or the national standard is introduced as an EN standard.

In Germany for example, the German Institute for Standardization (Deutsche Institut für Normung - DIN) is responsible for publishing national standards. Today it's common practice for DIN standards to be developed and published directly in conjunction with CEN or CENELEC as DIN EN ISO or DIN EN. The only difference between these standards is usually the national preface to the EN, ISO or IEC standard.

The same standard will come into effect at EU level as an EN ISO or EN IEC standard, while the identical German standard is called DIN EN ISO or DIN EN. In other European countries, the procedure is virtually the same except that a different institute publishes the standard. In Austria, this will be the Austrian Standards Institute (Österreichisches Normungsinstitut - ÖNorm), while Great Britain has the British Standard (BS).

If an ISO standard becomes an EN standard, its title will be EN ISO. If it then becomes a DIN standard, its full title will be DIN EN ISO. The more local the institute, the further forward it appears in the name. One curious aside: If an IEC standard becomes an EN standard, the IEC name is dropped. IEC 61508 becomes the European standard EN IEC 61508 or the German DIN EN IEC 61508.

While many countries such as China or Switzerland, for example, also follow the European procedure for a centralised standards institute, there are still some nasty surprises to be had elsewhere. In the USA, standards are published by ANSI, RSA and UL, among others. Sometimes there are co-operations such as ANSI ISO or UL IEC standards, but unfortunately there is no simple rule.

▶ 2.4 Standards

2.4.2 EN engineering safety standards

There is no intention at this point to provide a complete list of the European engineering safety standards. Over 760 standards are listed as harmo-

nised under the Machinery Directive alone. The following section addresses a selection of the general safety standards. They are explained in various degrees of detail, depending on the significance of the individual standard.

Standard	Harmonised	Title
EN 349:2008	Yes	Safety of machinery Minimum gaps to avoid crushing of parts of the human body
EN 547-1 to -3:2008	Yes	Safety of machinery Human body measurements
EN 574:2008	Yes	Safety of machinery Two-hand control devices – Functional aspects Principles for design
EN 953:2009	Yes	Safety of machinery Safety of machinery. Guards. General requirements for the design and construction of fixed and movable guards
EN 1005-1 to -4:2008 EN 1005-5:2007	Yes No	Safety of machinery Human physical performance
EN 1037:2008 identical to ISO 14118:2000	Yes	Safety of machinery Prevention of unexpected start-up
EN ISO 14119* Replaces EN 1088:2008 and ISO 14119:2006	Yes	Safety of machinery Interlocking devices associated with guards. Principles for design and selection
EN ISO 11161:2010	No	Safety of machinery Integrated manufacturing systems – Basic requirements
EN ISO 12100:2010 replaces EN ISO 12100-1 and 2; EN ISO 14121; EN 292	Yes	Safety of machinery General principles for design. Risk assessment and risk reduction
EN 12453:2000	No	Industrial, commercial and garage doors and gates. Safety in use of power operated doors – Requirements
EN ISO 13849-1:2009	Yes	Safety of machinery Safety-related parts of control systems – Part 1: General principles for design
EN ISO 13849-2:2012	Yes	Safety of machinery Safety-related parts of control systems – Part 2: Validation
EN ISO 13855:2010 replaces EN 999	Yes	Safety of machinery Positioning of safeguards with respect to the approach speeds of parts of the human body
EN ISO 13857:2008	Yes	Safety of machinery Safety distances to prevent hazard zones being reached by upper and lower limbs
ISO 14119:2006 equates to EN 1088:2007	No	Safety of machinery Interlocking devices associated with guards. Principles for design and selection

*Expected publication date: 2013 or 2014

▶ 2.4 Standards

Standard	Harmonised	Title
ISO TR 23849:2010 identical to IEC TR 62061-1:2009	No	Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery
EN 60204-1:2010	Yes	Safety of machinery Electrical equipment of machines - Part 1: General requirements
EN 60947-5-1:2009 EN 60947-5-2:2012 EN 60947-5-3:2005 EN 60947-5-4:2003 EN 60947-5-5:2013 EN 60947-5-6:2001 EN 60947-5-7:2003 EN 60947-5-8:2006 EN 60947-5-9:2007	Yes	Low voltage switchgear and controlgear Part 5: Control circuit devices and switching elements
EN 61326-3 Parts 1+2:2008	No	Electrical equipment for measurement, control and laboratory use. EMC requirements
EN 61496-1:2010	Yes	Safety of machinery Electrosensitive protective equipment – Part 1: General requirements and tests
IEC 61496-2:2013 CLC/TS 61496-2:2006:	No	Safety of machinery Electrosensitive protective equipment – Part 2: Particular requirements for equipment using active optoelectronic protective devices (AOPDs)
CLC/TS 61496-3:2008 replaces EN 61496-3:2003	No	Safety of machinery Electrosensitive protective equipment – Part 3: Particular requirements for active optoelectronic protective devices responsive to diffuse reflection (AOPDDR)
EN 61508 Parts 1-7:2010	No	Functional safety of safety-related electrical, electronic and programmable electronic control systems
EN 61511 Parts 1-3:2004	No	Functional safety – Safety instrumented systems for the process industry sector
EN 61784-3:2010	No	Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions
EN 61800-5-2:2007	Yes	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements. Functional
IEC/TS 62046:2008	No	Safety of machinery Application of protective equipment to detect the presence of persons
EN 62061:2011	Yes	Safety of machinery Functional safety of safety-related electrical, electronic and programmable electronic control systems
IEC/TR 62685:2010	No	Industrial communication networks – Profiles – Assessment guideline for safety devices using IEC 61784-3 functional safety communication profiles (FSCPs)
NFPA 79:2013	No	Industrial machinery

▶ 2.4 Standards

2.4.3 Generic standards and design specifications

2.4.3.1 EN ISO 12100 and EN ISO 14121

Standard	Harmonised	Title
EN ISO 12100:2010 replaces EN ISO 12100-1 and 2; EN ISO 14121-1 Transition period until 30.11.2013	Yes	Safety of machinery General principles for design. Risk assessment and risk reduction

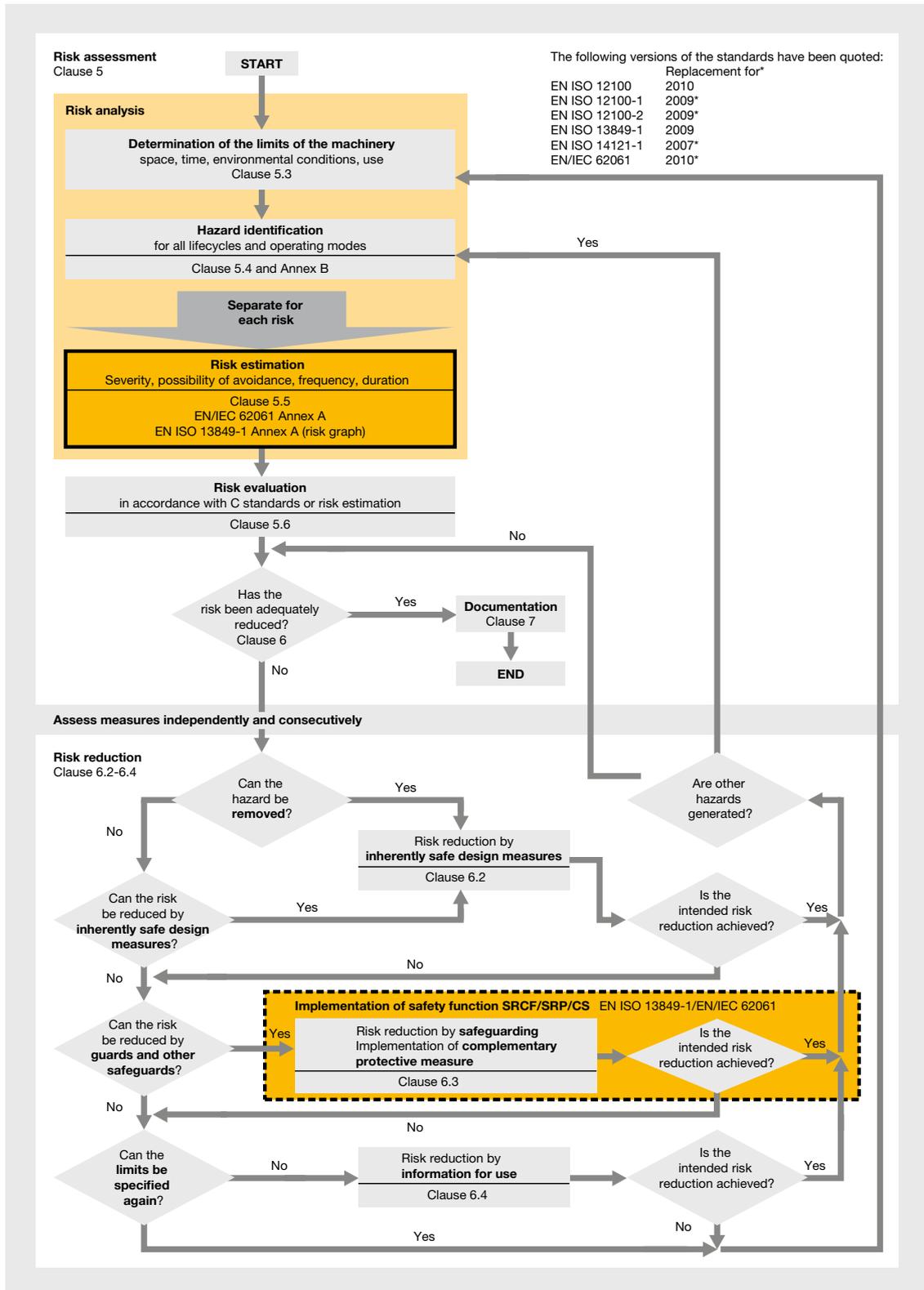
In 2010, EN ISO 12100 provided a further summary of EN 12100-1 and -2 plus EN 14121-1. This standard is identical in content to the named standards and simply summarises them within one document. The transition period in which the standards can coexist has been set until 30.11.2013.

The diagram overleaf (see page 3-21) identifies the individual elements examined in these standards. This standard provides a good selection of the hazards, risk factors and design principles that need to be considered.

Elements within the diagram that have a dark yellow background are the areas covered by the user standards EN ISO 13849-1 and EN/IEC 62061 and are examined there in greater detail. Where possible the diagram refers to the corresponding clauses that cover the relevant aspect within the standards. Some points can certainly be found in several standards, but the level of detail generally varies.



2.4 Standards



Risk estimation and risk reduction in accordance with EN ISO 12100.

▶ 2.4 Standards

2.4.3.2 IEC/TR 62685 Test requirements and EMC

Standard	Harmonised	Title
IEC/TR 62685:2009	No	Industrial communication networks – Profiles – Assessment guideline for safety devices using IEC 61784-3 functional safety communication profiles (FSCPs)

IEC/TR 62685 was produced from the test requirements of the German BGIA document GS-ET-26 and covers the requirements of safety components within a safety function. It covers the issue of labelling and EMC as well as mechanical and climatic tests. This closes some of the gaps left by EN ISO 13849-1 and EN 61784-3. Overall the

document is more relevant to safety component manufacturers than plant and machine builders. However, as the document contains a good comparison of EMC requirements, it may also be of interest to machine builders.

2.4.3.3 EN 61784-3 Safe fieldbuses

Standard	Harmonised	Title
EN 61784-3:2010	No	Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions

The EN 61784-3 series of standards covers a whole range of safety enhancements for different fieldbus profiles, based on the specifications of EN 61508. These enhancements are handled as security profiles and describe the mechanisms and technical details of these profiles. For the average machine builder, at most the generic part of EN 61784-3 will be of interest, as this is the part that describes the general safety principles. The profile documents EN 61784-3-x are mainly intended for device

manufacturers who wish to build their own safety devices in accordance with one of the published profiles. In this case, it makes sense to work in cooperation with the relevant user groups behind these profiles, as they will be familiar with the basic profiles described in the series EN 61784-1 and -2, as well as EN 61158. A complete profile consisting of the relevant parts of EN 61784 and EN 61158 will contain between 500 and 2,000 pages. All the profiles together amount to around 10,000 pages.

▶ 2.4 Standards

2.4.3.4 EN ISO 13849-1

Standard	Harmonised	Title
EN ISO 13849-1:2009	Yes	Safety of machinery Safety-related parts of control systems – Part 1: General principles for design
EN ISO 13849-2:2012	Yes	Safety of machinery Safety-related parts of control systems - Part 2: Validation

Content

EN ISO 13849-1 addresses the issue of risk assessment using a risk graph and also deals with the validation of safety functions based on structural and statistical methods. The objective is to establish the suitability of safety measures to reduce risks. EN ISO 13849-2 describes the validation aspect pertinent to EN ISO 13849-1. So together, both standards are practically equal (but not identical) to EN 62061.

The work involved in making the calculations required under this standard can be reduced considerably if appropriate software is used. Calculation tools such as the Safety Calculator PASCAL are available as free software:
<http://www.pilz.de/products/software/tools/f/pascal/index.de.jsp>



PASCAL Safety Calculator

Scope

EN ISO 13849-1 is a generic standard for functional safety. It has been adopted at ISO level and within the EU is harmonised to the Machinery Directive. It therefore provides presumption of conformity within the EU. The scope is given as the electrical, electronic, programmable electronic, mechanical, pneumatic and hydraulic safety of machinery.

Risk assessment/risk analysis

Risks are assessed in EN ISO 13849-1 with the aid of a risk graph. The assessed criteria include severity of injury, frequency of exposure to the risk and the possibility of avoiding the risk. The outcome of the assessment is a required performance level (PL) for the individual risks.

In subsequent stages of the risk assessment, the levels determined using the risk graph are aligned with the selected risk reduction measures. For each classified risk, one or more measures must be applied to prevent the risk from occurring or to sufficiently reduce the risk. The quality of the measure in the performance level must at least correspond to the level determined for the respective risk.

▶ 2.4 Standards

Determination of the required performance level PL_r

Just 3 parameters need to be examined to assess the performance level (PL):

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

Frequency and/or exposure to a hazard	F
Seldom to less often and/or exposure time is short	F ₁
Frequent to continuous and/or exposure time is long	F ₂

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

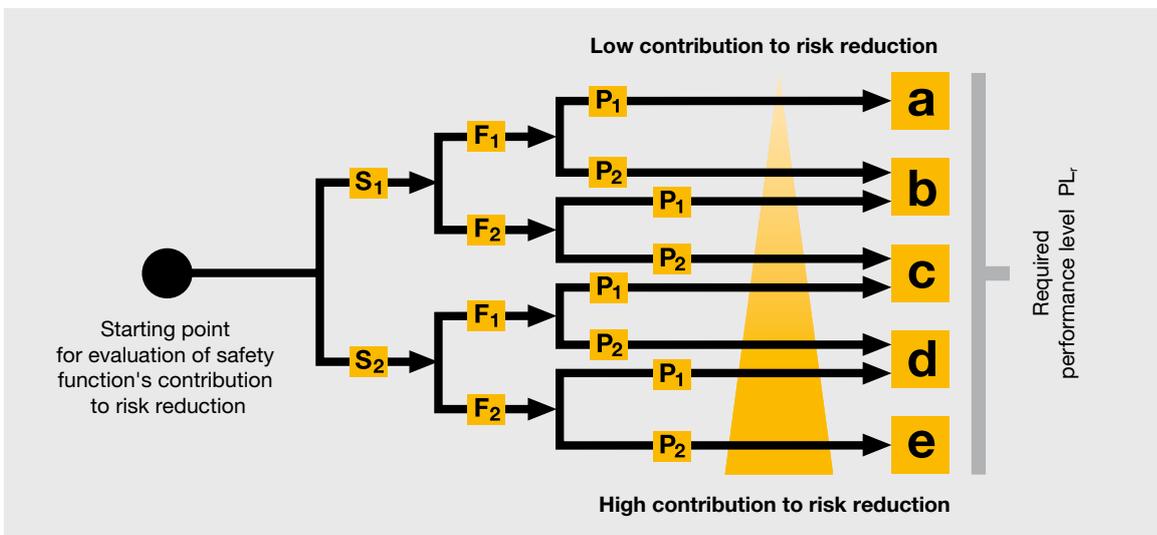
The required performance level PL_r is calculated using the following graph and the classification of the individual parameters.

Assessment of the risk begins at the starting point on the graph and then follows the corresponding path, depending on the risk classification. The required performance level PL_r a, b, c, d or e is determined once all the parameters have been assessed.

Assessing the implementation/examining the system

EN ISO 13849-1 works on the assumption that there is no such thing as a safe device. Devices only become suitable through an appropriate design for use in applications with increased requirements. As part of an assessment each device is given a PL, which describes its suitability. Simple components can also be described via their MTTF_d (Mean time to dangerous failure) or B10_d value (Mean number of cycles until 10% of the components fail dangerously).

The following considerations examine how the failure of devices or their components affects the safety of the system, how likely these failures are to occur and how to calculate the PL.



Risk graph in accordance with EN ISO 13849-1.

▶ 2.4 Standards

Determination of common cause failures – CCF factor

The CCF factor is determined through a combination of several individual assessments. One of the first key parameters to examine is the system architecture. Systematic effects in particular need to be assessed, such as the failure of several components due to a common cause. The competence and experience of the developers are also evaluated, along with the analysis procedures. An evaluation scale is used, on which a score of between 0 and 100% can be achieved.

Requirement	Score
Physical separation of safety circuits and other circuits	15 %
Diversity (use of diverse technologies)	20 %
Design/application/experience	20 %
Assessment/analysis	5 %
Competence/training	5 %
Environmental influences (EMC, temperature, ...)	35 %

With EN ISO 13849-1, the effect of the CCF is deemed acceptable if the total score achieved is > 65%.

PL assessment

IEC ISO 13849-1 uses the diagnostic coverage (DC), system category and the system's $MTTF_d$ to determine the PL (performance level). The first value to be determined is the DC. This depends on λ_{DD} (failure rate of detected dangerous failures) and λ_{Dtotal} (failure rate of total dangerous failures). In the simplest case this is expressed as:

$$DC = \Sigma \lambda_{DD} / \Sigma \lambda_{Dtotal}$$

On complex systems, an average DC_{avg} is calculated:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \dots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \dots + \frac{1}{MTTF_{dN}}}$$

The diagnostic coverage is determined from this DC value:

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

With homogenous or single-channel systems, the $MTTF_d$ value can be established approximately as the sum of the reciprocal values of the individual components, corresponding to the $MTTF_d$ value of a single channel:

$$\frac{1}{MTTF_d} = \sum_{i=1}^N \frac{1}{MTTF_{d,i}}$$

▶ 2.4 Standards

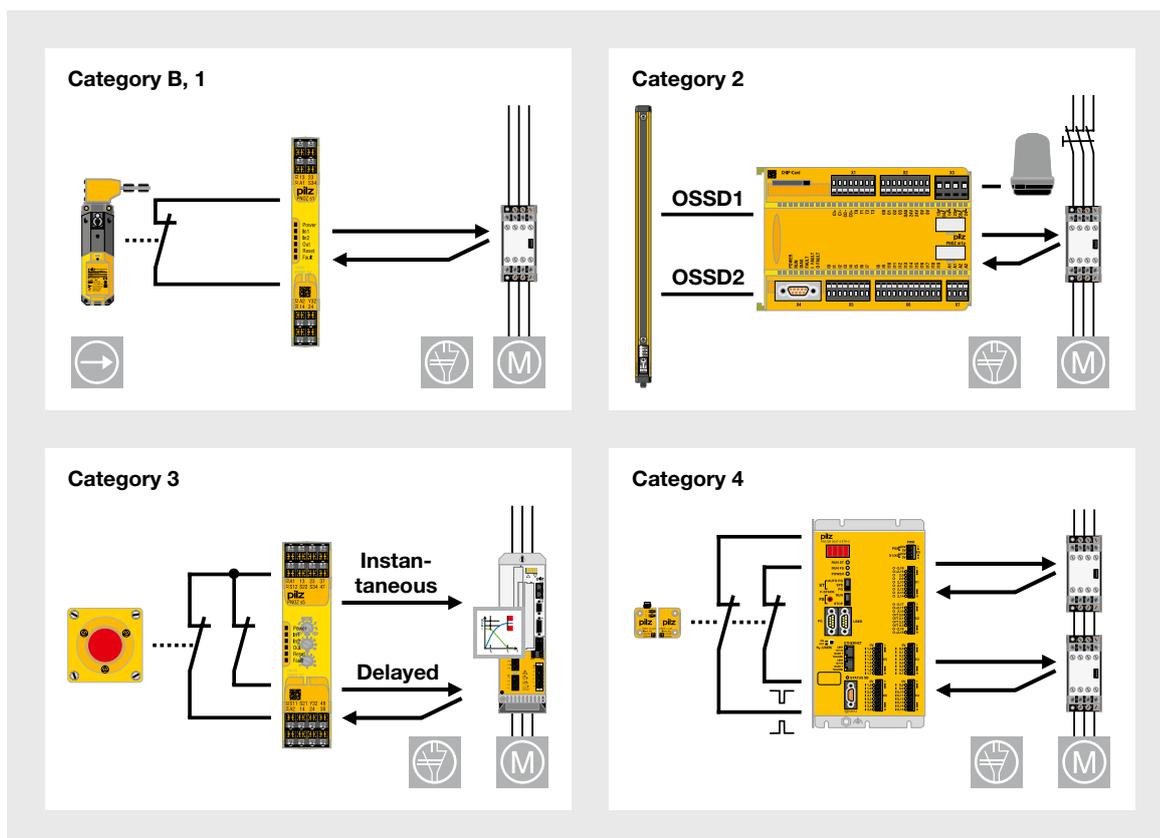
With dual-channel, diverse systems, the $MTTF_d$ value of both channels needs to be calculated separately. Both values are included in the calculation of the combined $MTTF_d$, using the formula below.

$$MTTF_d = \frac{2}{3} \left[MTTF_{d,C_1} + MTTF_{d,C_2} - \frac{1}{\frac{1}{MTTF_{d,C_1}} + \frac{1}{MTTF_{d,C_2}}} \right]$$

Here too, a table is used to derive a qualitative evaluation from the numeric value, which is then used in subsequent considerations.

Denotation of $MTTF_d$	$MTTF_d$
Low	$3 \text{ years} \leq MTTF_d < 10 \text{ years}$
Medium	$10 \text{ years} \leq MTTF_d < 30 \text{ years}$
High	$30 \text{ years} \leq MTTF_d < 100 \text{ years}$

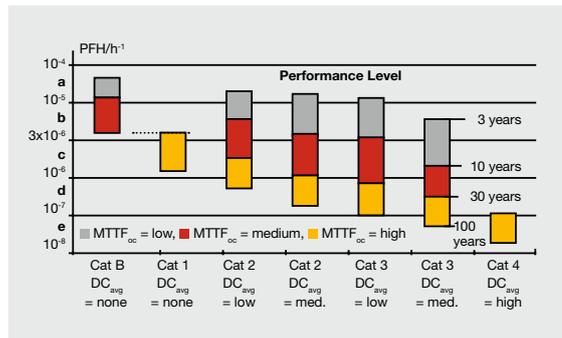
The system architecture can be divided into five different categories. The achieved category depends not only on the architecture, but on the components used and diagnostic coverages. The graphic below illustrates some classifications by way of example.



Examples for the categories in accordance with EN ISO 13849-1.

2.4 Standards

In a final assessment stage, a graphic is used to assign the PL based on the recently calculated values.



Graph to determine the PL in accordance with EN ISO 13849-1.

The most practical approach is to select the column for Category and DC first. Then choose the relevant $MTTF_d$ range from the bar. The PL result can now be read from the left-hand scale. In most cases, some interpretation will still be required, as often there is no clear relationship between the $MTTF_d$ range and the PL.

The final step is to compare the required PL_r level from the risk assessment with the achieved PL. If the achieved PL is greater than or equal to the required PL_r, the requirement for the implementation is considered to have been met.

Transition periods EN 954-1 and ISO 13849-1:1999 to EN ISO 13849-1:2009

Since 08.05.2007, EN 954-1 has ceased to be listed in the Official Journal of the EU and as such is no longer regarded as harmonised. However, it did still apply for some time, as it is named as a reference in its successor standard EN ISO 13849-1. The corresponding publication established that presumption of conformity for EN 954-1 applied until 31.12.2011. This transition period has also now elapsed.

At ISO level the current situation is that ISO 13849-1:1999 (identical content to EN 954-1) was replaced by ISO 13849-1:2006 with immediate effect. So ISO 954-1 ceased to apply in 2006. There is no transition period.

C standard refers to EN 954-1

So what happens now to the C standards, also known as product standards, which refer to EN 954-1 or ISO 13849-1:1999 and require a particular category in accordance with EN 954-1 or ISO 13849-1:1999 for specific safety functions, for example? CEN and EN have the task of resolving such problems quickly and of rewording these standards so that they refer to EN ISO 13849-1. However, the situation has arisen in which a series of C standards have not been adapted within the stipulated time. At the time of going to print (Autumn 2013), around 135 of more than 760 harmonised standards had still not been updated. The unexpected case has even arisen in which a newly published standard only quotes the (invalid) EN 954-1 and doesn't name its successor, EN ISO 13849-1.

As a result, there are valid standards that refer to the withdrawn standards EN 954-1 or ISO 13849-1:1999. References to ISO 13849-1:1999 are almost worthless as they have no direct validity in the EU. The usual procedure of referring to the successor of EN 954-1 will fail in this case because the way in which safety functions are considered has changed substantially and the categories required for implementation in EN ISO 13849-1:2009 mean something different. What does that mean for someone who needs to certify a machine for which such a C standard exists? In this case, EN 954-1 and ISO 13849-1:1999 will still be applicable, "through the back door" as it were.

▶ 2.4 Standards

Irrespective of this situation, the advice would be to carry out a separate risk assessment and certification in accordance with EN ISO 13849-1:2009. A helpful procedure is to estimate the risks described in the C standard and document the parameters S, F and P, which are present in both standards. This allows the relevant risk graphs to be used to carry out a clear risk classification for the two old standards as well as for EN ISO 13849-1:2009. If the results from the assessment in accordance with EN 954-1 or ISO 13849-1:1999 correspond to those of the C standard, this can be used to confirm the corresponding classification in accordance with EN ISO 13849-1:2009.

EN 954-1 despite the C standard referring to EN ISO 13849-1

Even if the relevant C standard for a product already refers to 13849-1:2009, it is still technically possible to apply EN 954-1. Ultimately, however, the possibility of EN 954-1 not being recognised as the state of the art in any legal dispute cannot be excluded, because it already has a successor standard (EN ISO 13849-1:2009). The state of the art is a basic requirement for the safety-related development of products in accordance with the Machinery Directive; as a result, the products concerned would not comply with the Machinery Directive, which would have direct consequences for product liability.

What does that mean for someone who needs to certify a machine for which such a C standard exists? In this case, EN 954-1 and ISO 13849-1:1999 will still be applicable, “through the back door” as it were, even after 29.12.2009. Irrespective of this situation, after this date the machine builder is still free to carry out his own risk assessment and certification in accordance with EN ISO 13849-1:2009.

As in the previous case, a helpful procedure would be to estimate the risks described in the C standard and document the parameters S, F and P, which are present in both standards. This would allow the relevant risk graphs to be used to carry out a clear risk classification for the two old standards as well as for EN ISO 13849-1:2009. If the results from the assessment in accordance with EN954-1 or ISO 13849-1:1999 correspond to those of the C standard, this can be used to confirm the corresponding classification in accordance with EN ISO 13849-1:2009.

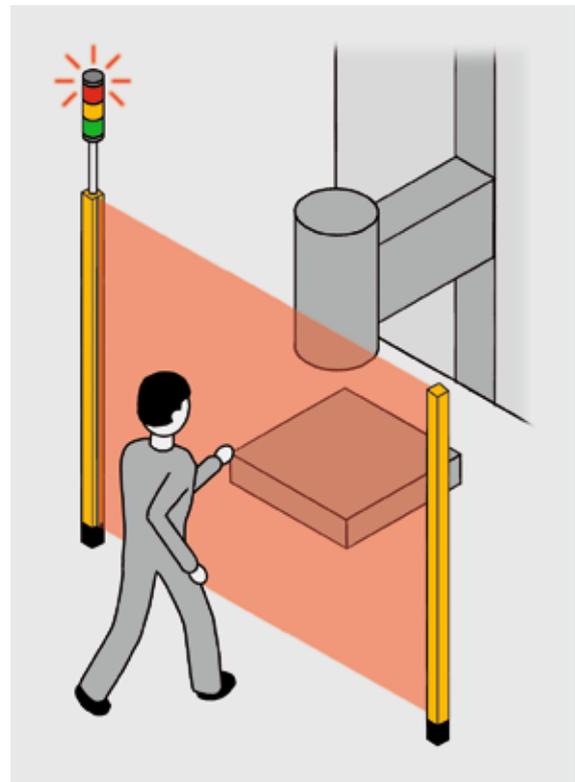
▶ 2.4 Standards

2.4.3.5 EN ISO 13855

Standard	Harmonised	Title
EN ISO 13855:2010 replaces EN 999	Yes	Safety of machinery Positioning of safeguards with respect to the approach speeds of parts of the human body

EN ISO 13855 primarily defines human approach speeds. These approach speeds need to be considered when designing safety measures and selecting the appropriate sensor technology. Different speeds and sizes are defined, depending on the direction and type of approach. Even an indirect approach is considered.

The problem regarding measurement of the overall stopping performance is considered alongside the measurement of safety distances. Clear specifications are provided as to how the overall stopping performance should and should not be measured.



Safeguards prevent operators from approaching hazardous movements.

2.4.3.6 EN ISO 13857

Standard	Harmonised	Title
EN ISO 13857:2008	Yes	Safety of machinery Safety distances to prevent hazard zones being reached by upper and lower limbs

EN ISO 13857 was first published in 2008 and examines the safety distances required to prevent hazard zones being reached by the upper and lower limbs. It is worth stressing that this standard makes it clear that different anthropometric data (size, length of limbs...) may apply for other populations or groups (e.g. Asian countries, Scandinavia,

children) and that this could give rise to other risks. Application of this standard may therefore be restricted, particularly in the public domain or when exporting to other countries.

▶ 2.4 Standards

2.4.3.7 EN 61511 Safety instrumented systems for the process industry sector

Standard	Harmonised	Title
EN 61511 Parts 1-3:2004	No	Functional safety – Safety instrumented systems for the process industry sector

The EN 61511 series of standards covers safety issues concerning plants and systems in the process industry. As a sector standard of EN 61508, the EN 61511 series is a sister standard of EN 62061. This is reflected in the similar observations and mathematical principles contained in the 3 standards. However, an important difference for most end users, as well as component manufacturers, is the differentiation between the demand modes. High demand modes have always been assumed in engineering, but EN 61511 also

recognises a low demand mode. The key characteristic for this mode is that a safety function is demanded (operated) less than once per year. As a result, EN 61511 introduced a PFD (Probability of failure on low demand) alongside the PFH (Probability of failure on high demand) and SILcl. It is particularly worth noting that the SILcl for “Low Demand Mode” may vary from the SILcl for High Demand Mode”.

2.4.3.8 EN 62061

Standard	Harmonised	Title
EN 62061:2013	Yes	Safety of machinery Functional safety of safety-related electrical, electronic and programmable electronic control systems

Content

EN 62061 addresses the issue of risk assessment using a risk graph, which in this case is in the form of a table. It also deals with the validation of safety functions based on structural and statistical methods. As with EN ISO 13849-1, the objective is to establish the suitability of safety measures to reduce risks.

As with EN 13849-1, there is considerable work involved in making the calculations required under this standard. This can be reduced considerably if appropriate software is used, such as the Safety Calculator PAScal. <http://www.pilz.de/products/software/tools/f/pascal/index.de.jsp>

Scope

EN IEC 62061 is one of the generic standards for functional safety. It has been adopted at IEC level and in the EU is harmonised as a standard within the Machinery Directive. It therefore provides presumption of conformity within the EU. The scope is given as the electrical, electronic and programmable electronic safety of machinery. It is not intended for mechanical, pneumatic or hydraulic energy sources. The application of EN ISO 13849-1 is advisable in these cases.

▶ 2.4 Standards

Risk assessment/risk analysis

Risks are assessed in IEC 62061 using tables and risk graphs. The evaluations made for each individual risk include the severity of potential injuries, the frequency and duration of exposure, the possibility of avoidance and the probability of occurrence. The outcome of the assessment is the required safety integrity level (SIL) for the individual risks.

In subsequent stages of the risk assessment, the levels determined using the risk graph are aligned with the selected risk reduction measures. For each classified risk, one or more measures must be applied to prevent the risk from occurring or to sufficiently reduce the risk. The SIL for that measure must at least correspond to the required SIL, determined on the basis of the risk.

Determination of the required SIL

According to EN IEC 62061 there are four different parameters to assess. Each parameter is awarded points in accordance with the scores in the following tables.

SIL classification, based on the above entries, is made using the table below, in which the consequences are compared with the Class CI. Class CI is the sum total of the scores for frequency, duration, probability and avoidance. Areas marked with OM indicate that the standard recommends the use of other measures in this case.

Frequency and duration of exposure	Fr < 10 min	Fr ≤ 10 min
≤ 1 hour	5	5
> 1 hour – ≤ 1 day	5	4
> 1 day – ≤ 2 weeks	4	3
> 2 weeks – ≤ 1 year	3	2
> 1 year	2	1

Probability of occurrence	Pr
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Avoidance	Av
Impossible	5
Rarely	3
Probable	1

Consequences	S	Class CI = Fr+Pr+Av				
		3-4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3
Reversible, medical attention	2			OM	SIL 1	SIL 2
Reversible, first aid	1				OM	SIL 1

OM = other measures recommended

Risk graph in accordance with EN IEC 62061.

▶ 2.4 Standards

Assessing the implementation/examining the system

The principle assumption is that there is no such thing as a safe device. Devices only become suitable through an appropriate design for use in applications with increased requirements. As part of an assessment each device is given an SIL, which describes its suitability. Simple components can also be described via their $MTTF_d$ or $B10_d$ value.

The following considerations examine how the failure of devices or their components affect the safety of the system, how likely these failures are to occur and how to calculate the SIL.

Determination of common cause failure – CCF factor

The CCF factor is determined through a combination of several individual assessments. One of the first key parameters to examine is the system architecture. Systematic effects in particular need to be assessed, such as the failure of several components due to a common cause. The competence and experience of the developer are also evaluated, along with the analysis procedures. An evaluation scale is used, on which there are 100 points to be assigned.

Requirement	Score
Physical separation of safety circuits and other circuits	20
Diversity (use of diverse technologies)	38
Design/application/experience	2
Assessment/analysis	18
Competence/training	4
Environmental influences (EMC, temperature, ...)	18

The next step is to determine the β factor (beta), based on the points achieved using the following table.

	β factor – Common cause factor
< 35	10 % (0.1)
35 - 65	5 % (0.05)
66 - 85	2 % (0.02)
86 - 100	1 % (0.01)

▶ 2.4 Standards

SIL assessment

In EN 62061, the maximum achievable SIL is determined via the dependency between the hardware fault tolerance and the safe failure fraction (SFF). The SFF is calculated by assessing all possible types of component failures and establishing whether each of these failures results in a safe or unsafe condition. The result provides the system's SFF.

The structural analysis also indicates whether there is any fault tolerance. If the fault tolerance is N, the occurrence of N+1 faults can lead to the loss of the safety function. The following table shows the maximum potential SIL, based on the fault tolerance and SFF.

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

The failure rates λ of the individual components and their λ_D fraction (dangerous failures) can be determined via PFH_D formulas, which are dependent on architecture. These formulas can be extremely complex, but always have the format:

$$PFH_D = f(\lambda_{Di}, \beta, T_1, T_2, DC_i)$$

where

T_2 Diagnostic test interval

T_1 Minimum test interval and mission time

The combined consideration of hardware, fault tolerance, category, DC, PFH_D and SFF provides the following SIL assignment. All conditions must always be met. If one single condition is not met, the SIL has not been achieved.

PFH _D	Cat.	SFF	Hardware fault tolerance	DC	SIL
$\geq 10^{-6}$	≥ 2	$\geq 60\%$	≥ 0	$\geq 60\%$	1
$\geq 2 \times 10^{-7}$	≥ 3	$\geq 0\%$	≥ 1	$\geq 60\%$	1
$\geq 2 \times 10^{-7}$	≥ 3	$\geq 60\%$	≥ 1	$\geq 60\%$	2
$\geq 3 \times 10^{-8}$	≥ 4	$\geq 60\%$	≥ 2	$\geq 60\%$	3
$\geq 3 \times 10^{-8}$	≥ 4	$> 90\%$	≥ 1	$> 90\%$	3

The final step is to compare the required SIL from the risk assessment with the achieved SIL. If the achieved SIL is greater than or equal to the required SIL, the requirement for the implementation is considered to have been met.

▶ 2.4 Standards

2.4.3.9 EN 954-1

This standard has been withdrawn and replaced by EN ISO 13849-1. See page 3-24 for details of the transition periods.

2.4.3.10 EN 60204-1

Standard	Harmonised	Title
EN 60204-1:2010	Yes	Safety of machinery Electrical equipment of machines – Part 1: General requirements

The harmonised standard EN 60204-1 considers the electrical safety of non-hand-guided machinery with voltages up to 1000 VDC and 1500 VAC. Its

scope is therefore such that there are very few industrial machines that it does not affect.

2.4.3.11 EN 61508

Standard	Harmonised	Title
EN 61508-1:2010 EN 61508-2:2010 EN 61508-3:2010 EN 61508-4:2010 EN 61508-5:2010 EN 61508-6:2010 EN 61508-7:2010	No	Functional safety of safety-related electrical, electronic and programmable electronic control systems

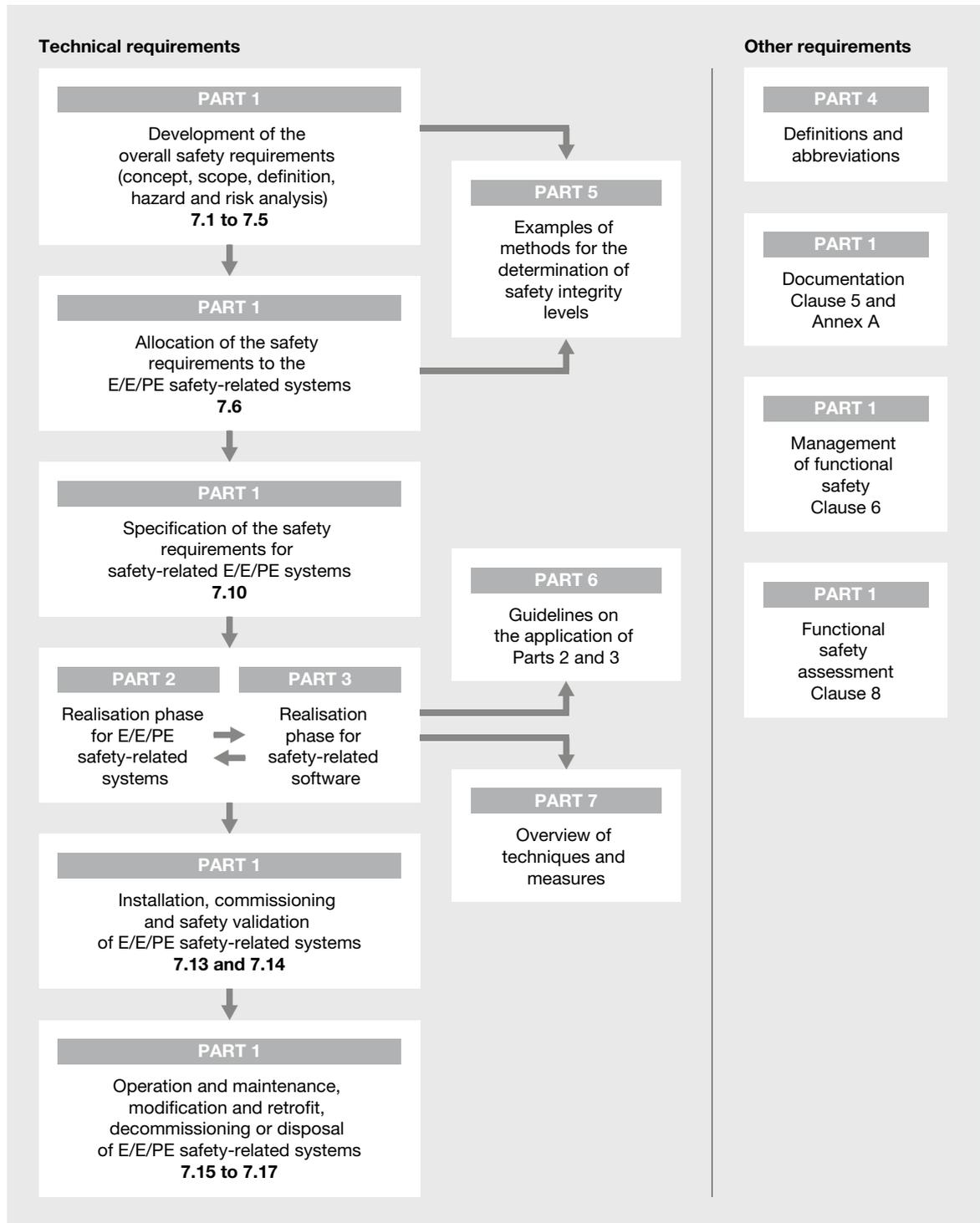
EN 61508 is the key standard dealing with the functional safety of control systems. It has 7 parts in total and all together contains around 1000 pages of text. It's important to note that EN 61508 has not been harmonised. Only its sector standard EN 62061 can claim harmonisation. The whole EN 61508 standards' package was completely revised in 2010 and Edition 2 is now available.

A key component of EN 61508 is the examination of the complete lifecycle from a safety perspective (in Part 1), with detailed requirements of the procedure and the content of the individual steps; it's essential to both machine builders and safety component manufacturers alike.

This standard is also focused on the design of electrical systems and their corresponding software. However, the standard is to be generally expanded and will also apply for all other systems (mechanics, pneumatics, hydraulics). Manufacturers of safety components such as safety relays, programmable safety systems and safety sensor/actuator technology are likely to derive the most benefit from this standard. Overall, when it comes to defining safety levels, end users or system integrators are better advised to use the much less complex EN 62061 or EN ISO 13849-1, rather than EN 61508.

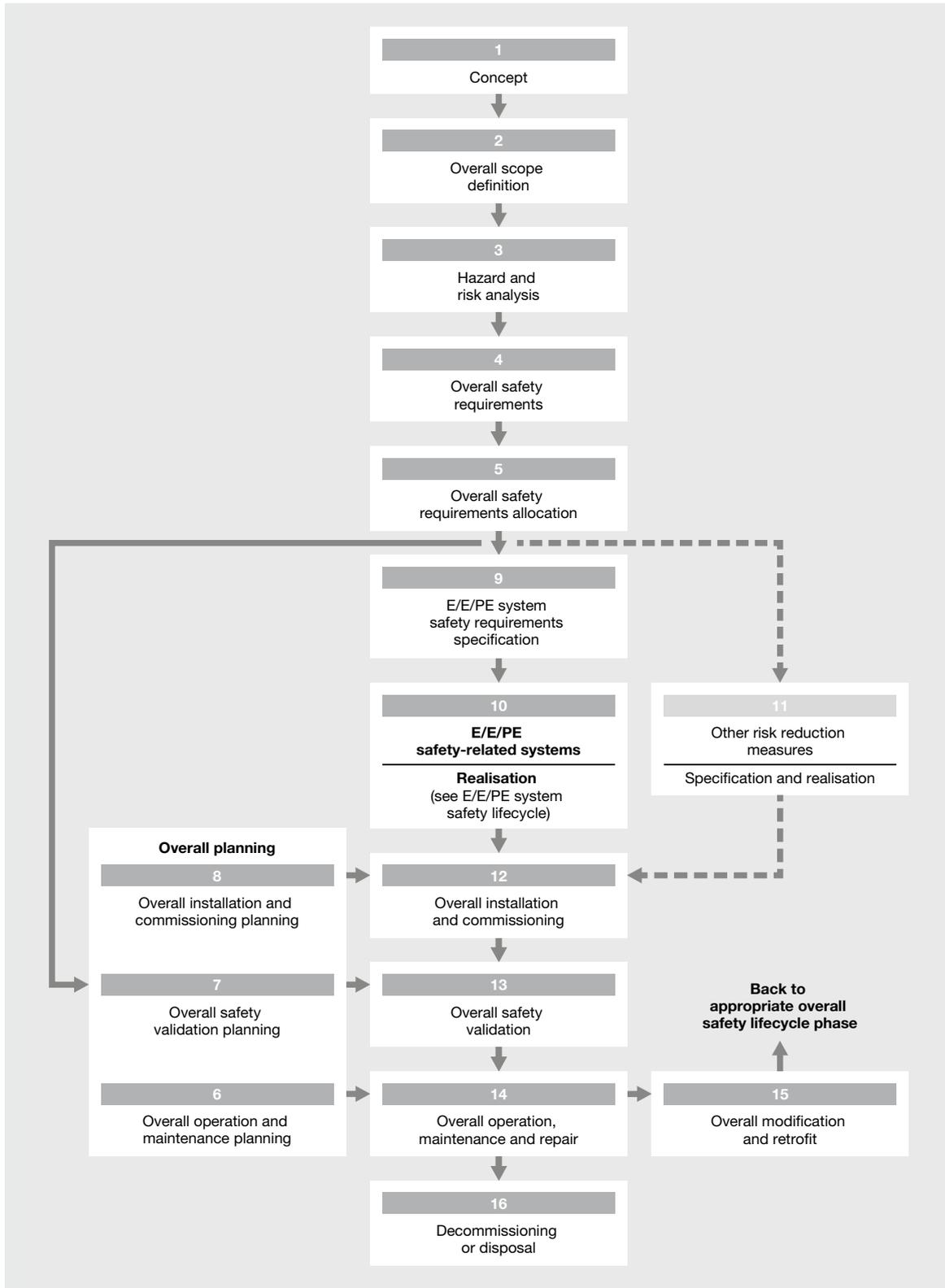
Another sector standard of EN 61508 is EN 61511, which is applicable for the process industry sector.

▶ 2.4 Standards



Extract from DIN EN 61508-1, overall framework of the safety assessment in accordance with EN 61508.
Overall framework of the IEC 61508 series of standards.

▶ 2.4 Standards



Overall safety lifecycle in accordance with EN 61508-1.

▶ 2.4 Standards

2.4.3.12 EN 61326-3

Standard	Harmonised	Title
EN 61326-3 Part 1 and 2:2008	No	Electrical equipment for measurement, control and laboratory use – EMC requirements

With the release of EN 61326-3-1 and EN 61326-3-2, since 2008 there have been two standards providing information on immunity requirements in respect of the EMC level on safety devices. Both parts have been specified with different immunity requirements. Part EN 61326-3-1 is the general section with more stringent requirements. This part was drawn up with a particular view towards mechanical engineering. In contrast, part EN 61326-3-2 was written with a view towards the process industry and the immunity requirements are significantly lower. In engineering, therefore, it should always be ensured that the test

requirements in accordance with EN 61326-3-1 are met as a minimum. As the origin of both these standards is still very recent and there are no fore-runners to refer back to, it will still be some time before they are reflected in the relevant device certificates. In general, it should be noted that product or sector standards also set EMC requirements, but these are mostly below the requirements stated in EN 61326-3-1.

2.4.4 Product standards

2.4.4.1 EN ISO 14119

Standard	Harmonised	Title
EN 1088:2007 EN ISO 14119* Replacement for ISO 14119:2006	Yes	Safety of machinery Interlocking devices associated with guards. Principles for design and selection
ISO/TR 24119*	No	Safety of machinery Evaluation of fault masking in conjunction with interlocking devices with potential-free contacts

*Expected publication date 2013 or 2014

Publication of EN ISO 14119 is planned for the turn of the year (positive vote already reached at the time of going to print, but publication still outstanding); this will combine the two predecessor standards EN 1088 and ISO 14119. The standard deals with guards, i.e. gates, covers or flaps, plus sensor technology that detects the position of such devices. The standard also covers guard locking devices.

The purpose of the standard is to specify exact requirements to improve provisions for reducing the ability of the machine operator to defeat safety

equipment. Investigations have shown that operators often attempt to defeat the safety function of an interlocking guard by defeating the interlock. The ability to defeat safety equipment can mainly be attributed to deficiencies in the machine design. ISO/TR 24119 will be published at the same time as EN ISO 14119; this is a spin-off from EN ISO 14119. ISO/TR 24119 deals with only one subject: Evaluation of interlinked safety gate switches. The context is the recurring accumulation of faults in conjunction with applications of this type, which can lead to the loss of the safety function.

▶ 2.4 Standards

2.4.4.2 EN 61496 and IEC/TS 62046

Standard	Harmonised	Title
IEC/TS 62046:2008	No	Safety of machinery Application of protective equipment to detect the presence of persons
EN 61496-1:2010	Yes	Safety of machinery Electrosensitive protective equipment – Part 1: General requirements and tests
IEC 61496-2:2013 CLC/TS 61496-2:2006:	No	Safety of machinery Electrosensitive protective equipment – Part 2: Particular requirements for equipment using active optoelectronic protective devices (AOPDs)
CLC/TS 61496-3:2008: replaces EN 61496-3:2003	No	Safety of machinery Electrosensitive protective equipment – Part 2: Particular requirements for active optoelectronic protective devices responsive to diffuse reflection (AOPDDR)

While the 61496 series describes product-specific requirements of electrosensitive protective equipment, IEC/TS 62046 focuses on the selection and measurement of electrosensitive protective equipment such as light beam devices, light grids or scanners. As such, it is one of the key standards for machine builders when it comes to designing machine access areas and safeguarding material channels.

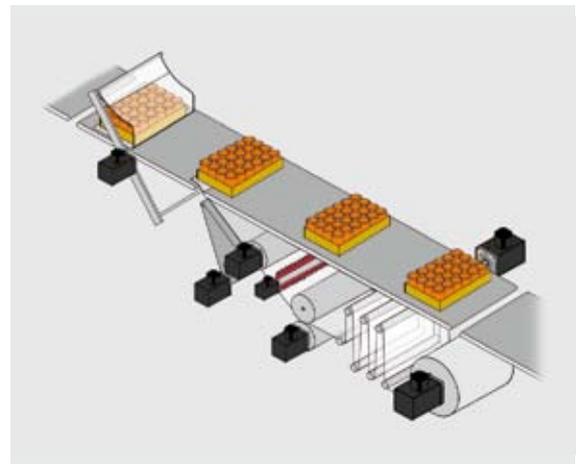
The EN 61496 series of standards considers electrosensitive protective equipment. This includes devices such as light grids, laser scanners, light beam devices, safe camera systems and other sensors, which can all be used for non-contact protection. As EN 61496 is a product standard for safety components, it is only relevant for the typical user if the safety components he has used are intended to conform to these standards. It is particularly worth noting the awkward situation that, at the time of going to print (Autumn 2013), 61496-2 is available in two different editions. The IEC version is available in Edition 3, dated 2013, while Edition 2 of the EN version (CLC/TS) still applies.

▶ 2.4 Standards

2.4.4.3 EN 61800-5-2

Standard	Harmonised	Title
EN 61800-5-2:2007	No	Adjustable speed electrical power drive systems Part 5-2: Safety requirements. Functional

The non-harmonised EN 61800-5-2 is aimed at both drive manufacturers and users. It deals with the issue of drive-based safety, but without specifying any requirements regarding safety-related suitability. No safety level is established, nor is there any definite hazard or risk evaluation. Instead, the standard describes mechanisms and safety functions of drives in an application environment, and how these are verified and planned within the drive's lifecycle. Technologically, the standard is based on EN 61508, even though proximity with EN ISO 13849-1 might have been anticipated, given the ever-present mechanical aspect of the drives.



Manufacturers of safe drives focus on EN 61800-5-2.

▶ 2.4 Standards

2.4.5 Application standards

2.4.5.1 EN ISO 11161 Integrated manufacturing systems

Standard	Harmonised	Title
EN ISO 11161:2010	No	Safety of machinery Integrated manufacturing systems – Basic requirements

This standard deals with the safety aspects when assembling machines and components into a manufacturing system (IMS). It does not deal with the requirements of the individual components and machines. The standard is of particular interest to

operators and system integrators who operate or design machine pools and plants incorporating machines and components. This standard should be applied in close co-operation with EN ISO 12100.

2.4.5.2 NFPA 79

Standard	Harmonised	Title
NFPA 79:2008	No	Industrial machinery

This standard is mainly important for the US market, though it may also be applied in Asia.

The standard is concerned with the safe design, operation and inspection of industrial machinery.

▶ 2.5 International comparison of standards, directives and laws

Most countries have binding regulations for making plant and machinery safe. After all, safe machinery plays a part in increasing the motivation and productivity of staff. The type of regulation varies from region to region and is designed to suit the respective legal and cultural environment, ranging from mandatory laws to recommendations of a non-binding nature. Even the level of jurisdiction to guarantee compliance varies enormously. Self certification is enough in some countries, while others have commercial institutions which carry out inspections in accordance with their own rules. In other parts of the world, certification is carried out by state-authorised institutions. This safety compendium is mainly concerned with European standards, directives and laws. However, the following section provides a brief overview of the situation in other parts of the world.

2.5.1 Directives and laws in America

2.5.1.1 North America



USA

The legal basis in the USA can be regarded 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. People there are mainly familiar with two types of standards: OSHA (Occupational Safety and Health Administration) and ANSI (American National Standards Institute). Government bodies publish OSHA standards and compliance is mandatory. OSHA standards are comparable with European directives, although OSHA is more concerned with describing technical property requirements than with abstract requirements.

ANSI standards, on the other hand, are developed by private organisations and their application is generally not absolutely mandatory. However, ANSI standards are still included in contracts and OSHA frequently adopts ANSI standards. 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.

Canada

Although the situation in Canada is comparable to that of the USA, there are a few differences. The central standards' organisation in Canada is the CSA (Canadian Standards Association). ANSI and NFPA are much less important in Canada. However, it's important to note that a considerable number of standards are published in identical form by CSA and ANSI, making portability between the two states somewhat easier. The CSA and its standards have no legal character in Canada.

On the legal side there is CCOHS (Canadian Centre for Occupational Health and Safety), which is the Canadian equivalent of OSHA. This organisation and its regional branches establish the formal reference between the standards and the law. However, as in the USA, this is a much more individual approach than that taken by the European directives.

▶ 2.5 International comparison of standards, directives and laws

2.5.1.2 South America



Brazil

NR 12 - Safety in Machinery and Work Equipment – has been available in Brazil since 2010. It is a document that's comparable with the European Machinery Directive and is concerned with the safety of machinery. It also looks at the obligations of operators and machine builders. The Brazilian Technical Standards Association (ABNT) has incorporated the standards ABNT NBR/IEC 61058-1 and ABNT NBR/IEC 61058-2-1. The possibility of harmonising the standards IEC 61508, IEC 61511 or IEC 62061 has not yet been analysed. Due to increasing globalisation and market requirements, the larger Brazilian companies are independently changing to ISO/IEC standards before ABNT has the chance to incorporate them into Brazilian legislation. Multinational companies or businesses working in the process industry, such as in oil and gas, often apply international ISO/IEC standards such as IEC 61508.

Argentina

The situation in Argentina largely corresponds to that of Brazil; indeed, the Argentine Institute of Standardization and Certification (IRAM) has placed advertisements advising companies to adopt the standards at national level. However, only a few companies from the oil and gas industry implement them, even in part.

Chile

The Chilean National Standards Institute (INN) has adopted some of the standards from the IEC field of electrical engineering. However, a study of IEC 61508, IEC 61511 or IEC 62061 is neither being developed, nor is its implementation planned.

2.5.2 Directives and laws in Asia

2.5.2.1 Russia and the CIS states



Russia and the CIS states have implemented GOST-R certification for some years now. Under this procedure, technical devices included on a specific product list must undergo a certain certification process. A European notified body performs a type-examination on machinery and any corresponding technical accessories. The Russian-based approvals body generally recognises this examination. From a safety point of view, therefore, the same requirements apply as in Europe.

▶ 2.5 International comparison of standards, directives and laws

2.5.2.2 Japan



The Industrial Safety and Health Law places demands on design issues relating to certain machinery (crane, lift etc.). The law also states that the machine operator is responsible for carrying out risk analyses. He also has to ensure safety in the workplace. It is assumed that the machine operator will ask the machine manufacturer to issue a risk analysis report at the time of purchase and that the machine is designed safely. The law also contains requirements for pressure vessels, personal protective equipment, packaging machines for the food industry and machines that are moved on the public highway.

Japan adopts most of the IEC and ISO standards as JIS standards (Japan Industrial Standards); however, the Industrial Safety and Health Law does not yet refer to each of these standards. There are plans to publish a supplementary law to this one, which will look specifically at the issue of performing risk analyses. It is anticipated that this law will refer to JIS (or ISO).

2.5.2.3 China



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

▶ 2.5 International comparison of standards, directives and laws

2.5.3 Directives and laws in Oceania

2.5.3.1 Australia



In Australia, states and territories have the responsibility of drafting and implementing safety laws. Fortunately the individual laws on industrial safety and their requirements are very similar. The relevant legislation is based on the Occupational Health and Safety (OHS) Act. This defines the obligations and duty of care of people with various responsibilities. Numerous regulations and codes of practice for the various safety areas fall under the state OHS legislation. These regulations are legally binding.

Although the codes of practice are not generally legally binding, they are frequently consulted as a benchmark in the respective legal system, whenever it is necessary to assess whether sufficient measures have been taken to design a safe workplace. For this reason, failure to comply with codes of practice can have very serious consequences. As well as referring to the codes of practice, regulations also sometimes refer to the Australian standards drafted by an independent organisation called "Standards Australia". However, with a few notable exceptions, Australian standards are not legally binding, although courts frequently consult them in order to assess the measures that have been taken to reduce risks. The most important machinery safety standard in Australia is AS4024.1, for example. Although compliance is not strictly mandatory, it does represent an excellent defence

in case of any action relating to neglect of duty of care. Failure to comply, on the other hand, may have serious legal consequences.

Many Australian standards are based on international standards, particularly:

- ▶ Standards issued by the International Electrotechnical Commission (IEC)
- ▶ European standards (EN)
- ▶ British standards (BS, nowadays often in the form of combined BS/EN standards) or
- ▶ Standards issued by the International Organization for Standardization (ISO)

Standards Australia's official policy is to adopt international standards (ISO or IEC) where possible in the interests of international alignment. In contrast, US American standards (ANSI standards) rarely correspond to Australian, ISO or EN standards and are of little relevance in Australia.

2.5.4 Summary

The comparison illustrates key differences in the way standards are applied. It makes it clear that knowledge of the respective national circumstances is indispensable when exporting. In particular, it illustrates the importance of European standards: In most countries, certification in accordance with IEC, EN and even ISO standards is now hugely important, as these standards are often used as the basis for national regulations. It doesn't automatically mean that certificates will be accepted, but certification in these countries will be considerably easier if certification to European standards is in place.

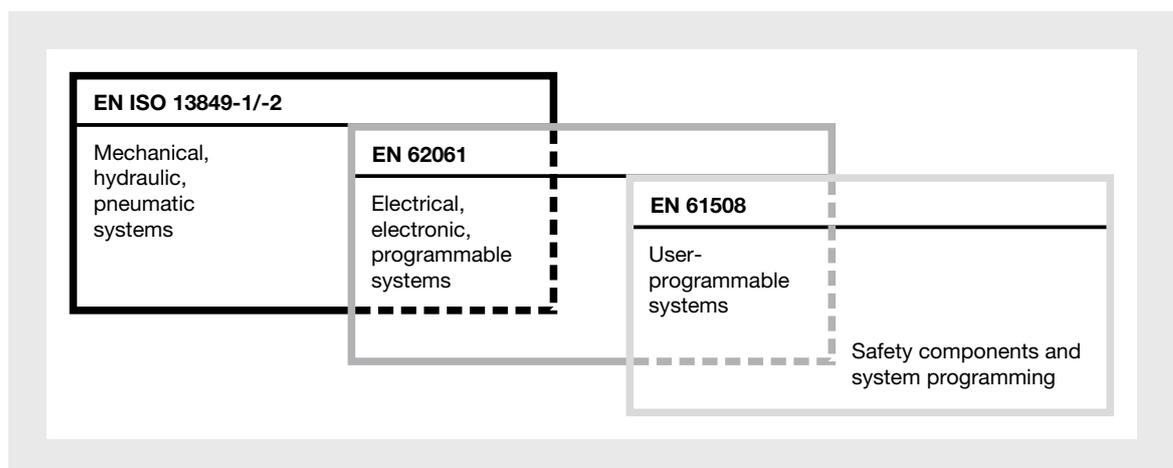
Validation (from lat. validus: strong, powerful, healthy) describes the testing of a plan or solution approach with regard to the task it is intended to fulfil and the associated solution to a problem. Verification describes the procedure for testing a plan or solution approach with regard to a corresponding specification. Together, both processes are used to demonstrate the suitability of a specific solution approach.

▶ 2.6 Validation

In mechanical engineering, a validation process must provide evidence that the plant or machine meets the requirements of its specific intended use. The process of verification also examines the functionality of the technical equipment and the safety-related parts of control systems, thereby confirming that they fulfil their functions safely, in accordance with the specification. Documentation of the results and solutions from the verification and validation process ensures that the intended target has actually been achieved.

With its basic terminology, general principles for design, procedures for evaluating risks (analysis and estimation), plus principles of risk assessment and risk reduction, the harmonised standard EN ISO 12100 defines important practices for safety-related systems and safety-related parts of plant and machine control systems. Other harmonised standards use this essential standard as a basis for describing the design, structure and integration of safety-related parts of control systems and safeguards: standards such as EN ISO 13849-1/-2 and EN 61508 with its sector standard EN 62061 (the origin of validation). In

contrast to EN 62061, EN ISO 13849-1/-2 is not restricted to electrical systems but can also be applied to mechanical, pneumatic and hydraulic systems. Both standards (EN ISO 13849-1/-2 and EN 62061) specify essential requirements for the design and implementation of safety-related control systems on machinery and are successors to EN 954-1, which is no longer relevant. In the application of EN ISO 13849-1/EN 62061, there are a number of differences in the design and implementation of safety-related parts of control systems and their subsequent assessment within the validation process.



Structure and overlap of generic and sector standards.

▶ 2.6 Validation

2.6.1 Verification of safety functions in accordance with EN ISO 13849-1/2

Required characteristic data: PL, Category, $MTTF_d$, DC, CCF, $B10_d$

The stipulated requirements form the basis for the design and implementation of the safety function (selection of components and architecture). The planned components are grouped into subsystems and the achievable performance level (PL) is defined. Verification of the planned safety function: Achieved PL \geq PL_r. The validation process confirms the conformity of the configuration and function of the safety-related parts of control systems within the overall specification of the plant and machinery. Note: Guidance on how to implement a validation process and validation tools for various technical systems can be found in EN ISO 13849-2.

2.6.2 Verification of safety functions in accordance with EN 62061

Required characteristic data: PFH, SIL, $MTTF_d$, DC, CCF, $B10_d$. The implementation of safety functions is designed on the basis of the formulated requirements. This involves the selection of appropriate components and the development of a coherent architecture. The planned components are grouped into subsystems and are the basis for determining the safety integrity level (SIL). Verification of the planned safety function: Achieved SIL \geq Required SIL.

PL (EN ISO 13849-1)	SIL (EN 62061)
a	-
b	1
c	1
d	2
e	3
-	4

Comparison chart: performance level (PL) and safety integrity level (SIL).

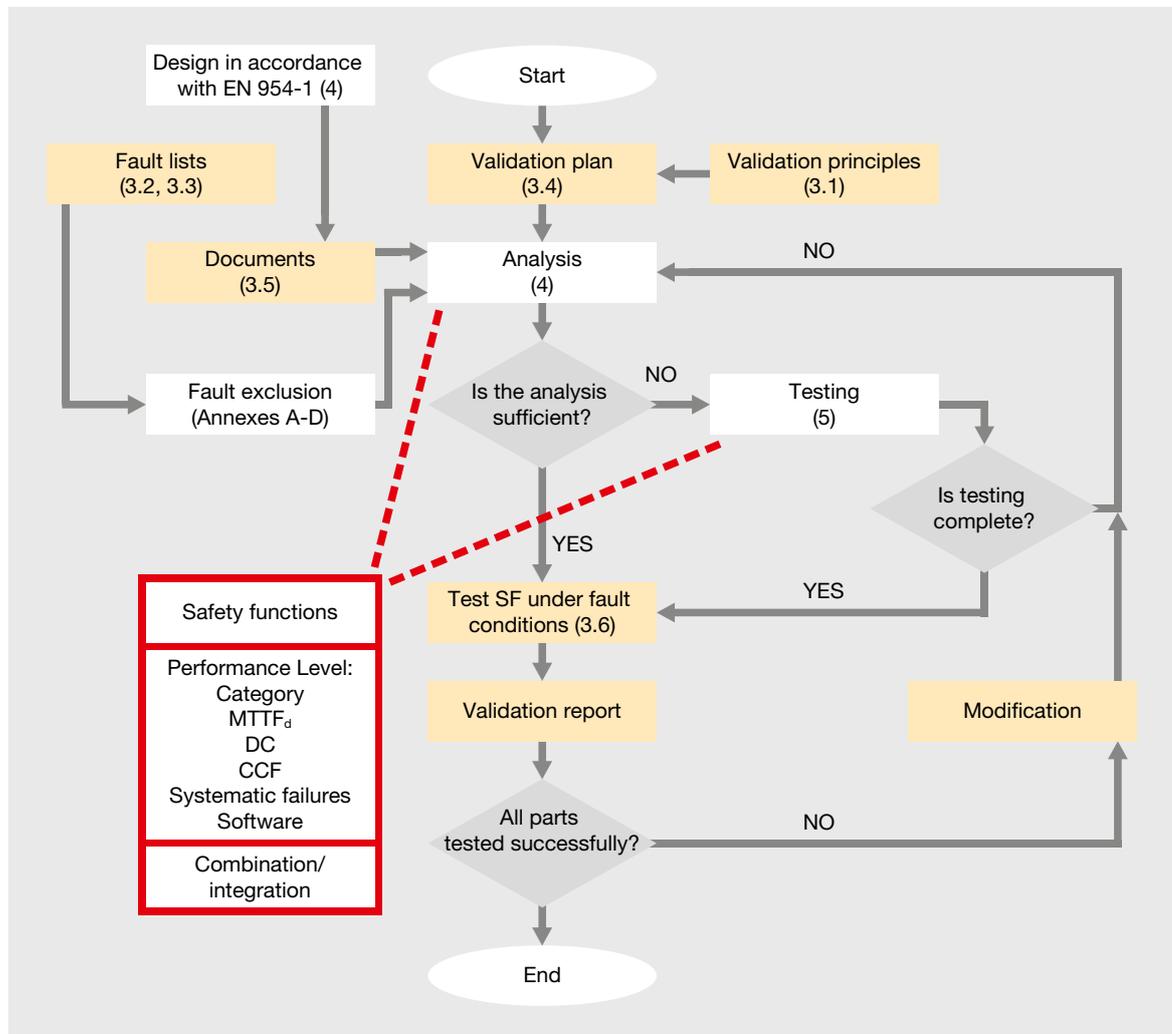
The verification of safety-related parts of control systems must demonstrate that the requirements and specifications have been met in accordance with the applied standard and the safety-related specification. These requirements refer specifically to

- ▶ the properties of a safety function, as defined in accordance with the risk assessment
- ▶ the standard-compliant architecture of the category defined for the safety function.

Verification of the safety-related parts of control systems consists of a thorough analysis and, if necessary, the carrying out of additional (function) tests and fault simulations. It is advisable to start the analysis right at the beginning of the design process so that any faults and/or problems can be identified early and dealt with accordingly.

The way in which the analysis and tests are carried out will depend on the size and complexity of the control system and the way it is integrated within the plant or machine. It makes sense, therefore, to carry out certain analyses and tests only once the control system has been developed to a certain level. An independent person or body should be commissioned to ensure that the analysis is independent. However, this does not necessarily mean that a third-party needs to be involved. To carry out the validation, a validation plan must first be produced to establish the scope of the analysis and tests. The exact scope and balance between the two processes always depends on the technology that is used and its complexity. The diagram overleaf provides a schematic overview of the validation process.

▶ 2.6 Validation



Validation plan in accordance with EN ISO 13849-2.

2.6.3 General information about the validation plan

The validation plan must describe all the requirements for carrying out the validation of the specified safety functions and their categories. The validation plan must also provide information about the means to be employed to carry out the validation. Depending on the complexity of the control system or machine that is to be tested, the validation plan must provide information about:

- ▶ the requirements for carrying out the validation plan
- ▶ the operational and environmental conditions
- ▶ the basic and well-tried safety principles
- ▶ the well-tried components
- ▶ the fault assumptions and fault exclusions
- ▶ the analyses and tests to be applied

The validation plan also contains all the validation documents.

▶ 2.6 Validation

2.6.4 Validation by analysis

The validation of safety-related parts of control systems is primarily carried out by analysis. Evidence must be provided to show that all the required properties of a safety function [SRCF] are actually present. The following factors are included in the analysis:

- ▶ the hazards identified in association with the machine
- ▶ the reliability
- ▶ the system structure
- ▶ the non-quantifiable, qualitative aspects which affect system behaviour
- ▶ deterministic arguments such as empirical values, quality features and failure rates

“Top-down”/“Bottom-up” analysis techniques

There are two different techniques to choose from when selecting the analysis technique: the deductive “top-down” technique and the inductive “bottom-up” technique. The “deductive” top-down technique can be applied in the form of a fault tree analysis or event tree analysis. Examples of the inductive “bottom-up” technique are the failure modes and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA).

2.6.5 Validation by testing

When validation by analysis is not sufficient to demonstrate the achievement of a specified safety function, further tests will be needed to complete the validation. As many control systems and their requirements are extremely complex, further tests need to be carried out in the majority of cases.

In practice the test requires a test plan, which must include the following:

- ▶ the test specifications
- ▶ the expected results
- ▶ the chronology of the individual tests

The test results must be documented in a way that is traceable; the test records must include the following as a minimum:

- ▶ the name of the person and/or body undertaking the test
- ▶ the environmental conditions at the time of the test
- ▶ the test procedures and equipment used

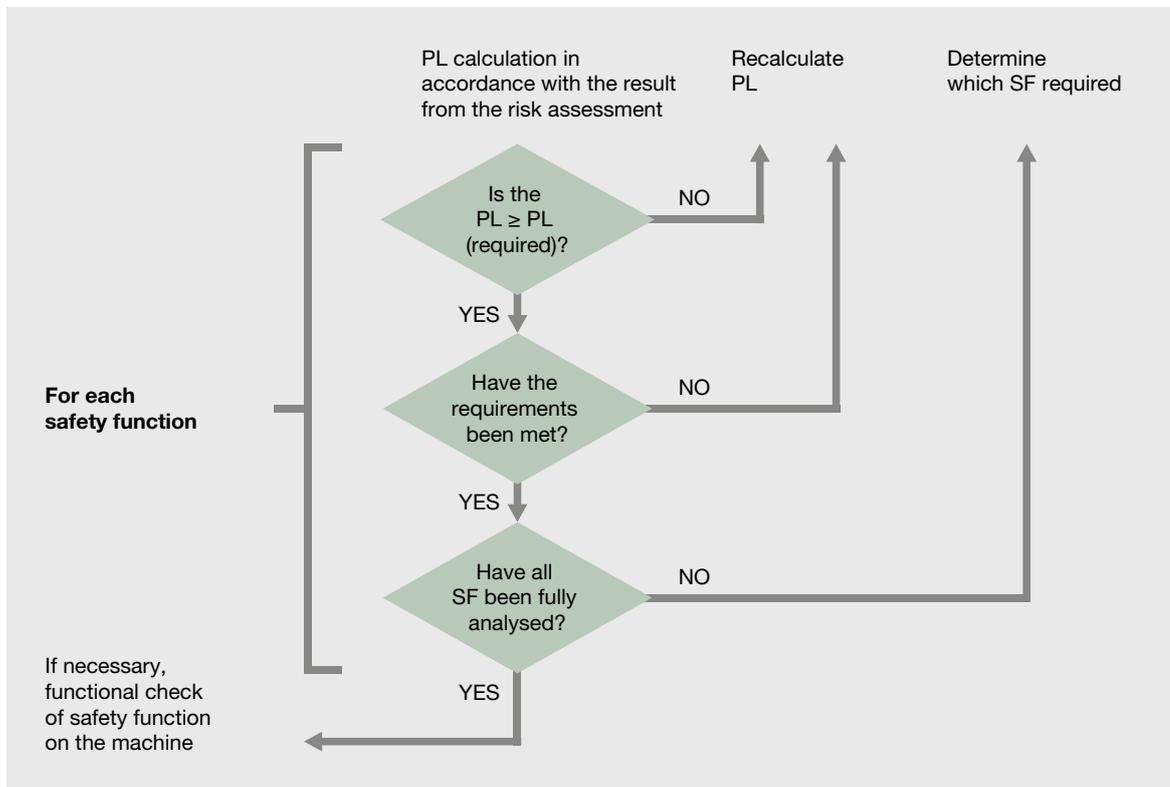
To demonstrate that the target and defined safety objective has actually been achieved, the test results are then compared with the specifications from the test plan.

2.6.6 Verification of safety functions

An important part of validation is verification that the safety functions comply with the intended specifications, functions, categories and architectures. It is important to validate the specified safety functions in all of the plant/machine’s operating modes. Alongside the basic validation of each safety function, the validation of the PL and/or SIL value within the safety function also has a key role to play. The following steps are required when verifying the safety function that a PL has achieved:

- ▶ Validation of the category
- ▶ Validation of the $MTTF_d$ values
- ▶ Validation of the DC values
- ▶ Validation of the measures against common cause failures/CCF
- ▶ Validation of the measures against systematic faults

▶ 2.6 Validation



Verification and validation flowchart (source: Pilz training materials)

The validation of safety functions is a really complex process and so it is advisable in this case to use a software tool (e.g. PASCAL), which can help you to calculate the planned and/or implemented safety functions. Based on the safety-related characteristic values of the planned/employed components, these calculation tools validate the values that have been achieved, including the required/demanded default values PL_r or SIL. The advantage of software-based tools is that they guide you step-by-step through the individual stages involved in validating safety functions. The option within the tool for graphic modelling of safety functions gives the tester additional security in his calculations and helps to make the results more traceable.

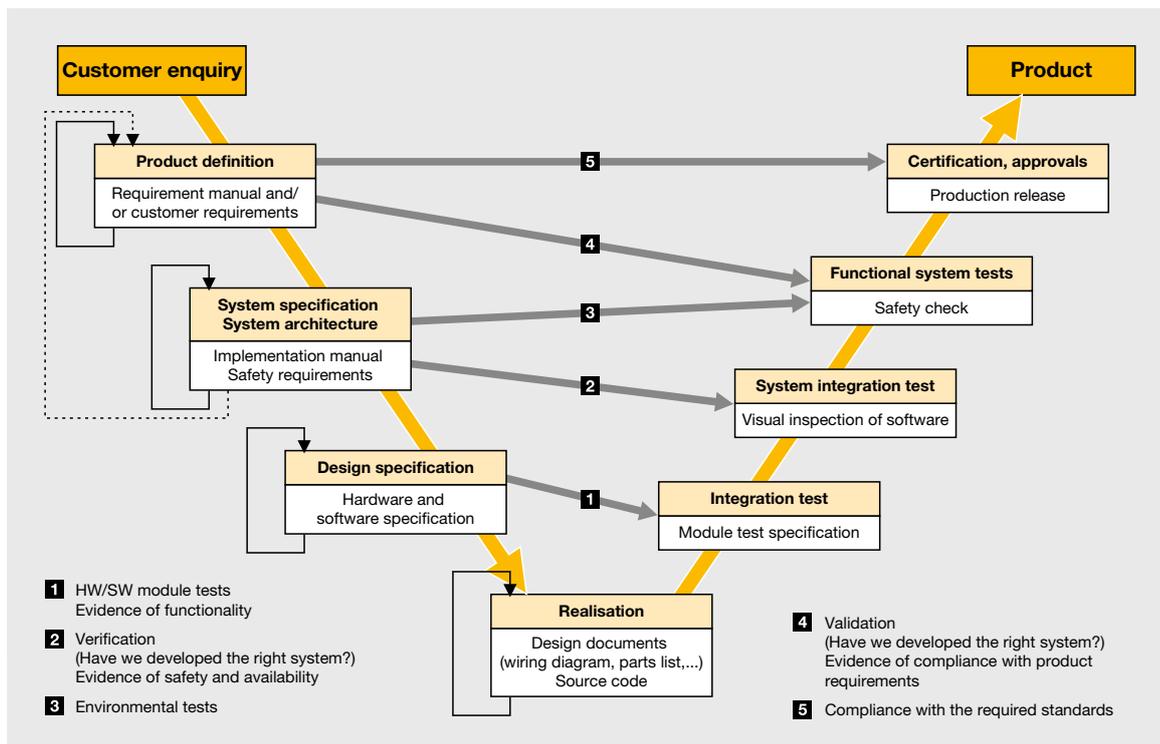
▶ 2.6 Validation

2.6.7 Validation of software

The provisions in the standards EN 62061 and EN ISO 13849-1/-2 allow the development of safety-related software in the machine sector for all performance levels and safety integrity levels. As a result, software assumes a high level of responsibility and largely determines the quality of the safety function to be implemented. It is therefore of the utmost importance that the software created is clear, legible and can be tested and maintained. To guarantee the quality of the software, it is also subjected to a validation process during development. The basic principles are:

- ▶ Working to a V-model (development lifecycle incl. verification and validation)
- ▶ Documentation of specification and design
- ▶ Modular and structured programming
- ▶ Functional testing
- ▶ Appropriate development activities after modifications or adjustments

A corresponding report is also produced in this case, to confirm that the software conforms to the safety requirement specification; this report forms part of the validation report for the plant or machine. As with the validation of the safety functions, the software should not be validated by the programmer himself but by an independent person.



Pilz GmbH & Co. KG's V-Model for engineering projects

▶ 2.6 Validation

Today there are some very good, certified software tools available to develop and program safety-related software for the relevant safety control system. The use of software tools simplifies the whole validation process, as the blocks contained within the software are essentially pre-certified and at the same time validated. The more these software blocks are used within an application, the less validation work will be needed. The same is true when using parameterisable user software; this also contains pre-validated blocks. The subsequent series of function tests must demonstrate whether the safety functions operate in accordance with their specification. This includes simulation of anticipated faults.

2.6.8 Validation of resistance to environmental requirements

When determining the performance of safety-related parts of control systems, environmental conditions such as the environmental site and the way in which the control system will subsequently be used, play an important role in respect of the system. Relevant key words include waterproofing and vibration protection. The system must therefore be validated by analysis. In specific terms, the analysis must show that the control system or system has the mechanical durability to withstand the wide range of stresses from environmental influences such as shock, vibration and ingress of contaminants. Safety-related parts of control systems must maintain a safe condition under all circumstances. The analysis should also consider factors such as temperature, humidity and electromagnetic compatibility.

2.6.9 Production of validation report

Finally, after all the verification and validation steps have been carried out, the validation report is produced. This contains all the information about the analyses and tests that have been carried out in traceable form, for both the hardware and software. Cross-references to other documents are permitted provided these are traceable and identifiable. Any safety-related parts of control systems which have failed the validation process should be named, along with the factors that led to their exclusion.

2.6.10 Conclusion

Maintenance and repair/periodic tests

Naturally, the ravages of time also gnaw away at the performance of safety-related control systems. Wear and tear, corrosion and sustained (mechanical) stresses lead to a reduction in safety; in an extreme case they can even lead to dangerous failures of control components, even the whole control system. For this reason, it is necessary to maintain the safety-related parts of control systems at regular intervals and to carry out periodic tests to check functional safety. A maintenance and repair plan should be available in written form along with records from the periodic tests. The function tests must be carried out by a competent person. Based on the hazard assessment in accordance with §3 of the industrial safety regulations (BetrSichV), the machine or plant operator should define the type, scope and frequency of the periodic tests. To provide details of the industrial safety regulations and more information on our services can be found on www.pilz.com, webcode: 7057

▶ 2.6 Validation

2.6.11 Appendix

The talk, therefore, surrounds basic, well-tried safety principles and safety components, as well as fault exclusions. The tables correspond to the specifications of EN ISO 13849-1 and EN ISO 13849-2 and provide a brief overview of the safety-related considerations.

Basic safety principles in accordance with EN ISO 13849-1/EN ISO 13849-2

Features of basic safety principles may be:

- ▶ Use of suitable materials and manufacturing methods, taking into account stress, durability, elasticity and wear
- ▶ Correct dimensioning and shaping, taking into account stresses and strains
- ▶ Pressure limiting measures such as pressure control valves and chokes
- ▶ Speed limiting measures

Annexes A-D of EN ISO 13849-2 contain a list of the basic safety principles affecting mechanical, hydraulic, pneumatic and electrical/electronic systems.

Well-tried safety principles in accordance with EN ISO 13849-1/EN ISO 13849-2

Features of well-tried safety principles are, for example:

- ▶ Avoiding faults, e.g. through the safe position of moving parts of components
- ▶ Reducing the probability of error, e.g. by over-dimensioning components
- ▶ Defining the failure mode, e.g. through positive electrical separation/positive opening contacts
- ▶ Reducing the effect of failures, e.g. by multiplying parts

Annexes A-D of EN ISO 13849-2 contain a list of the basic safety principles for mechanical, hydraulic, pneumatic and electrical/electronic systems.

Well-tried components in accordance with EN ISO 13849-1/EN ISO 13849-2

A component can be regarded as well-tried when it has been

- ▶ widely used in the past with successful results in similar applications
- ▶ made using principles which document the suitability and reliability of the component

Annexes A-D of EN ISO 13849-2 contain a list of well-tried components for mechanical systems, such as screws, springs and cams for example, as well as components for electrical and electronic systems, such as contactors and relays. There are currently no well-tried components listed for pneumatic and hydraulic systems.

Fault exclusions in accordance with EN ISO 13849-2

The requirements for applying a fault exclusion must be indicated in the validation plan. It is important that each fault exclusion can be justified with a reasonable, traceable explanation. Annexes A-D of EN ISO 13849-2 provide an overview of possible fault exclusions based on their presumed faults. For example, these may be:

- ▶ Fracture due to over-dimensioning, on mechanical systems
- ▶ Spontaneous change due to safety device, on pneumatic systems
- ▶ Change of switching times due to positive action, on hydraulic systems
- ▶ Short circuits between adjacent contacts insulated from each other, on electrical/electronic systems

▶ 2.6 Validation

What can Pilz do for you?

Pilz GmbH & Co. KG offers a wide range of services, including validation within the lifecycle of the plant and machinery. By mirroring the risk assessment and the safety concept, the developed solutions are adapted to suit the actual requirements. Validation by Pilz is followed by an objective and systematic review of the implemented measures, evaluation of the technical safeguards and finally function tests. Compliance with all applicable safety standards and directives is assured. With a wealth of experience in validating machinery, Pilz engineers have developed structured methods for inspecting safety-critical elements of plant and machinery. The PAScal calculation tool helps to verify the performance level that has been achieved for the respective safety function.

Validation by Pilz includes:

- ▶ Mirroring of the requirements from the risk assessment and safety concept
- ▶ Verification of the achieved performance level in accordance with EN ISO 13849-1/ EN IEC 62061, based on the calculation tool PAScal, Sistema, etc.
- ▶ Verification of the operating manual
- ▶ Function testing and fault simulation (safety check)
- ▶ Testing of the safety-related software and hardware functions
- ▶ Testing of the sensor/actuator technology and its wiring
- ▶ Measurements (protective earth conductor, sound level,...)
- ▶ Production of a test report with detailed information about the results
- ▶ Acceptance of responsibility as the “authorised representative” by signing the declaration of conformity

How you benefit from validation with Pilz

- ▶ Opt for professional methods during the certification process
- ▶ Consider all relevant aspects of validation and certification
- ▶ Delegate responsibility to Pilz
- ▶ Trust in the safety experts.

Complete your overall safety process with CE certification

To complete your machine’s safety lifecycle, Pilz can offer CE certification as a final service. In this case, Pilz undertakes the whole conformity assessment process, assuming responsibility for the whole procedure. By signing as the authorised representative on the declaration of conformity, Pilz confirms that the requirements of the directives have been met. As a result you obtain the “passport” your machine needs throughout the European internal market.

Regular inspections and up-to-date knowledge of standards, directives and product developments are essential to anyone wishing to operate their plant or machine safely on a long term basis. In accordance with the industrial safety regulations (BetrSichV) § 10, it is essential that electrosensitive protective equipment (for example: light grids, light beam devices, scanners etc.) is properly configured and installed and undergoes regular inspection. Responsibility for this lies fully in the hands of the operator.

Regular inspections keep you on the safe side

An independent inspection body, accredited by DAkkS (German Accreditation Body) in accordance with DIN EN ISO 17020, guarantees objectivity, high availability for your plant and machine, plus the highest possible safety for your staff. At the end of the process Pilz will submit the inspection report and discuss all the results with you. If the inspection is passed, the plant is given a Pilz quality seal.

▶ 2.7 Certification and accreditation

Customers are increasingly regarding certificates, or service providers with third-party certification, as a guarantee of quality. In principle, however, certificates are not legally binding and can be issued by practically anyone. They are merely an indication that a third-party has checked that certain work practices are carried out in accordance with the relevant specifications. The certificates actually say nothing about the quality of this third-party inspection. That's why it is important to have accurate knowledge about the competence of the certifying company or to make enquiries if necessary.

The situation is different with accredited companies: Accreditations are legally binding and can only be issued by national bodies. With accreditation, the public accreditation body confirms that a company or institution possesses the competence to perform certain conformity assessment tasks. Conformity assessment is a procedure which checks whether certain specifications have been met, by definition or objective. If an accredited company or institution issues a certificate, the customer can assume that it has the necessary competence to do so.

2.7.1 Accreditation: Quality seal for customers

Accredited conformity assessment bodies, accredited bodies for short, are generally institutions such as test or calibration laboratories, inspection or certification bodies. They provide services such as tests, inspections, certifications, of management systems, persons and products for example, in order to assess the conformity of products, plants or management systems. The assessment is usually part of a test procedure that has to demonstrate that certain requirements, such as those listed in the standards, have been met.

In Europe, accreditation is uniformly regulated through the Accreditation Directive 765/2008/EC. Since 01.01.2010, all member states have been obliged to operate a single national accreditation body. This will accredit the conformity assessment bodies and evaluate them at regular intervals through audits, to guarantee continued compliance with the requirements. Among other things, the accreditation process checks the independence of the organisation, quality management, training of staff, management of calibrated measuring devices, work instructions and handling of records and test reports, to ensure they conform to the relevant EN/ISO standard. The national accreditation bodies will also examine and evaluate the practical implementation of the on-site certification tasks. Accreditation is beneficial to both the accredited institution and its customers in equal measure: It shows the the customer that the institution is carrying out its work correctly and in accordance with the standards. At the same time, the customer obtains an assessment benchmark to safeguard that competence.

Organisations generally work in isolation and rarely, if ever, receive an independent technical assessment of their performance. A regular assessment by an accreditation body examines all aspects of a facility's operations with regard to the continuous production of accurate and reliable data. The accreditation body identifies and discusses areas for improvement; at the end of the assessment, a detailed report is available. If required, the accreditation body can monitor subsequent activities. So the company can be sure that it has introduced appropriate corrective actions.

► 2.7 Certification and accreditation

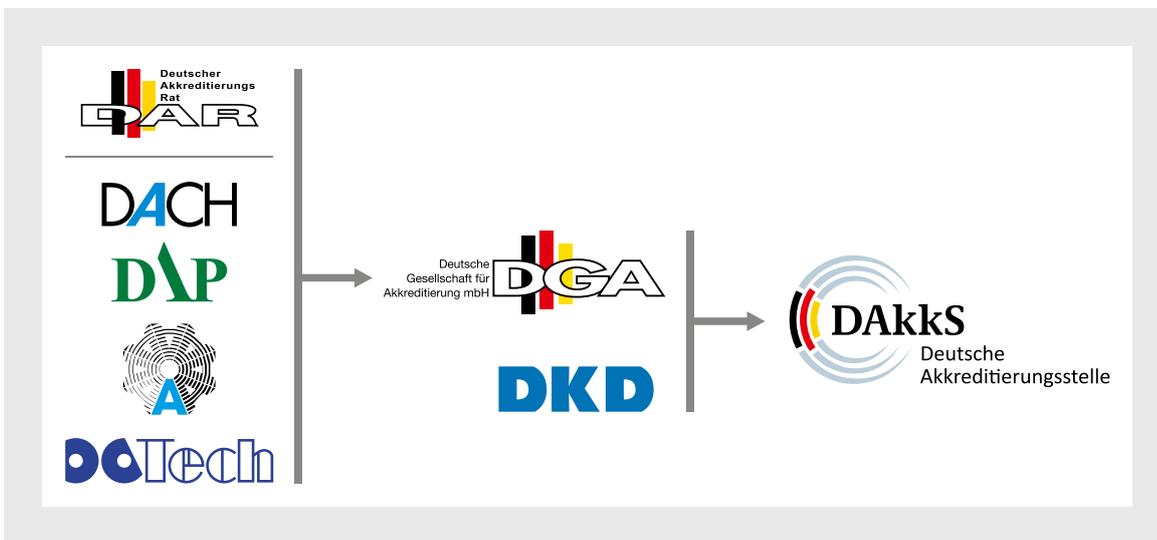


Some examples of accreditation bodies in Europe.

▶ 2.7 Certification and accreditation

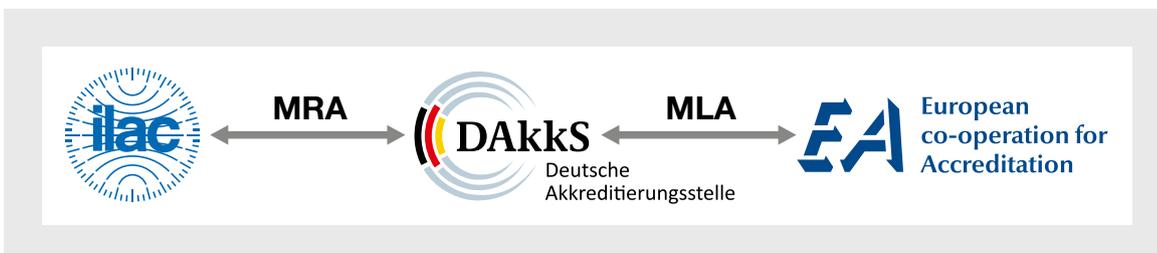
In Germany the German Accreditation Body (Deutsche Akkreditierungsstelle GmbH* [DAkks]) that was founded by the Federal Ministry of Economics and Industry is responsible. All previous accreditation bodies (DACH, DAP, TGA/DATECH and DKD) were merged within DAkks early in 2010.

* In Austria: bmwfi,
in Switzerland: SWISS INSPECTION



Merging the German accreditation bodies into DAkks.

Accreditation continues to enjoy worldwide recognition due to agreements between DAkks and the International Laboratory Accreditation Cooperation (ILAC), the International Accreditation Forum (IAF) and the European co-operation for Accreditation (EA).



International recognition of DAkks.

MRA = Mutual Recognition Agreement

MLA = Multilateral Recognition Arrangement

▶ 2.7 Certification and accreditation

These agreements ensure that all accredited bodies worldwide have a standard level of competence and that the services that are carried out satisfy the very highest quality requirements. Both nationally and internationally, accreditation is highly regarded as an indicator of technical competence. Many industry sectors routinely specify accreditation for suppliers of testing services.

Unlike certification to ISO 9001, for example, accreditation uses criteria and procedures specifically developed to determine technical competence, thus assuring customers that the test, calibration or measurement data supplied by the laboratory or inspection service is accurate and reliable. Accredited bodies can be recognised by the symbol of the relevant accreditation body, which is usually found on test or calibration reports. A list of the accredited bodies in Germany is available at www.dakks.de.



Example of the DAkKS logo for the Pilz inspection body.

2.7.2 Accreditation or certification

Accreditation uses criteria and procedures specifically developed to determine technical competence. Specialist technical assessors conduct a thorough evaluation of all factors in an organisation that affect the production of test or calibration data. The criteria are based on international standards such as ISO/IEC 17020, ISO/IEC 17025 or ISO 15189, which are used worldwide to evaluate accredited organisations. Accredited bodies use this standard specifically to assess factors relevant to technical competence, such as:

- ▶ Technical competence of staff
- ▶ Validity and appropriateness of test methods
- ▶ Traceability of measurements and calibrations to national standards
- ▶ Suitability, calibration and maintenance of test equipment
- ▶ Testing environment
- ▶ Sampling, handling and transportation of test items
- ▶ Quality assurance of test and calibration data

By this process, accreditation assures organisations and their customers that test and calibration data produced by their accredited body is accurate and reliable.



Certification, to the standard ISO 9001 for example, is widely used by manufacturing and service organisations. It demonstrates that products, services and procedures meet the required quality standards. The aim in certifying an organisation's quality management system to ISO 9001, for example, is to confirm that the management system conforms to this standard. Although laboratories and inspection bodies can be certified to ISO 9001, unlike accreditation, such certification makes no claim regarding technical competence.

▶ 2.7 Certification and accreditation

2.7.3 Tests in accordance with industrial safety regulations (BetrSichV) and accreditation

All European employers are legally obliged to provide employees with safe work equipment. In Germany, this has been regulated since October 2002 at the latest by the industrial safety regulations* (BetrSichV). This regulation is the mandatory implementation of the Work Equipment Directive 104/2009/EC, which was adopted by the EU back in 1989 and has meanwhile been revised.

* In Austria: Work equipment regulation (AM-VO)
In Switzerland: Accident insurance law (UVG)

The employer is obliged to guarantee this requirement the first time the work equipment is put into use and through subsequent regular testing. He must determine the test intervals himself, taking account of statutory specifications. He must also ensure that these tests are only carried out by “competent persons”. Technical rule TRBS 1203 defines the requirements placed on a “competent person”. Essentially the person must have professional training, a certain amount of professional experience, recent professional activity and regular relevant continuing training in the field to be inspected. The employer is free to decide which staff member will be named the “competent person”. He must merely be convinced of his competence and be able to prove this in court.

Alternatively a company can also outsource these tests to an external provider. However, this does not absolve it of the responsibility of checking the competence of the company that will conduct the tests. Unlike certified companies, accredited bodies prove particularly helpful in this regard, because only accreditation makes a legally binding statement about the competence of such bodies, thereby satisfying the burden of proof.

Pilz GmbH & Co. KG operates an accredited inspection body, which companies can appoint to undertake the testing of safeguards on plant and machinery. Due to accreditation, the services are recognised worldwide. The inspection body has access to qualified inspectors in Germany as well as other EU member states. As a result, Pilz can offer its services not only within the EU but worldwide. In 2010, the German Accreditation Body (DAkkS) renewed the accreditation. This shows that Pilz meets all the requirements of DIN EN ISO/IEC 17020:2004 for a Type C inspection body in the mechanical engineering sector and is competent to carry out the predefined conformity assessment tasks. Pilz can even carry out very complex examinations. The inspection body offers the following services:



Example of implementation of the EU Work Equipment Directive

▶ 2.7 Certification and accreditation

- ▶ Inspection of electrosensitive protective equipment ESPE (light curtains, scanners, safe camera systems)
- ▶ Measurement of stopping performance to confirm the specified safety distances
- ▶ Inspection of additional safeguards (E-STOP, safety gates, 2-hand)
- ▶ Verification of compliance with the minimum specifications of the industrial safety regulations
- ▶ Verification of compliance with the minimum requirements of the Machinery Directive (CE)

If the customer selects an accredited inspection body that meets his testing or measurement needs, he can be sure that the inspection body can provide accurate and reliable results. The technical competence of an inspection body depends on factors such as:

- ▶ Qualifications, training, experience of staff
- ▶ The right equipment, correctly calibrated and maintained
- ▶ Appropriate quality assurance procedures
- ▶ Adequate test procedures
- ▶ Validated test methods
- ▶ Inspections based on national standards
- ▶ Precise recording procedure and report production
- ▶ Suitable test facilities

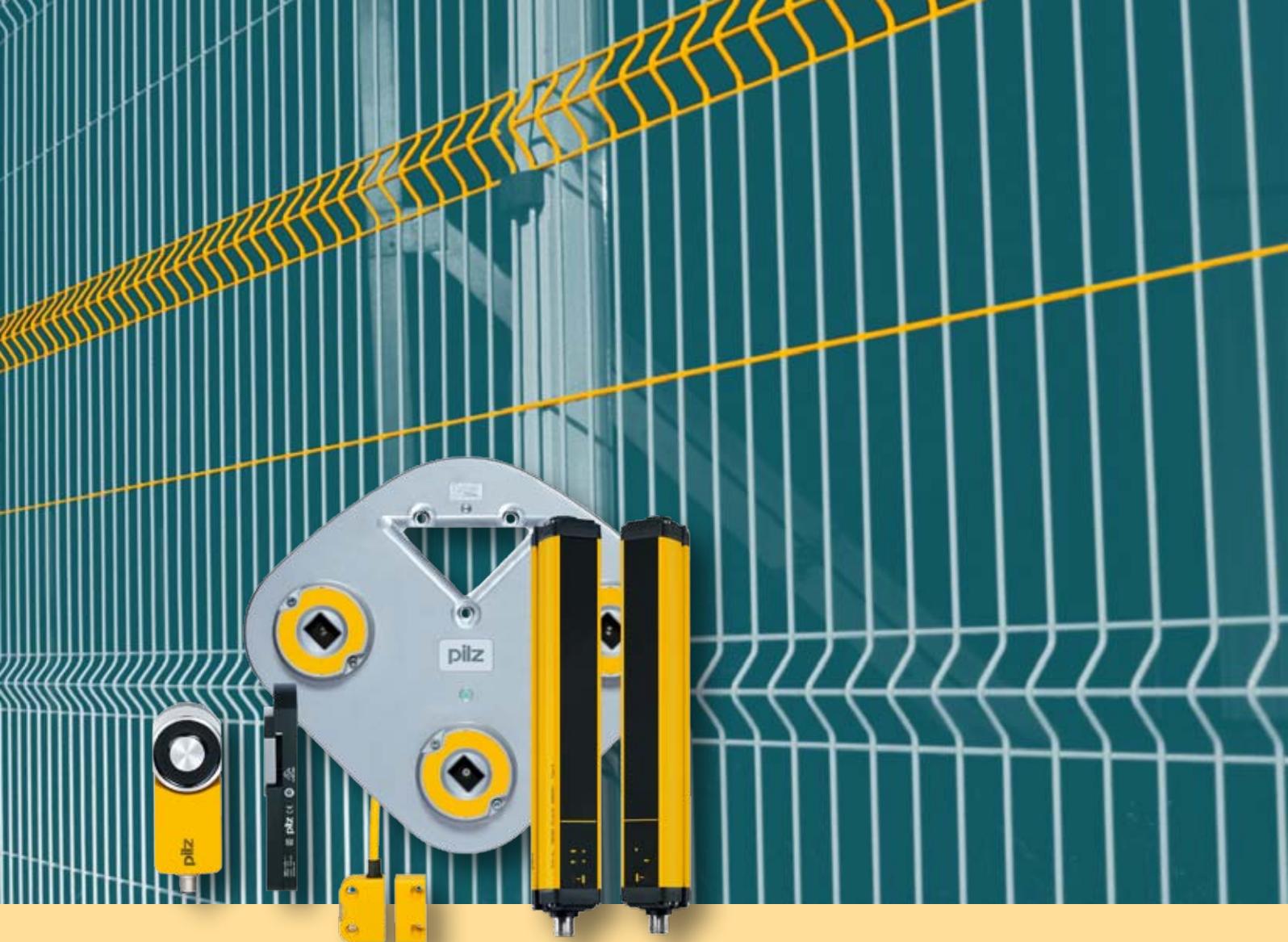
All these factors help to ensure that an accredited inspection body is technically competent and able to carry out the tests it offers.

2.7.4 Conclusion

Essentially, every company is free to have its work equipment inspected by its own staff or to appoint an external company to do the work. However, in every case, the person conducting the inspection must be competent to do the job. If a staff member is selected, the employer can normally assess his competence. If he opts for an external provider, he will have to rely on written evidence. Certificates are generally not sufficiently compelling; in the event of a legal dispute, they do not usually meet the formal requirements. In contrast, accreditations for the relevant services provide reliable, legal security.

Informative links:

- ▶ DAkkS: <http://www.dakks.de/>
- ▶ EA: <http://www.european-accreditation.org/>
- ▶ ILAC: <http://www.ilac.org/>



3

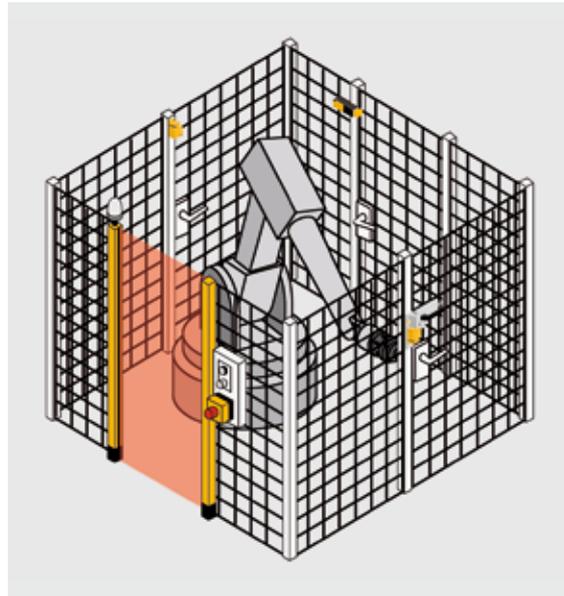
Safeguards

▶ 3 Safeguards

Chapter	Contents	Page
3	Safeguards	3-3
3.1	European Union standards, directives and laws relating to safeguards	3-3
3.1.1	Standards for guards	3-7
3.1.2	Standards for dimensioning of guards	3-7
3.1.3	Standards for the design of protective devices or electrosensitive protective equipment	3-7
3.2	Guards	3-8
3.2.1	Fixed guards	3-8
3.2.2	Movable guards	3-9
3.2.3	Further aspects on the design of safeguards	3-12
3.3	Protective devices	3-17
3.3.1	Active optoelectronic protective devices	3-17
3.3.2	Further important aspects in connection with electrosensitive protective equipment	3-19
3.3.3	Other sensor-based protective equipment	3-21
3.4	Manipulation of safeguards	3-24
3.4.1	Legal position	3-24
3.4.2	Conduct contrary to safety – What does that mean?	3-26
3.4.3	What can designers do?	3-28
3.4.4	User-friendly guards	3-29
3.4.5	Conclusion	3-31

▶ 3.1 European Union standards, directives and laws relating to safeguards

Safeguards are necessary to provide operators with as much protection as possible from hazards that may arise during machine operation. They are primarily fences or barriers, which make physical access to the machine difficult. However, sometimes it's neither possible nor sensible to select a fixed guard of this type. In this case, the decision will fall in favour of a control technology solution which shuts down part or all of the machine, should anyone approach a source of danger, or brings the machine to a safe status by another means. Should this type of hazard protection also prove unsuitable, or if potential hazards remain despite the application of these measures, then indicative safety technology is the final option: In this case, the residual dangers are indicated in the operating manual or on the machine itself.



Guard barriers and safety devices protect against dangers.

▶ 3.1 European Union standards, directives and laws relating to safeguards

There are a vast number of regulations that deal with safeguards on machinery. First of all, we'll consider the statutory regulations of European Directive 2006/42/EC.

Machinery Directive (2006/42/EC)

1.4. Required characteristics of guards and protection devices

1.4.1. General requirements

Guards and protective devices must:

- ▶ *be of robust construction*
- ▶ *be securely held in place*
- ▶ *not give rise to any additional hazard*
- ▶ *not be easy to by-pass or render non-operational*
- ▶ *be located at an adequate distance from the danger zone*
- ▶ *cause minimum obstruction to the view of the production process, and*
- ▶ *enable essential work to be carried out on the installation and/or replacement of tools and for maintenance purposes by restricting access exclusively to the area where the work has to be done, if possible without the guard having to be removed or the protective device having to be disabled.*
- ▶ *Guards must, where possible, protect against the ejection or falling of materials or objects and against emissions generated by the machinery.*

1.4.2. Special requirements for guards

1.4.2.1 Fixed guards

Fixed guards must be fixed using systems that can be opened or removed only with tools. Their fixing systems must remain attached to the guards or to the machinery when the guards are removed. Where possible, guards must be incapable of remaining in place without their fixings.

1.4.2.2. Interlocking movable guards

Interlocking movable guards must:

- ▶ *as far as possible remain attached to the machinery when open*
- ▶ *be designed and constructed in such a way that they can be adjusted only by means of an intentional action*

▶ 3.1 European Union standards, directives and laws relating to safeguards

Interlocking movable guards must be associated with an interlocking device that:

- ▶ *prevents the start of hazardous machinery functions until they are closed and gives a stop command whenever they are no longer closed*

Where it is possible for an operator to reach the danger zone before the risk due to the hazardous machinery functions has ceased, movable guards must be associated with a guard locking device in addition to an interlocking device that:

- ▶ *prevents the start of hazardous machinery functions until the guard is closed and locked, and*
- ▶ *keeps the guard closed and locked until the risk of injury from the hazardous machinery functions has ceased*

Interlocking movable guards must be designed in such a way that the absence or failure of one of their components prevents starting or stops the hazardous machinery functions.

1.4.2.3. Adjustable guards restricting access

Adjustable guards restricting access to those areas of the moving parts strictly necessary for the work must be:

- ▶ *adjustable manually or automatically, depending on the type of work involved, and*
- ▶ *readily adjustable without the use of tools*

1.4.3 Special requirements for protective devices

Protective devices must be designed and incorporated into the control system in such a way that:

- ▶ *moving parts cannot start up while they are within the operator's reach*
- ▶ *persons cannot reach moving parts while the parts are moving, and*
- ▶ *the absence or failure of one of their components prevents starting or stops the moving parts. They must be adjustable only by means of intentional action.*

▶ 3.1 European Union standards, directives and laws relating to safeguards

A number of points in the above requirements are considered separately here:

Guards must, where possible, protect against the ejection or falling of materials or objects and against emissions generated by the machinery. The active direction of the protection is described here: It is not only necessary to consider the hazardous approach of people towards the danger zone; many hazards arise from the machinery itself and therefore require protection.

Safeguards must cause minimum obstruction to the view of the production process.

A further requirement for a fixed guard is that its fixing systems remain attached to the machinery or to the guard itself once the guard is removed. So in future, screws on protective covers for example will need to be fixed in such a way that they cannot be lost once the guard is removed.

This very strict requirement throws up a number of questions in respect of feasibility. For example, does this apply to all the screws on a safety fence? In an extreme case, even the floor fixings of the safety fence would be subject to this requirement.

The commentary entitled “Guide to application of the Machinery Directive 2006/42/EC – 2nd Edition – June 2010” issued by the European Commission provides an interpretation: The requirement is for a type of fixed guards to be used where it is expected that the machine operator will remove them. A practical example would be opening up the guard for a monthly clean. In contrast, this does not need to apply to guards which are removed solely for general overhaul or for more major repairs. It is therefore advisable for machine manufacturers to classify their equipment accordingly.

Protective devices must be adjustable only by means of intentional action. This requirement makes particular sense in relation to light beam devices or light curtains. These devices are adjusted as the machine is put into service, after which point they should not be adjustable without good reason, otherwise the necessary safety distance may no longer be guaranteed.

▶ 3.1 European Union standards, directives and laws relating to safeguards

3.1.1 Standards for guards

In addition to the statutory regulations of the Machinery Directive, the following European standards currently exist relating to safeguards:

Standard	Title
EN 953:1997+A1:2009	Safety of machinery Guards. General requirements for the design and construction of fixed and movable guards
EN ISO 14119*	Replaces EN 1088:2008 and ISO 14119:2006

*Expected publication date: 2013 or 2014

3.1.2 Standards for dimensioning of guards

Standard	Title
EN ISO 13857:2008	Safety of machinery Safety distances to prevent hazard zones being reached by upper and lower limbs (ISO 13857:2008)
EN 349:1995+A2:2008	Safety of machinery Minimum gaps to avoid crushing of parts of the human body

3.1.3 Standards for the design of protective devices or electroresponsive protective equipment

Standard	Title
EN 61496-1:2010	Safety of machinery Electrosensitive protective equipment – Part 1: General requirements and tests
IEC 61496-2:2013 CLC/TS 61496-2:2006	Safety of machinery Electrosensitive protective equipment – Part 2: Particular requirements for equipment using active optoelectronic protective devices (AOPDs)
CLC/TS 61496-3:2008 replaces EN 61496-3:2003	Safety of machinery Electrosensitive protective equipment – Part 3: Particular requirements for active optoelectronic protective devices responsive to diffuse reflection (AOPDDR)
EN ISO 13855:2010	Safety of machinery Positioning of safeguards with respect to the approach speeds of parts of the human body

▶ 3.2 Guards

A guard is part of a machine which is specifically required as a form of physical barrier to protect persons from the hazards of machinery. In some cases the same safeguards can simultaneously protect the machine from persons, for example,

if time-critical processes may not be interrupted by persons approaching at random. The study below considers the first scenario only.



Examples of guards

A “guard” forms a physical barrier between the machine operator and the hazard, in contrast to “protective devices” or “electrosensitive protective equipment” such as light curtains and light beam devices, which are covered later. Safeguards of this type do not prevent access to a hazard, but detect a person or part of a person’s body when a hazard is approached. In this case, the hazard is shut down via a downstream control system so that the danger is removed before the hazard zone is reached. Depending on its design, a guard may be implemented as housing, casing, shield, door, cover or some other format. Guards are available in a wide range of types and formats, therefore.

3.2.1 Fixed guards

Fixed guards are permanently attached to the machine. This type of safeguard is suitable when it is unnecessary to remove the guard under normal operating conditions or when access is not required during the work process. Examples would be chain covers or grilles in front of motor fans.

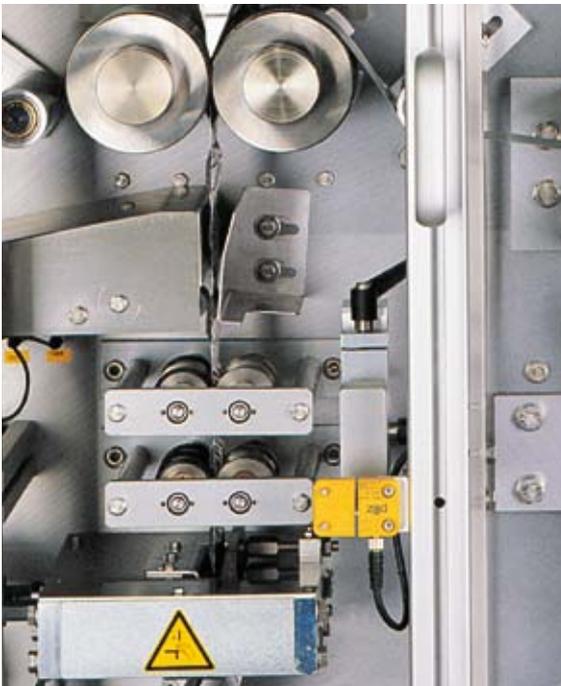


▶ 3.2 Guards

3.2.2 Movable guards

If access is required to the danger zone, a movable guard can be used, e.g. a safety gate.

The frequency with which access is required will determine whether the guard needs to be fixed or movable. The standards can help you make this decision.



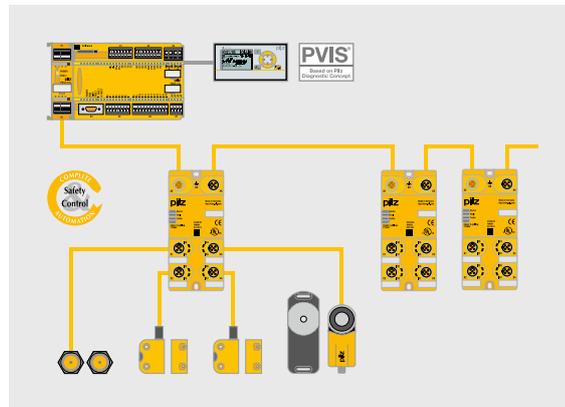
EN 953

Where access is required only for machine setting, process correction or maintenance, the following types of guard should be used:

a) Movable guard if the foreseeable frequency of access is high (e.g. more than once per shift), or if removal or replacement of a fixed guard would be difficult. Movable guards shall be associated with an interlock or an interlock with guard locking.

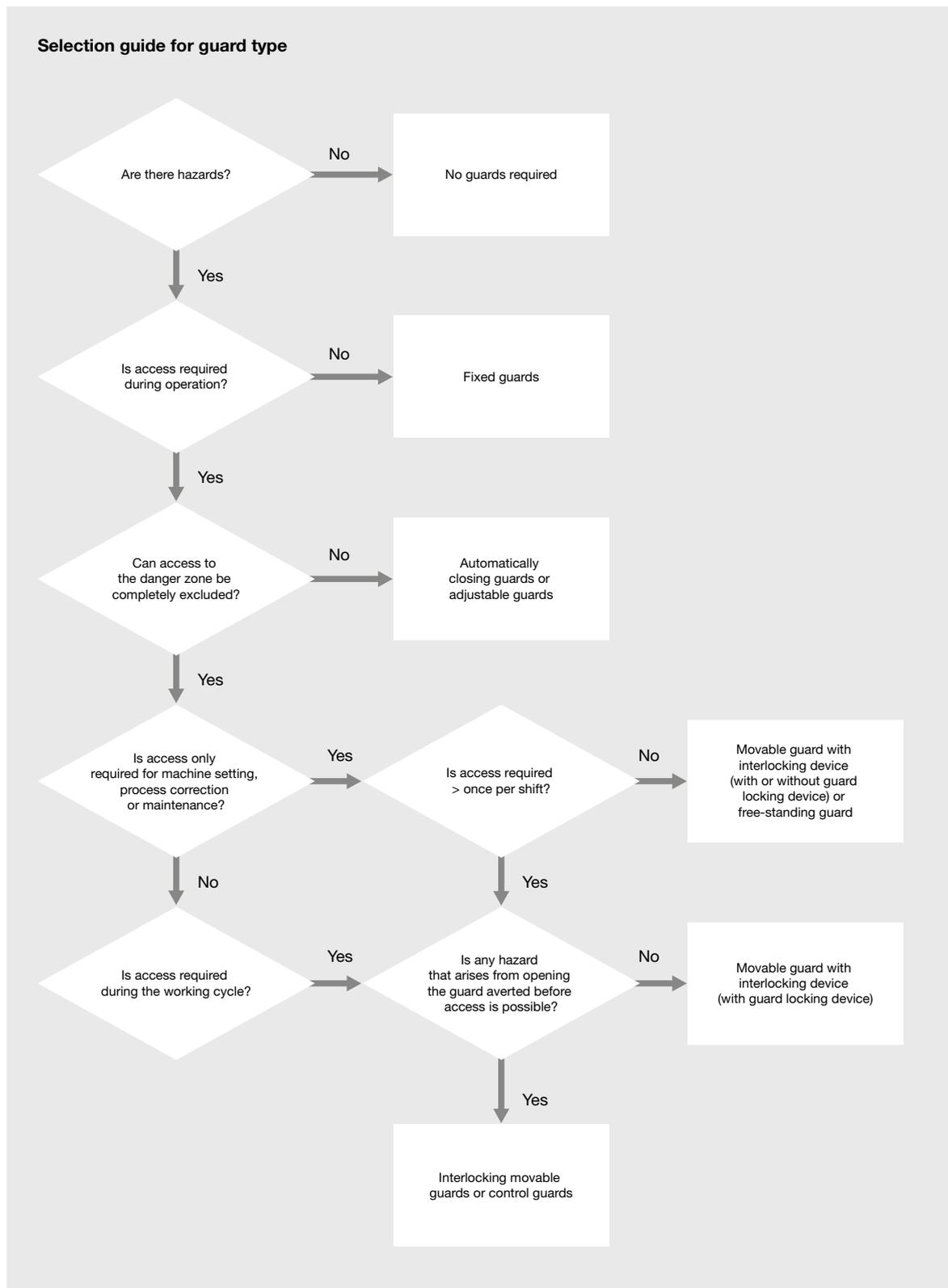
b) Fixed guard only if the foreseeable frequency of access is low, its replacement is easy, and its removal and replacement are carried out under a safe system of work.

Note: In this case, the term “interlock” means the electrical connection between the position of the safeguard and the drives to be shut down. In safety technology, the commonly understood mechanical “interlock”, meaning a lock, is called a “guard locking device”.



Monitoring several safety gates with one evaluation device thanks to individual diagnostics.

▶ 3.2 Guards



In accordance with EN 953 Annex A

▶ 3.2 Guards

EN 1088

7.5 Frequency of access

(frequency of opening the guard for access to the danger zone)

7.5.1 For applications requiring frequent access, the interlocking device shall be chosen to provide the least possible hindrance to the operation of the guard.

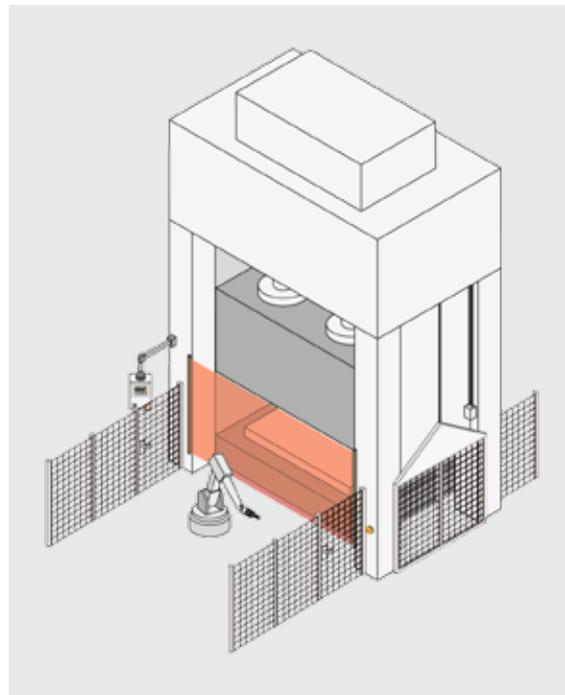
A clear distinction should be made between the following:

- ▶ the concept of frequent access required by the normal operation of the machine, as e.g. once per cycle to feed raw products to the machine and remove finished products
- ▶ the concept of occasional access, e.g. to carry out adjustment or maintenance interventions, or for random corrective actions in danger zones

Each of these concepts is associated with an order of magnitude differing greatly as to the frequency of human intervention in the danger zone (e.g. one hundred times per hour in the case of one access per cycle, and several times per day in the case of occasional access for adjustment or maintenance during an automatic production process).

Summary

Guards which need to be opened during production mode are generally designed as movable guards. These are in complete contrast to fixed guards, which are only operated rarely, for example, when they are opened to carry out maintenance or repair. This classification also needs to be well-founded because different costs will be associated with the type or selection of guard.



Fixed guards for maintenance or repair work.

▶ 3.2 Guards

3.2.3 Further aspects on the design of safeguards

Once the decision has been made to use a movable guard, the next step is to perform a risk assessment in accordance with EN 62061, EN ISO 13849-1 to determine the safety level of the corresponding position monitoring request (category, safety integrity level SIL or performance level PL). The corresponding control system is then designed and validated.

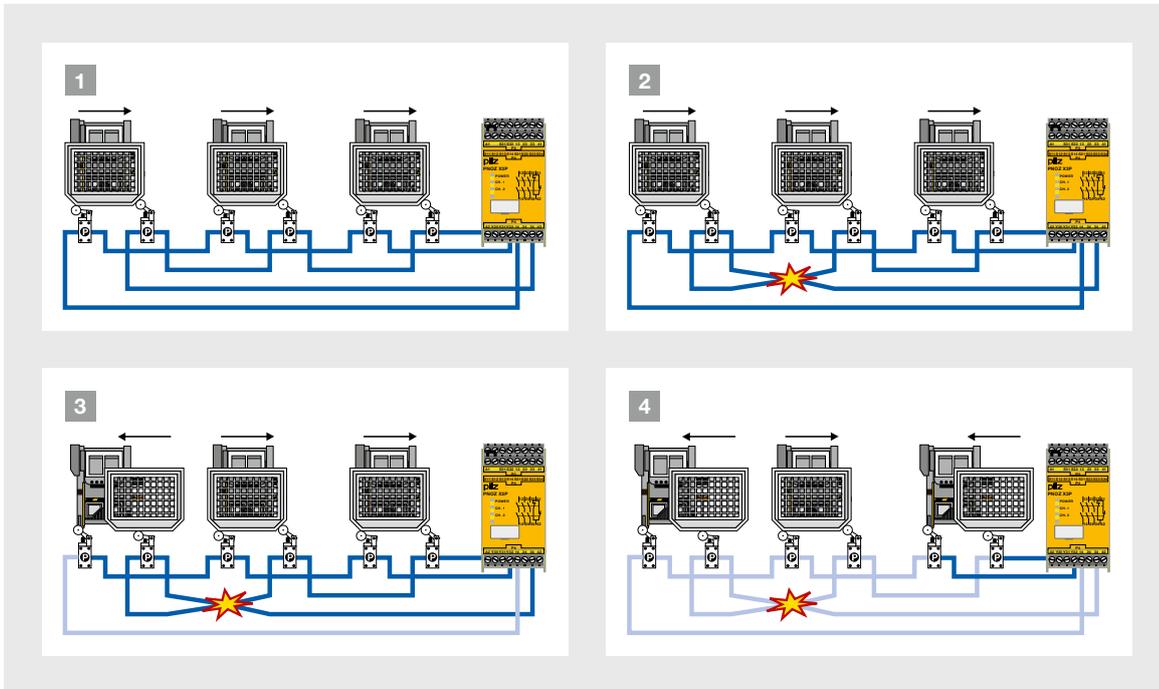
These control systems will include sensors in the form of switches, which detect the position of the guard. Via this detection feature, hazardous movements can be stopped as a result of the guard being opened. An additional safety function can prevent drives starting up unexpectedly when a safety gate is opened. The drive's stopping time will need to be considered: When a safety gate is opened, if it can be assumed that a drive with a long stopping time will generate a hazardous movement, this gate will require a guard locking device. The guard locking device must be unlocked by actively operating a

release. This is the only way to guarantee that the safety gate is not released unintentionally as the result of a power failure, for example. In this case, it's also important to note that a person who is in the danger zone at the time of the power failure and has shut the safety gate behind him cannot be released by an unlock command on the machine control system. Such a case may be rare, but it is conceivable, so any guard locking devices that are considered will have a mechanical release function. However, operating staff must be sure to have the appropriate actuation tool available or to be aware of how to operate the emergency release.

Safety gates connected in series

When selecting sensors to scan movable guards, the question arises as to whether such sensors can be connected in series to an evaluation device, and if so, how many? The answer to this question depends on the faults that can be anticipated (see fault lists in EN 13849-2). The following example of safety gates connected in series is intended to illustrate this point:

▶ 3.2 Guards



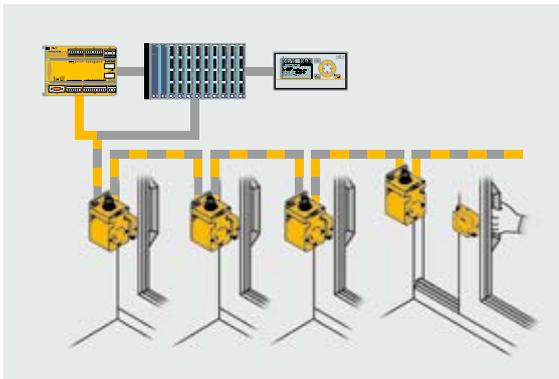
Example of safety gates connected in series.

- 1** The example shows three safety gates connected in series to an evaluation device. Initially all the safety gates are closed and the relay's outputs are "on", i.e. the machine can be operated.
- 2** On the left-hand safety gate, a short circuit occurs in the line to the switch with the N/C contact: At first the fault is not detected and the machine can continue operating.
- 3** The left-hand safety gate is then opened, an event which the left switch signals to the relay. During a feasibility comparison of the two switches the relay discovers an inconsistency and switches to a fault condition, i.e. once the safety gate is closed the machine cannot be restarted.
- 4** Now the right-hand safety gate is also opened. Via these signals the relay once again detects a normal condition. The fault condition is reset, the safety gates can once again be closed from left to right and the machine is ready to start up again.

This example illustrates an undetected fault in the safety circuit. An additional fault could cause the whole safety gate guard to fail to danger. These and similar faults are described by the term fault masking. In the current standards, the maximum diagnostic coverage (DC) that the switch can achieve is restricted, depending on the masking probability.

▶ 3.2 Guards

The occurrence of this type of masking should be taken into account on mechanical switches and magnetic proximity switches alike. Only switches with internal diagnostics and an OSSD output, as commonly found on RFID based switches, are unaffected by this.



Safety switches with integrated fault detection.

In practice, a single switch pair that is evaluated by a safety relay can achieve a DC = 99%. Based on this premise, in ISO/TR 24119, the maximum DC for a group of interlinked switches is stated based on the number of switches connected in series and their frequency of operation.

As you can see in the table on the next page, masking restricts the maximum achievable DC, and as a direct result, the achievable PL. If a series of interlinked switches is required to meet PL e, a technical solution is available using switches with integrated fault detection. As masking cannot occur in this case, it is possible to have interlinked switches without restricting the DC or PL.

Mechanical switches

In this context, the question also arises as to the need for mechanical redundancy and the number of independent switches on a safety gate. When installed correctly, magnetically operated and RFID proximity switches are often designed so that a single mechanical fault does not lead to the loss of the safety function; however, on mechanically operated switches (reed or roller switches), particular attention needs to be paid to the single-channel mechanical actuator. The documentation for the switch should always be checked carefully to establish whether the switch itself has any assured properties and if so, which. This is particularly important when a dual-channel electrical switching element is present. If not explicitly confirmed by the switch manufacturer under intended use, fault exclusions for the mechanical part of these switches must be justified by the user. This is often very difficult if not impossible to achieve, as it is difficult to estimate the effects of wear, vibration, corrosion, inappropriate mechanical stress, for example. In cases such as these, to achieve PL d or PL e you should either use two mechanical gate switches per gate, one dual-channel magnetic switch or one RFID switch with OSSD output.

▶ 3.2 Guards

Number of used frequently used movable guards ^{1) 2)}		Number of additional movable guards ³⁾	Maximum achievable (DC) ⁴⁾
0	+	2 to 4	Medium
		5 to 30	Low
		> 30	None
1	+	1	Medium
		2 to 4	Low
		≥ 5	None
> 1	+	≥ 0	None

¹⁾ If the frequency is higher than once per hour.
²⁾ If the number of operators capable of opening separate guards exceeds one then the number of frequently used movable guards shall be increased by one.
³⁾ The number of additional movable guards may be reduced by one if one of the following conditions are met:
- When the minimum distance between any of the guards is more than 5 m or
- When none of the additional movable guards is directly reachable.
⁴⁾ In any case, if it is foreseeable that fault masking will occur (e. g. multiple movable guards will be open at the same time as part of normal operation or service), then the DC is limited to none.

Maximum achievable DC (simplified).

The table does not describe how to handle safeguards that are rarely operated. A standards committee is currently busy working on this issue (status 11/2013). It's safe to assume that this situation will be covered in a future Technical Report ISO TR 18673 (Safety of machinery – Evaluation of fault masking in serial connections of guard interlocking devices with potential-free contacts). The concept is expected to be similar: lots of sensors connected in series without their own diagnostic device will lead to a reduction of the DC and thereby restrict the max. PL that can be achieved.

When additional parameters such as wiring type, test pulses and switch type are taken into account, more complex considerations can be provided beyond the values shown in the table. These can lead to better results in individual cases, but are always restricted to a maximum DC = medium.

There is also the question of how to proceed with a series connection of sensors with their own PL. In this case the diagnostics are an integral part of the sensor and are not influenced or reduced by a series connection. Nevertheless, the switch signal of the first sensor in the chain must be guided through all the other sensors before it can be processed by an evaluation device. A safety-related failure of another sensor in the chain could prevent it being forwarded. That's why in this case it's necessary to add up the failure probabilities of all the sensors in the chain – even if only the first sensor belongs to the safety function that is under examination.

▶ 3.2 Guards

Assessment of magnetic switches

One problem has proved to be critical when using magnetically operated gate switches (with reed contacts). If pairs of switches and safety relays are used and their mutual suitability has not been tested by the manufacturer, the machine builder must ensure that peak currents within the switch do not cause premature wear. This mainly affects pairs of reed switches with relay-based safety units.

For the assessment it is necessary to calculate the maximum occurring peak current I_S (see Formula 1) and to compare this with the permitted peak current of the switch I_{Smax} . All switches in series connections must be considered, which is why the lowest of all the permitted peak currents must be greater than or equal to the maximum switching current (see Formula 1).

$R_{Smin(i)}$	Minimum internal resistance of switch i
$I_{Smax(i)}$	Maximum permitted peak current of switch i
U_{Pmax}	Maximum voltage
R_{Pmin}	Minimum internal resistance of safety relay
I_S	Maximum switching current

$$I_S = \frac{U_{max}}{R_{Pmin} + \sum_i R_{Smin(i)}}$$

Formula 1

$$I_S \leq \text{MIN} (I_{Smax(i)})$$

Formula 2

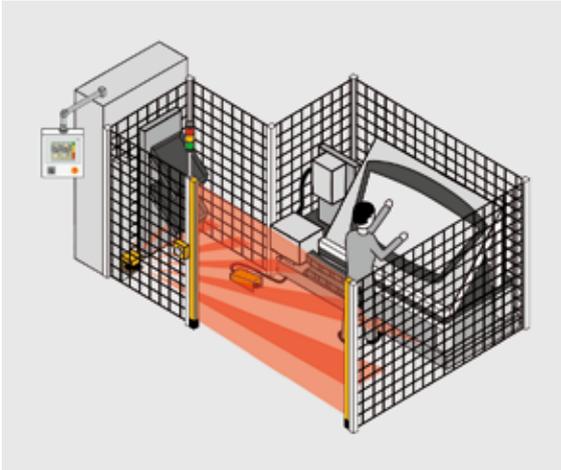
The problem of premature wear does not normally occur on mechanically operated switches and switches with OSSD output because wear on these switches is primarily determined via the average current and the thermal behaviour.

There is another new factor to consider from ISO 13855 relating to the consideration of switches on movable guards. This involves a potential hazard which might arise when a gate in a safety fence can be opened to such an extent that a person can access the danger zone through the opening without the corresponding gate switch receiving a signal change. This is more of a theoretical hazard but it can be averted by increasing the safety distance proportionate to the size of the undetected gate opening. In practice, the problem should never arise in the first place with the installation of a door switch that has been selected and fitted to meet the requirements of the situation.

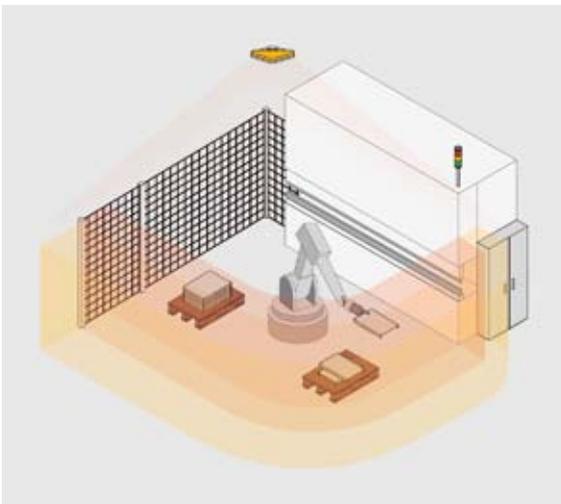
In this respect, the actual safety distance between the gate and site of the hazard is of greater practical relevance. Here, the question arises as to what happens when the safety gate in a safety fence is opened and a person enters the danger zone but the machine is still running down or braking. In this case, the relevant danger zones can still be reached if the person approaches at sufficient speed and the machine has a correspondingly long braking time. According to the standard, the calculation for the use of light curtains can be used in this case. Safety distance S is calculated as $S = (K \times T)$. K is the walking speed of the person of 1,600 mm/s and T is the time from the triggering of the gate switch to the machine stopping (i.e. safe status is achieved). The time that it takes to open the gate may be deducted. This can be identified either by considering how long this may take in theory or by timing it in practice, as no standard values are provided.

▶ 3.3 Protective devices

3.3.1 Active optoelectronic protective devices



Monitoring production areas in which active intervention is required.



Safe camera system for three-dimensional zone monitoring.

Protective devices (electrosensitive protective equipment, abbreviated to ESPE below) are always used when access to the corresponding hazard zone is intended to be particularly easy to achieve and there are no hazardous repercussions to be anticipated from the machine itself (example: welding or grinding processes). To ensure that a potential hazard can be shut down quickly enough, the protective device must be installed at an appropriate distance. This distance or safety distance (S) is defined in EN ISO 13855 and depends in particular on the following factors:

- ▶ t_1 = Response time of the protective device itself.
- ▶ t_2 = Response time of the machine, i.e. the machine's stopping performance in response to the signal from the protective device
- ▶ C = Potential approach towards a danger zone undetected by the protective device, e.g. reaching through two beams of a light curtain undetected, depending on the distance of these beams
- ▶ K = Anticipated approach speed of the human body or parts of the human body. This factor is defined in EN ISO 13855 as 1,600 mm/s for walking speed and 2,000 mm/s for hand speed.

The distance to be implemented is therefore

$$S = K * (t_1 + t_2) + C$$

▶ 3.3 Protective devices

EN 13855 defines the following preferential distances:

Resolution	Calculation formula (Distance S [mm])	Remarks
$d \leq 40 \text{ mm}$	$S = 2000 \times T + 8 (d - 14)$	If the result is $< 100 \text{ mm}$, a distance of at least 100 mm must be maintained.
	If the result is $> 500 \text{ mm}$, you can use $S = 1600 \times T + 8 (d - 14)$ as the calculation	In this case, S may not be $< 500 \text{ mm}$.
$40 < d \leq 70 \text{ mm}$	$S = 1600 \times T + 850$	Height of the lowest beam $\leq 300 \text{ mm}$
		Height of the highest beam $\geq 900 \text{ mm}$

Multiple single beams		No. of beams	Beam heights in mm
Multibeam	$S = 1600 \times T + 850$	4	300, 600, 900, 1200
		3	300, 700, 1100
		2	400, 900
Single beam	$S = 1600 \times T + 1200$	1	750
		If the risk assessment permits a single beam arrangement	

If the ESPEs form horizontal or inclined protected fields above an accessible area which requires safeguarding, the fields must be positioned at a minimum height, as pre-determined by the application and ESPE. Here too, the safety distance between the outer edge of the protected field and the danger point to be safeguarded should be such that the possibility of injuries resulting from the hazardous movement in the danger zone is excluded, bearing in mind the machine's stopping performance.

▶ 3.3 Protective devices

- ▶ Even when a guard has been carefully designed, any means of defeating it must be taken into account. Any possibility of reaching over or around a detection field needs to be excluded. As it is not always possible to cover any gaps alongside the detection field and an adjacent safety fence, safety distances between the person and the danger zones need to be observed here as well. The calculation of these distances is very similar to those for safety distances that apply to access to danger zones through a detection field. Particular attention needs to be paid to this important difference.

In practice, it could for example be the case that access to a danger zone is protected by a vertically installed light grid. This light grid however is often not as high as a person might be able to reach and - depending on a guardrail, for example - may be only 1,100 mm high. In this case, a person would therefore be able to stand just in front of the light grid without interrupting the detection field. Furthermore, they can in this case still lean forward and with an outstretched arm access the area behind the light grid with their hand. In order to avert hazards in this situation, minimum distances between the danger zone and light curtain are defined. These minimum distances are comprised of two components: Walking speed and hand speed multiplied by the system's reaction time plus an additional value which depends on the height of the danger zone and the height of the safeguard. This additional value may be up to 1,200 mm. Where space is limited, it is worth looking at covering all possible means of defeating the system permanently.

- ▶ Information on positioning and sizing of pressure-sensitive mats can be found in Clause 7 of EN ISO 13855. Here as well, the familiar formula of $S = (K \times T) + C$ is used. In this case K equals 1,600 mm/s, derived from normal walking speed. A minimum distance of $C = 1,200$ mm is required to protect an outstretched arm or hand that will not be detected by the pressure-sensitive mat.
- ▶ The design of the safety distance S for the arrangement of two-hand control devices is based on the formula $S = (K \times T) + C$. In this case, C is 250 mm and K is 1,600 mm/s (hand speed).

3.3.2 Further important aspects in connection with electro-sensitive protective equipment

3.3.2.1 Restart

Once a protective device has been triggered, a machine may not be restarted automatically once the protected field has been cleared. This should only be possible via a reset on a control device outside the danger zone, with visual contact.

3.3.2.2 Encroachment from behind

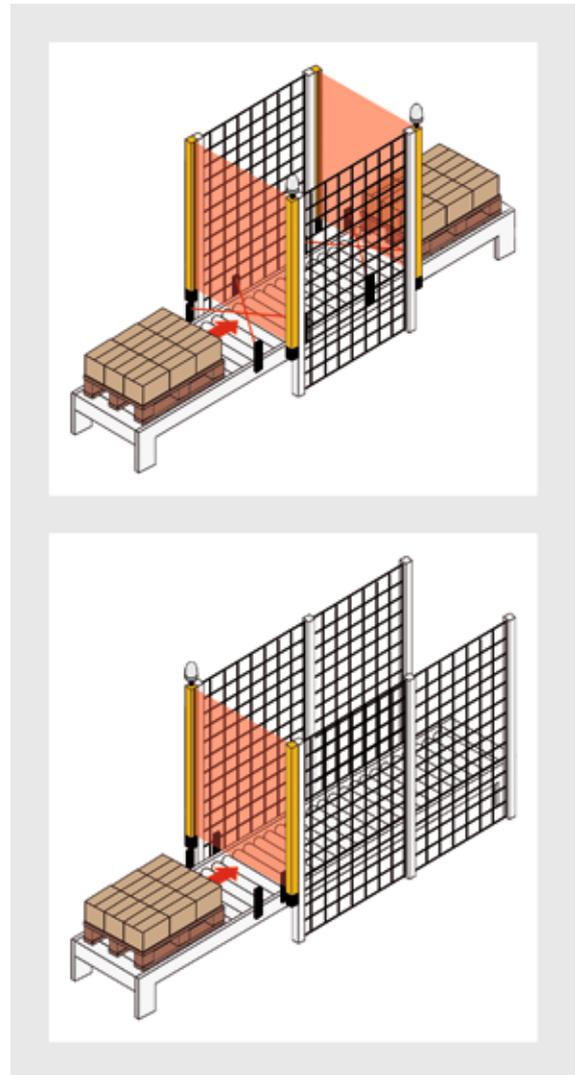
As well as the obvious protection for the danger zone it's also necessary to consider the possibility of reaching over, under or around the device, as well as encroaching from behind. A purely mechanical safeguard or another light curtain can be used to provide protection against encroachment from behind. If there is any possibility of defeating the safeguards, additional measures must be taken to protect them.

▶ 3.3 Protective devices

3.3.2.3 Muting

Muting is the safe, temporary, automatic suspension of electrosensitive protective equipment (ESPE), so that material can be transported into and out of a danger zone. Special sensors are used to ensure the muting controller only starts the muting cycle when the material is being transported through the protected field. The sensors must be positioned in such a way that persons cannot activate the muting sensors. If anyone should access the protected area, the potentially dangerous movement is shut down immediately.

The industry has developed special safety relays with muting function specifically for this case. Some light curtains also provide the option to mute the protected field only partially (blanking). In this process for example, the precise section through which the item is being transported is rendered passive. However, under no circumstances should anyone be able to reach the danger zone undetected via this deactivated section of the protected field. A design measure (e.g. a cover for the remaining free space) should be used to ensure that nobody can reach the danger zone from the side, in between the item and the protective device.



Protective beam limited double muting/muting with four muting sensors.

▶ 3.3 Protective devices

3.3.3 Other sensor-based protective equipment

3.3.3.1 Laser scanners

A second ESPE installed horizontally or at an angle is often used to protect against encroachment from behind. Often this only covers a small area, so a scanner can be used for additional optical monitoring of encroachment from behind. A laser beam scans the area to be monitored. If the beam is reflected by a foreign body, this will be detected and the hazardous movement will be shut down.

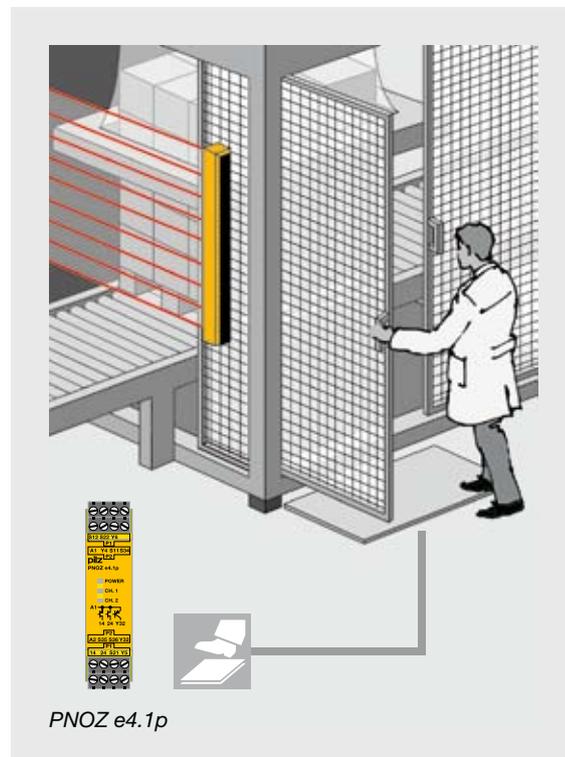
3.3.3.2 Safe camera systems

The latest developments on the market are safe camera systems for monitoring freely configurable zones. In contrast to simple sensors, they are able to record and analyse detailed information about the whole monitored zone. This way potentially hazardous work processes are safely monitored, protecting man and machine.

3.3.3.3 Pressure-sensitive mats

Many pressure-sensitive mats operate in accordance with the normally open principle: They require the use of special evaluation devices, which account for this actuation principle and guarantee appropriate fault detection. Pressure-sensitive mats that operate to the normally closed principle are also available, however; where a low safety level is required and the electrical loads are low, these can be used to activate contactors directly.

The most popular material used on pressure-sensitive mats is EPDM, but as this is not permanently oil-proof, it has limited suitability for use in a machine environment. Other materials such as NBR are available, but they reduce the sensitivity of the sensor.



Using electronic safety relays to evaluate pressure-sensitive mats.

▶ 3.3 Protective devices

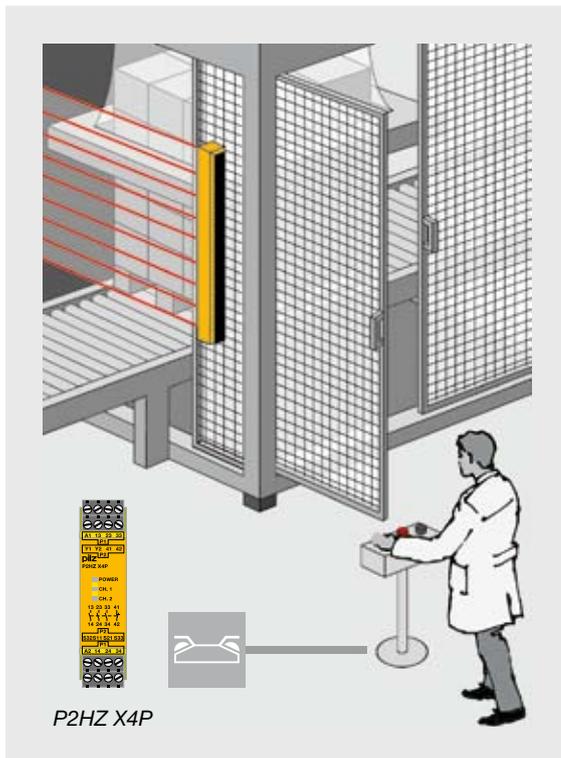
3.3.3.4 Two-hand control devices

Two-hand control devices are used on a workstation to keep both of the operator's hands committed to a two-hand circuit; while the devices are operated, the hands are kept away from the

danger zone. Various types of two-hand circuits are defined and can be applied to suit the necessary level of protection:

Requirement levels for two-hand control devices:

Requirements	EN 574 Clause	Types				
		I	II	III		
				A	B	C
Use of both hands	5.1	◆	◆	◆	◆	◆
Release of either actuator initiates the cessation of the output signal	5.2	◆	◆	◆	◆	◆
Prevention of accidental operation	5.4	◆	◆	◆	◆	◆
Protective effect shall not be easily defeated	5.5	◆	◆	◆	◆	◆
Re-initiation of output signal only when both actuators are released	5.6	◆	◆	◆	◆	◆
Output signal only after synchronous actuation within max. 500 ms	5.7			◆	◆	◆
Use of category 1 in accordance with EN 954-1	6.2	◆		◆		
Use of category 3 in accordance with EN 954-1	6.3		◆		◆	
Use of category 4 in accordance with EN 954-1	6.4					◆



The current edition of EN 574 still refers to the withdrawn standard EN 954-1. That's one of the reasons why EN 574 is currently under revision (status 11/2013).

Evaluation of two-hand control circuits.

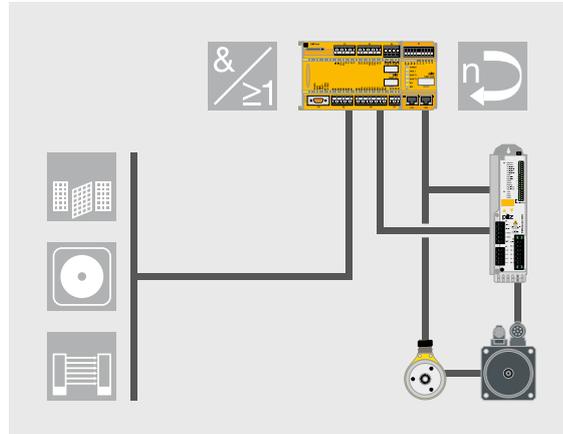
▶ 3.3 Protective devices

3.3.3.5 Functional safeguards

Protection against unexpected start-up in accordance with EN 1037

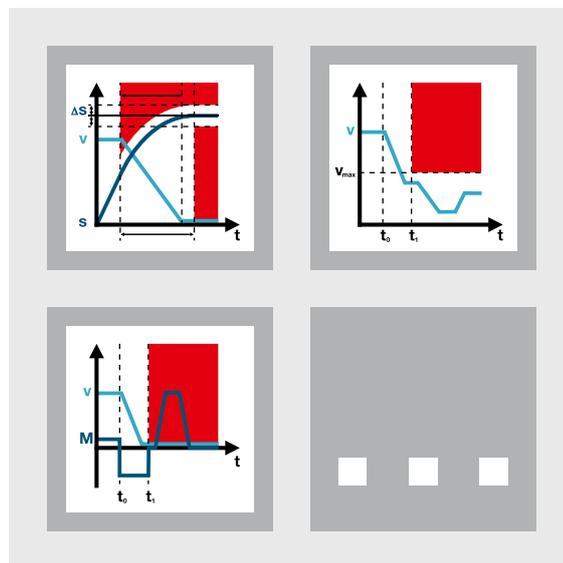
When an operation is in progress, the same question always arises: when a machine is brought to a halt via an operational stop command, how safely is the machine prevented from starting up unintentionally: What happens in this situation should a fault occur in the control system and a drive is started up unexpectedly? This is an issue which is just as important as the consideration of functional safety associated with “more obvious” safeguards. A key point to consider is the issue of converter-controlled drives. These drives are often stopped by signals such as “Zero Speed” or “Controller Inhibit”. The desire is often to avoid shutting down the power supply so as not to lose any data about the current drive status. In some cases, spontaneous shutdown of the connection between the mains and the converter or even between the converter and the drive is linked to device defects and so cannot be considered.

In cases such as these the machine designer has two options: If isolation from the energy supply is possible without damaging the unit and without initiating other hazardous movements, standstill monitoring can be used. Although the converter-controlled drive is stationary it is still active, so it is monitored to check it does not move. Should any movement occur on account of an error, the supply to the whole branch is shut down via a contactor. This solution assumes that the slight drive movement which occurs in the event of an error does not cause a hazard. The movement itself consists of two parts: The part which activates the sensor technology for monitoring and the part occurring before the protection circuit has reacted and a contactor has switched. These influences must be examined in a risk assessment.



External drive monitoring through the PNOZmulti safety system with speed monitoring.

If an unintended movement such as this is unacceptable, safe drive technology must be used, which will prevent such faulty behaviour from the start (see also Chapter 7: Safe motion control).



Drive-integrated safety.

▶ 3.4 Manipulation of safeguards

Dealing with safeguards and their manipulation is an issue in which the true causes have long been largely taboo. It's a situation that's difficult to understand, for without negative feedback, where can you start to make positive changes in the design of plant and machinery?

This situation has now changed: The confederation of commercial trade associations has published a study showing that safety equipment had been manipulated on almost 37% of the metal processing machinery examined. In other words: In a good third of cases, manipulations have been detected and examined, although it's safe to assume that the unreported number may be somewhat higher.

One fact that hasn't changed, however, is the number of accidents recurring on machinery on which the safeguards are manipulated, as the BG bulletins regularly show. The report also reveals that in at least 50% of all cases, the reasons for manipulation can be traced right back to the design departments.

3.4.1 Legal position

The legal position is clear: European and domestic law (e.g. EC Machinery Directive, EN standards, German Product Safety Act [ProdSG]) mean that it is the responsibility of machine manufacturers only to place on the market products that have an adequate level of safety. Manufacturers must establish all the potential hazards on all their machines in advance and assess the associated risks. They are responsible for developing a safety concept for the respective products, implementing that concept and providing the relevant documentation, based on the results of the hazard analysis and risk assessment. Potential hazards must not be allowed to impact negatively on subsequent users, third parties or the environment. Any reasonably foreseeable misuse must also be included. Operating instructions should also clearly define the products' intended use and prohibit any known improper uses.

Design engineers must therefore make reasoned decisions regarding situations in which events may be above and beyond what you would normally expect. This is a subject which is generally familiar and is considered these days, as CE marking clearly shows. However, despite the formal declarations from manufacturers that they themselves have taken responsibility for complying with all the essential health and safety requirements, behaviour-based accidents continue to occur on machinery. Although the plant or machinery complies with the formal specifications, the design still failed to meet needs or satisfy safety requirements.

▶ 3.4 Manipulation of safeguards

Design engineers should never underestimate the technical intelligence and creativity of machine users, as revealed by some dubious practices for defeating safeguards: It begins with crude but effective access to the mechanical structure of the signal flow chain and extends to skillfully filed keys for type 2 safety switches. It includes loosened, positive-locking shaft/hub connections on switch cams, which are difficult to detect, as well as sophisticated short and cross circuits and disguised, carefully hidden but rapidly accessible override switches in N/C / N/O combinations, in the connection lead between the control system and the safety switch. This is only a small sample of the manipulations that are detected; it is by no means all.



Design engineers should also consider that machine workers generally have a fair level of technical understanding and manual dexterity and also have considerably more time to become annoyed at ill-conceived operating and safety concepts and to consider effective “improvements” than the designers had for their development and implementation. Quite often they will have been reliant purely on the normative specifications, without being aware of the realistic, practical requirements.

The task of working out potential manipulations in advance is therefore contradictory: Design engineers with little experience in this area are supposed to simulate the imagination and drive of the machine operators, who may frequently work under pressure but still have enough time and energy to work out alternative solutions. They are supposed to incorporate their expertise into their designs and, under today’s usual time constraints, convert this into safety measures which are manipulation-proof. A task that’s not always easy to resolve.

BGIA has developed a check list of manipulation incentives, which performs a valuable service in predicting potential manipulations. From the author’s point of view, however, enormous progress would be made if designers in future would increasingly put themselves in the user’s position and honestly and candidly ask themselves what they would do with the available operating and safety concept.

▶ 3.4 Manipulation of safeguards

3.4.2 Conduct contrary to safety – What does that mean?

Terminology

Defeat in a simple manner

Render inoperative manually or with readily available objects (e.g. pencils, pieces of wire, bottle openers, cable ties, adhesive tape, metallised film, coins, nails, screwdrivers, penknives, door keys, pliers; but also with tools required for the intended use of the machine), without any great intellectual effort or manual dexterity (see also EN ISO 14119).

Manipulation

In terms of safety technology: an intentional, unauthorised, targeted and concealed intervention into a machine's safety concept, using tools (see also EN ISO 14119).

Sabotage

Secret, intentional and malicious intervention into a technical system, in order to harm employees or colleagues. Word's origin: The wooden shoe (Fr.: sabot) of an agricultural worker or Luddite in the 19th century, which was thrown into a lathe.

When designing and constructing machinery, manufacturers specify what the machines can and should be able to achieve. At the same time they also specify how the user should handle the machine. A successful design involves much more than simply the machine fulfilling its technological function in terms of the output quantity documented in the implementation manual, and the quality and tolerances of the manufactured products. It must also have a coherent safety and operating concept to enable users to implement the machine functions in the first place. The two areas are interlinked, so they ought to be developed and realised in a joint, synchronous operation.

Numerous product safety standards (e.g. EN 1010 or EN 12717) are now available, offering practical solutions. Nonetheless, planning and design deficiencies are still to be found, even on new machinery. For example:

- ▶ Recurring disruptions to the workflow, brought about for example by deficiencies in the technological design or in the precision of the components (direct quote from a plant engineer: "The greatest contribution design engineers can make to active health and safety is to design the machines to work exactly in the way which was promised at the sale.")
- ▶ Opportunities for intervention or access, e.g. to remove the necessary random samples, are either difficult or non-existent
- ▶ Lack of segmented shutdowns with material buffers, so that subsections can be accessed safely in the event of a fault, without having to shut down the entire plant and lose valuable time starting it up again

Ill-conceived safety concepts are still found in practice on a regular basis. Many errors are made with interlocked safeguards, for example, when

- ▶ Non-hazardous or frequently operated function elements, e.g. actuators, storage containers, filler holes, are installed behind (interlocked) safeguards
- ▶ The interlock interrupts the hazardous situation quickly and positively when a safeguard is opened, but afterwards the machine or process is unable to continue or must be restarted

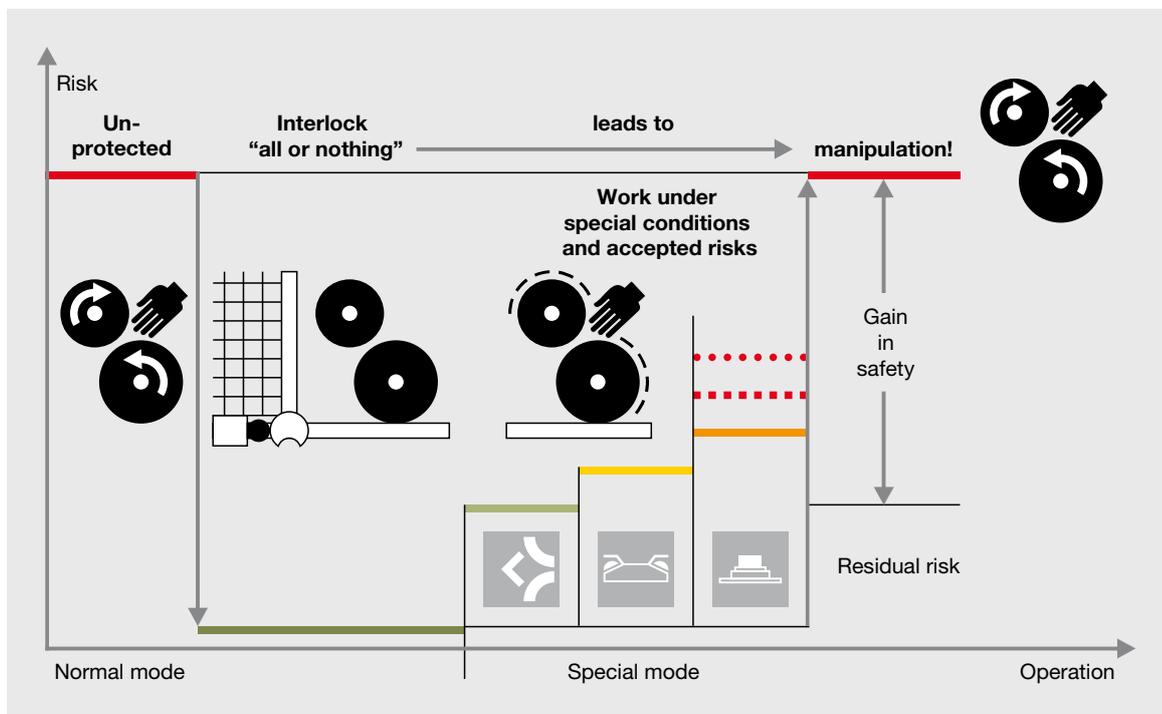
▶ 3.4 Manipulation of safeguards

Nobody has any doubt that designers act to the best of their knowledge and belief when they design and implement technological functions as well as those functions relating to persons or operators. One can't really blame them for assuming that subsequent users will behave reasonably and correctly when using the machinery. But it's precisely here that caution is advised: Human behaviour is mainly benefit-oriented, both in everyday and in working life. People strive to perform the tasks they are given or have set themselves as quickly and as well as necessary, with the least exertion possible.

People will also try to intervene actively in support of a process, if it isn't running quite as it should. They will make every effort to rectify troublesome faults as quickly and simply as possible. If they can't because of the design (and the fault rectification procedure set down in the operating manual), they will find a way out by defeating the interlock, for example. They will often regard the additional

work as a personal misfortune for the smooth performance of their work function. By defeating the safety measures that have been provided the procedure is much less complex, and is therefore seen as a success. Successful behaviour tends to be repeated until it is reinforced as a habit, which in this case is unfortunately contrary to safety and indeed dangerous.

The more such rule breaches are tolerated at management level and go unsanctioned, the greater the probability that the rules will continue to be breached without punishment. Incorrect conduct becomes the new, informal rule. For over the course of time, the awareness of the risks that are being taken will lessen and those involved become convinced that they have mastered the potential hazards through vigilance. But the risk is still there; it's just waiting for its chance to strike.



Interlocking concept for special operating modes.

▶ 3.4 Manipulation of safeguards

There's no question that the factors that trigger an accident seem initially to rest with the conduct of those affected. However, design errors on the machine encourage the misconduct that's so dangerous (even life threatening) to those involved. Such machines do not comply with the EC Machinery Directive. In other words: It is the manufacturer's responsibility to design protective measures in such a way that they provide a sufficient level of safety, in accordance with the determined risk, while still guaranteeing the functionality and user friendliness of the machine. Ultimately it is always better to accept a calculable, acceptable residual risk with a carefully thought out safety concept, tailored to the practical requirements, than to expose the machine operator to the full risk of insecure processes following successful manipulation.

3.4.3 What can designers do?

Designing safety-related machinery means more than simply complying with regulations and other legal stipulations. Consulting the relevant regulations and standards, dismissively asking "Where does it say that?!" – to ensure that only those safety measures that are strictly necessary are implemented – is no substitute for deep consideration of solutions that are not only right for safety and right for people but are also fit for purpose.

Most of all, designers must be more sensitive to operators' demands for operability of machines and safety devices and provide a serious response, because their demands are based on practical experience. This does not make the safety-related design more difficult, but is the basis on which to build user-friendly, safety-related machinery. It's essential that the actual development and design is preceded by a detailed, candid analysis of the operational requirements, the results of which are recorded in a binding requirement specification. If not, the situation may arise in which the machine and its incorporated safety measures may not be accepted. What's more, they could provoke users into creating "new ideas", most of which do not support health and safety. These in turn could conjure up a whole new set of hazards, which were far from the minds of the original designers.

Experience shows that the first part of this challenge can be met at reasonable cost and with a sufficient level of success through systematic troubleshooting, using function structures and signal flow paths. As for the second part of the task, counteracting manipulation attempts, designers must rely on their tried and trusted methods, as with any other design task. After all, safety-related design is hardly a dark art!

Nonetheless: Manipulation rarely occurs voluntarily; it usually indicates that machine and operating concepts are not at their optimum. Conduct contrary to safety should always be anticipated when:

- ▶ Work practices demand actions which do not have a direct, positive impact on outcomes
- ▶ Work practices enforce constant repetition of the same work steps, or fresh approaches are always required in order to achieve work targets
- ▶ Safeguards restrict the line of vision and room for manoeuvre required to perform the activity
- ▶ Safeguards impede or even block the visual/auditory feedback required to work successfully
- ▶ Troubleshooting and fault removal are impossible when the safeguards are open

▶ 3.4 Manipulation of safeguards

In other words: Manipulations must always be anticipated when restricted machine functions or unacceptable difficulties tempt, even force, the machine user to “improve” safety concepts. Manufacturers must design protective measures so that the functionality and user friendliness of the machine are guaranteed at a tolerable, acceptable level of residual risk: They must predict future manipulation attempts, use design measures to counteract them and at the same time improve machine handling.

The obligations of machine manufacturers are threefold:

1. Anticipate reasons and incentives for manipulation, remove the temptation to defeat interlocks by creating well thought-out operating and safety concepts for machinery.
2. Make manipulation difficult by design, e.g. by installing safety switches in accessible areas, using hinged switches, attaching safety switches and their actuators with non-removable screws, etc.
3. Under the terms of the monitoring obligation specified in the German Product Safety Act (ProdSG), systematically identify and rectify any deficiencies through rigorous product monitoring with all operators (reports from customer service engineers and spare part deliveries are sometimes very revealing in this respect!).

The client who places the order for a machine can also help to counteract manipulation by talking to the machine manufacturer and candidly listing the requirements in an implementation manual, binding to both parties, and by talking openly about the faults and deficiencies within the process, then documenting this information.

3.4.4 User-friendly guards

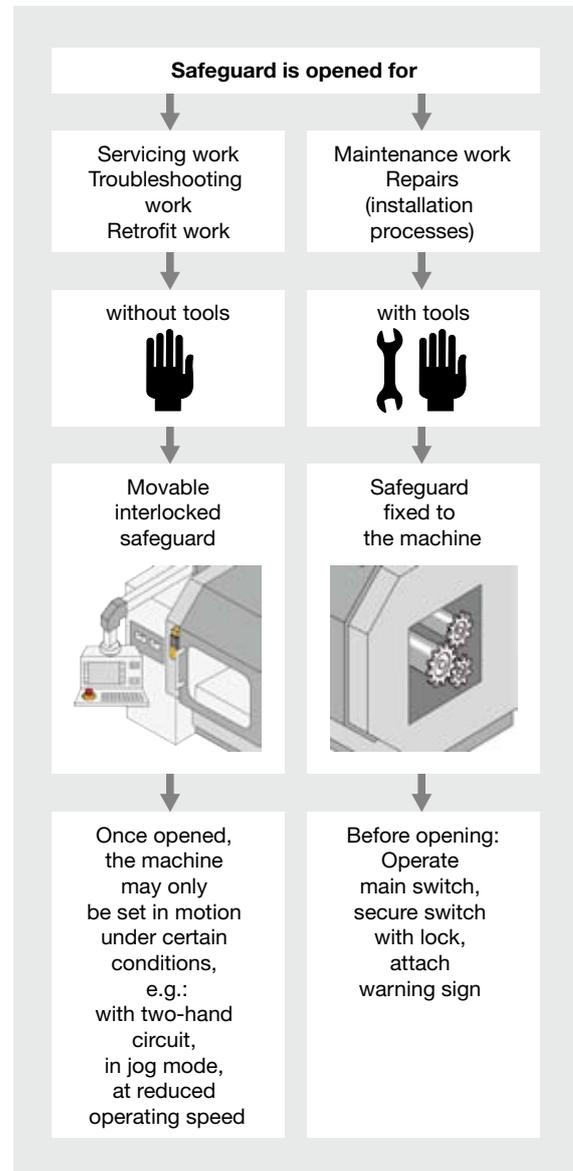
It's important to recognise that safeguards – even interlocked guards – are always willingly accepted and are not manipulated when they do not obstruct but actually support or even simplify the workflow. Faults in the safety concept which force operators to manipulate safeguards are genuine design faults, for which the machine manufacturer is liable in some circumstances. Safety-related solutions with an acceptable residual risk must be put in place, not just for fault-free normal operation, but also for set-up, testing, fault removal and troubleshooting.

Simply to make manipulation attempts more difficult on a technical level, only appears to solve the problem (see also EN ISO 14119). For if there is enough pressure, a “solution” will be found. It's more important to eliminate the reason for manipulation. What's needed is not excessive functionality (even in terms of safety technology), but user friendliness. If there's any doubt as to whether the safety concept is adequate, it's recommended that you seek expert advice from the relevant employer's liability insurance association or from the safety component manufacturer.

▶ 3.4 Manipulation of safeguards

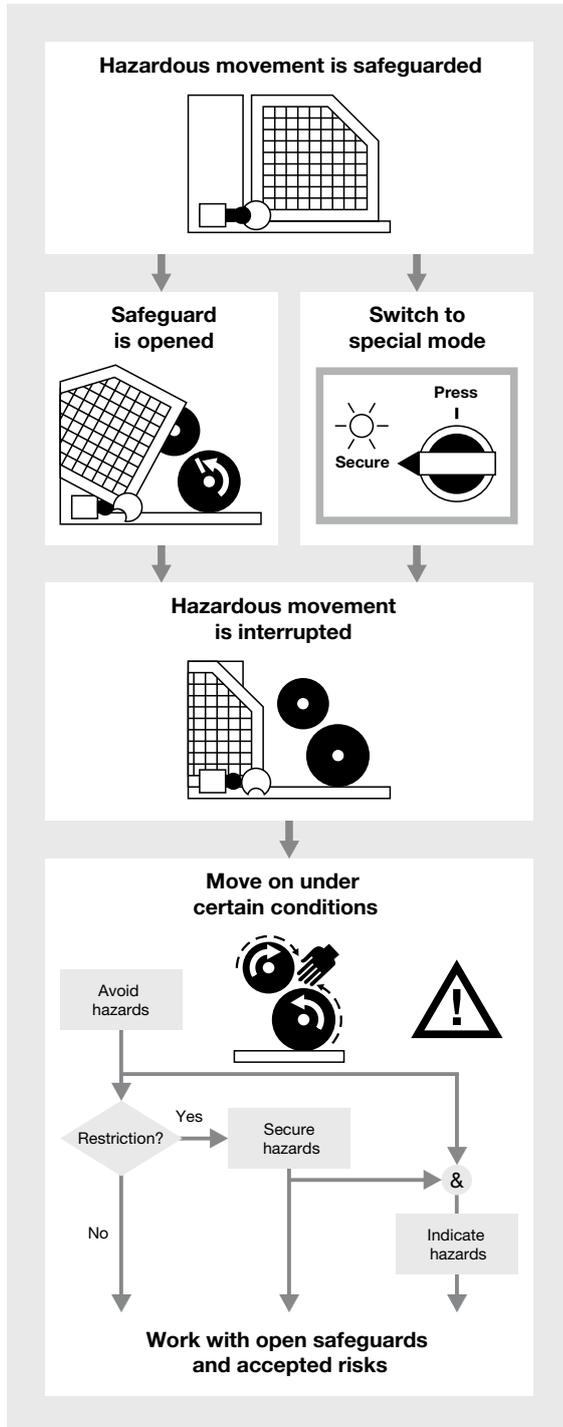
Guards use physical barriers to stop people and hazardous situations coinciding in time and space. Their essential design requirements are stated in EN 953 and EN ISO 14119. Safety-related and ergonomic aspects must be taken into account alongside questions regarding the choice of materials and consideration of mechanical aspects such as stability. These factors are decisive, not just in terms of the quality of the guard function but also in determining whether the safeguards, designed and constructed at considerable expense, will be used willingly by employees or be defeated and even manipulated.

Experience shows that despite all the protestations, almost every safeguard has to be removed or opened at some point over the course of time. When safeguards are opened, it's fundamentally important that hazards are avoided where possible and that employees are protected from danger. The reason for opening, the frequency of opening and the actual risk involved in carrying out activities behind open safeguards (see the following illustrations) will determine the procedures used to attach and monitor safeguards.



Opening procedures on safeguards.

▶ 3.4 Manipulation of safeguards



Interlocking concept for safeguards.

Where safeguards are opened as a condition of operation or more frequently (for example: at least once per shift), this must be possible without using tools. Where there are hazardous situations, use of an interlock or guard locking device must be guaranteed. Further protective measures must be adjusted to suit the resulting risk and the drive/ technological conditions, to ensure that the activities which need to be carried out while the safeguards are open can be performed at an acceptable level of risk. This procedure conforms to the EC Machinery Directive. It allows work to be carried out while the safeguards are open as a special operating mode and gives this practice a legal basis.

3.4.5 Conclusion

Just some final words in conclusion for all designers: Designing interlocks so that absolutely no movement of the machine or subsections is possible once the safeguard has been opened actually encourages the type of conduct which is contrary to safety and, ultimately, leads to accidents. Nevertheless, it is the causes you have to combat, not the people. If a machine does not operate as intended, users will feel they have no choice but to intervene. In all probability, the machine will “reciprocate” some time with an accident. Which is not actually what it was designed to do!



4

**Safe control
technology**

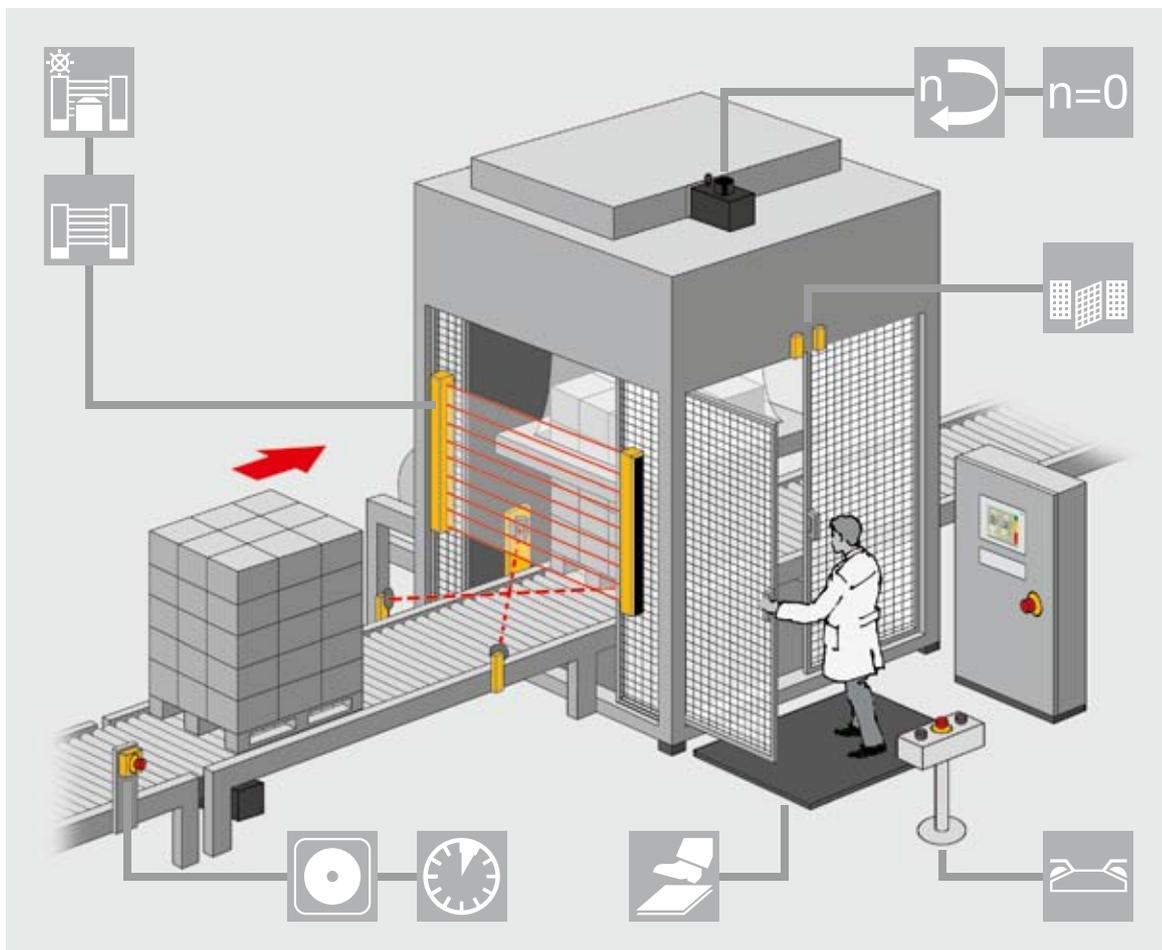
▶ 4 Safe control technology

Chapter	Contents	Page
4	Safe control technology	4-3
4.1	Safety relays	4-4
4.1.1	Overview of safety relays	4-4
4.1.2	Structure and function of safety relays	4-4
4.1.3	Relays and electronics	4-6
4.1.4	Greater flexibility during installation	4-7
4.1.5	Special features and functions	4-10
4.2	Configurable safety relays	4-11
4.2.1	Safety-related and non-safety-related communication	4-13
4.2.2	Customer benefits from application blocks	4-16
4.3	Today's safety control systems	4-21
4.3.1	Overview of safety control systems	4-21
4.3.2	Integration within the automation environment	4-22
4.3.3	Safe decentralisation and enable principle	4-24
4.3.4	Function blocks in safe control systems	4-26
4.3.5	Mission time of safety functions	4-27
4.3.6	Use of used components	4-27
4.4	Using safety control systems to achieve safe control technology	4-28
4.4.1	Overview	4-28
4.4.2	Safe control technology	4-29
4.4.3	Modularisation of the automation function	4-30
4.5	Safe control technology in transition	4-31
4.5.1	New safety technology requirements	4-31
4.5.2	Complex yet simple – no contradiction	4-33
4.5.3	Outlook – from static to dynamic safety	4-37

► 4 Safe control technology

In the early days of control technology, the focus in the control system was on the function and therefore the process image. Relays and contactors activated plant and machinery. Where there were shutdown devices or devices to protect personnel, the actuator was simply separated from the supply when necessary. However, people gradually realised that this type of protection system could be rendered inoperational in the event of an error: The protective function would no longer be guaranteed. As a result, people began to consider the options for safeguarding this type of separation function. Special relay circuits, such as the 3 contactor combination, were one of the initial outcomes of these considerations. These device combinations ultimately led to the development of the first safety relay, the PNOZ.

Safety relays, therefore, are devices which generally implement safety functions. In the event of a hazard, the task of such a safety function is to use appropriate measures to reduce the existing risk to an acceptable level. These may be safety functions such as emergency off/emergency stop, safety gate function or even standstill monitoring on a drive. Safety relays monitor a specific function; by connecting them to other safety relays they guarantee total monitoring of a plant or machine. The first safety-related control system ultimately came from the desire to connect functions flexibly through programming, similar to the way this is done on a programmable logic controller (PLC).



Safety functions for all requirements.

▶ 4.1 Safety relays

Configurable safety relays like PNOZmulti are a combination of safety relay and safety control system. Having considered the advantages and disadvantages of both systems, they combine the simplicity of a relay with the flexibility of a safety control system. Although the primary focus for safety relays and safety control systems is to monitor safety functions, the current trend is towards intelligent dovetailing of safety and automation functions within one system.

4.1 Safety relays

4.1.1 Overview of safety relays

Safety relays perform defined safety functions: For example, they:

- ▶ Stop a movement in a controlled and therefore safe manner
- ▶ Monitor the position of movable guards
- ▶ Interrupt a closing movement during access

Safety relays are used to reduce risk: When an error occurs or a detection zone is violated, they initiate a safe, reliable response. Safety relays are encountered in almost every area of mechanical engineering, mainly where the number of safety functions is quite manageable. However, increasing efforts are being made to integrate diagnostic information into control concepts as well as overall concepts. That's why in future safety relays with communications interfaces will be more prevalent in plant and machinery.

Safety relays have a clear structure and are simple to operate, which is why no special training measures are required. To use these devices successfully, all that's generally needed is some simple, basic electrical knowledge and some awareness of the current standards. The devices have become so widely used because of their compact design, high reliability and, importantly, the fact that the safety relays meet all the required standards. They have now become an integral component of any plant or machine on which safety functions have a role to play.

Since the first safety relays were developed – initially with the sole intention to monitor the emergency off/emergency stop function – a wide range of devices have become established, performing some very specific tasks in addition to simple monitoring functions: For example, monitoring speeds or checking that voltage is disconnected on a power contactor. The devices are designed to work well with the sensors and actuators currently available on the market. Today, a safety relay is available for practically every requirement. With their diverse functionality, safety relays can implement almost any safety function, for example, monitoring the whole safety chain from the sensor to the evaluation logic, through to activation of the actuator.

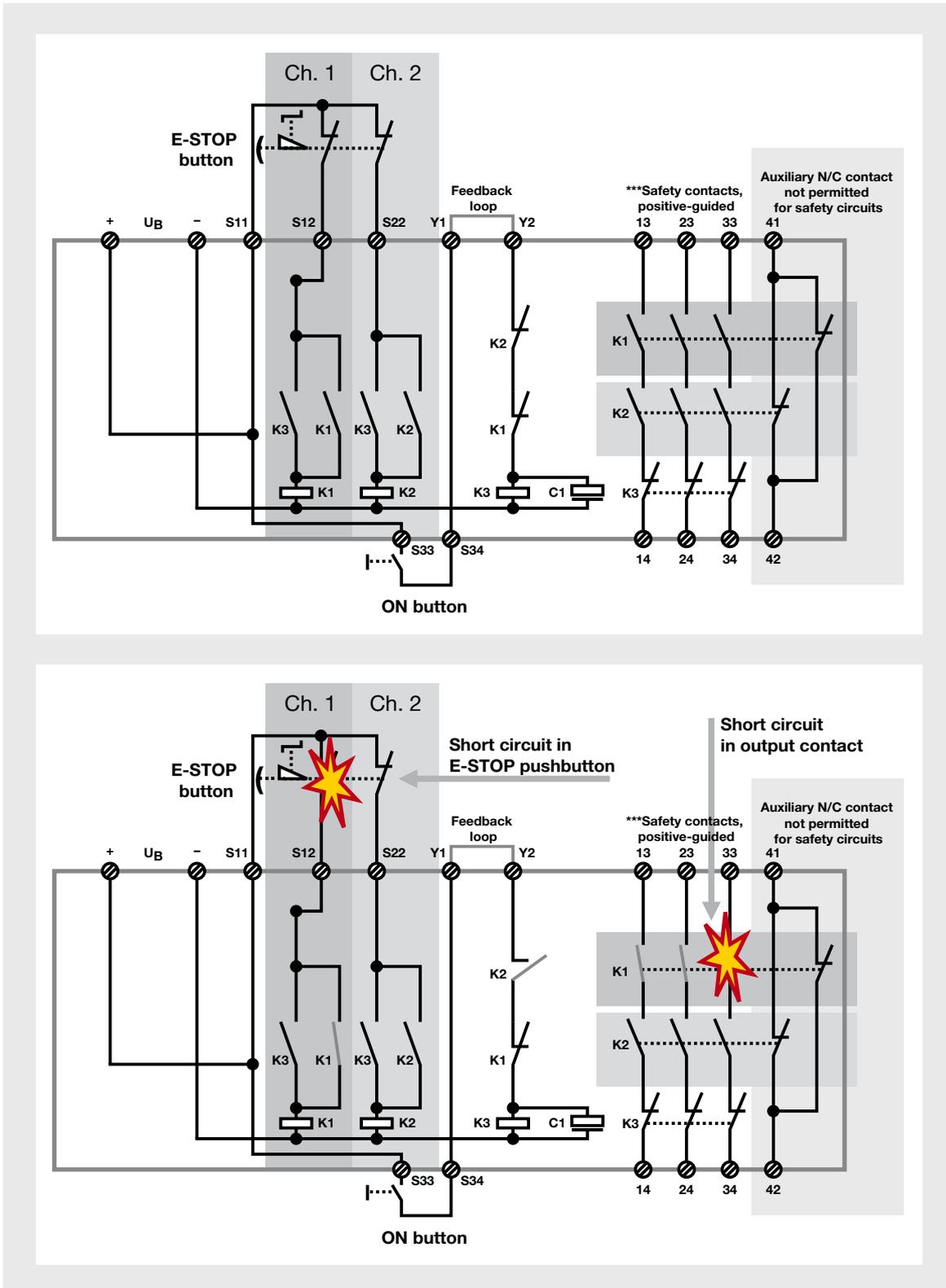
4.1.2 Structure and function of safety relays

Today's safety relays are distinguished primarily by their technological design:

- ▶ Classic contact-based relay technology
- ▶ With electronic evaluation and contact-based volt-free outputs
- ▶ Fully electronic devices with semiconductor outputs

Nothing has changed in the fundamental requirement that safety relays must always be designed in such a way that – when wired correctly – neither a fault on the device nor an external fault caused by a sensor or actuator may lead to the loss of the safety function. Technological change has advanced the development of electronic safety relays, which offer much greater customer benefits: Electronic devices are non-wearing, have diagnostic capabilities and are easy to incorporate into common bus systems for control and diagnostic purposes.

▶ 4.1 Safety relays



Structure and function of a safety relay.

▶ 4.1 Safety relays

The typical design of a first generation safety relay in relay technology is based on the classic 3 contactor combination. The redundant design ensures that wiring errors do not lead to the loss of the safety function. Two relays (K1, K2) with positive-guided contacts provide the safe switch contacts. The two input circuits CH1 and CH2 each activate one of the two internal relays. The circuit is started via the start relay K3. There is another monitoring circuit between the connection points Y1 and Y2 (feedback loop). This connection is used to check and monitor the position of actuators which can be activated or shut down via the safety contacts. The device is designed in such a way that any faults in the input circuit are detected, e.g. contact welding on an emergency off/emergency stop pushbutton or on one of the safety contacts on the output relay. The safety device stops the device switching back on and thereby stops the activation of relays K1 and K2.

4.1.3 Relays and electronics

The latest generation of safety relays operates using microprocessor technology. This technology is used in the PNOZsigma product series, for example, and offers further additional benefits over conventional relays. There is less wear and tear thanks to the use of electronic evaluation procedures and the diagnostic capability, plus the safety relays also reduce the number of unit types: One device can now be used for a variety of safety functions, e.g. for emergency stop, safety gate (contact-based switches as well as switches with semiconductor outputs), light beam devices, light curtains and two-hand control devices. As electronic safety relays have a more compact design, they take up much less space.

The reduced size enables more functions to be implemented in the same effective area. Selectable operating modes and times allow for flexible application of the devices. As a single device type can implement several different safety functions at once, savings can be made in terms of stockholdings, configuration, design and also when commissioning plant and machinery. Not only does this reduce the engineering effort in every lifecycle phase, it also simplifies any additions or adjustments that are required.



Electronic safety relays can be expanded in the simplest way possible. Whether you use additional contact blocks or function modules: Adapting to the specific requirements of the respective plant or machine is a simple, straightforward process, with contacts expanded via connectors. With just a single base unit, plus additional expansion units if required, users can fully implement all the classic functions.

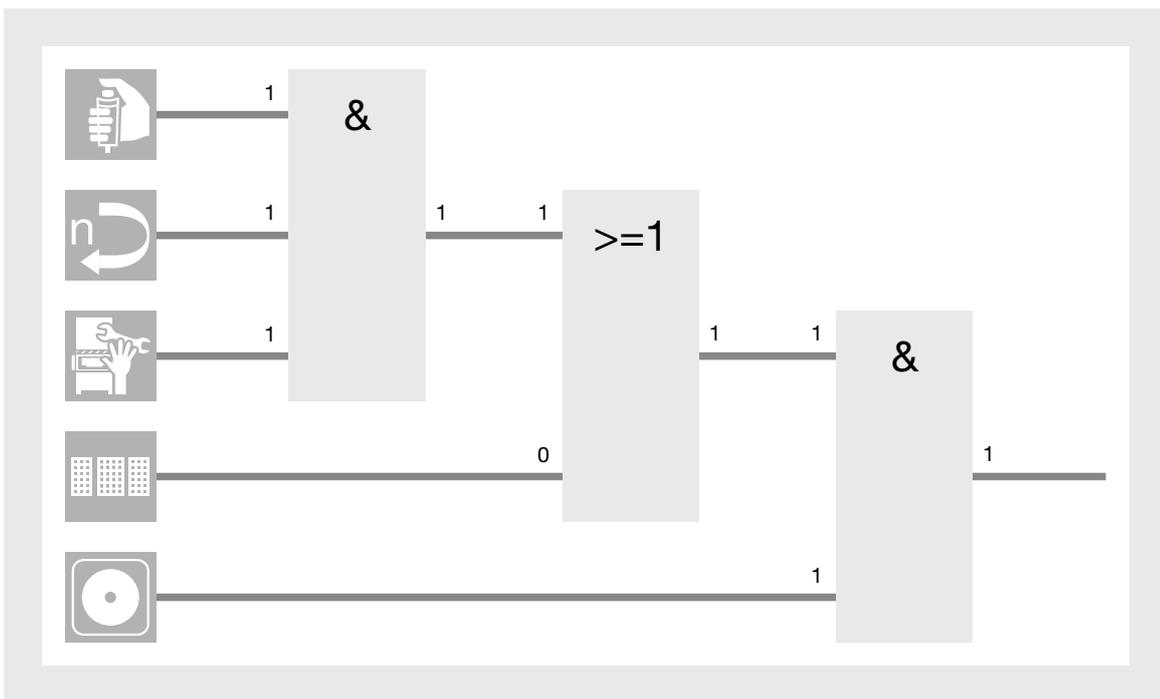
▶ 4.1 Safety relays

4.1.4 Greater flexibility during installation

For many years, wiring of the individual functions on safety relays was a complex, problematic procedure which had a negative impact on the installation process. Imagine the following situation on a machine: A safety gate is intended to prevent random, thoughtless access to a danger zone. Access is only possible once the hazardous movement has been stopped and the machine is in a safe condition, at least within the danger zone. However, the intention is for various drives to be operable at reduced speed, even when the gate is open, for installation and maintenance purposes for

example. An enable switch has therefore been installed, which must be operated simultaneously.

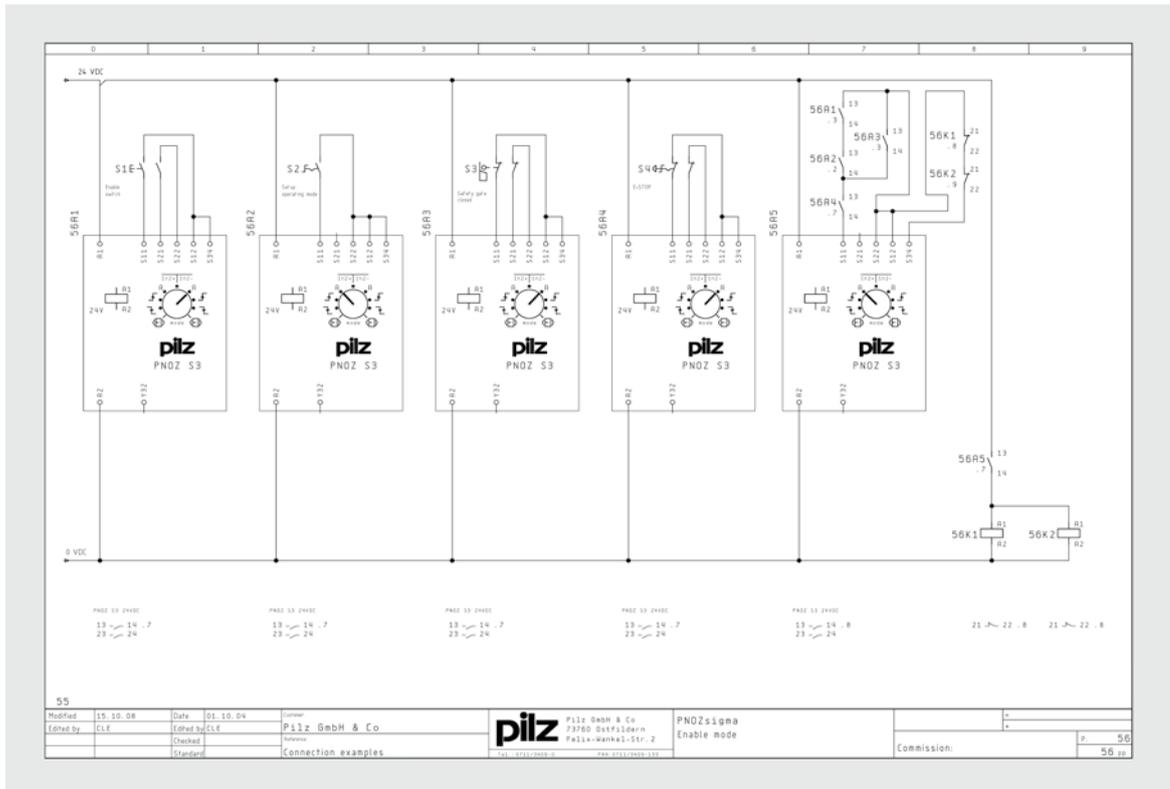
If these requirements are to be implemented in practice, so that the operator is protected from potential hazards, a substantial amount of wiring will be needed to connect the individual safety devices. As well as the actual protection for the safety gate, safety relays will also be required for the enable switch, to monitor “Setup” mode, and for the master emergency off/emergency stop function. Reduced purely to the logic relationships, the connections could look as follows:



Wiring example

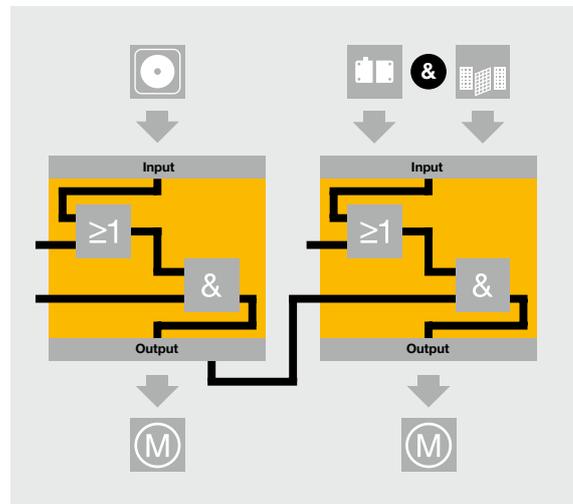
▶ 4.1 Safety relays

If this application is implemented using classic contact-based devices, the design will correspond approximately to the diagram below:



Wiring example using contact-based safety relays.

The diagram shows that implementation via contact-based devices produces a result which is not entirely comprehensible; it is also very cost intensive due to the vast amount of wiring involved. In recognition of this fact, consideration almost inevitably turned to a simpler form of implementation, using logic connections between the safety relays. Thus started the development of a new type of device with integrated connection logic.



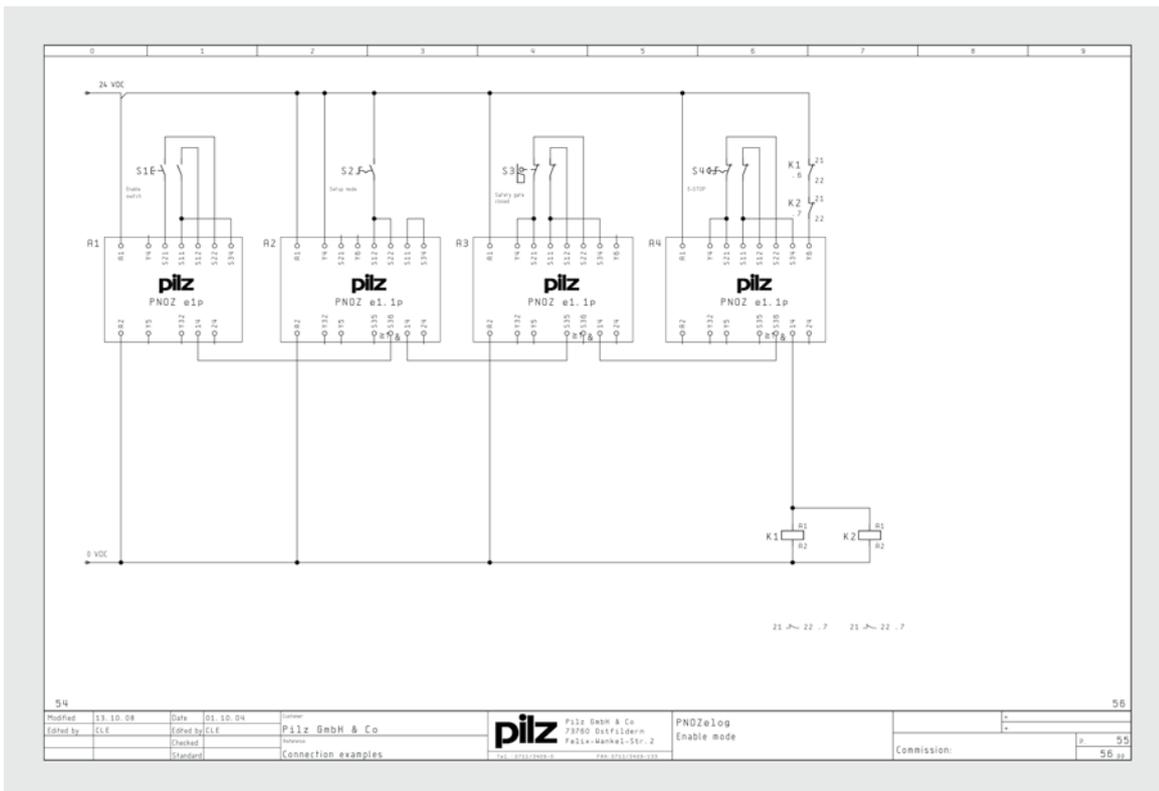
Less wiring due to linkable outputs.

▶ 4.1 Safety relays

Microprocessor technology opened up a whole new range of possibilities, as expressed by the predominantly electronic devices in the PNOZelog product series, for example. It laid the foundations for previously unimagined flexibility: One device can now be set for different application areas, another device for different safety functions. Unlike conventional safety relays, these new relays have electronic safety outputs and auxiliary outputs that use semiconductor technology. As a result, they are low-maintenance and non-wearing and are therefore suitable for applications with frequent operations or cyclical functions. In addition to the actual basic function, such as monitoring a safety gate or an emergency stop function for example, these devices

contain a logic block with special inputs, enabling logic AND/OR connections between the devices. An output block with auxiliary outputs and safety outputs completes the safety relay.

The following application example shows how the above example is implemented using electronic safety relays from the stated product series. Compared with a design using contact-based technology, the diagram is much clearer and the amount of wiring is drastically reduced.



Wiring example using electronic safety relays.

▶ 4.1 Safety relays

4.1.5 Special features and functions

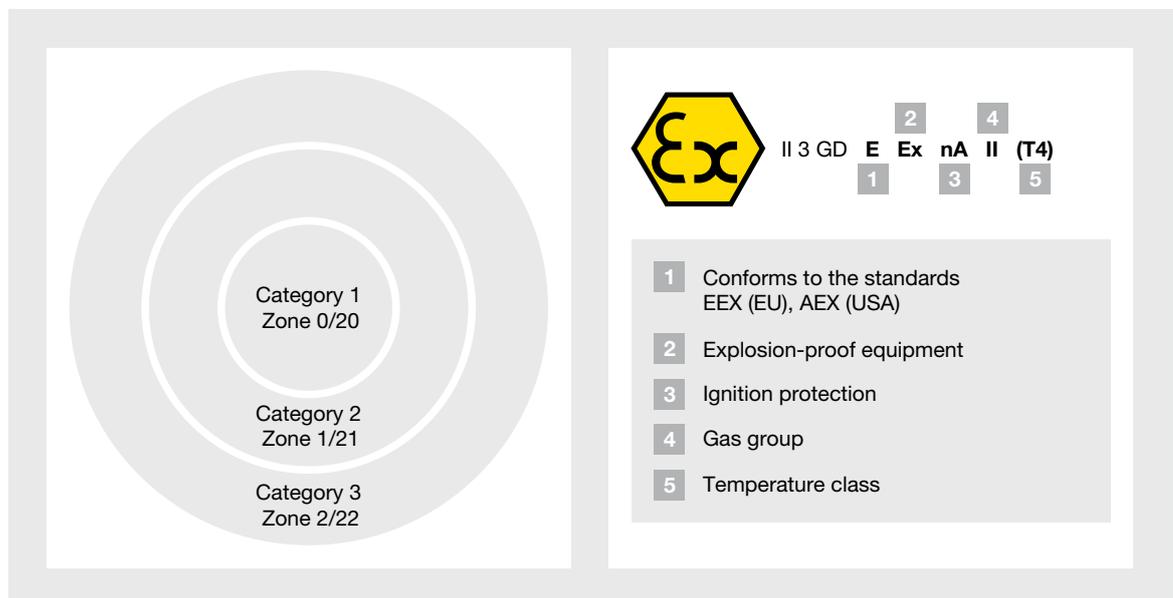
A key benefit of safety relays is their ability to specialise. They have a clear, self-contained task to fulfil, so specific customer requirements have led to a wide range of safety relays with particular functions and features: These include devices with muting function, with safe monitoring of speed, standstill and monitored disconnection, as well as safety relays with special properties for the Ex area. The examples below illustrate some of these functions.

4.1.5.1 Muting function

The muting function is used to automatically and temporarily suspend a safety function implemented via a light curtain or laser scanner for a particular purpose. A muting function is frequently used to transport material into and out of a danger zone.

4.1.5.2 Safety relays for the Ex area

Some of the most hazardous plant and machines are those that manufacture, transport, store or process dust, flammable gases or liquids. Explosive compounds may be produced during these processes, which could present a danger beyond the immediate environment. Potentially explosive atmospheres like these require special devices, on which electrical sparking on contacts is excluded. Such safety relays must provide an intrinsically safe output circuit and volt-free contacts for potentially explosive areas. These devices are approved for Ex area II (1) GD [EEx ia] IIB/IIC.

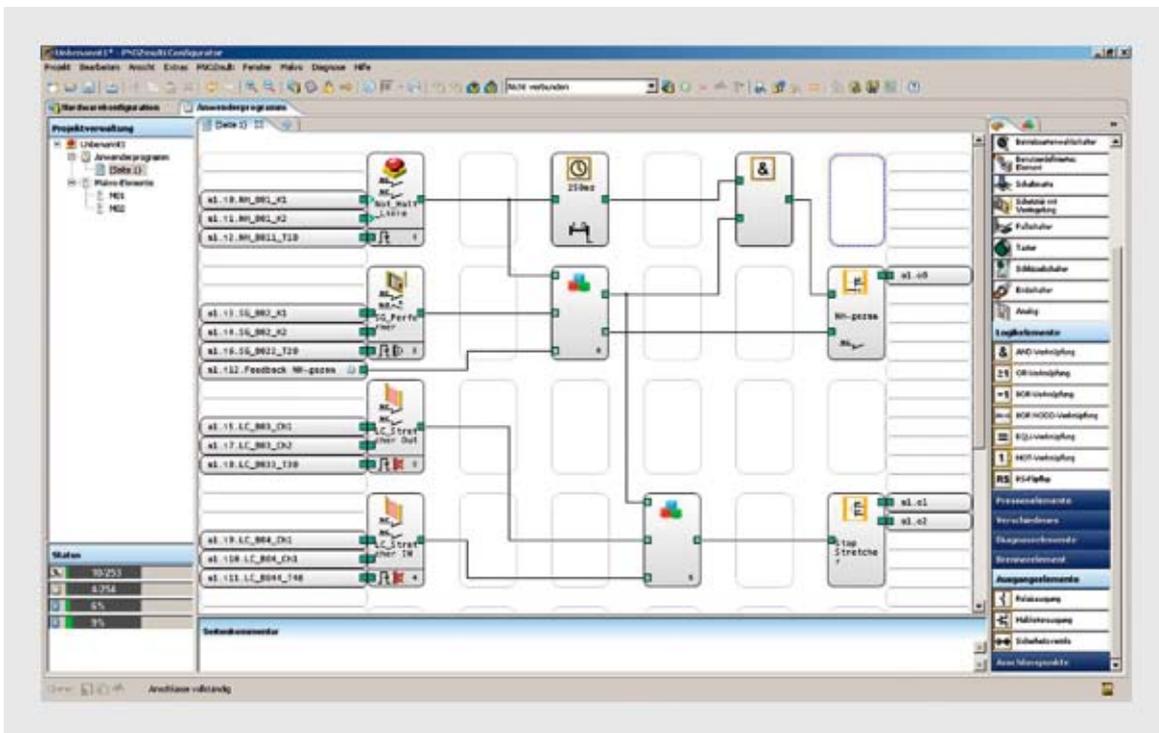


ATEX Directive on explosion protection.

▶ 4.2 Configurable safety relays

Similar to progress in the automation technology sector, safety technology has gradually developed from hard-wired relay technology to contact-based safety relays and devices with integrated logic function and beyond to flexible, configurable safety relays. The idea was to make safety technology more transparent and manageable for the user. This was the major driving force behind development of the devices and ultimately led also to the development of new types of configuration tools, which graphically display function and logic and then forward the configured setting to the relay via memory chip. The result is a high degree of flexibility for the responsible electrical design engineer; the plans only have to consider the number of digital and analogue inputs/outputs required. They can incorporate the functions at some later date and adapt them to suit the changed situation if necessary. At the same time, any work involved in wiring the logic functions also disappears.

With this generation of devices, the safety functions and their logic connections are configured exclusively via the software tool. The manufacturer provides the safety functions within application blocks; certified bodies such as BG or TÜV will have already tested them for safety. With the help of safe application blocks and the logic connections between these blocks, the plant or machine builder creates the safety-related application they require, an application which they would previously have implemented by wiring contactors and relays in a laborious, time-consuming process. Contacts and wires are replaced by lines between the ready-made application blocks. An electrical circuit diagram showing the logic functions is no longer required.

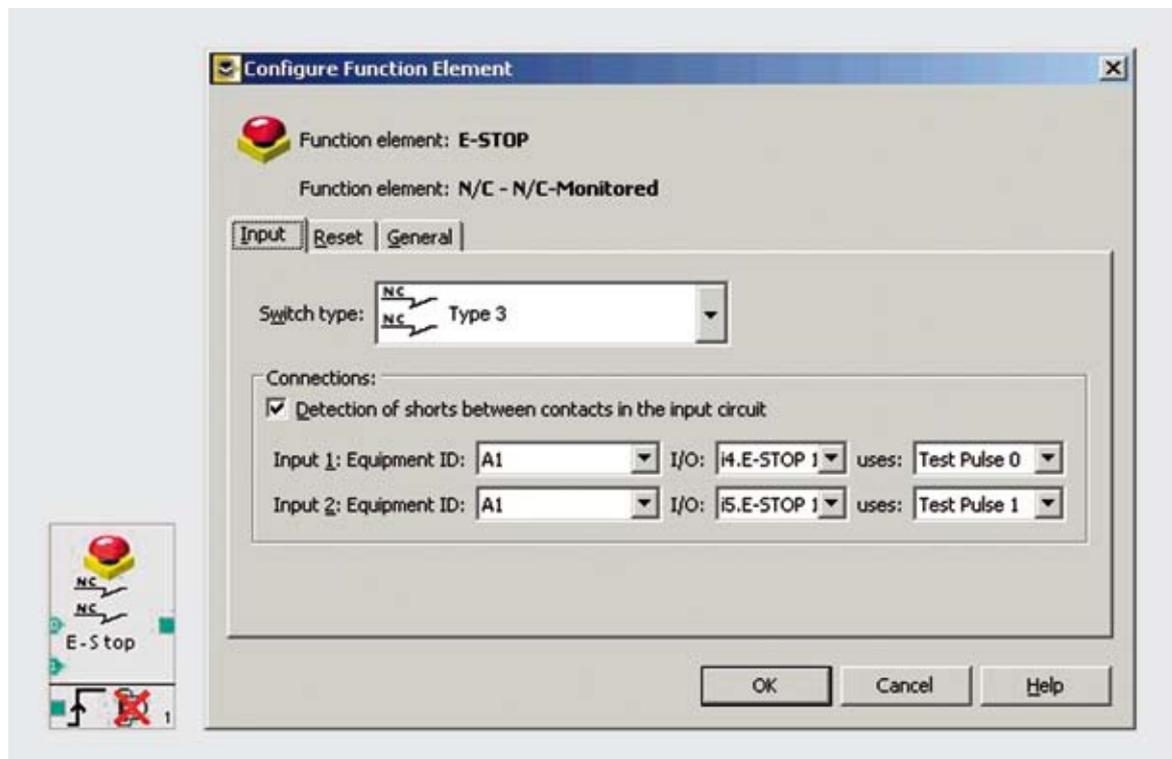


Logic connections between the blocks for simple configuration.

▶ 4.2 Configurable safety relays

Not only is it easy to connect the application blocks to each other, a simple click of the mouse is all it takes to adapt them fully to the requirements of the relevant application. Block properties define the behaviour of the individual blocks within the application: whether single or multi-channel, with or

without automatic reset, e.g. when a safety gate is closed. Parameters that determine how a block will behave can be easily set in accordance with the application's safety requirement.



Configure function elements

The parameters available in the “Configure Function Element” window (see illustration) essentially mirror the familiar functions from the safety relays. They no longer have to be set laboriously on the device or be selected via jumpers; with the parameter tool everything operates in the simplest way possible. Users will find all the useful, proven elements from the world of the classic safety relays, just represented in a different format. This new configuration method has another quite simple, safety-related benefit: Once the configuration has been selected, it cannot easily be modified by unauthorised persons via screwdriver or device selector switch.

Simple configuration of the required input and output modules, plus the availability of special modules for speed or analogue processing, enable the user to create a safety system that suits his own individual needs. Functions can be added or adapted later with relative ease. The user simply selects these modules from a hardware list and then creates the necessary logic functions.

▶ 4.2 Configurable safety relays

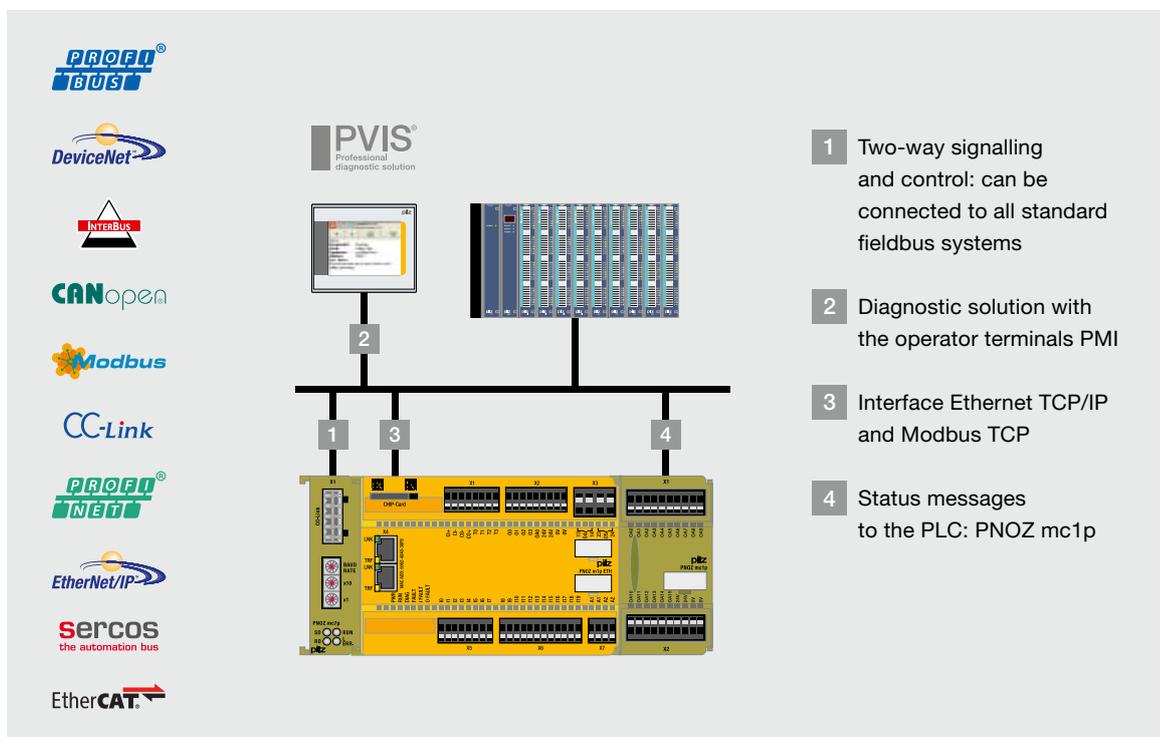
4.2.1 Safety-related and non-safety-related communication

4.2.1.1 Non- safety-related communication of standard signals and diagnostic data

Communication on contact-based safety relays is very limited. Simply displaying fault conditions can sometimes prove difficult. Switching to electronic versions already makes communication somewhat easier: LEDs flash, sometimes with varying frequencies, to distinguish between specific malfunctions. LCD displays indicate errors and/or operating states in plain text.

Configurable safety relays offer a whole new set of options: They can be connected to almost any fieldbus via fieldbus modules. This enables a simple, two-way exchange of signals and information. This produces closer dovetailing of safety and standard and therefore of the whole automation structure. In this case, the safety relays behave just like any other fieldbus subscriber in the fieldbus system. These connections can be used to transfer diagnostic data to any automation system, leading to a significant reduction of plant and machine downtimes.

Integrated, user-friendly diagnostic concepts enable targeted fault detection and remedial action. Using Active-X elements, data can be displayed directly on operator terminals via the Pilz OPC Server.

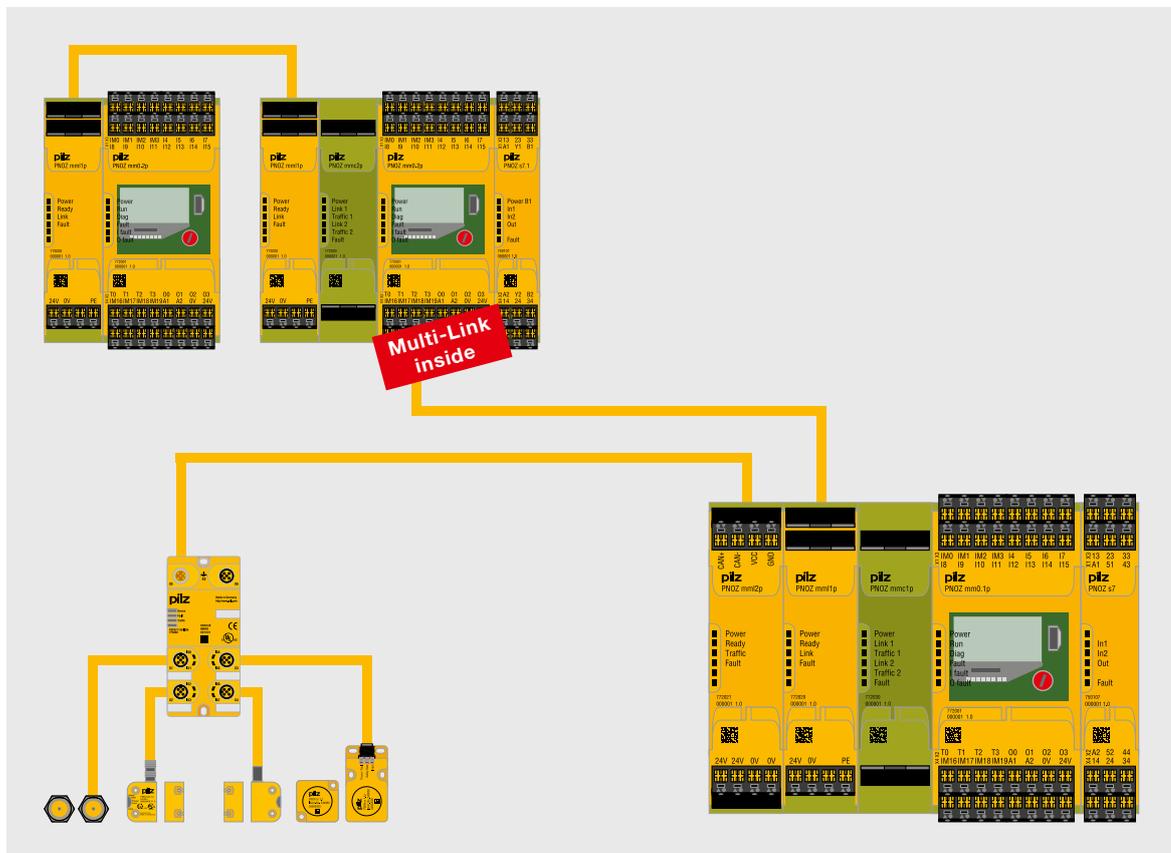


▶ 4.2 Configurable safety relays

4.2.1.2 Safety-related communication with configurable safety relays

Progressive networking has forced its way up to the level of configurable safety relays. These use special interconnection modules or protocols to exchange safety-related data up to Performance Level e of EN ISO 13849-1. Safe data transfer using this technology opens up new horizons in the field of configurable relays. If several machines are working together in a close network, for example, safety requirements will demand that safety signals are exchanged between the control systems.

Previously, this could only be achieved by exchanging hardware signals. This is a laborious process and is extremely inefficient due to the high cost for each piece of information transmitted. If interconnection modules are used to replace the previous hard-wired solution, the amount of wiring is reduced along with the cost, while the amount of information data is increased.



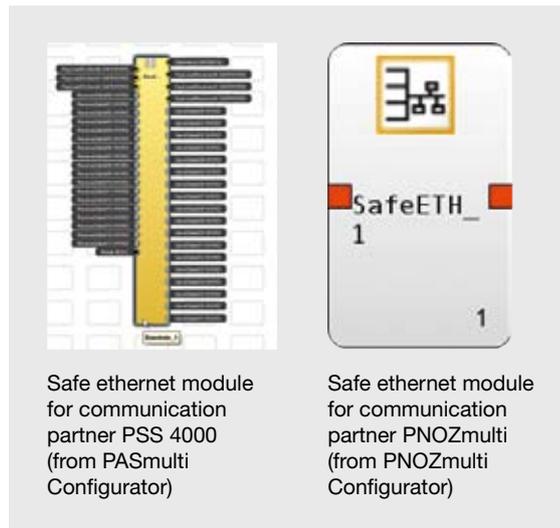
Connecting configurable safety relays.

▶ 4.2 Configurable safety relays

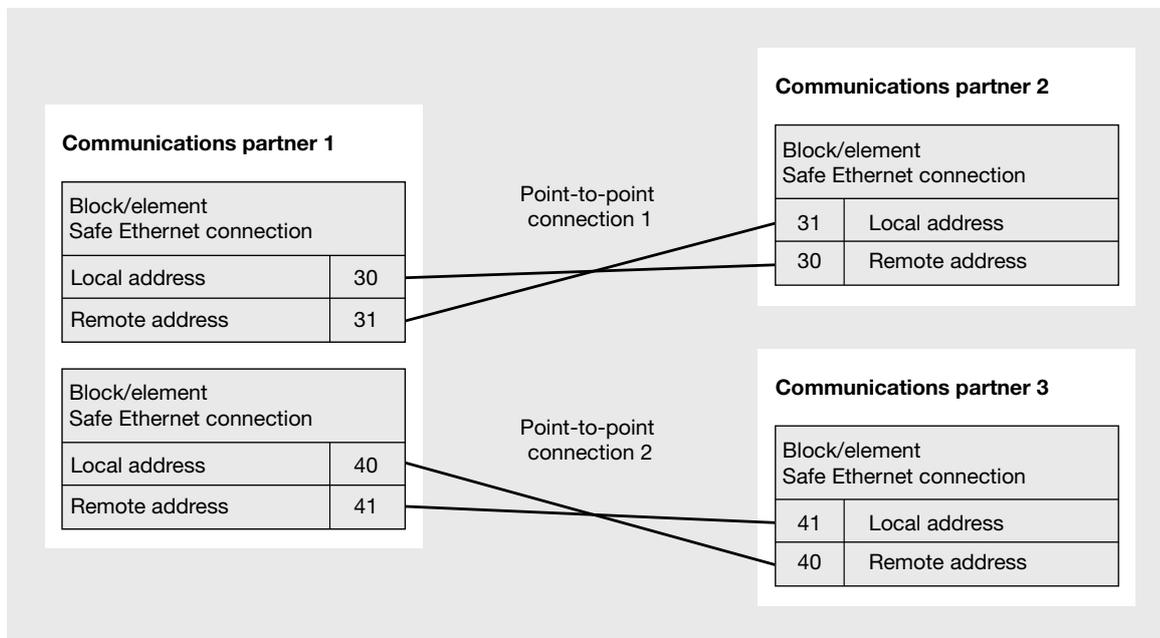
In addition to these special interconnection modules, more and more Ethernet-based safety protocols are now being used, even in the field of safety relays. The black channel principle enables the Ethernet network to be used in parallel with standard and safety protocols.

An application block has been developed to transfer safety information; this makes it easy for users to exchange data with the safety system PSS 4000 in complex networks.

Transferring this safe communication into software-based blocks or special hardware is probably the most efficient solution that is currently available in networking.



Screenshots from Pilz-Software-Tools



Connection addresses with two point-to-point connections.

▶ 4.2 Configurable safety relays

4.2.2 Customer benefits from application blocks

Configurable safety relays offer a wide range of predefined application blocks. These blocks form the basis for implementing the safety technology requirements of plant and machinery. The availability of blocks for the widest possible range of applications and functions enables the user to implement his requirements quickly and effectively.

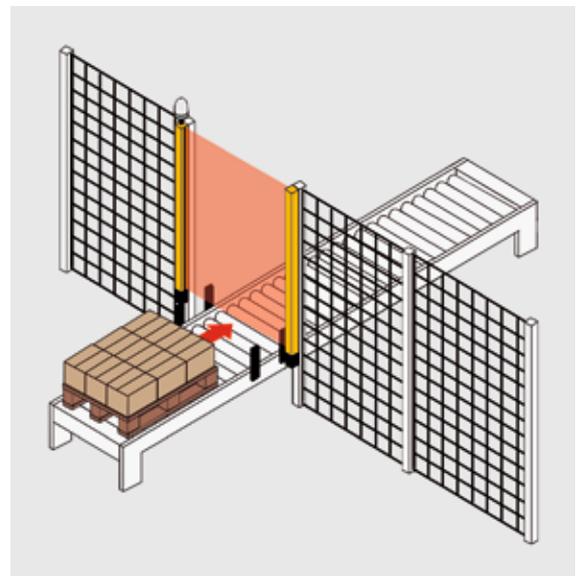
4.2.2.1 Application blocks for muting function

The “muting function” is one of those laborious functions which previously required the application of special relays, but which can now be implemented easily using configurable safety relays. This function is used to automatically and temporarily suspend a safety function, such as a light curtain or laser scanner. It is often applied, for example, to transport material into or out of a danger zone. A distinction is made between sequential and cross muting. Typical application areas include the automotive industry, on palletising and drink dispensing machines, or in the manufacture of stone products (concrete blocks, tiles etc.). Additional sensor technology is used to distinguish between persons and objects.

Example: Sequential muting

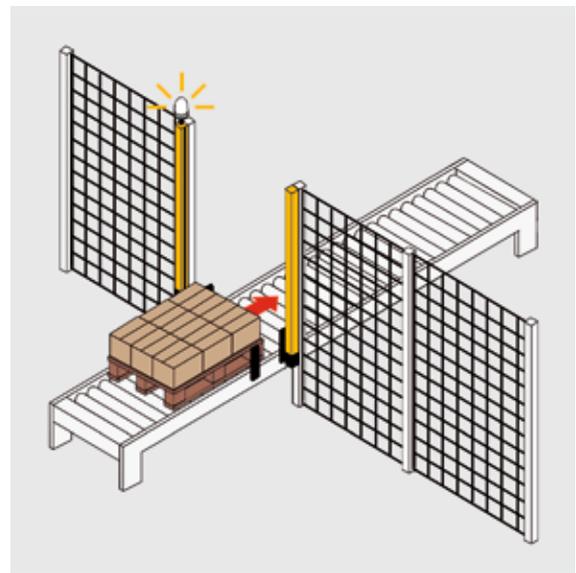
Muting phase 1:

- ▶ Material in front of the danger zone
- ▶ Light beam device active
- ▶ Muting lamp off



Muting phase 2:

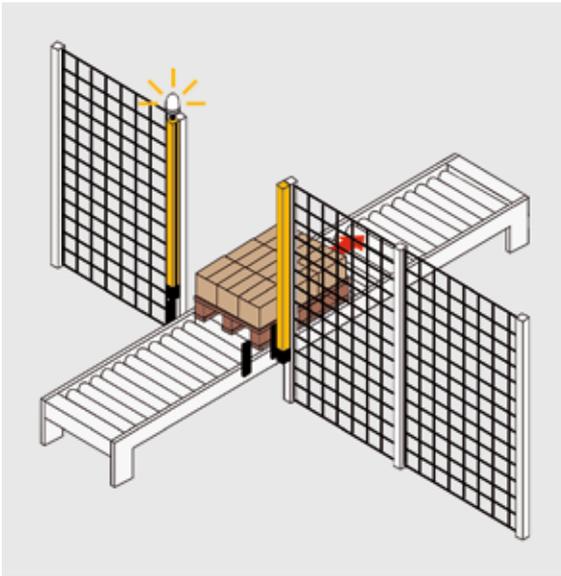
- ▶ Muting sensors 1 and 2 operated
- ▶ Light beam device suspended
- ▶ Muting lamp active



▶ 4.2 Configurable safety relays

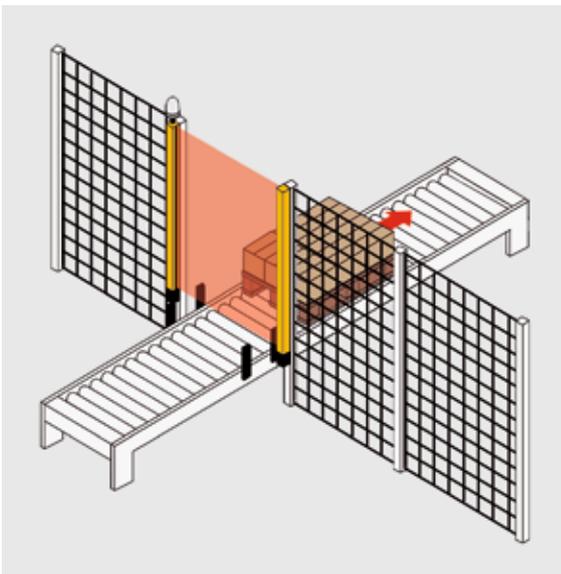
Muting phase 3:

- ▶ Muting sensors 3 and 4 operated
- ▶ Light beam device suspended
- ▶ Muting lamp active



Muting phase 4:

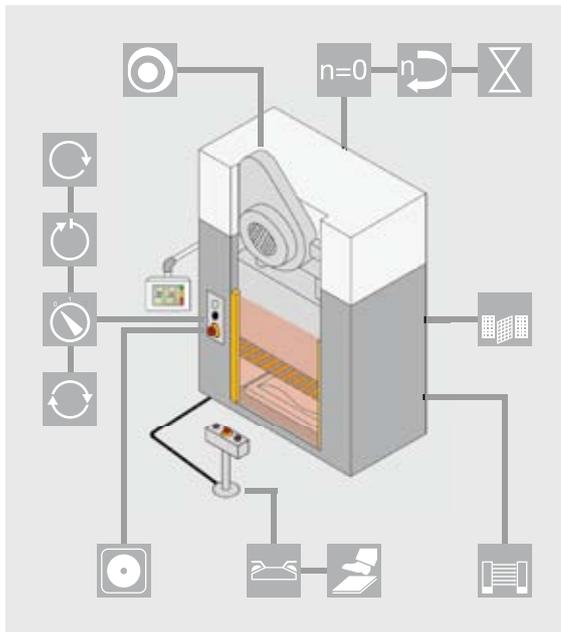
- ▶ Muting process ended
- ▶ Light beam device reactivated
- ▶ Muting lamp off



▶ 4.2 Configurable safety relays

4.2.2.2 Application blocks for press applications

In addition to application blocks for individual functions, complete application packages are also available for specific self-contained applications such as mechanical and hydraulic presses, for example. Such packages are designed to perform control functions as well as meeting safety-related requirements. The package contains all the basic functions that a press needs, e.g. blocks for setup, single-stroke and automatic operating modes; monitoring a mechanical camshaft; run monitoring to monitor the mechanical transmission for shearpin breakage; monitoring of electrosensitive protective equipment in detection and/or cycle mode; monitoring and control of the press safety valve plus cycle initiation via a two-hand control device.



Safe control and monitoring of presses.

4.2.2.3 Application blocks for burner applications

Another self-contained application is available for burner applications. The burner application block is designed to control and monitor burners (automatic burner control system) in accordance with the standards that are mostly needed in this case, such as EN 50156-1, EN 298 or EN 676, for example.

The block monitors safety chains, combustion air pressure, ignition, flame, external compound controller or tightness control. Functions such as safety valves, ignition valves, ignition or also external compound controllers can also be controlled. By setting the parameters for the application block, these functions / monitoring functions can be adapted flexibly for the specific burner type. The burner cycle has several phases, in which various steps are run through, based on the burner type. If the input signals for that particular step are correct, the next step in the cycle is carried out. If not, a safety shutdown or fault lockout is carried out, depending on the configuration.

▶ 4.2 Configurable safety relays

4.2.2.4 Application blocks for the drive environment

In addition to general safety functions such as monitoring of safety gates, emergency stop function or light curtain evaluation, configurable safety relays also offer special expansion modules and specific application blocks for advanced options such as the safe detection of movement and standstill on drives. Two axes are possible per expansion module, each with eight limit values for speed monitoring, standstill monitoring and detection of clockwise and anti-clockwise rotation. In this way, motion information can be integrated directly into the safety system, irrespective of the drive system you are using.

With normal standard encoders, monitoring is possible up to Performance Level d of EN ISO 13849. This is significant for two reasons: Firstly, there is no need for expensive, safe encoders and secondly, laborious wiring is no longer necessary thanks to the simple “listening function” of the encoder signals – “tapping” the encoder cable via a T-junction. The direct signal tap on the motor encoder minimises the work involved in the mechanical and electrical design through appropriate adapter cable for the widest range of drives. Speed and standstill detection, including evaluation via customised application blocks, is available in the simplest way possible, via plug and play.

▶ 4.2 Configurable safety relays

4.2.2.5 Application blocks for safe analogue processing

In the past, processing analogue signals safely using safety relays was as good as impossible. Only the integration of special expansion modules and the availability of customised application blocks has made safe analogue processing possible. In a similar procedure to that of the drive environment, configurable safety relays can be used to evaluate sensor information from the analogue process environment. This may relate to process conditions such as fill level, position or speed for example; there's practically no limit to the extended application options. For analogue signals it is also possible to define limit values, threshold values or value ranges, within which a measured value may move; this is done through the module configuration or by setting parameters in the user block. Reliable monitoring therefore becomes a reality; all values can be evaluated and further processed.

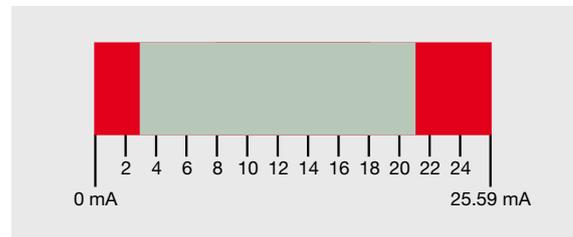
Example: Range monitoring 4 ... 20 mA current loop

With range monitoring, the first step is to define the permitted value range. Depending on the selected condition ("greater than" or "less than"), the output for threshold value monitoring is set to "0" if the recorded value exceeds or drops below a range limit.

2 range limits are to be defined in this example:

- ▶ $I < 3 \text{ mA}$ monitors for open circuit and
- ▶ $I > 21 \text{ mA}$ monitors for encoder error

	Error if		Comment
	Condition	Value	
R1	<	3 mA	Open circuit
R2	>	21 mA	Encoder error



Example: Monitoring the position of a control valve via range monitoring

Control valves in process technology, e.g. to control flow rates, are generally controlled in analogue; feedback on the valve position is also analogue. Without safe analogue processing, until now, only special switches have been able to evaluate position signals from valves. The new technology allows you to set as many valve positions as you like and to monitor compliance, safety and reliably.

▶ 4.3 Today's safety control systems

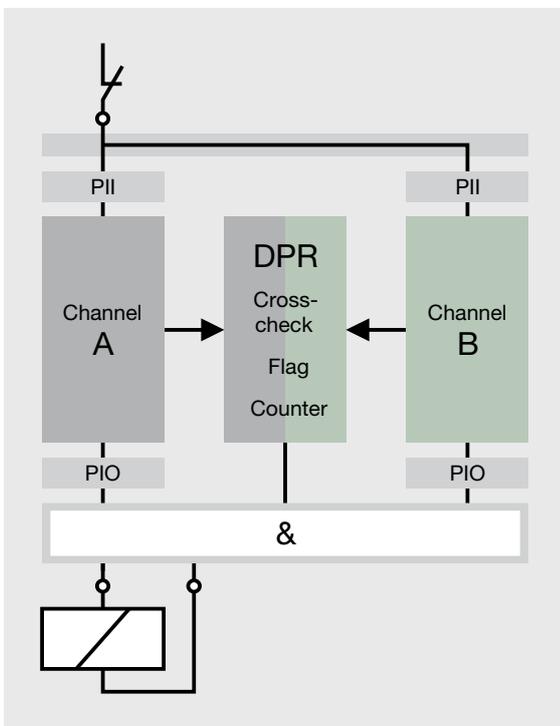
4.3.1 Overview of safety control systems

Safety control systems essentially came about because of the desire to connect safety through programming, in a similar way to that of a PLC control system. It's no surprise then, that safety control systems are following the example of the PLC world. Centralised systems came first, followed by decentralised systems in conjunction with safe bus systems. Programming followed the same formula, except that the instruction set was drastically reduced from the start to just a few languages, such as IL (Instruction List) or LD (Ladder Logic/ Ladder Diagram). These measures were taken for reasons of safety, for the opinion was that limiting the programming options would minimise the errors made in generating the program. Initial systems clearly focused on processing safety functions. Although even at the start it was possible to program the safety control system for standard automation, in practice this application found very limited use.

Safety-related features aside, there is little to distinguish safety control systems from standard automation control systems in terms of their actual function. Essentially a safety control system consists of two PLC control systems which process the application program in parallel, use the same process I/O image and continuously synchronise themselves. It sounds so simple, but the detail is quite complex: Cross-comparisons, testing of the input/output level, establishing a common, valid result, etc. are all multi-layer processes, which illustrate the internal complexity of such systems. Ultimately, of course, the user is largely unaware of this; with the exception of some specific features, such as the use of test pulse signals to detect shorts across the contacts, modern systems behave in the same way as other PLC control systems.

Structure of a safe control system:

- ▶ Two separate channels
- ▶ Diverse structure using different hardware
- ▶ Inputs and outputs are constantly tested
- ▶ User data is constantly compared
- ▶ Voltage and time monitoring functions
- ▶ Safe shutdown in the event of error/danger



Elementary structure of a safe control system.

▶ 4.3 Today's safety control systems

4.3.2 Integration within the automation environment

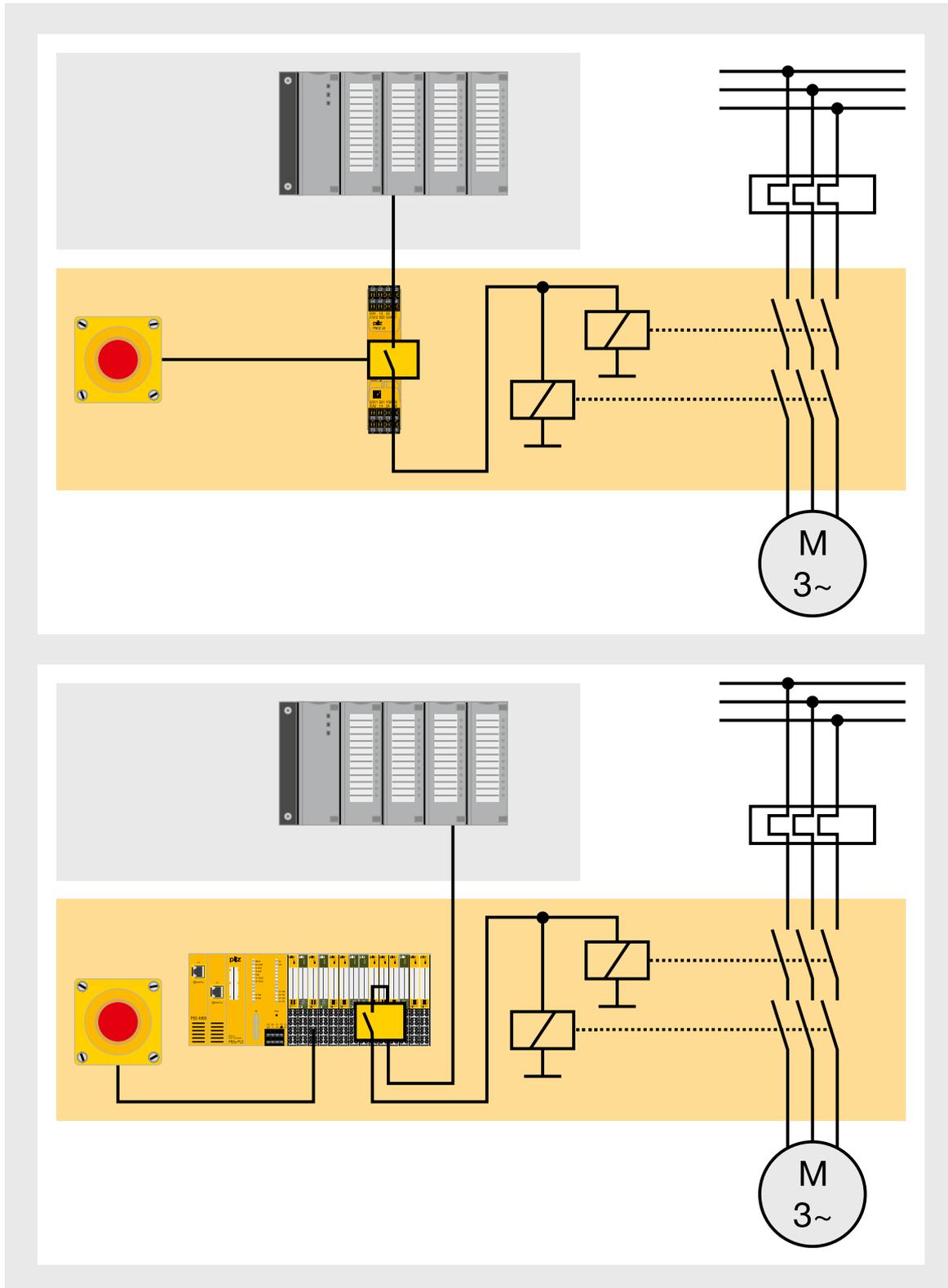
Cycle times are becoming ever shorter, while productivity and the demands on plant and machine control systems are increasing. In addition to the technical control requirements, the need for information regarding process and machine data is constantly growing. As a result, communication technologies from the office world are increasingly making their mark on control technology. One consequence of this trend, for example, is the growth of Ethernet-based bus systems in automation technology, right down to field and process level.

Until now safety technology has been characterised more or less as a “monitoring function” and has been incorporated as such into the automation chain. The process control system dominates and defines the actual process stages. As a “monitoring instrument”, the safety control system either agrees or disagrees with the decisions of the process control system. The diagram overleaf illustrates the principle:

Monitoring is limited to safety-relevant control functions, as is the enable. Process outputs without a safety requirement are unaffected. A distinct benefit of such a procedure is the fact that the tasks, and therefore the responsibilities, are clearly separated. A separate system is responsible for the design and monitoring of the safety technology; another separate control system manages the machine and the process. This way it is possible to guarantee the absence of feedback: Changes made primarily in the standard control system will not adversely affect the safety control system. This is an essential safety requirement of a safety system.

The division of duties also has a number of positive aspects: On the one hand, it increases overall performance, because each unit simply concentrates on the matters for which it has been designed and configured. Productivity increases do not just impact positively on the output of the plant or machine: They can also be beneficial in terms of handling, if faster reaction times enable safety distances to be minimised, for example. On the other hand, separation can be used to transfer responsibility for the individual systems to different individuals. That helps both sides, because everyone can concentrate on the task in hand.

► 4.3 Today's safety control systems



"Enable" operating principle, with safety relay or safety control system.

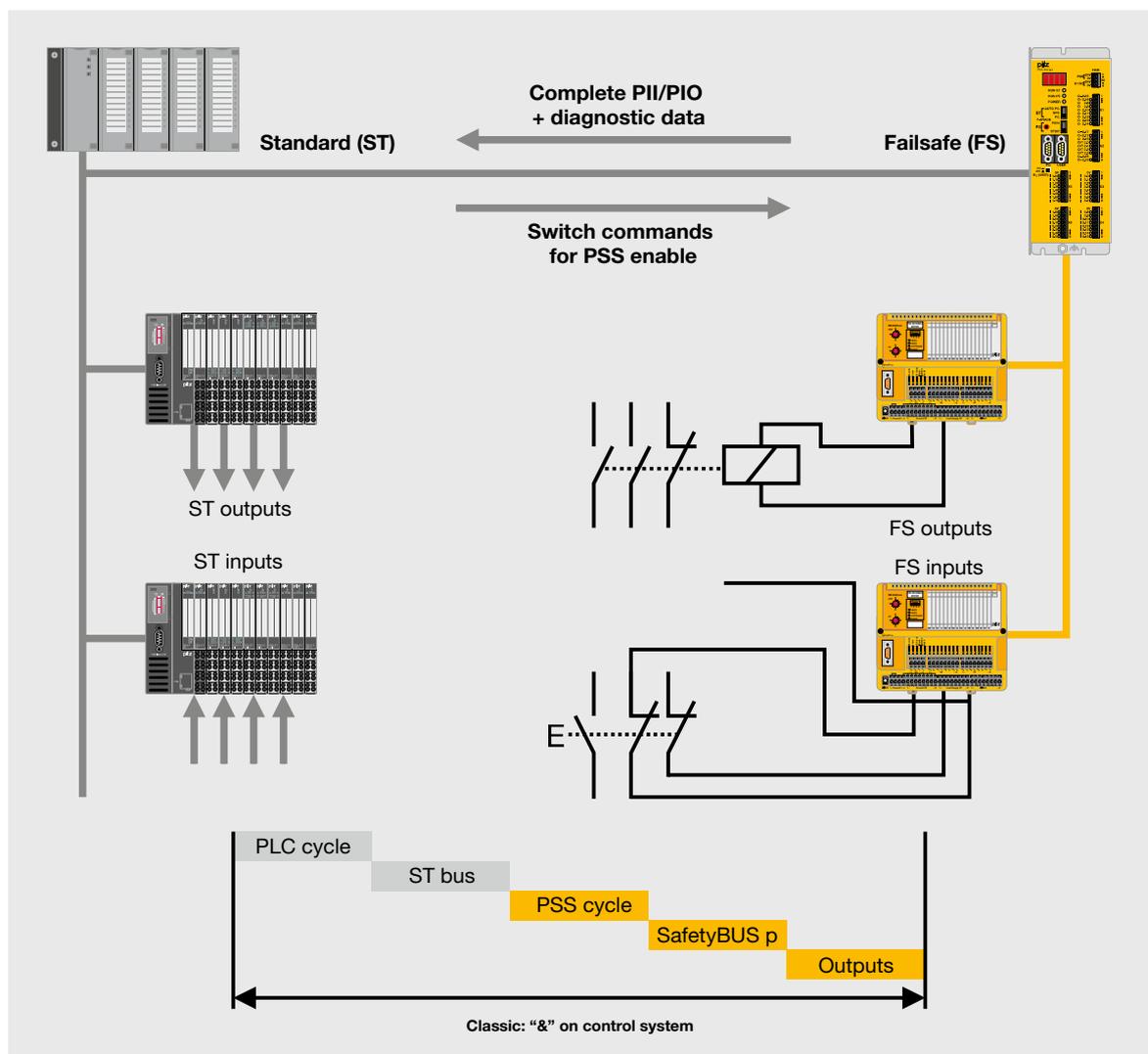
▶ 4.3 Today's safety control systems

4.3.3 Safe decentralisation and enable principle

As explained already, in many cases safety technology follows the developments made in standard control technology. The benefits from transferring the input/output level to the field via decentralisation have resulted in the same process being applied to safety-related inputs and outputs. This was followed by the development of a safety bus system, which not only allows field inputs and outputs but also a safety-related connection between safety control systems.

The diagram below illustrates a typical application in which the enable principle has been implemented. The safety control system switches the safety-related outputs, and the standard PLC transfers the switch command for the corresponding output to the safety control system via fieldbus.

Essentially it is a really simple principle, if you ignore the disadvantage that the switch command from the standard control system must be considered in the program for the safety control system. Graphically speaking, the situation is this: The standard control system must place the switch command on the



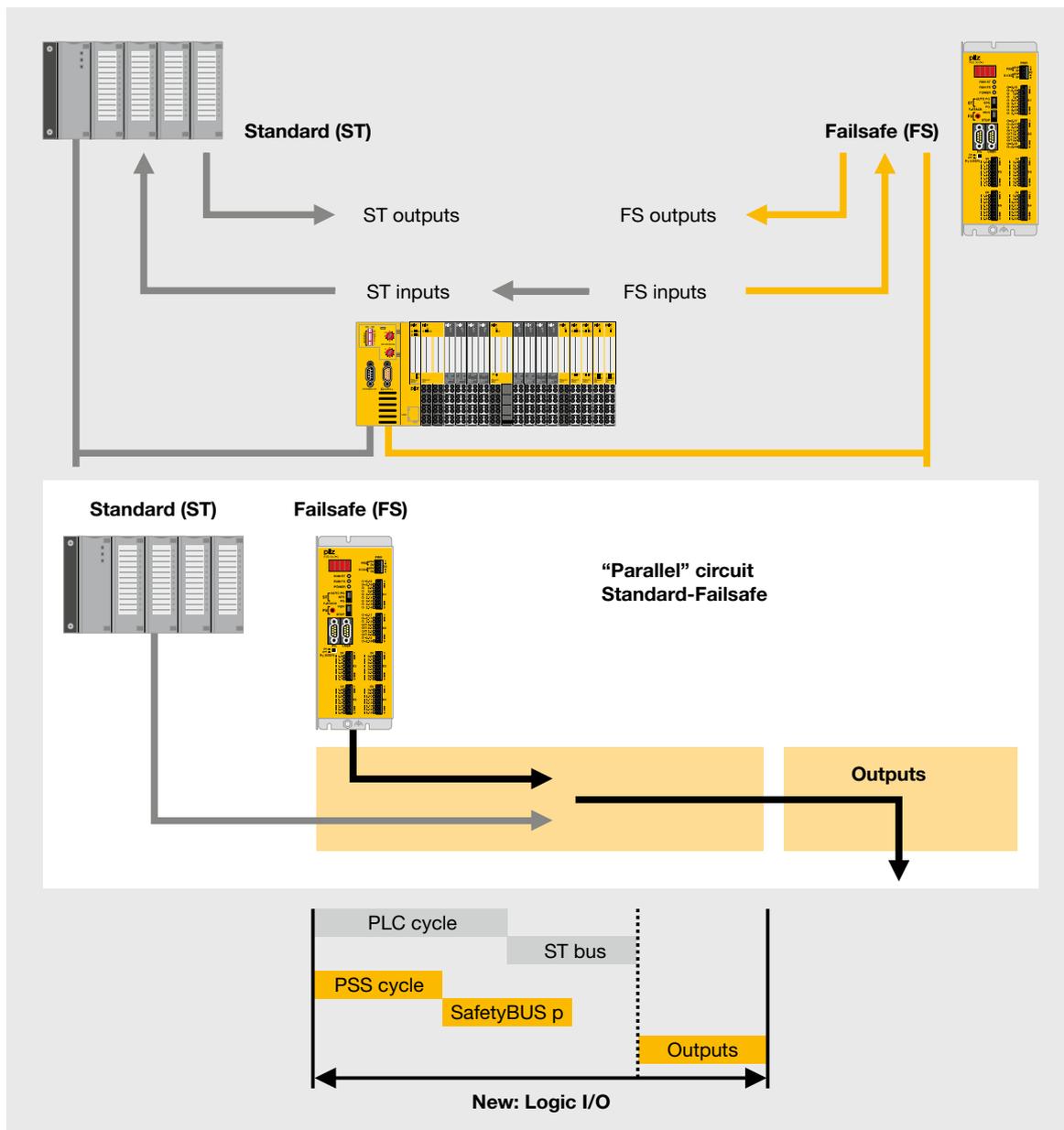
Circuit diagram for the enable principle.

▶ 4.3 Today's safety control systems

fieldbus, from where the failsafe control system retrieves it before inserting it into the output's control program as an AND function. Programming becomes unclear, because the control task and safety function are mixed within the safety control system. A further development of the field transfer principle helps to simplify this case.

The diagram below illustrates the extension of the enable principle. The enable for the control

command from the standard control system now takes place directly at input/output level. Handling is simplified tremendously as a result; both control systems can be programmed and tested independently. Performing the enable in the I/O system means there are no delay times from processing within the safety control system, and it's no longer necessary to pass on the control commands via the fieldbus.



Extending the enable principle.

▶ 4.3 Today's safety control systems

4.3.4 Function blocks in safe control systems

Function blocks for safety-related functions are the key to the success of safety control systems. Although initially they were more or less an image of the functions and properties found on safety relays, gradually the range has been developed to include blocks for special uses such as press applications or burner management. Today, function blocks are available for almost every conceivable safety-related application. All of these have been tested by certified bodies and offer users optimum safety for everyday use.

The concept of function blocks was originally intended for the safety control system, but was then developed to form configurable function blocks for configurable safety relays as described, making applications more customer-friendly. This approach of using configurable function blocks will also be part of a continually developing programming environment for the safety control systems. The user can choose between classic programming e.g. in IEC 61131 and a configuration similar to that of the configurable safety relays.



Certified function blocks in hardware and software.

▶ 4.3 Today's safety control systems

4.3.5 Mission time of safety functions

What happens with safety functions (designed in accordance with ISO 13849) at the end of the mission time (T_m)?

The duration of use of the relevant modules has been an issue since the application of DIN EN 13849 for design and validation of safety-related control functions. The standard specifies a period of 20 years as the default value for safety-related components. However, it is also possible to use components with a shorter mission time, provided the machine's accompanying documentation clearly refers to this component and the need to exchange it.

Even if the issue is largely excluded at the moment: On long-lasting machines, the time will come in which the configured mission time has elapsed, but the machine is to continue in use. In this case, safety-related integrity can only continue to be guaranteed if the relevant components are replaced. By this time the original machine manufacturer will probably have no more obligations regarding the machine, so responsibility passes to the operator. The relevant components must be identified and replaced. The new components must have similar or better safety-related characteristic data (PL, SIL, $B10_d$, $MTTF_d$, etc.). This process can be made easier if the original machine manufacturer provides this data from the outset (e.g. by verifying the design using a calculation program such as PASCAL). In this situation it is conceivable that components will be exchanged that appear perfect from the outside and continue to perform their control function without difficulty. Nonetheless they need to be exchanged because the probability of a dangerous failure has risen to beyond an acceptable level.

In theory it is possible to have the manufacturer inspect the used component, for example, and maybe repair it in such a way that a new mission time (T_m) begins. However, this approach is rarely cost effective and only ever on very valuable components.

4.3.6 Use of used components

This section sets out the use of used components in accordance with DIN EN ISO 13849: If used components are to be used in new safety functions, it's important to estimate the proportion of mission time (T_m) that has already elapsed and how much remains. Other characteristic data, particularly the $B10_d$ value on components that wear due to operation, can be partially utilised. Such components can only be used if their previous application has been traced and documented. These (reduced) values must then be used in the calculations when validating the new safety function.

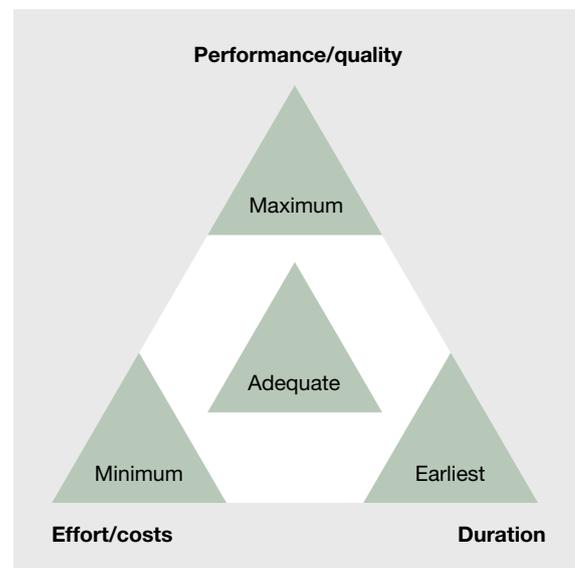
▶ 4.4 Using safety control systems to achieve safe control technology

4.4.1 Overview

In which direction is safety technology developing? Which control systems provide the highest user benefits? How will the various disciplines of safety, control, motion, CNC and visualisation work together in future? Will it be possible to implement economical solutions, despite the increasing complexity? Even in future there will be a number of different approaches to take to resolve requirements. One potential approach is to modularise plant and machinery into functional units. This is already happening today, albeit primarily for the mechanical part of plant and machinery. This approach has only partially been used in control technology as yet.

Whether the issue is safety-related or automation functions: The demands on plant and machinery continue to grow, so there's an increasing need for techniques which will allow applications to be well structured and therefore manageable. The requirement for minimum effort and associated cost reductions is increasingly the focus. The aim is to reduce engineering times still further.

The graphic below illustrates the compromise that has previously been reached between minimum costs, maximum quality and rapid implementation:



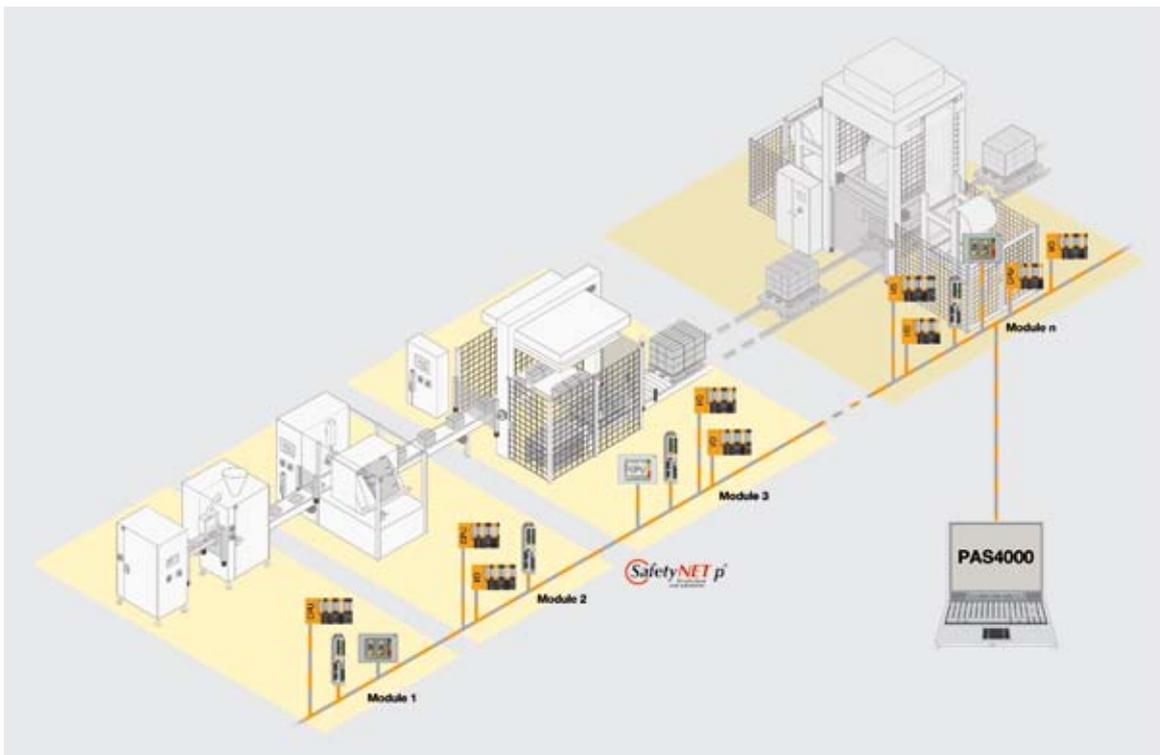
However, excellent support during the engineering phase, through an appropriate programming model, a user-friendly programming environment and an extensive library, can lead to higher quality in shorter time and at a lower overall cost.

▶ 4.4 Using safety control systems to achieve safe control technology

4.4.2 Safe control technology

The model of safety technology as a pure “monitoring function” is changing drastically: Safety technology may have been almost exclusively associated with emergency off/emergency stop, safety gate, light curtains and interlocks for a long time, but it would now be unthinkable not to regard the issue of safety on drives, for example. Other areas will include safe pneumatics and hydraulics. Applications will emerge from areas which are not yet the focus of our attention, but one thing is clear: Safety is an integral part of the overall plant and machine function, so it must be considered appropriately, right from the start. In simple language, safe control technology means: Make the control function safe! Safe control technology becomes reality when safety enjoys the same mechanisms, the same handling and the same flexibility as the standard section, at all levels of automation technology.

This does not mean that safety and standard functions have to be combined inside one device. What’s important is that they work together to process tasks as a system, without impeding each other. Each device, each control system, should do what it does best. The system’s backbone is an extremely powerful bus system, which manages data traffic in the background. The result of this technological development is a system which uses the intrinsic benefits of technology control systems. For example, it makes no sense for a safety control system to have to carry out motion functions, when that’s a specific task of the motion technology control system.



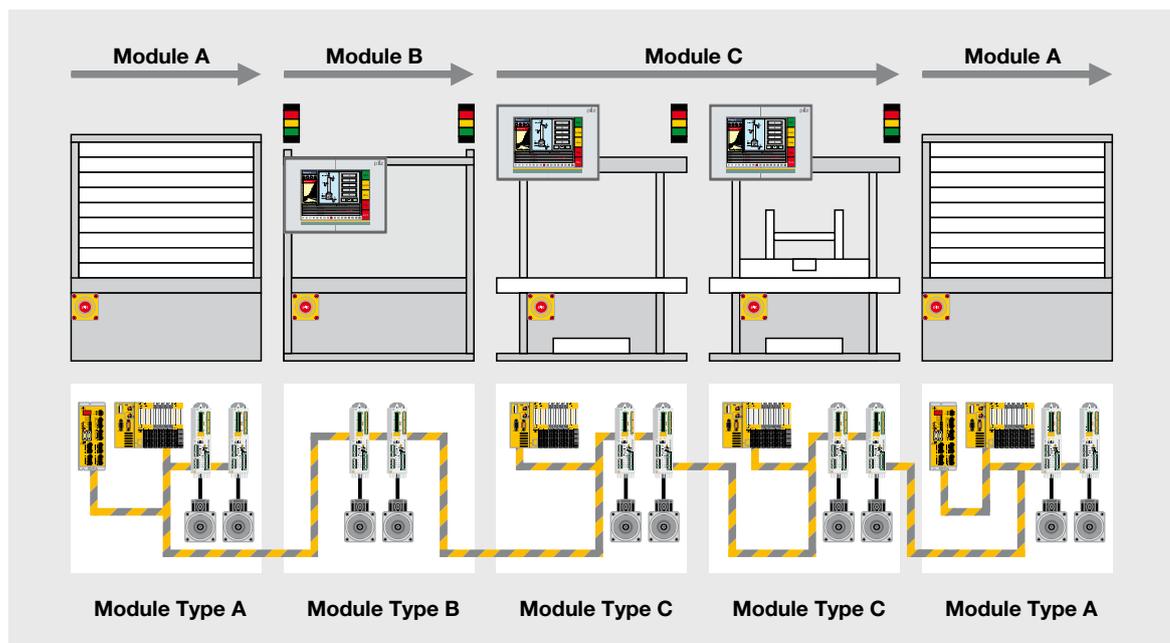
Safety and standard control functions combined in one system.

▶ 4.4 Using safety control systems to achieve safe control technology

Ultimately however, this means that all the control systems have to be able to share access to the same data, without the user being required to organise it this way. The system must perform this task automatically in the background. In future, even the tools must have the same look and feel, plus standardised handling. Whether it's motion, control or visualisation: Handling of the various functions and tasks must be seamless.

4.4.3 Modularisation of the automation function

Modularisation as an approach to solving the control technology requirement of the future ultimately involves division of the control technology into corresponding units or modules, and decomposition right down to the technology functions.



Modularisation of a machine and distribution of tasks across various control systems.

Whatever can be decomposed mechanically can also be decomposed into single parts or components with regard to automation. A components-based approach must not be limited to individual stations (such as Modules A to C in the diagram, for example), but must extend right down to the individual function units (known as mechatronic units). Future applications will be implemented much more effectively if comprehensive libraries can provide these units as reusable component blocks.

Even when division into modules and mechatronic units makes sense, it's important not to lose sight of the overall picture: Programming models which keep the units together and represent them as a whole are a much greater benefit to customers than those that merely provide components with interfaces and ultimately expect the user to look after these interfaces.

▶ 4.5 Safe control technology in transition

Sometimes safety technology appears complex and confusing, but behind it is the ongoing quest for simple “formulas”: Safety must be simple, clear, traceable and verifiable. As a result, safety technology leaves little room for an unconventional approach to solutions; it is almost by definition a conservative part of control and automation technology. Innovative trends or flows are mostly introduced after somewhat of a time lag. This mindset is also manifested in the current perception that, if an error occurs or safety is called upon (for example if the E-STOP function is operated), safety technology must always shut down safely, by electromechanical means wherever possible and without using any additional electronic components.

What is this perception based on? Safety technology is intended to protect man from all hazards emanating from plant and machinery. As such, safety technology is informed by norms and standards like almost no other sector. Last but not least, if regulations and specifications are presented in a way that is transparent, making it simpler to understand how they are implemented, this also helps to achieve safety.

The usual formulas and perspectives may still apply and essentially still make sense, but safety control systems are also undergoing a massive transition in the course of general technological progress. Even in the past, safety technology has continuously adapted to circumstances in control technology: How else would we have today’s safety solutions, which would have been totally unthinkable in the eighties and would not have conformed to the standards at that time because only electro-mechanical solutions were permitted. Electronic safety solutions only came into use gradually following extensive test procedures carried out by notified bodies (TÜV, BG, etc.). Modern manufacturing techniques require new technical approaches; process and manufacturing cycles are constantly changing. Clearly, safety technology must keep pace with developments in the automation technology sector. Customers expect innova-

tive products and solutions with integrated safety concepts that increase productivity, support efficient work processes and create additional benefits.

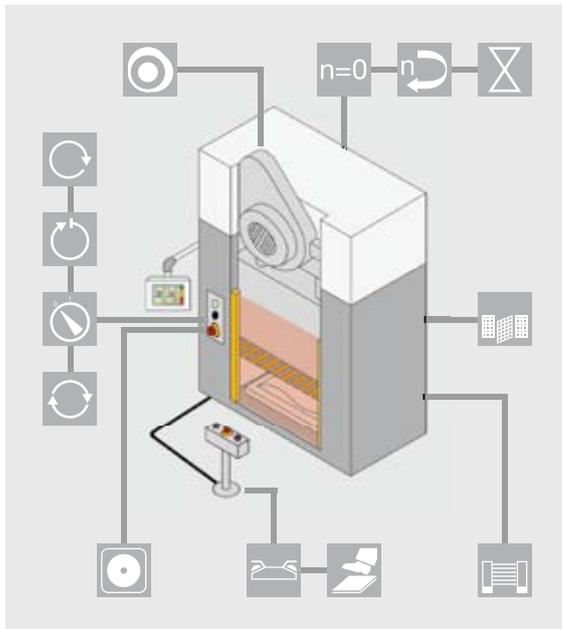
4.5.1 New safety technology requirements

What are the challenges facing safety technology today? Current requirements for greater flexibility in configuration and programming or for increased communication, for example, are already being taken into account. There are other requirements, however, which cannot yet be identified explicitly, nor do they have a name. Henry Ford once said “If I’d listened to my customers I wouldn’t have built cars, I’d have bred stronger horses”. This illustrates the point that successful developments should not be geared solely at superficial needs but must always deal with the core requirement. Far-sighted vision is required if innovative products and solutions, in the true sense of the word, are to be the end product. If you transfer this insight to safety technology it is clear that the formulas commonly used today cannot solve the tasks of the future; companies need to offer new solutions.

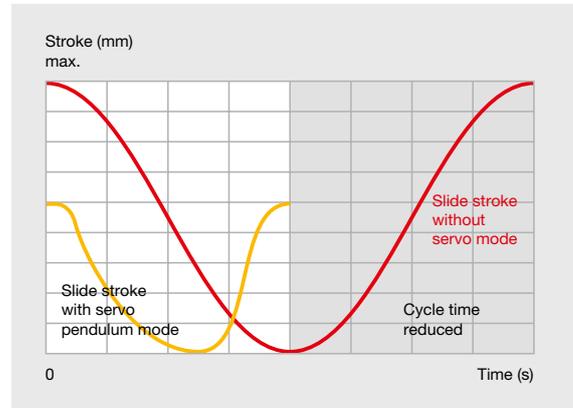
Even today, in many companies safety operates by removing power to every drive, even the whole plant, once a protected zone has been accessed. With increasing productivity requirements, however, it must be possible to access defined detection zones in a plant without having to halt the entire production process. At the same time the safety of the operator must be guaranteed. That’s why the demand is for intelligent, dynamic safety solutions. In future, to react to a safety-related event with a total shutdown can only be regarded as a last resort.

▶ 4.5 Safe control technology in transition

With some justification, a whole new generation of safety control systems is expected from safety technology manufacturers in future. Compare it with your car, where assistance functions are increasingly used to help drivers and offer additional safety (features such as distance monitoring and automatic speed reduction); in the same way, useful, extra safety-enhancing features will increasingly make their mark in mechanical engineering. An example from forming technology, where servo presses are becoming increasingly important, clearly illustrates the changed requirements: On conventional presses a mechanical rotary cam arrangement was enough to control the safety of the stroke movement, but the motion sequence on servo presses is fundamentally different. A press stroke is no longer the 360° rotation of an eccentric cam but a pendulum movement between variable angle settings. Previously well-tried procedures can no longer guarantee safety on such applications; the demands on the evaluation device are much more complex than before.



Servo press with slide stroke.



Slide stroke with and without servo mode.

The graphic examples are intended to show that in future, safety technology will need to make wide-ranging calculations in order to meet the specified requirements. Safety control systems must be able to record, process and output complex measured variables. The necessary means to do this are significantly different to anything currently available. It involves not only the sensors and actuators, but above all the processing logic functions, for which simple instruction sets are no longer sufficient due to the increased requirements. To summarise, plant and machine processes are becoming more complex and dynamic due to the demands that are placed on them. Safety technology of the future must take these changed requirements into account.

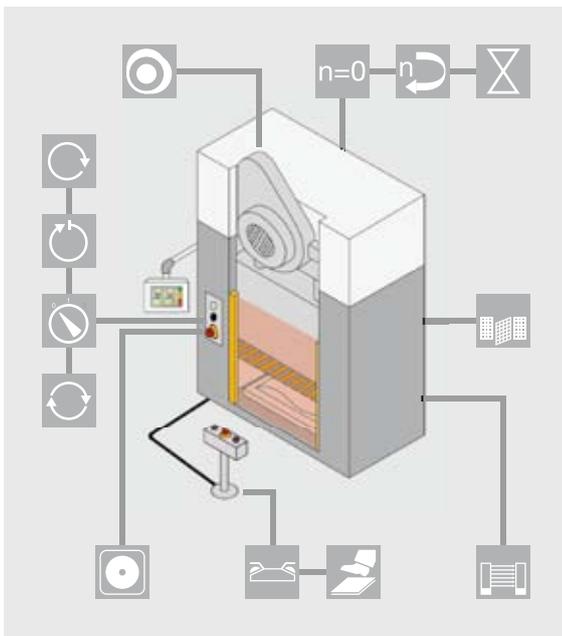


Safety function in accordance with EN 13849-1 with sensor, logic and actuator.

▶ 4.5 Safe control technology in transition

4.5.2 Complex yet simple – no contradiction

The classic, widespread view of safety technology today revolves mainly around safety functions such as those illustrated below. Common functions are those such as emergency stop, safety gates, two-hand control, operating mode selection, valve control, monitoring the direction of rotation or rotary cam arrangement; these cover the majority of the required safety functions. They are basic functions, which are needed on almost every machine, whether in this form or similar.



Safety functions on an eccentric press.

Where safety on plant and machinery is limited to basic functions, there will still be a requirement in future for simple safety control systems, on which a manageable number of safety functions can be implemented simply. That is one of the strengths of configurable safety relays such as PNOZmulti: Programming could not be simpler, using graphic symbols and drag and drop. This has now become the state of the art; indeed it has practically been the market standard since the turn of the millennium. To date, PNOZmulti has been both role model and technological forerunner within this device class.

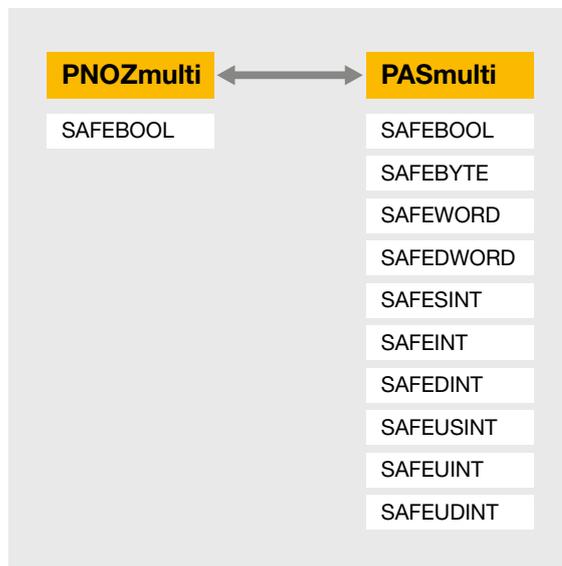
4.5.2.1 Configurable safety relays continue to develop

Originally, the “configurable safety relay” device class was intended for 4 to 10 safety functions. However, because the tool and hardware were so easy to handle, applications that were originally the reserve of “genuine”, high-performance safety control systems have gradually been migrating to the configurable safety relays. In principle, that does not present a problem, provided the devices meet the requirements. However, the user is increasingly confronted with the fact that the relay is reaching the limit of its capabilities. That’s because some wide-ranging configurations can be developed, to such an extent that even the programmer is at risk of losing oversight. At this point a contradiction can quickly arise: The more you add to the functionalities reproduced in the configurable relays, the more you lose oversight and the benefit of simple usability. But the latter is exactly what the user values.

▶ 4.5 Safe control technology in transition

4.5.2.2 Latest generation configurable relays

What distinguishes the latest generation of devices such as the PSSu multi from established devices such as the PNOZmulti? The new devices are significantly more powerful than today's configurable relays and constitute a whole new device class of "configurable safety control systems". The new generation of devices differs from its predecessors in two key areas: The ability for expansion with additional data types is a fundamental feature. The devices cannot only handle Boolean variables but can also process any form of data type, just like "fully fledged" control systems. The graphic options have also been extended so that complex composite data structures can be displayed graphically on individual lines in the Editor. This promotes clarity, without losing important information.

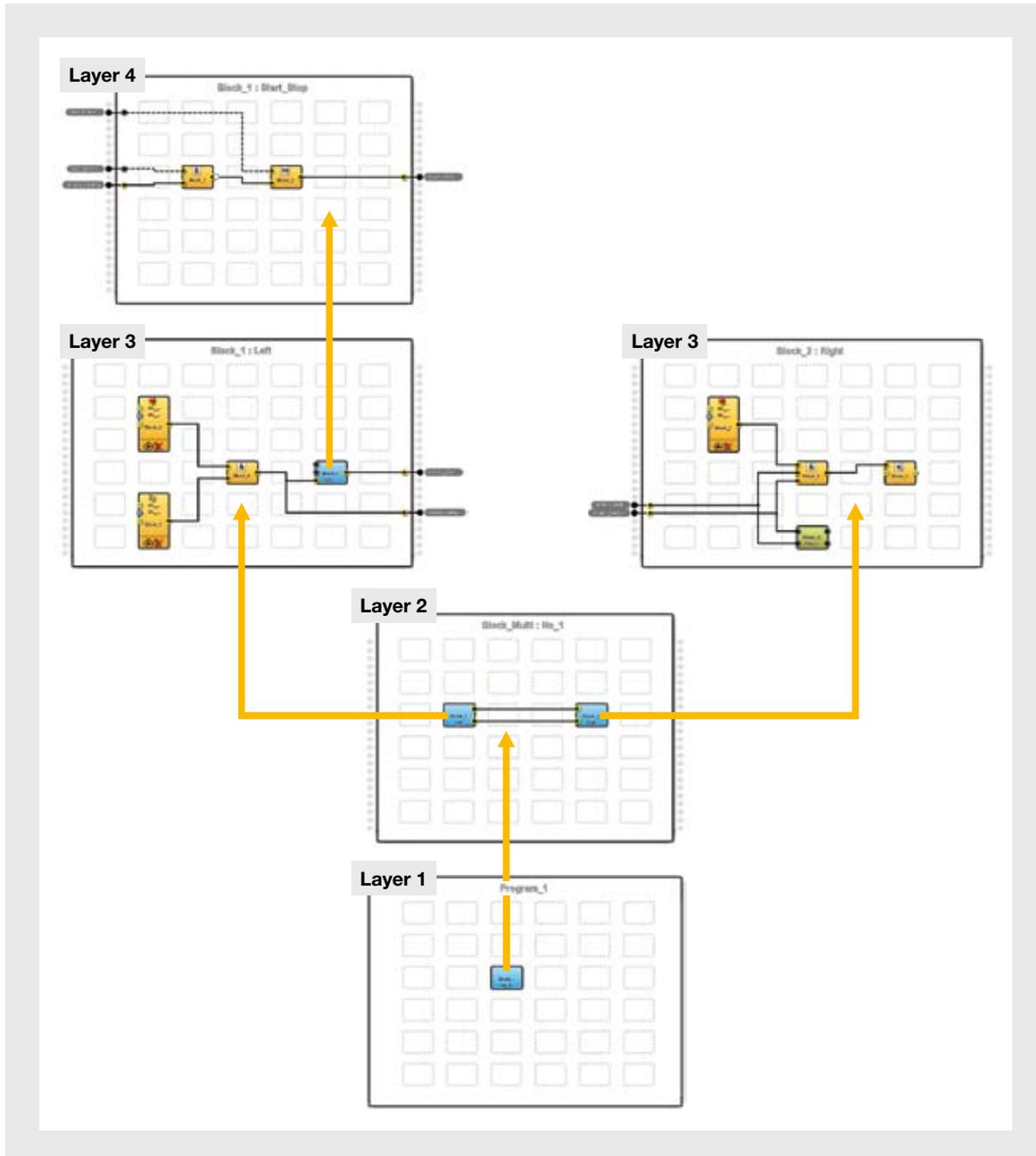


Comparison between PNOZmulti and PSSu multi data types.

Another fundamental change concerns the program structure. From the perspective of a PLC control system it is customary for programs to have a hierarchical structure. Programs contain function blocks, which in turn call up functions or blocks. A feature of configurable relays is that the program is displayed on a single plane. To date it has not been possible to reproduce the hierarchical structures familiar from PLC control systems. It is a sensible solution for simple applications, indeed it has contributed to the success of this device class. However, this type of programming soon becomes confusing when applications are more complex.

Now this feature has been added to the device class of configurable safety control systems. Program sections can be combined into one block, making the program clearer, without losing any of the information contained in the program section. If a function is created in the customary "flat" format, it can be selected and merged into a new block. The new block "inherits" all open interfaces as its external interface and can be opened, expanded or modified by double-clicking on it. As a result it is possible to view the block's internal structure at any time.

► 4.5 Safe control technology in transition



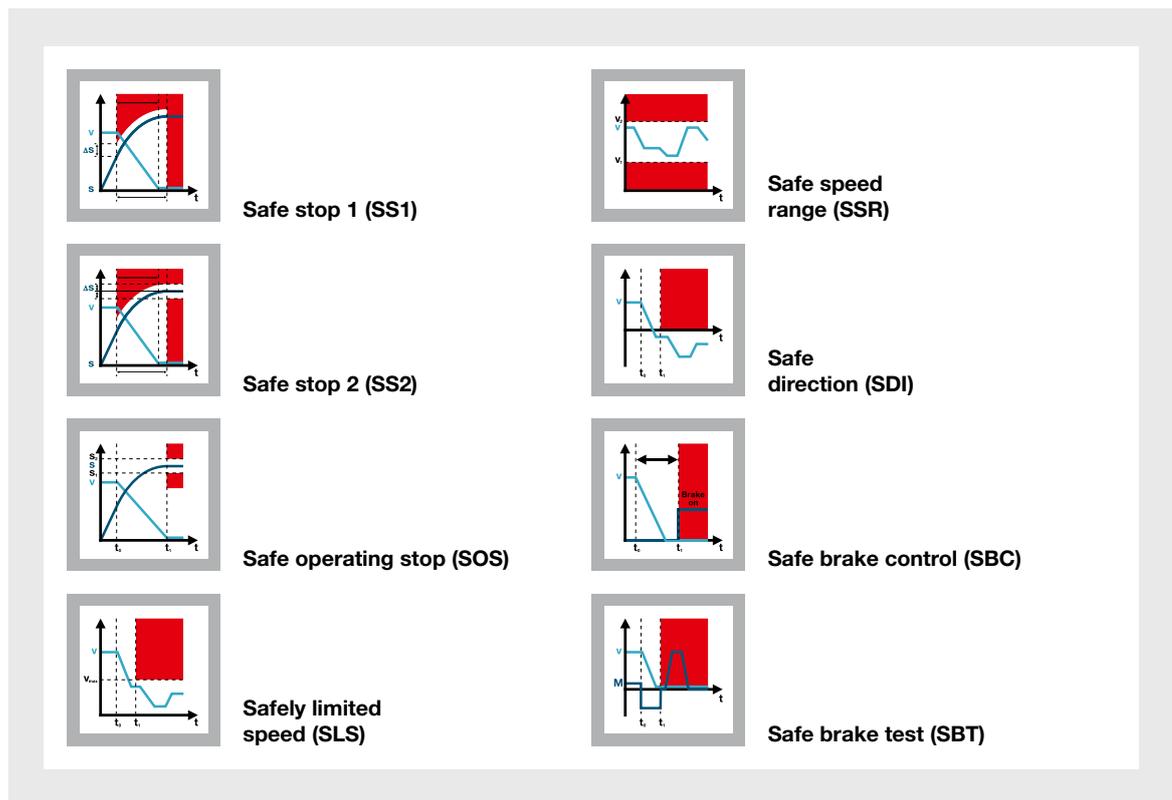
Hierarchical grouping with configurable relays.

▶ 4.5 Safe control technology in transition

4.5.2.3 Integration of automation and safety technology

Today's safety control systems are characterised primarily by the ability to program them freely, in a similar way to a standard PLC. However, there are some restrictions. To ensure that programs remain clear and understandable, on most systems the instruction set and/or number of available editors is restricted. This hasn't been a problem, and indeed isn't a problem, provided plant and machinery only require simple safety measures. However, a structural transition is currently taking place regarding safety technology requirements.

Processes are becoming increasingly dynamic, there is a greater need for controlled access to the process and productivity requirements are higher, so safety technology is gradually changing as a result. In the future, the previous strategy of shutting down safely when the safety function is called upon or when an error occurs will no longer be acceptable. Safety technology must open up to innovative processes, as currently illustrated by examples of safe drive functions.



Drive-integrated safety with PMCprotego DS.

▶ 4.5 Safe control technology in transition

But that's just the beginning! Step by step, safety technology needs to become a permanent feature of automation technology, as is already the case with drive technology with dynamic speed or standstill monitoring. Future safety concepts will need to be much more dynamic, including functions such as torque monitoring, based on the position of one or more axes. The available safety control systems will only partly satisfy these new requirements. Instruction sets will be required that can meet the need for dynamisation of safety functions. And yet programming will still need to be built on simple, manageable base elements that enable a safe programming procedure, as required by the IEC 61508 standards, for example.

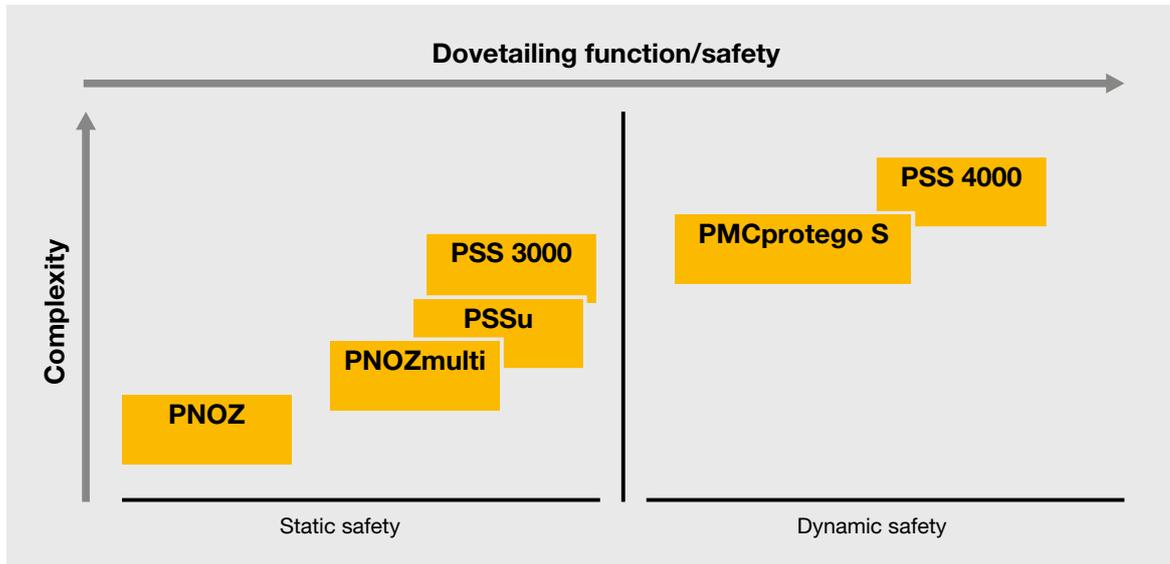
Ultimately, modern safety control systems offer a sensible combination of the programming procedure from a PLC and the configuration benefits from the "configurable safety control system" device class. Specifically this means that today's safety control system needs to have a large number of editors. The "instrument" that the user is handed shouldn't span only one octave, but if possible should cover the whole "audible" range. Care should be taken to ensure that the editors also meet the needs of the various industries and target groups. Complex safety functions should be capable of being created and tested in a high level language. After the test phase it must be possible to convert to a graphic display.

4.5.3 Outlook – from static to dynamic safety

Changes are happening at system level as well as device level. The signs are beginning to emerge in the safe drive technology sector. Previously, the safety function was connected to the control system but now it is distributed, i.e. the function migrates to the local function controller, for example the drive. At the same time, separation of the safety and control functions is becoming increasingly fuzzy; the control function could ultimately be safety-related. Looking at today's plant and machinery it is clear that not only have safety technology requirements changed, both in the number of safety functions and the way in which they are linked, but that the desire for more flexible solutions continues to grow. Why is this? The main factor behind what have sometimes been major changes in engineering over the past few years has been the trend of replacing mechanics with electronics. In addition to economic considerations this has also brought new degrees of technical freedom, which are now reflected in the safety technology requirements.

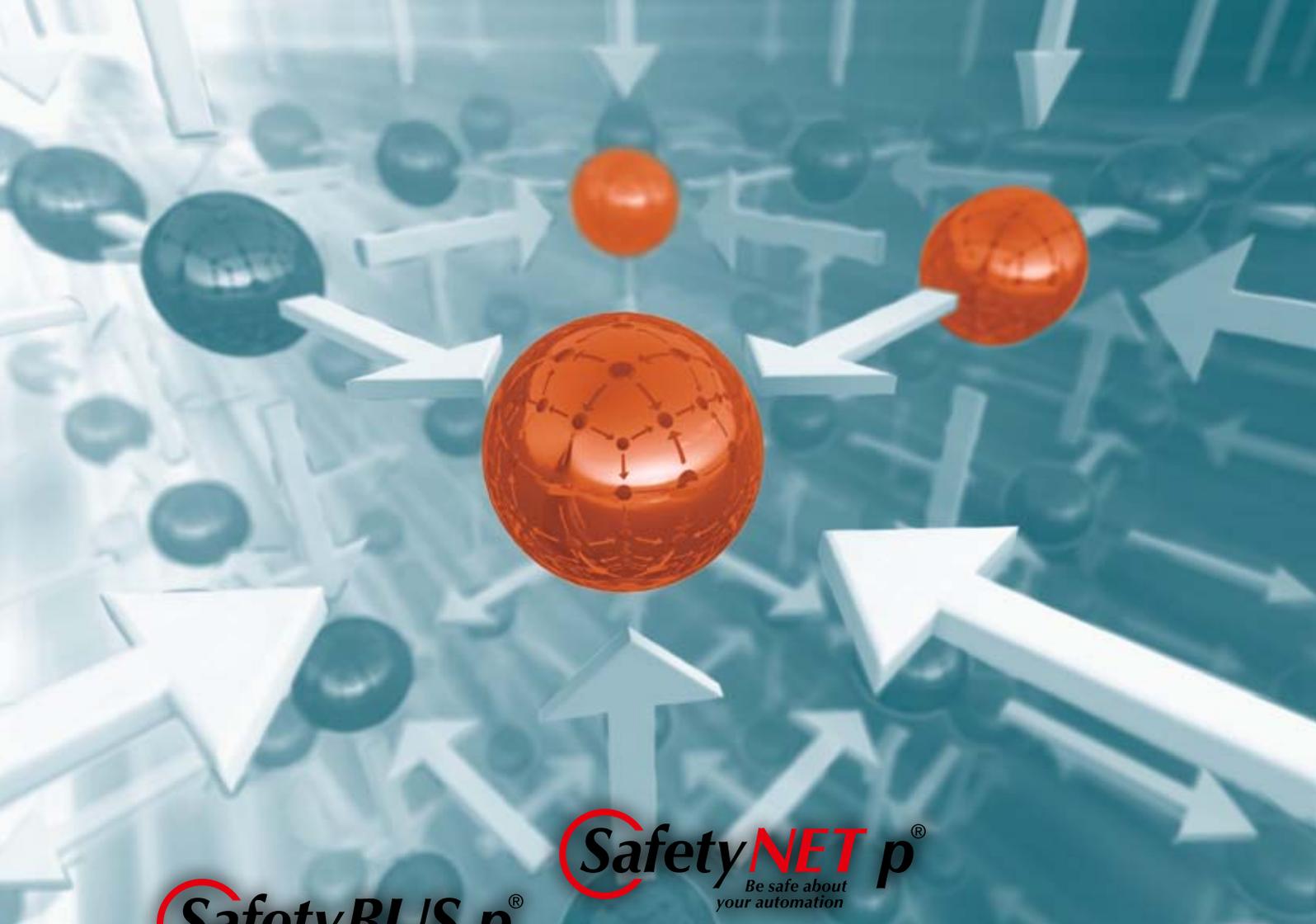
In the past, safety was primarily influenced by static events such as the operation of an emergency stop device, the opening of a safety gate or the interruption of a light curtain, but the focus today is on requirements that enable the safety function to react in a way that's tailored to the machine's dynamic processes. Reactions are no longer triggered only by simple logic connections, but by complex states or results of intricate calculations, to which the safety function must react appropriately.

▶ 4.5 Safe control technology in transition



Static and dynamic safety.

How does this affect developments in safety technology? Dynamic safety needs the control function to dovetail closely with safety. That's why it's necessary to think more in terms of systems. If subfunctions are to fit seamlessly together, functions cannot simply be superimposed, they must be an integral part of the overall system. Developments in the control technology sector have already seen functions executed across device boundaries; similar developments will also become established in safety technology. Ultimately, the challenge lies in integrating the functions into the overall system. With highly complex dynamic tasks, insular solutions will generate no added value.



SafetyBUS p[®]
The Safe Standard!

SafetyNET p[®]
*Be safe about
your automation*

5

**Safe
communication**

► 5 Safe communication

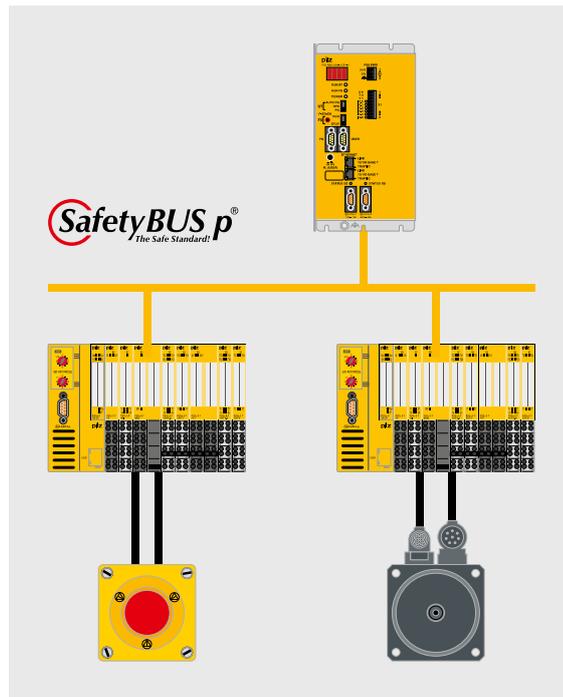
Chapter	Content	Page
5	Safe communication	5-3
5.1	Basic principles of safety-related communication	5-3
5.1.1	Principle of decentralised safety technology	5-3
5.1.2	Handling communication errors	5-3
5.1.3	Principle of redundancy	5-5
5.2	Safe fieldbus communication with SafetyBUS p	5-6
5.2.1	System description SafetyBUS p	5-7
5.2.2	Security measures	5-7
5.2.3	Technical details	5-8
5.2.4	Separation of safety-related and standard communication	5-8
5.2.5	Certification	5-9
5.2.6	Diagnostics	5-9
5.2.7	Communication media	5-9
5.2.8	Industries, applications	5-10
5.3	Safe Ethernet communication with SafetyNET p	5-13
5.3.1	Why Ethernet in automation technology?	5-13
5.3.2	System description SafetyNET p	5-13
5.3.3	UDP/IP-based communication with RTFN	5-15
5.3.4	Hard real-time communication with RTFL	5-16
5.3.5	CANopen application layer	5-17
5.3.6	Safe communication via SafetyNET p	5-18
5.3.7	Safe communication in the OSI reference model	5-18
5.3.8	Safe telegram structure	5-19
5.3.9	Safe communication in distributed control systems	5-19
5.3.10	Application example of a modular machine design	5-20

▶ 5.1 Basic principles of safety-related communication

Safety-related communication has replaced the long tradition of parallel wiring in many of today's mechanical engineering applications. There are many reasons for this: It reduces complex wiring, simplifies diagnostics and troubleshooting and increases the availability of the whole application. The following chapter explains how safe communication operates, using SafetyBUS p and SafetyNETp as an example, and also demonstrates some applications.

5.1.1 Principle of decentralised safety technology

Depending on the desired safety level, periphery devices such as E-STOP switches are generally connected to a safety control system in a dual-channel configuration. The redundancy and additional cable tests mean that faults such as short circuits or open circuits can be detected and managed. A bus cable uses single-channel, serial communication, which does not provide physical line redundancy. That's why additional measures in the protocol are needed to uncover faults such as a disconnected bus cable or communication problems.



Principle of decentralised safety technology.

5.1.2 Handling communication errors

The sections below describe typical errors and measures which may occur when safety-related data is communicated via an industrial communication system, and ways in which these can be handled.

5.1.2.1 Message repetition

Malfunctions within the bus subscriber can lead to telegram repetition. Each message is given a sequential number so that repeated messages are detected. The receiver is “expecting” the sequential number, so it will detect repeated telegrams and initiate appropriate measures.

▶ 5.1 Basic principles of safety-related communication

5.1.2.2 Message loss

Messages may be deleted as a result of a malfunction on a bus subscriber or the receiver may stop receiving telegrams because the bus cable has been disconnected, for example. The receiver uses a sequential number to detect the loss of data packets. A timeout on the receiver also monitors the latest time by which a new message must arrive. Once this timeout has elapsed, the receiver is able to bring the application to a safe condition.

5.1.2.3 Message insertion

Additional messages may creep in as the result of a malfunction on a bus subscriber. As with message repetition, the sequential number can be used to detect and manage this situation.

5.1.2.4 Incorrect message sequence

Errors on a bus subscriber or on telegram-storing elements such as switches and routers can corrupt the telegram sequence. However, this will be detected through the sequential numbers.

5.1.2.5 Message corruption

Malfunctions on a bus subscriber or faults on the communication medium, e.g. problems due to EMC, can corrupt messages: A data security mechanism (check sum) applied to the safety-related telegram content will recognise this and detect the corrupted message.

5.1.2.6 Message delay

A malfunction on the bus subscriber or an incalculable data volume in the bus system can lead to delays: A timeout on the receiver will detect the delays and initiate appropriate measures.

5.1.2.7 Combining safety-related and non-safety-related communication functions

In mixed systems containing safety-related and non-safety-related subscribers, receivers will sometimes interpret a telegram from a standard subscriber as a safety-related telegram. Such mistakes on the part of the receiver can be avoided using measures such as unique IDs across the network and varied data security features for safety-related and non-safety-related messages.

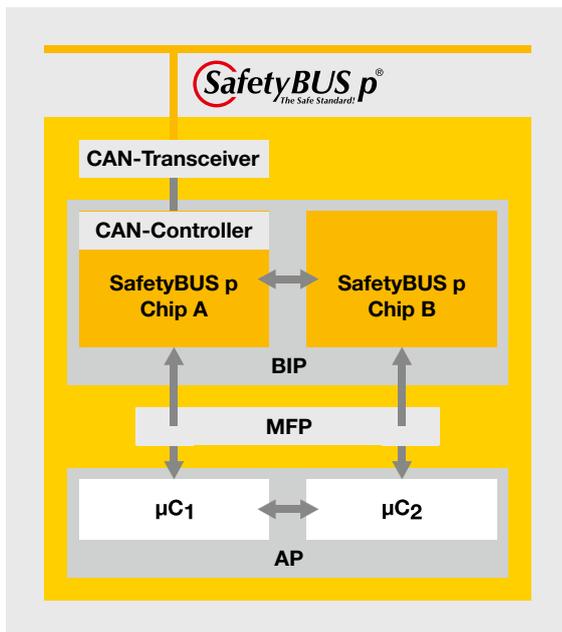
Error	Measures per message				
	Sequential number	Timeout	ID for transmitter and receiver	Data security	Varied data security for safety-related and non-safety-related messages
Repetition	◆				
Loss	◆	◆			
Insertion	◆		◆		
Incorrect sequence	◆				
Message corruption				◆	
Delay		◆			
Combining safety-related and non-safety-related messages			◆		◆

Errors and measures, using SafetyNET p as an example, taken from BIA GS-ET 26.

▶ 5.1 Basic principles of safety-related communication

5.1.3 Principle of redundancy

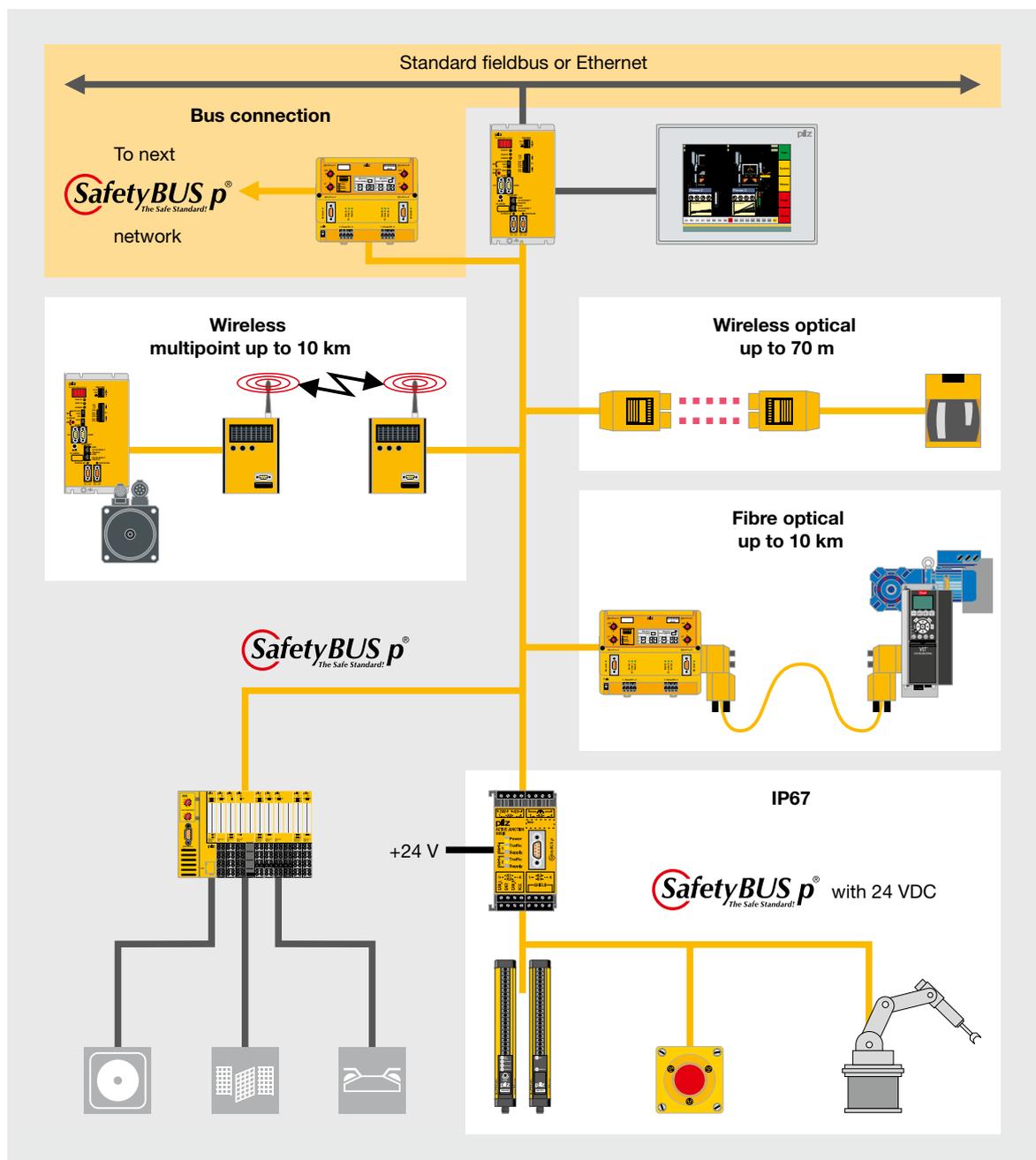
In order to control potential errors when recording and processing safe signals in bus subscribers, each function is processed by at least two different components or methods, which monitor each other. When an error is detected, these components or methods are used to bring about a safe condition. On the safe bus system SafetyBUS p, for example, the application software is processed by redundant microprocessors, which compare their respective results before transferring them to the redundant SafetyBUS p chip set. This then generates the actual safety-related message.



Redundant hardware, using SafetyBUS p as an example.

► 5.2 Safe fieldbus communication with SafetyBUS p[®]

The function and application of a safe fieldbus is explained below, using the popular safety-related fieldbus system SafetyBUS p as an example.



System overview of SafetyBUS p.

▶ 5.2 Safe fieldbus communication with SafetyBUS p[®]

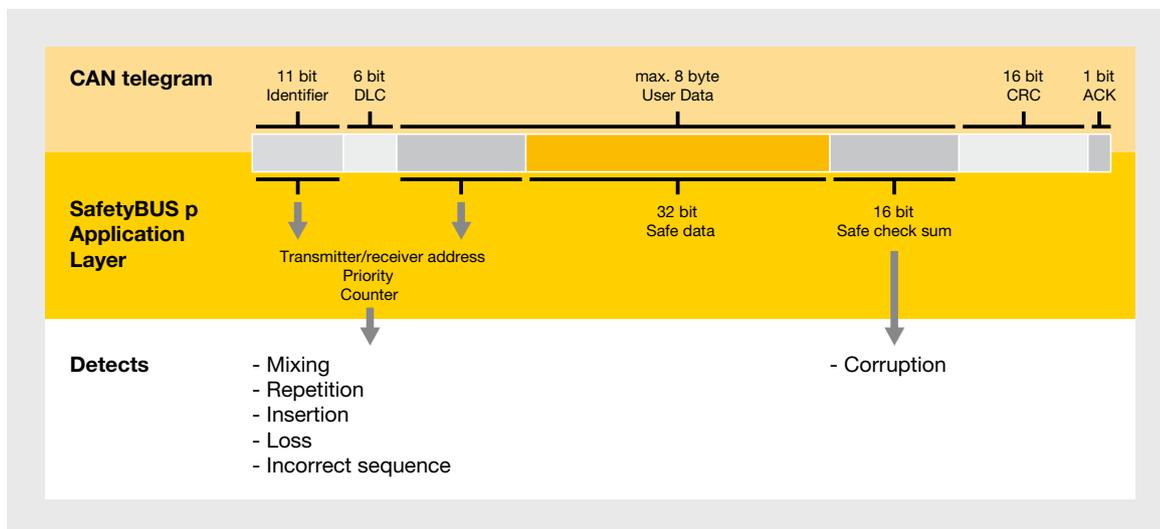
5.2.1 System description SafetyBUS p

SafetyBUS p is a communication standard for the implementation of safety-related applications in industrial automation technology. SafetyBUS p has been proven in thousands of applications since its launch in 1999. The system is used exclusively for the communication of safety-related data. The underlying communication is based on the CAN communication standard. The physical properties on SafetyBUS p, such as the linear bus structure, maximum cable length and number of subscribers, are the same as on CAN. A wide range of devices are now available for connection to SafetyBUS p. These include safety control systems, digital inputs and outputs, light curtains and drives. Structural components such as routers, bridges and active junctions are available for flexible network configurations.

5.2.2 Security measures

The following security measures are implemented on SafetyBUS p in order to detect communication errors:

- ▶ Counters
- ▶ Addresses
- ▶ Acknowledgements
- ▶ Time monitoring (timeout)
- ▶ Connection monitoring
- ▶ Cyclical polling with timeout
- ▶ Safe hardware
- ▶ Redundant and diverse chips



SafetyBUS p telegram.

► 5.2 Safe fieldbus communication with SafetyBUS p[®]

5.2.3 Technical details

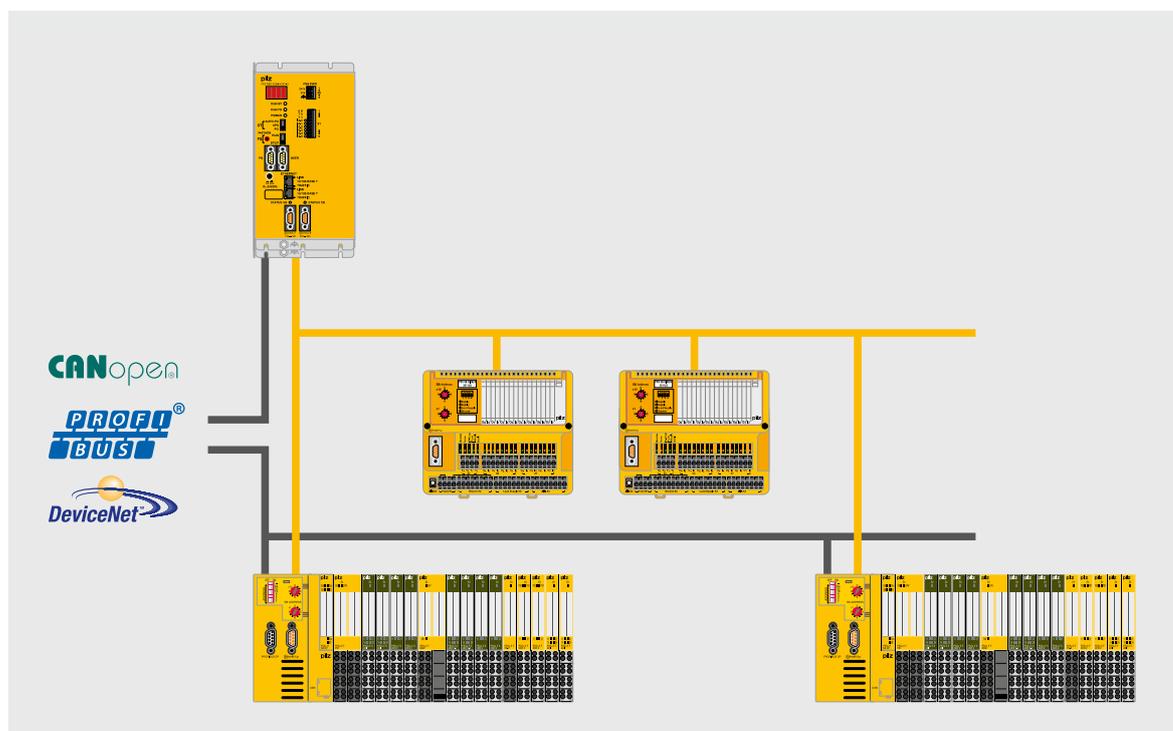
Up to 64 safe devices can be implemented within a network using the multimaster system SafetyBUS p. This can even be extended to up to 128 subscribers if networks are interconnected, enabling 4,000 inputs and outputs per network.

Further technical features:

- ▶ Guaranteed error reaction times up to 25 ms
- ▶ Safe usable data per telegram: 32 bit
- ▶ Maximum cable length:
Copper cables: 3.5 km; fibre-optic: 40 km
- ▶ Multiple networks can be safely interconnected
- ▶ Gateways to standard fieldbuses
- ▶ Optional supply voltage via bus cable

5.2.4 Separation of safety-related and standard communication

On SafetyBUSp, safety-related data is communicated separately from standard data, via separate bus cables. This division makes troubleshooting easier when faults occur. It also increases the system's availability, as there's no feedback between standard and safety-related communication. The reduced bus load also leads to faster reaction times. There is a clear allocation of responsibility for the data. As a result, unwanted or accidental modifications in the standard section will not influence the safety-related section. The restriction to a purely safety-related system means that complexity is low, which simplifies the engineering and approval process.



Separation of safety and standard.

▶ 5.2 Safe fieldbus communication with SafetyBUS p[®]

5.2.5 Certification

Notified bodies such as TÜV and BG have approved safe communication via SafetyBUS p for use in safety-related applications in accordance with the following standards:

- ▶ SIL 3 in accordance with IEC 61508
- ▶ PLe in accordance with ISO 13849
- ▶ SIL 3 in accordance with IEC 62061

5.2.6 Diagnostics

Diagnostic information from the subscriber is made available to the Management Device, which is usually a safety control system. The safety control system can provide this information to established standard communication systems such as Profibus DP, CANopen or Ethernet/IP, for example.

5.2.7 Communication media

A wide range of communication media is available to SafetyBUS p, enabling it to satisfy the varied application requirements. Communication may therefore be copper, wireless, light or fibre-optic-based.

5.2.7.1 Fibre-optic communication

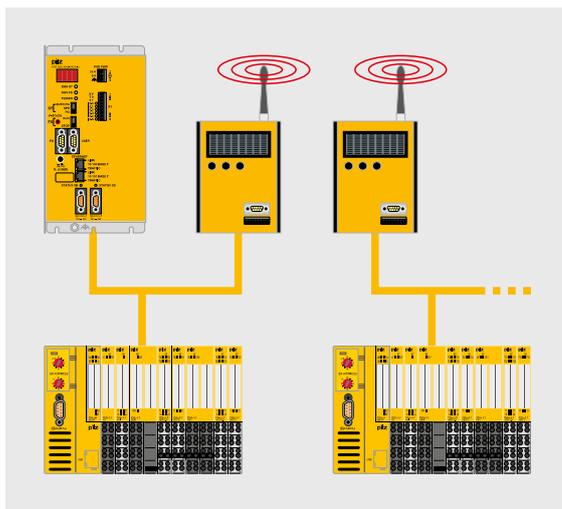
With fibre-optic (FO) communication, fibre-optic cables, transmitters and receivers are used instead of copper cables. Fibre-optic routers are used on SafetyBUS p for this purpose. For safety control systems with SafetyBUS p interface, the fibre-optic routers are totally transparent, i.e. copper-based communication can simply be swapped for fibre-optic communication, without having to reconfigure the control system. SafetyBUS p has a number of different devices for creating fibre-optic paths. Fibre-optic converters can be selected for glass fibre paths from 4 to 40 kilometres, depending on the application. Integrated routing functions enable network segmentation. As a result, different transmission rates are possible within the segments connected via FO. The FO router also filters messages in SafetyBUS p, so that they only reach the segments for which they are intended. This reduces the network load in the remote bus segment.

Today, FO communication is found in a wide range of applications. It's important where a high EMC load would disrupt communication, as would be the case with welding robots in the automotive industry, for example. Fibre-optic paths are also used for safety-related communication between the mountain and valley stations on cablecars, where it's necessary to span long distances outdoors. This technology is also used to reduce reaction times in safety technology. On copper-based networks, the data transmission rate depends on the cable runs, so the reaction time of the safety technology increases with the length of the bus cable. This dependency is lower on FO-based networks, so a short reaction time is guaranteed, even over long distances.

► 5.2 Safe fieldbus communication with SafetyBUS p[®]

5.2.7.2 Safe wireless communication

SafetyBUS p data can be transmitted wirelessly using wireless routers. From the safety control system's perspective the wireless routers are transparent, i.e. they are not visible as subscribers in the network and therefore don't need to be configured. The wireless bus segment behaves in the same way as a segment connected via cable. Wireless transmission does not affect the safety level of SafetyBUS p.



Safe wireless communication.

Safe wireless communication is used when it's necessary to span long distances between safety-related subscribers but it is too complex and therefore cost inefficient to lay cables. Another application would be mobile subscribers, on which the wearing sliding contacts are replaced by wireless transmission for data transfer. These may be rotating or linear-moved plant sections, such as those found on automatic guided vehicle systems or cranes. When safe wireless technology is employed, high demands are placed above all on the quality of the wireless connection, as this affects the number of telegrams that are lost and can cause safety-related shutdowns of the application. This in turn will impact on the application's availability. To guarantee the quality of the wireless connection, particular attention should be paid to selecting wireless and antenna technology that is appropriate for the application. Operating ranges of up to a kilometre can be implemented using an omnidirectional antenna, while up to 10 kilometres are possible with a directional antenna.

► 5.2 Safe fieldbus communication with SafetyBUS p[®]

5.2.8 Industries, applications

Today, safe bus systems such as SafetyBUS p are used worldwide in a wide range of industries and applications. The list below represents only a selection.

5.2.8.1 Automotive industry

The automotive industry uses SafetyBUS p to safeguard and control presses. Applications range from small standalone presses to multi-stage transfer presses, demanding the very highest

safety and performance requirements of a safety bus. Even on the conveyor technology, where the safety and reaction time requirements are not so high, safety-related fieldbuses are used to collect widely distributed, safe I/O signals such as E-STOPS. Robot cells are frequently found in the automotive industry and normally require safety gates, light curtains and E-STOP pushbuttons as safety equipment. With SafetyBUS p, multiple robot cells can be networked together and monitored via a safety control system.



SafetyBUS p in a robot application.

▶ 5.2 Safe fieldbus communication with SafetyBUS p[®]



5.2.8.2 Airports

Airports contain baggage handling and conveying technology applications in which long distances have to be covered. Safety-related equipment such as E-STOP pushbuttons and grab wires are distributed across the whole route. SafetyBUS p collects the safety-related signals and makes them available to the safety control system, which shuts down the drives safely if necessary.



5.2.8.3 Passenger transportation

SafetyBUS p is also used for communication on cable cars: Safety-related signals are exchanged between the mountain and valley stations and signals are collected en route. Wireless or fibre-optic communication is used to cover the long distances.

▶ 5.3 Safe Ethernet communication with SafetyNET p[®]

5.3.1 Why Ethernet in automation technology?

Automation technology is currently developing away from a centralised control system with simple binary sensors and actuators into complex, intelligent systems. The proportion of control and process capacity within the sensors and actuators is constantly growing. This trend changes the communication requirements dramatically: Instead of the usual master/slave system that we see today, in future, more and more data will be exchanged directly between the network subscribers. Today's individual, largely passive bus subscribers will increasingly assume the function of bus masters, with their own computing capacity.

Modern IT technology – as seen in office communication with personal computers and office network technology such as switches, routers etc. – currently offers a wide range of system components at favourable prices. There is huge potential for innovation. That's why users are increasingly keen to modify this technology to make it usable for industrial automation technology. Ethernet, which is practically standard in today's office communication, has a prominent role to play. When developing modern fieldbus systems, the aim in future must be to exploit the benefits of Ethernet to a greater extent. The installation of Ethernet systems must become simpler; compared with current fieldbus systems, Ethernet in its current form is still too complex.

The requirements of the individual elements of a production plant also continue to grow. This affects scan times, precision/frequency of measurements, data amounts and processor power, to name but a few. As far as the automation system is concerned, the performance of the process computer and communication systems must satisfy these growing requirements. As a modern, Ethernet-based fieldbus system, SafetyNET p meets these new requirements. At the same time, SafetyNET p is as simple to install and as reliable as today's available fieldbus systems.

5.3.2 System description SafetyNET p

Safety-related communication via Ethernet is explained below, using the real-time Ethernet communication system SafetyNET p as an example. SafetyNET p is a multi-master bus system, i.e. all devices on the network have equal rights. The bus scan time of SafetyNET p can be adapted to suit the application requirements.

5.3.2.1 Security

The protocol includes a safe data channel, which is certified for data transfer in accordance with SIL 3 of IEC 61508. Both safety-related and non-safety-related data is transferred via the same bus cable. Non-safety-related subscribers have direct access to safety-related data and can use it for further non-safety-related processing tasks.

► 5.3 Safe Ethernet communication with SafetyNET p[®]

5.3.2.2 Flexible topology and scan time selection

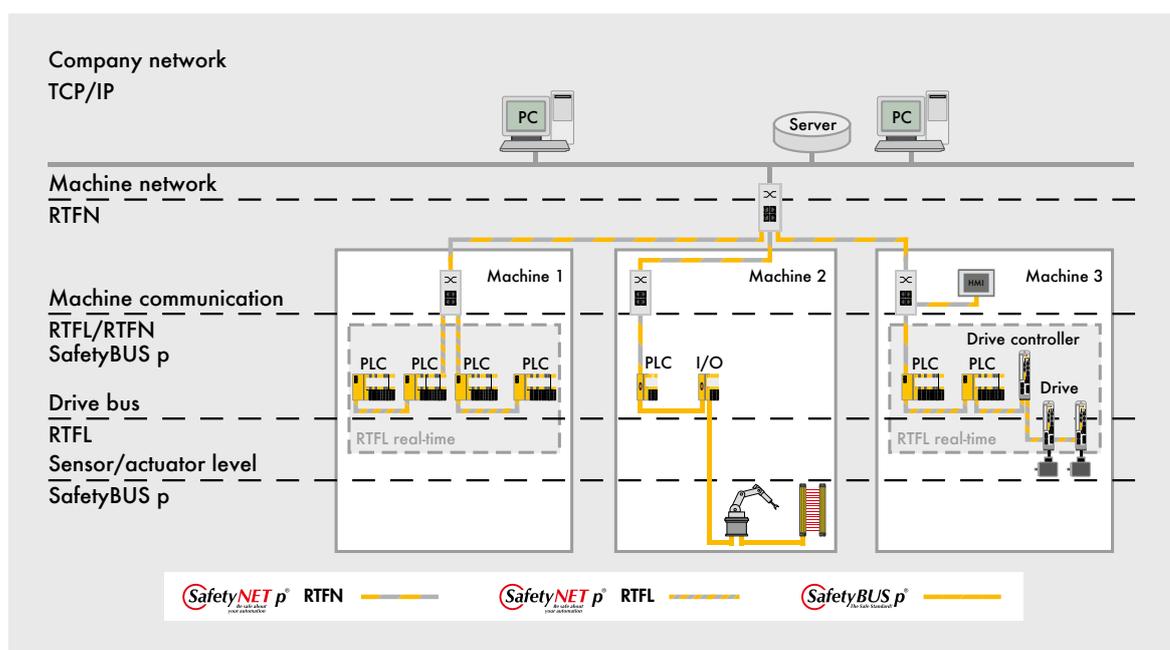
SafetyNET p is extremely flexible, not just when it comes to selecting a suitable bus scan time, but also on the issue of the appropriate topology: The multi-master bus system supports linear, star, tree and ring topologies. The RTFL communication principle (Real Time Frame Line) is suitable for intra-cell communication, as it allows the fastest scan times. A minimum bus scan time of 62.5 µs can be achieved. Jobs and events can be recorded and executed with high precision across the entire network. Absolutely essential for real-time applications: A jitter of around 100 ns can be achieved in real-time control loops. As a result, it's even possible to use SafetyNET p in a frequency converter control loop between a rotary encoder and a speed regulator. Other highly dynamic applications are also possible, of course. RTFN mode (Real Time Frame Network) is used at higher levels, as it offers maximum coexistence capability with existing services.

5.3.2.3 Application layer

The interface with the application is made via widely-used CANopen technology. Existing CANopen devices can be converted to SafetyNET p devices simply by changing the transport layer.

5.3.2.4 Standard Ethernet technology

SafetyNET p uses Ethernet technology. The interface depends on the required performance level: If fastest possible communication is required, the RTFL communication principle is used, which is based on Ethernet OSI Layer 2 (MAC Frames). For communication via mixed Ethernet-based networks, from cell to cell or in general networks, UDP/IP communication is used. Conventional, standard Ethernet infrastructures can be used if the performance is satisfactory. This includes connectors, cables, routers, switches, gateways or communication channels.



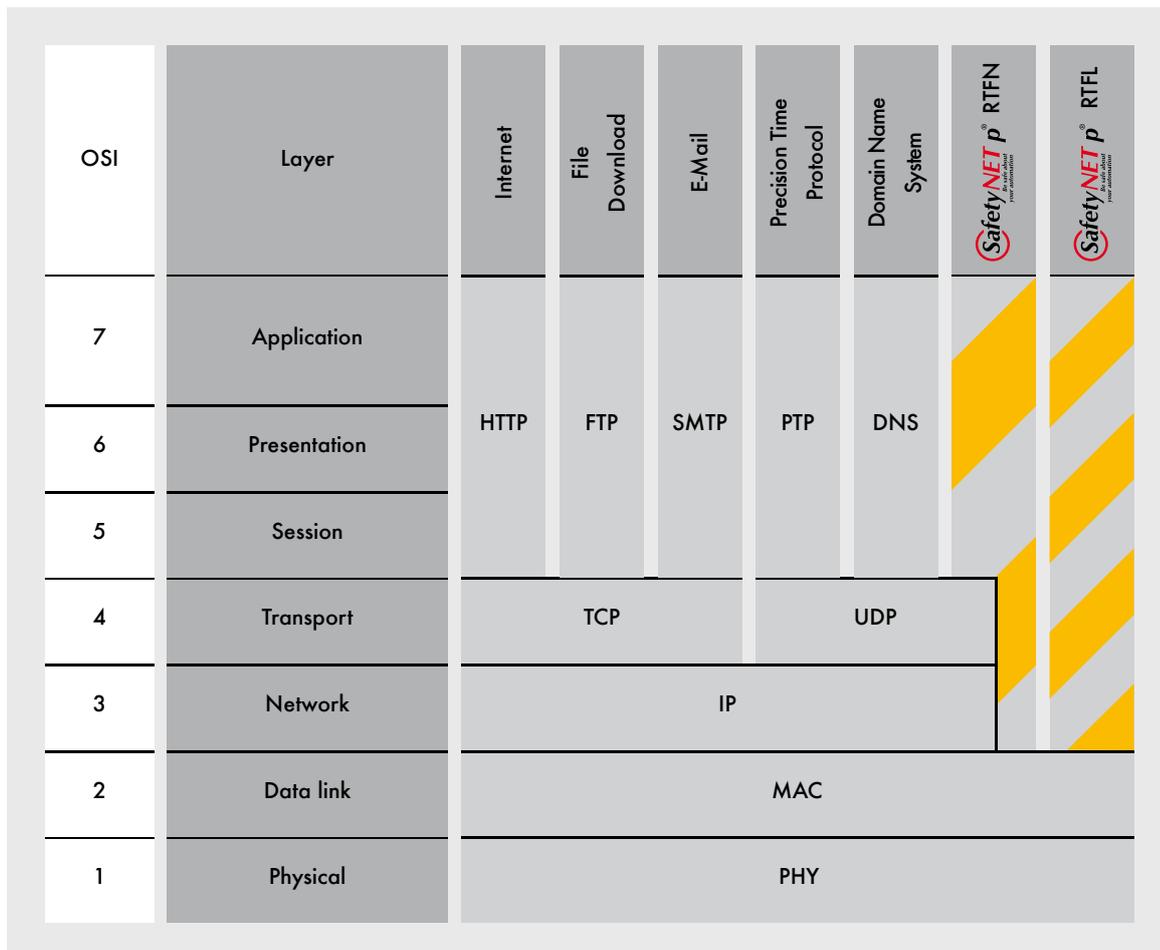
SafetyNET p in the communications hierarchy.

▶ 5.3 Safe Ethernet communication with SafetyNET p[®]

5.3.3 UDP/IP-based communication with RTFN

The RTFN transport layer of SafetyNET p can be used at process control and manufacturing cell level, where standard Ethernet protocols are in demand and the real-time requirements are lower. RTFN is used to network the RTFL real-time cells and to connect standard Ethernet subscribers, such as visualisation devices or service PCs. The RTFN level typically has a tree topology as used in office communication, i.e. with conventional Ethernet. Switches are used to connect the network subscribers in individual point-to-point connections.

RTFN can use two different mechanisms: The Ethernet MAC frame is used in closed networks. The devices are addressed directly via their MAC address. Then there's the UDP protocol, which is available on most office PCs. In this case, the devices are addressed by their IP address. If IP-based communication is used, the RTFN frames may also be routed from network to network.



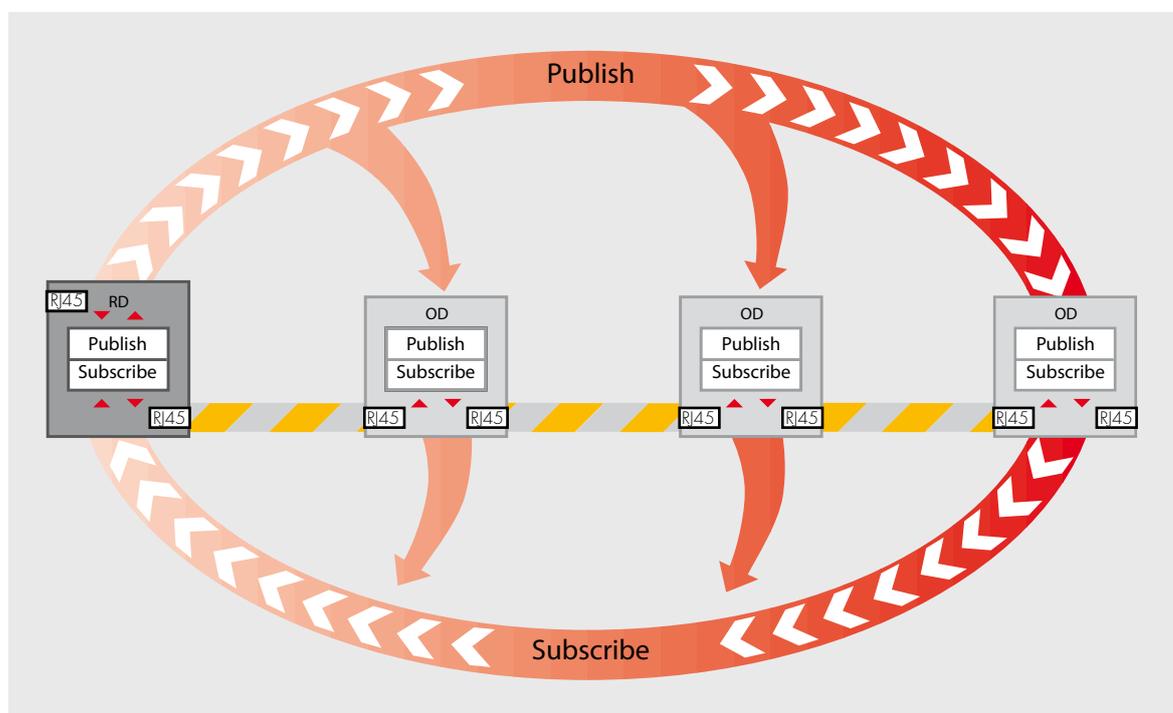
SafetyNET p in the ISO/OSI reference model.

▶ 5.3 Safe Ethernet communication with SafetyNET p[®]

5.3.4 Hard real-time communication with RTFL

The RTFL transport layer of SafetyNET p is optimised for the fastest real-time applications. Typically the devices are networked in a linear structure, as with traditional fieldbus systems. All the bus subscribers have equal rights. Data is exchanged in accordance with the publisher/subscriber principle. As a publisher, each device can provide data to the other devices (subscribers) via SafetyNET p. In turn, these subscribers can read the published data from individual subscribers or all subscribers. This way it is possible to exchange data efficiently between all the subscribers. The communication mechanism used by RTFL is a very fast cyclical data transfer in one single Ethernet

data frame or multiple data frames per cycle. Communication is initiated by a special device called the Root Device (RD). The Ethernet frame generated within the Root Device is then transferred to the other devices (OD – Ordinary Device). The ODs fill the Ethernet frame with data to be published and extract from the Ethernet frame the data to be read. The devices are addressed via their MAC address. Each RTFL network requires just one Root Device. Each RTFL device has two Ethernet interfaces, which enables the familiar daisy chain wiring often found on fieldbuses.



SafetyNET p RTFL communication.

▶ 5.3 Safe Ethernet communication with SafetyNET p[®]

5.3.5 CANopen application layer

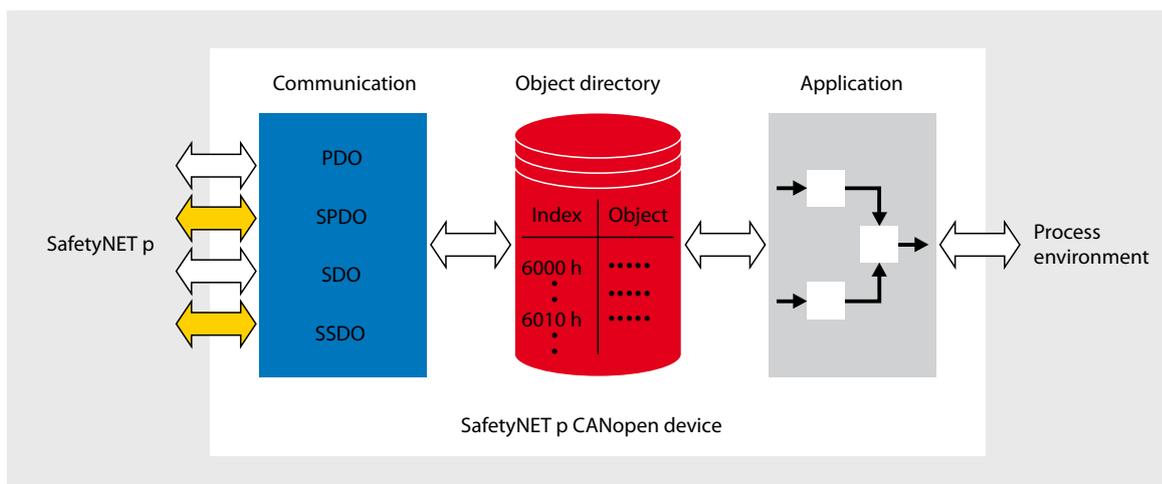
The application layer of SafetyNET p adapts the mechanisms of CANopen to the conditions of SafetyNET p. CANopen is an open, manufacturer-independent fieldbus standard specified/standardised by CiA (CAN in Automation). SafetyNET p therefore has a standardised application layer for industrial applications. This includes the standardisation of communication, i.e. the technical and functional features used to network distributed field automation devices and standardise application objects via device profiles.

The SafetyNET p application layer is largely based on the CANopen standard. The changes that have been made are mainly in the communications area and in the way safe application data is handled. The key element in CANopen is the object directory, which acts as the interface between the application and the communication subsystem. Essentially it is a grouping of objects and functions, which can then be stored and called up as application objects. The integration of safety functions into the applica-

tion layer means that the object directory, as the interface to the safe application, needs to be redundant in design.

Generally, there are two possibilities for communication between devices: Application data can be merged into process data objects/PDOs (mapping) and then published via the communication system. This is achieved via the cyclical data channel in SafetyNET p. The second possibility is the SDO (service data object), which is used for acyclic data and is applied when setting control system parameters, for example.

A wide range of device profiles have been developed for CANopen. For example, profiles for digital and analogue I/O devices or drives. By using the CANopen application layer it is possible to use these in SafetyNET p.



CANopen object directory.

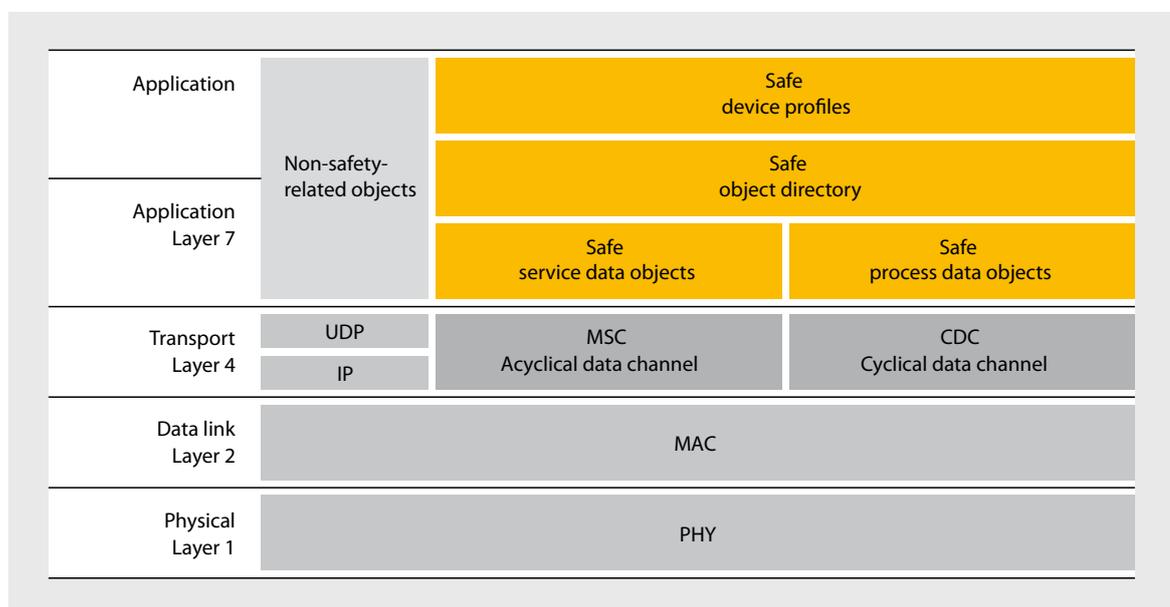
▶ 5.3 Safe Ethernet communication with SafetyNET p[®]

5.3.6 Safe communication via SafetyNET p

SafetyNET p can also communicate safety-related data through an integrated safe communication layer. The security mechanisms are designed to meet up to SIL3 of IEC 61508. The safety-related data is sent encapsulated within SafetyNET p telegrams. As a result, all other network components such as switches or cable may be standard Ethernet components, which have no impact on safety. Even non-safety related network subscribers such as PCs or standard control systems, for example, have no impact on safety-related communication. As a result it is possible to mix the operation of safety and non-safety-related devices within a network. On SafetyNET p, safety-related objects are stored in a safe object directory, similar to the CANopen object directory.

5.3.7 Safe communication in the OSI reference model

On SafetyNET p, the safe application layer is implemented in Layer 7, the application layer of the OSI reference model. Cyclical, safety-related objects are communicated via safe process data objects (SPDO). SPDOs are mapped on the cyclical data channel, the CDCN, and sent in defined intervals. When necessary, acyclical, non-time-critical safety-related data is sent as SSDOs (safe service data objects) via the MSCN (Message Channel).



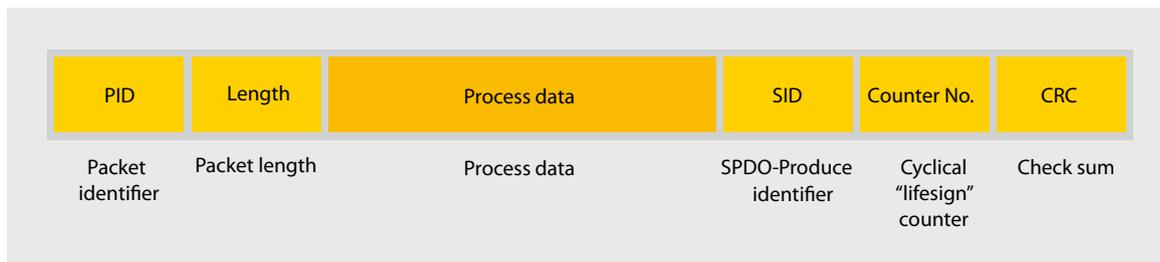
Safety layer in the OSI reference model.

▶ 5.3 Safe Ethernet communication with SafetyNET p[®]

5.3.8 Safe telegram structure

Cyclical data in SafetyNET p is communicated as safe PDOs (SPDOs) and has the following format:

- ▶ PID (Packet Identifier): Used with the SID for unique data packet identification
- ▶ Length: Complete length of packet in bytes
- ▶ Process data: Safe process data
- ▶ SID (Safe ID): 16 bit unique network-wide ID, through which both the sender and the SPDO are uniquely identifiable
- ▶ Counter No.: 8 bit cyclical counter for life sign monitoring on subscribers
- ▶ CRC: 32 bit check sum covering the whole safe data packet



Safe PDO message.

5.3.9 Safe communication in distributed control systems

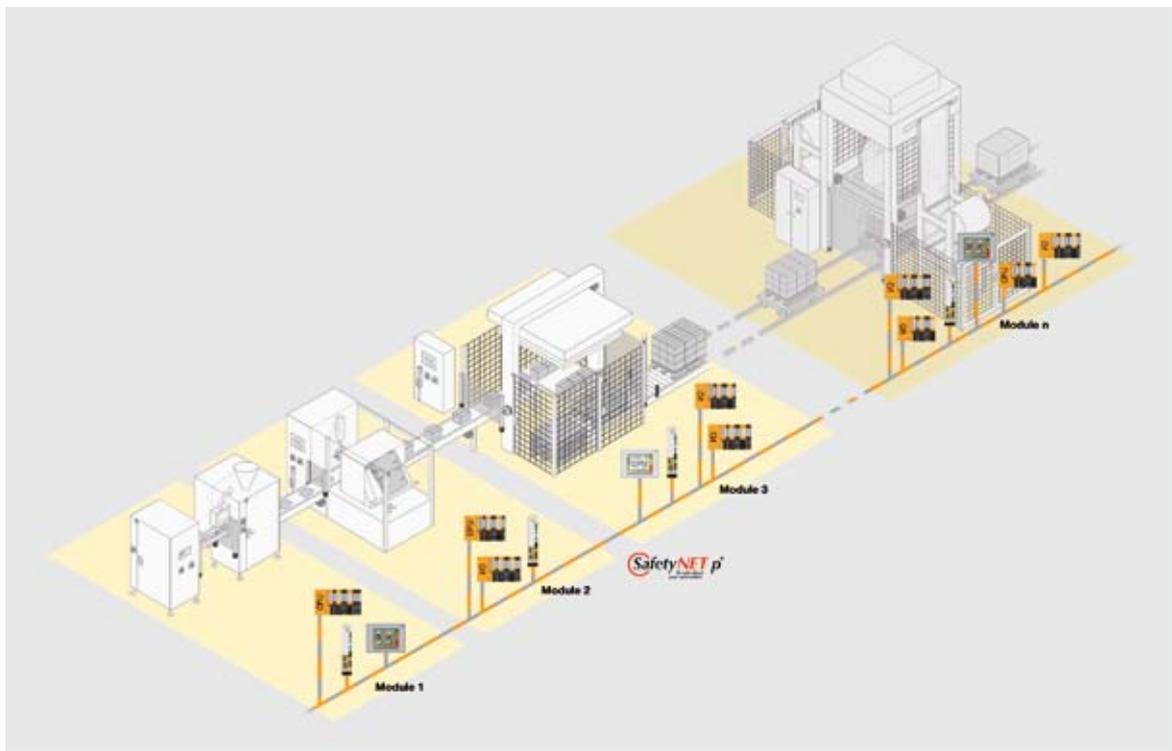
The publisher/subscriber communication principle is used universally on SafetyNET p. To enable the publisher/subscriber approach to also be used for safe communication, some new security mechanisms have been developed for SafetyNET p. For example, telegram delays can be managed by a runtime measurement initiated by the receiver. The advantage over previous standard solutions is that the transmitter of the message does not need to know the receiver. So the publisher/subscriber approach can also be applied in safety technology, which enables distributed, safe control systems.

▶ 5.3 Safe Ethernet communication with SafetyNET p[®]

5.3.10 Application example of a modular machine design

Plant and machinery are becoming increasingly modular. This means that they are being segregated into mechatronic units with separate functions. In a concept such as this, the electrical engineering follows the mechanical structure of the machine, bringing wide-ranging benefits. Once the machine modules have been developed they can be reused in various machines, which ultimately reduces the development effort. Modules can also be manufactured separately and joined together only during final assembly. What's more, modules can be developed in isolation from each other, so tasks can be run in parallel, saving time during development.

This type of engineering follows the building-block principle and enables customised solutions to be implemented at lower cost. Current fieldbus systems prevent this modular approach, as they are mainly based on a centralised master/slave approach. In safety technology in particular, one central instance is usually available: the Master. The publisher/subscriber communication principle applied universally on SafetyNET p does not use a central instance, thereby enabling a modular machine design.



Modular machine design.



6

Safe motion

▶ 6 Safe motion

Chapter	Contents	Page
6	Safe motion	6-3
6.1	Definition of safe motion	6-3
6.2	Basic principle	6-4
6.2.1	Safe isolation of the motor from the energy supply	6-4
6.2.2	Safe motion monitoring	6-6
6.2.3	Safe limit value specification	6-9
6.3	Standard EN 61800-5-2	6-10
6.4	Safety functions	6-12
6.4.1	Stop functions and their standard reference	6-12
6.4.2	Safety functions in accordance with EN 61800-5-2	6-12
6.5	System examination	6-22
6.5.1	Drive electronics	6-23
6.5.2	Motor	6-24
6.5.3	Safe logic	6-24
6.5.4	Safe braking	6-25
6.5.5	Motion monitoring	6-25
6.5.6	Motion control	6-26
6.5.7	Implementation examples	6-26
6.6	Examples of safe motion	6-28
6.6.1	Performance level of safety functions	6-28
6.6.2	Reaction times of safety functions	6-42

▶ 6.1 Definition of safe motion

Safe drive functions have recently made their mark on standards, products and applications and today can be considered as state of the art. They are part of the functional safety of plant and machinery and, as measures that boost productivity, are increasingly gaining ground in the market. The protection of machinery and equipment is also increasing in importance alongside personal protection.

When you examine the application of the failsafe principle within classic safety functions, initiation of the safety function causes the outputs to shut down, and this is called a “safe condition”. If safe drive functions are used, an application may look like this: When a safety gate is opened, the motor is braked safely with a defined ramp and then remains at standstill under active control. The motor will then move in jog mode at safely reduced speed. In other words: If static detection zone monitoring has been violated, production can continue at a reduced number of cycles and with safely monitored movements.

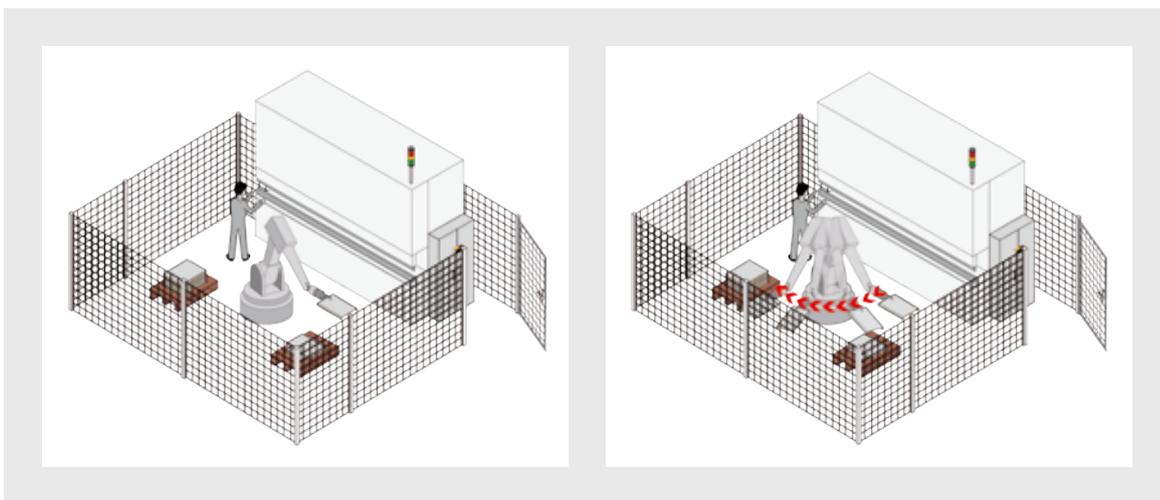
What this simple example illustrates is the transition from static to dynamic safety. Dynamic means something different in the various disciplines. In safety technology, dynamic is understood to be the ability to adapt the safety functions to the

changing detection zones. The functional safety requirements for variable speed drives specified in EN/IEC 61800-5-2 open up new horizons on this issue.

The main requirements of safe drive systems in terms of dynamic safety are:

- ▶ Safe monitoring of kinematic variables such as acceleration, speed, distance, for example
- ▶ Short reaction times to reduce stopping distances
- ▶ Variable limit values, which can be adapted to suit the runtime

Drive-integrated safety technology, fast, safe drive buses, high-performance programmable safety systems and safe camera systems are all products suitable for high-end safety solutions. The term “safe motion” is interpreted differently, depending on your perspective. Drive manufacturers generally understand safe motion to be drive-integrated safety, whereas control manufacturers associate it with external solutions. Looking at the issue analytically we can establish that the term “safe motion” only refers in the first instance to the implementation of a safe movement.

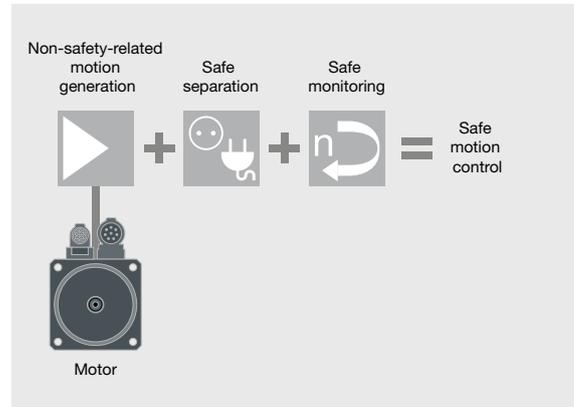


Comparison of static and dynamic safety.

▶ 6.2 Basic principle

The objective of safety technology has always been to prevent potentially hazardous movements. Nothing, then, is more obvious than to dovetail safety technology with motion generation. For technical and economic reasons, the drive electronics – servo amplifiers and frequency converters – have remained non-safety-related components within automation. So safety is guaranteed through additional safe components, which bring the drive to a de-energised, safe condition in the event of a fault, or safely monitor the movement of the connected motor. The current market trend is to integrate these safe components into the drive.

In accordance with the current state of the art, a safe motion controller is a combination of safe motion monitoring, safe isolation of the motor from the energy supply and non-safety-related motion generation.

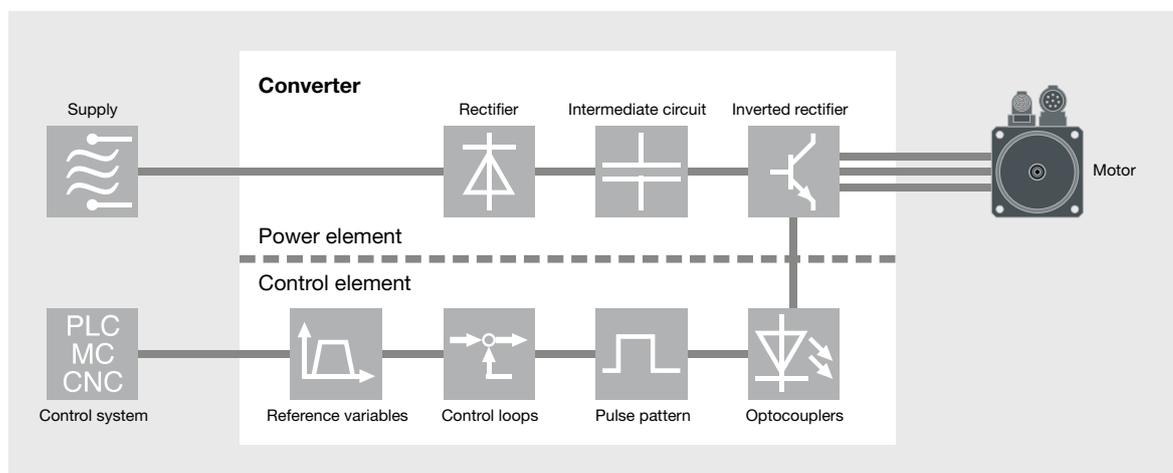


Components used in safe motion control.

The following details refer to three-phase drive systems, as currently used in an industrial environment. To apply them to other actuator systems (e.g. DC drives, servo valves, ...) is only possible under certain conditions and needs to be examined separately.

6.2.1 Safe isolation of the motor from the energy supply

Before explaining the different shutdown paths on a converter it's necessary to understand the fundamental mode of operation.



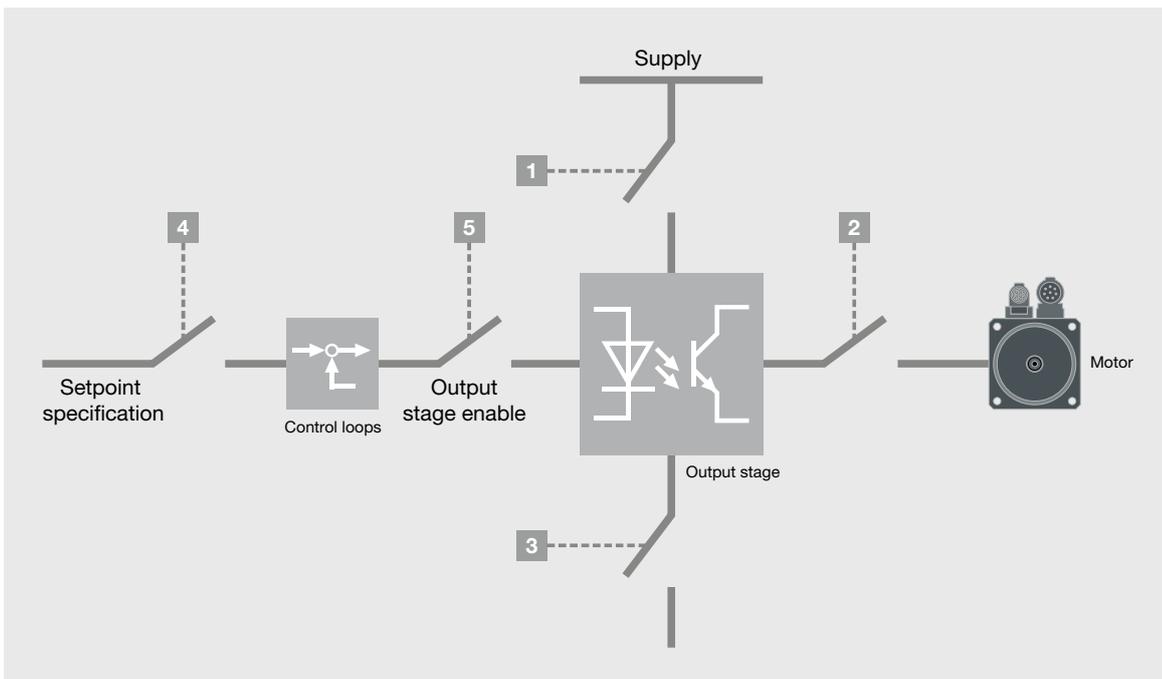
Converter's fundamental mode of operation.

▶ 6.2 Basic principle

Internally a converter is divided into a control element and a power element. Both elements are galvanically isolated from each other via optocouplers. The power element is where the power fed in from the mains is prepared. A terminal voltage with variable amplitude and frequency is generated from the mains voltage and its constant amplitude and frequency. First of all, the sinusoidal mains voltage in the rectifier is converted into a pulsating DC voltage. This is smoothed through a downstream capacitor – also known as an intermediate

circuit. The intermediate circuit is also used to absorb the braking energy. The inverted rectifier then generates an output voltage with sinusoidal fundamental wave through cyclical switching of positive and negative intermediate circuit voltages. The converter's control element uses reference variables to generate pulse patterns, which are used to drive the power semiconductors on the inverted rectifier module. There are several shutdown paths that can be used to isolate the motor from the energy supply:

Shutdown path	Device	Technology
1 Mains isolation	Mains contactor	Isolation of supply voltage to the converter
2 Motor isolation	Motor contactor	Isolation of the motor terminal voltage
3 Drive-integrated isolation	Safe pulse disabler	Isolation of the control signals to the power semiconductors
4 Isolation of reference variable	Setpoint setting to zero	Control system does not generate control variables (processor-based)
5 Isolation of control variable	Control enable	No control signals are generated for the power semiconductors.



Converter's shutdown paths.

▶ 6.2 Basic principle

If the energy supply is isolated via the mains or motor, the mains or motor contactor must have positive-guided contacts. If the N/C contact is linked to the start signal on the converter, an error on the contactor contact will be detected. The highest category can be achieved if two contactors are connected in series and each is fed back to the N/C contacts. The disadvantage of mains isolation is that the intermediate circuit capacitor on the power element is discharged each time power is isolated and must be recharged when restarting. This has a negative impact on restart time and machine availability and also reduces the service life of the intermediate circuit capacitors, because the charge/discharge processes accelerate ageing of the capacitors.

If the motor was isolated, the intermediate circuit would stay charged, but disconnecting the motor cable for wiring the contactor is a very complex process, so it is only rarely used in practice. Also, the use of motor contactors is not permitted on all converters. Potential overvoltages when isolating the contacts may damage the inverted rectifier. If there is a frequent demand to isolate the energy supply as a safety function, there will also be increased wear on the positive-guided contacts on the mains or motor contactor. Isolation of the reference variable (setpoint specification) or control variable (output stage enable) can be combined with the above shutdown paths. As the setpoint specification and output stage enable are frequently processor-based functions, they may not be used in combination, so that common cause failures are excluded.

The drive-integrated solution is based on the principle that the pulse patterns generated by the processor are safely isolated from the power semiconductors. On the drive systems examined in this case, motor movement results from an in-phase supply to the winding strands. This must occur in such a way that the overlap of the three resulting magnetic fields produces a rotating field. The interaction with the moving motor components creates a force action, which drives the motor. Without the pulse patterns, no rotating field is created and so there is no movement on the motor. The optocouplers, which are used for galvanic isolation between the control and power element within a converter, are ideally suited as a shutdown path. For example, if the anode voltage of the optocoupler is interrupted and combined with the isolation of the control variable (control enable) mentioned previously, motor movement is prevented through two-channels.

6.2.2 Safe motion monitoring

Motion is described through the kinematic variables acceleration, speed and distance. As far as potential hazards are concerned, torques and forces also play a key role. The above variables are covered by the safety functions listed in the standard EN/IEC 61800-5-2. The implementation of safety-related monitoring is heavily dependent on the sensor technology used within the system. The sensor technology used within the drive technology is generally not safety-related and must be monitored for errors. For example, a critical status would occur if the rotary encoder was unable to supply a signal due to a defect, while power is applied to the motor and it is accelerating.

▶ 6.2 Basic principle

Moved axes in safety-related applications need redundant positional information in order to carry out relevant safety functions. There are various ways to obtain independent position values: One possibility is to detect the defect through a second encoder. In this case, a safe component would have to monitor both encoders and guarantee that the plant is switched to a safe condition if an error occurs. Sometimes the advantage of this solution is that the two encoder systems detect the movement at different points on the machine and so can detect defective mechanical transmission elements.

Rotary encoders generally have several signal tracks, enabling them to detect direction or defined positions within a revolution, for example. These signals can also be consulted for feasibility tests, so that a second encoder system is not required. However, this is not a universal dual-channel structure as the movement is recorded from a shaft or lens. Dual encoder systems are also now available on the market. Such systems are suitable for functions such as safe absolute position. With

a strict, diverse, dual-channel design it is even possible to achieve SIL 3 in accordance with EN/IEC 61508. In addition to an optical system, a magnetic sensing system may also be used, for example. In terms of costs, however, an increase by a factor of two to three is to be expected compared with a non-safety-related encoder system.

Multi-turn encoders offer a more economical solution; they set their separate multi-turn and single-turn tracks in proportion and can therefore detect errors. In this case, safety-related pre-processing takes place within the encoder system itself. Another option is to use motor signals: By recording voltages and/or currents, calculations can be used to indicate the mechanical movement of the motor. A comparison with the encoder signals will uncover any dangerous failures.

Encoder signal	Description
	Initiator signal: generated by scanning a cam or cogwheel, analogue signal with TTL, 24V level.
	Two analogue signals, 90° out of phase, either square or sinusoidal (level: TTL, 24V, 1Vss).
10101	Digital interface, which transmits coded positional information (SSI, fieldbus).
10101 sin  cos 	Digital motor feedback interface with additional analogue signals (EnDat, Hiperface, BiSS).
10101 CRC	Safe digital interface, which transmits coded positional information (SafetyNET p, CANopen Safe, PROFIBUS and PROFINET with PROFIsafe, ...).

Standard encoder interfaces

▶ 6.2 Basic principle

Encoder system	Description	Safety integrity
<p>Standard encoder</p>	Evaluation of two signal tracks on a common lens.	Low
<p>Two encoders</p>	Two totally separate channels, expensive.	Very high
<p>One encoder and initiator</p>	Two totally separate channels, expensive, imprecise.	Average
<p>Safe encoder</p>	Two independent encoder systems in one housing, without safe pre-processing.	High
<p>Safe encoder</p>	Two independent encoder systems in one housing, with safe pre-processing.	High
<p>Safe encoder</p>	Dual-channel diverse structure in one encoder housing, with safe pre-processing.	High
<p>Standard encoder and motor signals</p>	Two totally separate and diverse channels.	Very high

Encoder systems for safety-related applications.

▶ 6.2 Basic principle

6.2.3 Safe limit value specification

Safe motion monitoring requires not just safe motion detection but also the opportunity to specify limit values safely. The way in which this is achieved depends on the level of dynamics and the flexibility within the machine.

Limit values	Description	Dynamics
Constant	Fixed during commissioning and cannot be amended during operation.	-
Selectable	Possible to select/change the appropriate value from a fixed set of limit values during operation.	0
Dynamic	Limit values are calculated and adjusted during operation.	+

Dynamic and static limit values.

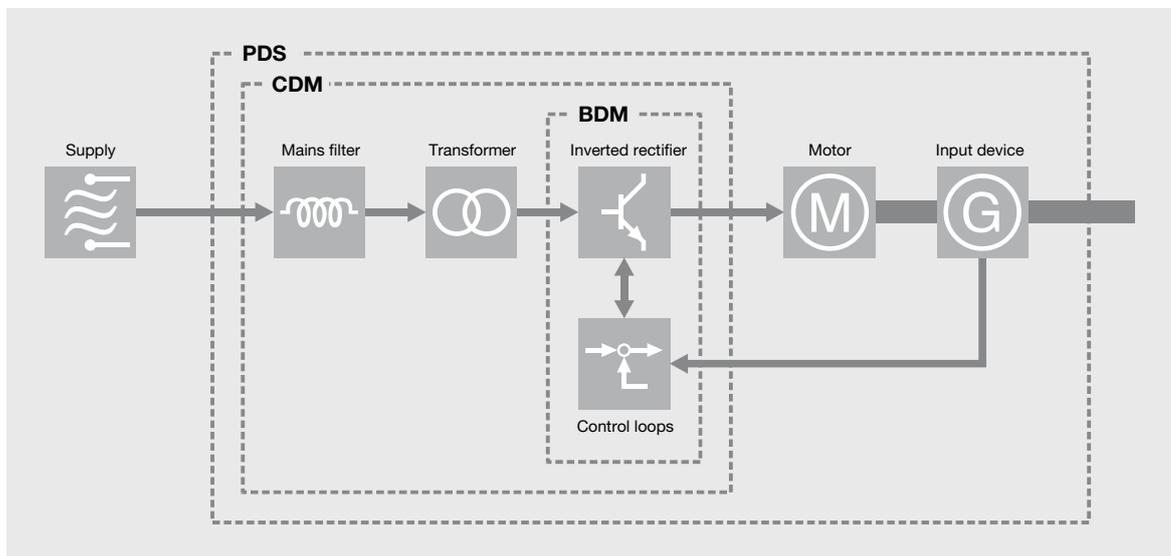
Relay-like systems often use constant limit values. For example, a fixed limit value can be defined by setting jumpers or via other setting options on the device. On safe control systems, multiple limit values can be defined via configuration or programming user interfaces. Selection can be made during operation via a safe I/O interconnection, through evaluation of sensor signals or through specification via a safe fieldbus, for example. Dynamic limit values can only be used in conjunction with a powerful, safe control system or a safe bus system with real-time capabilities. When combined with optical monitoring of the protected field in robot applications, for example, safe speed can be reduced based on the distance of the operator from the danger zone: The closer the operator comes to the danger zone, the slower the motors move.

▶ 6.3 Standard EN 61800-5-2

Adjustable speed electrical power drive systems – Part 5-2: Safety requirements. Functional: Part 5-2 of the standard series EN 61800 is a product standard for electrical drive systems with integrated safety functions. It defines the functional safety requirements for developing safe drives in accordance with the standard EN/IEC 61508. It applies to adjustable speed electrical power drive systems, as well as servo and frequency converters in

general, which are dealt with in other parts of the standard series EN 61800.

EN 61800-2 Part 2: General requirements - Rating specifications for low voltage adjustable frequency a.c. power drive systems, lists a series of new terms, which are explained in greater detail below:



Definition of a power drive system (PDS)

Power drive system (PDS)

System comprising power equipment (power converter module, AC motor, feed module, ...) and control equipment. The hardware configuration consists of a complete drive module (CDM) plus a motor or motors with sensors, which are mechanically connected to the motor shaft (the driven equipment is not included).

PDS/Safety-related (SR)

AC power drive system for safety-related applications.

Complete drive module (CDM)

Drive system without motor and without a sensor connected mechanically to the motor shaft; it comprises, but is not limited to, the BDM and expansions such as the feed module and auxiliary equipment.

Basic drive module (BDM)

Drive module consisting of a power converter module, control equipment for speed, torque, current, frequency or voltage and a control system for the power semiconductor components, etc.

▶ 6.3 Standard EN 61800-5-2

Manufacturers and suppliers of safe drives can demonstrate the safety integrity of their products by implementing the normative provisions of this part of EN 61800. This enables a safe drive to be installed into a safety-related control system by applying the principles of EN/IEC 61508, its sector standards (e.g. IEC 61511, IEC 61513, IEC 62061) or EN ISO 13849.

This part of EN 61800 does NOT define any requirements for:

- ▶ *The hazard and risk analysis for a specific application*
- ▶ *The specification of safety functions for this application*
- ▶ *The assignment of SILs to these safety functions*
- ▶ *The drive system, with the exception of the interfaces*
- ▶ *Secondary hazards (e.g. through failures within a production process)*
- ▶ *Electrical, thermal and energy safety considerations covered in EN 61800-5-1*
- ▶ *The manufacturing process of the PDS/Safety-related (SR)*
- ▶ *The validity of signals and commands for the PDS/Safety-related (SR)*

▶ 6.4 Safety functions

6.4.1 Stop functions and their standard reference

Stop functions are found on almost all machines. EN 60204-1 defines 3 categories of stop function for the various functional requirements:

- ▶ Stop category 0
- ▶ Stop category 1
- ▶ Stop category 2

A category 0 stop leads to an immediate removal of power to the machine actuators. Activation of the mains isolating device automatically triggers a category 0 stop, as power is no longer available to generate the movement. With a category 1 stop, power to the actuators is maintained to enable a controlled stop. Stop category 2 is used if power is required even in a stop condition, as power is maintained after the controlled stop. These stop categories should not be confused with the categories in accordance with EN ISO 13849-1, which categorise structures with a specific behaviour in the event of an error. For speed-controlled drive systems, EN 61800-5-2 assigns stop functions to the stop categories listed in EN 60204-1.

EN 60204-1	EN 61800-5-2
Stop category 0	Safe torque off (STO)
Stop category 1	Safe stop 1 (SS1)
Stop category 2	Safe stop 2 (SS2)

6.4.2 Safety functions in accordance with EN 61800-5-2

Today's state-of-the-art technology enables stop functions to have a drive-integrated solution. This solution reduces the space requirement in the control cabinet and also the amount of wiring necessary, as additional external components required in the past, such as contactors, are now superfluous. Even additional components to monitor standstill or speed are now surplus to requirements. Servo amplifiers with integrated safety functions in accordance with EN 61800-5-2 are now available, providing much simpler solutions, even for complex safety requirements. The standard EN 61800-5-2 divides safety functions into stop functions and miscellaneous safety functions. The description is only rudimentary and allows a great deal of freedom in how it is implemented and interpreted. This is particularly evident with the stop functions, which are among the most complex of safety functions. The implementation method can vary greatly, but so too can the external behaviour of the safety functions.

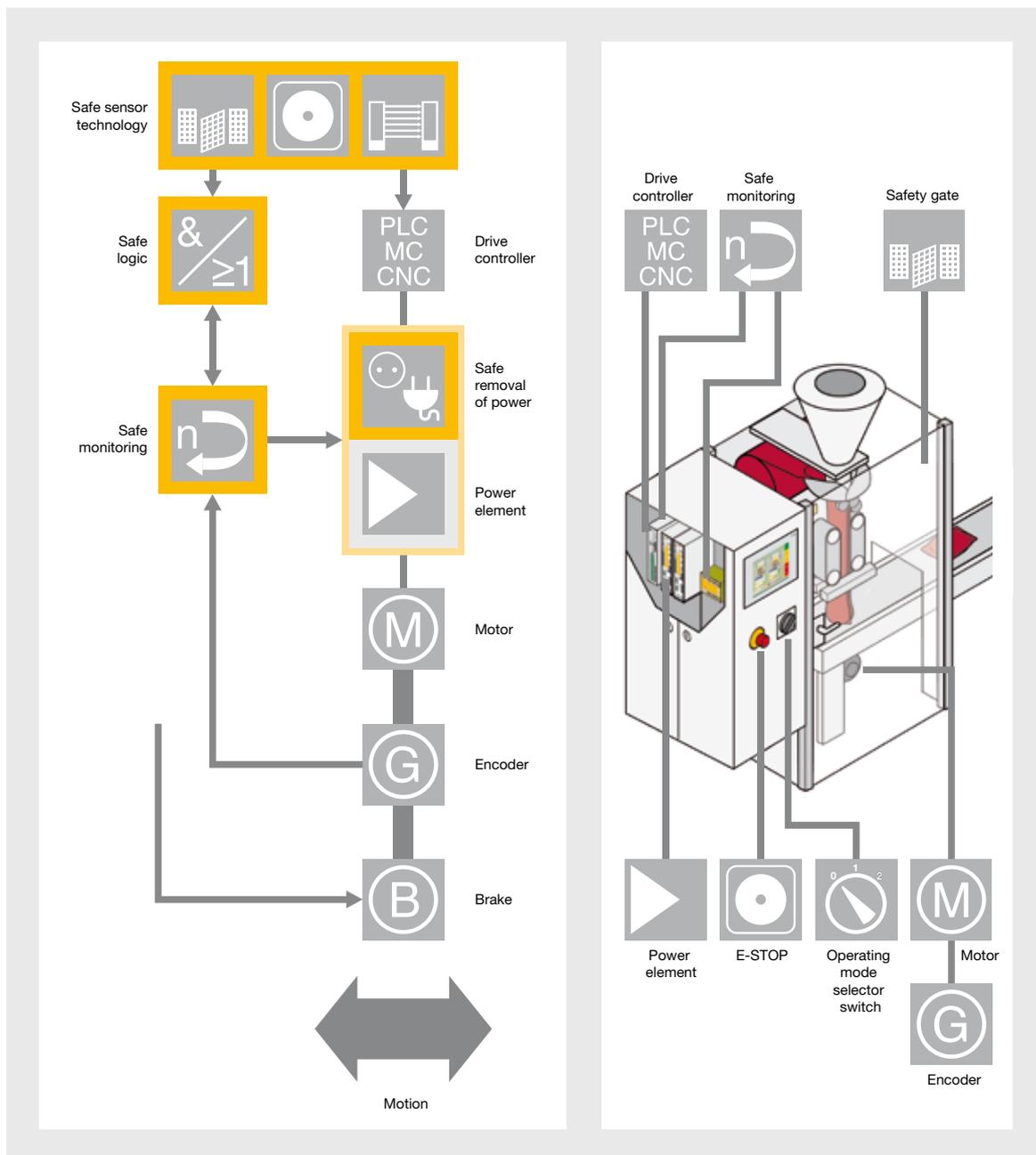
When the safety functions are operated in practice, subsequent effects can often be attributed to the poor quality of the sensor signals or to the actual behaviour of an electrical drive in general. Poorly tuned control loops and EMC are frequently the cause of restricted availability of safe drive axes. One example of this is the definition of standstill: On a closed loop system, zero speed is more of a theoretical value. Depending on the quality of the control loops, some jitter may be observed around the zero position; if the limit value was set to zero, this would immediately trigger a reaction on account of a limit value violation. The safety function would shut the drive down safely – at the expense of system availability. In this case, it helps to define a standstill threshold > 0 , where the permitted speed is still non-hazardous. An alternative is to define a position window, from which the motor may not deviate. In this case, even the slightest movements would not lead to a limit value violation.

▶ 6.4 safety functions

To guarantee the security of the manufacturing and production process as well as the safety of personnel, safety functions may also be permanently active, without the requirement of the plant remaining in a special operating mode. Several components and their respective interfaces must be considered in order to implement the safety

functions; the whole safety chain must be considered when calculating the required safety integrity.

It is not mandatory for the safety functions listed in EN 61800-5-2 to be implemented using drive-integrated safety. An external solution may also be used.



Safety chain.

▶ 6.4 Safety functions

6.4.2.1 Safe stop functions

When considering safety on axes, the main factors are to prevent the axes from starting up unexpectedly and to shut down moving axes safely in the case of danger. The corresponding functions are summarised here under the heading of “Safe stop functions”.

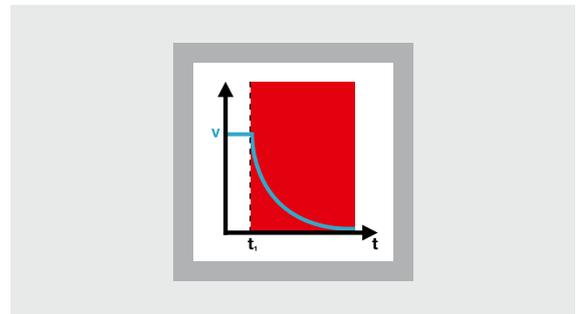


Safe stop functions

Safe torque off (STO)

The power to the motor is safely removed, so that no further movement is possible. It is not necessary to monitor standstill. If an external force effect is to be anticipated, additional measures should be provided to safely prevent any potential movement (e.g. mechanical brakes). Classic examples are vertical axes or applications with high inertia. This safety function corresponds to a category 0 stop (uncontrolled stop) in accordance with IEC 60204-1. If the function is triggered during operation, the motor will run down in an uncontrolled manner, which is not desirable in practice. That is why this function is generally used as a safe reset lock or in conjunction with the safety function SS1.

Modern servo amplifiers include an integrated safe shutdown path, so safe devices are now available that prevent unexpected start-up and shut down safely in the case of danger.



Safe torque off

▶ 6.4 Safety functions

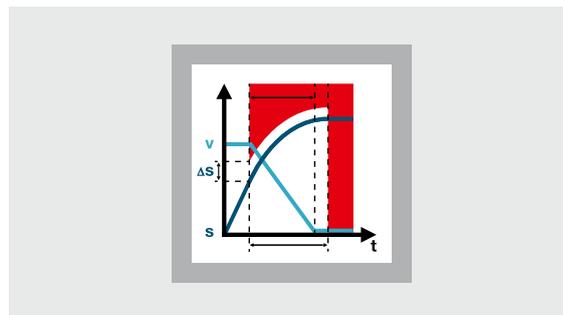
Safe stop 1 (SS1)

With safe stop 1 (SS1), defined motor braking is part of the safety function. When the motor is at standstill, the STO function is triggered. There are various options for implementing these requirements; the key factor is the dovetailing of safety

technology and drive technology. This safety function corresponds to a category 1 stop (controlled stop) in accordance with IEC 60204-1.

Implementation	Description
Monitored time delay	Triggering of the safety function starts an application-specific, safe time delay, after which the power is safely removed from the motor. Motor braking is a function of the non-safety-related drive technology. Should the motor accelerate during this time delay, it will not be detected.
Automatic standstill detection with monitored time delay	The monitored time delay is combined with standstill detection. If the motor reaches standstill before the time delay has elapsed, the STO function will be triggered. Here too, motor acceleration during the time delay will not be detected.
Monitoring of the braking ramp	A monitored braking ramp provides the highest quality in terms of functional safety. During the braking process, values are continuously compared with a limit value or a permitted drag error. If the limit value is violated, the STO function is triggered.

In many applications, drives cannot simply be shut down because they would then run down slowly, which could cause a hazard. Also, an uncontrolled run down of this type often takes considerably longer than controlled axis braking. The safe stop 1 function (SS1) monitors controlled braking of the axis directly within the servo amplifier. Once the set braking ramp has run its course, the drive is shut down safely. The reaction times are reduced compared with external monitoring solutions; as a result, in many cases the safety distances to the danger points can also be reduced. This provides a number of benefits, such as improved ergonomics for the plant operator, space savings due to the reduced distance between the guards and the danger points and, last but not least, cost savings.



Safe stop 1

▶ 6.4 Safety functions

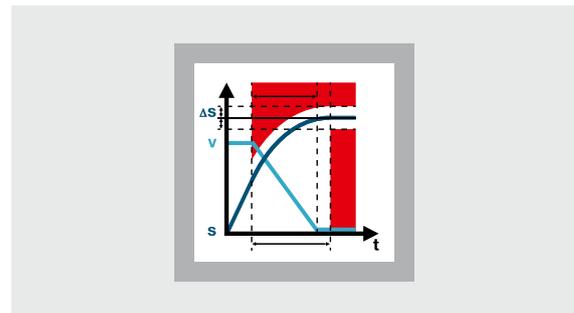
Safe stop 2 (SS2)

With safe stop 2 (SS2), defined motor braking is again part of the safety function. When the motor is at standstill, a safe operating stop (SOS) is triggered. Unlike safe stop1 (SS1), the motor at standstill is in closed loop operation. This means that the standstill position is held precisely, due to the

active control loop. Again, there are several options for implementing these requirements. This safety function corresponds to a category 2 stop (controlled stop) in accordance with IEC 60204-1.

Implementation	Description
Monitored time delay	Triggering the safety function starts an application-specific, safe time delay, after which a safe operating stop is triggered. Motor braking is a function of the non-safety-related drive technology. Should the motor accelerate during this time delay, it will not be detected.
Automatic standstill detection with monitored time delay	The monitored time delay is combined with standstill detection. If the motor reaches standstill before the time delay has elapsed, the safe operating stop will be triggered. Here too, motor acceleration during the time delay will not be detected.
Monitoring of the braking ramp	A monitored braking ramp provides the highest quality in terms of functional safety. During the braking process, values are continuously compared with a limit value or a permitted drag error. If the limit value is violated, the STO function is triggered, otherwise a safe operating stop will follow.

So what are the benefits of the safe stop 2 (SS2) function? If the axes no longer need to be shut down at standstill, they will actively hold their current position, so the synchronisation between axes and process is no longer lost. As a result, the axes can be restarted immediately at any time, which clearly increases plant availability. Here too, the drive-integrated function leads to shorter reaction times, thereby minimising the risks. The monitoring functions' response times have a direct influence on the potential channels available until a safety shutdown occurs. As the reaction times are used in the calculation of the safety distances, the benefits listed for the safe stop 1 function will also apply here.



Safe stop 2

▶ 6.4 Safety functions

6.4.2.2 Safe motion functions

Modern drive solutions not only examine how axes are switched on and off, but also look at the potential risks that may arise during operation of the axes. The functions employed to avoid/reduce these risks are summarised here under the heading of “Safe motion functions”.

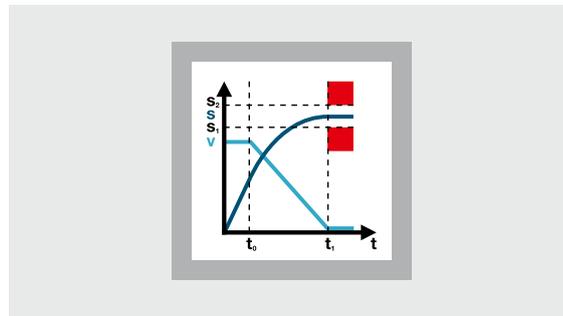


Safe motion functions

Safe operating stop (SOS)

The safe operating stop (SOS) has already been described with the safe stop2 (SS2) safety function. It monitors the standstill position while the motor is in a controlled loop status. Once the safety function has been lifted, the production or machining process can be continued with no loss of precision. This function is generally used in combination with a safe stop 2 (SS2) function, as standstill monitoring usually involves a braking process. As described above, the limit value can be specified as both a speed threshold and a position window.

Application of the safe operating stop (SOS) function is generally intended for the standstill phases of a process. A typical situation would be access to a danger point during process intervention. An operator stops production using a command such as “Stop at end of cycle”, for example. Once the plant has stopped, the safe operating stop (SOS) function is activated, after which the guard locking device on the access gate is unlocked. The plant can now be accessed without risk.



Safe operating stop

Safely limited acceleration (SLA) and Safe acceleration range (SAR)

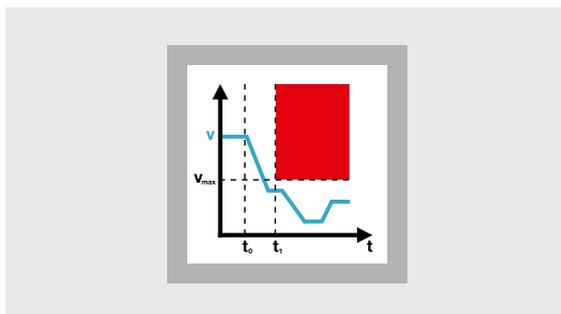
Safety functions relating to acceleration monitoring are not widely used in the current state-of-the-art technology. In servo drive technology, Ferraris sensors are used to detect acceleration only in special applications of machine tools or printing machinery. Standard drives cannot process these signals in their control loops; monitoring of these acceleration signals is very complex in practice.

▶ 6.4 Safety functions

Safely limited speed (SLS)

Safely limited speed (SLS) is probably the best known safety function. In practice, this safety function is often applied as safely reduced speed. As a result, a defined transition from the operating speed in automatic mode to the reduced speed in setup mode must be guaranteed. If the monitoring function detects that the limit value has been violated, the drive must be shut down safely. The manner in which the shutdown is achieved depends on the application; it is best to aim for defined braking using the SS1 function, followed by removal of power.

Without drive-integrated safety functions, the implementation of this function was associated with high material costs or functional restrictions. Where axes are moved in jog mode during setup, the potential axis speed in the event of an error is a key aspect of any risk analysis. Operators must be protected from any hazard that would lead to an uncontrolled axis start-up in the event of an error. When the safely limited speed (SLS) function is used for these jog functions, the solution provides the shortest possible reaction time in the event of an error. This reduces the risks to the operator significantly, as any uncontrolled axis start-up would be detected at the onset and would result in a safe shutdown.

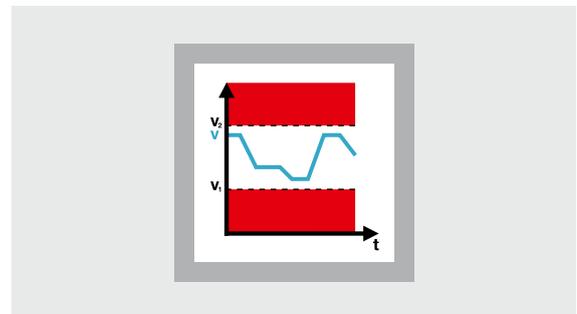


Safely limited speed

Safe speed range (SSR)

The safe speed range (SSR) can be used to monitor a safe minimum speed, for example. Again, the reaction that occurs when a value falls below the stated limit value depends heavily on the application. Drive axes may be coupled, in which case an appropriate reaction must be triggered when shutting down the drive (e.g. selective shutdown).

Safe speed range (SSR) can generally be used for permanent process monitoring. Risks cannot always be eliminated just by limiting the capacity for speeds to suddenly increase. Speeds that reduce suddenly as the result of an error can also present a risk. If axes are operating at a defined distance, a speed that drops abruptly on just one of the two axes may create a risk of crushing. These are the cases for which the safe speed range (SSR) function have been defined and developed. This function would be used to shut down the relevant axes, thereby eliminating any hazard to the machine operator.



Safe speed range

▶ 6.4 Safety functions

Safely limited torque (SLT) and safe torque range (STR)

Like acceleration monitoring, the problem with torque or force monitoring is the lack of suitable or established sensor technology. Torque measuring systems are not widely used on standard drives, but servo drive technology provides the option for indirect measurement via the motor current. The motor current is proportional to the motor's force or torque, so the hazard resulting from a hazardous movement is limited. Non-hazardous values as regards the effect of forces can be found in the limit value list 2003, in the BIA Report. Such a procedure may only be carried out via drive-integrated safety technology.

Safely limited position (SLP)

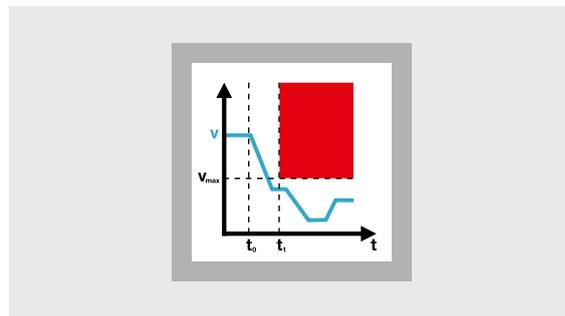
Safe position monitoring ensures that the motor does not exceed a preset position limit value. If a limit value is violated, the motor is braked using a safe stop. The stopping performance achievable from a technical point of view must be taken into account. Below the limit value there are no restrictions in terms of acceleration or speed of the motor. Absolute position detection is required for this safety function. Absolute encoders may be used or relative measuring systems may be combined with a safe reference run.

Safely limited increment (SLI)

The motor is allowed to travel a permitted distance following a start command. A safe stop function must be triggered once the limit value is reached. If the permitted distance is exceeded, this must be detected and the drive must be safely brought to a standstill. Encoder systems with relative measurement are sufficient for this safety function.

Safe direction (SDI)

This prevents the motor from moving in an invalid direction. This safety function is frequently used in combination with safely limited speed (SLS) in setup mode. Here too, the drive-integrated solution enables the fastest possible shutdown.



Safe direction

Safe cam (SCA)

A safe output signal indicates whether the motor is positioned inside a specified range. These ranges are absolute position windows within a motor rotation. The basic function involves safe monitoring of absolute positions, which is why appropriate sensor systems must be used.

Safe speed monitoring (SSM)

The safe speed monitoring safety function (SSM) is very closely related to safely limited speed (SLS). However, if a limit value is violated there is no functional reaction from the components that are monitored, merely a safe message which can be evaluated and processed by a higher level safety control system. On one side the control system can perform more complex reaction functions, while on the other, the safety function can be used for process monitoring.

▶ 6.4 Safety functions

6.4.2.3 Safe brake functions

Functions related to holding brakes and service brakes have been summarised under the heading of safe brake functions.



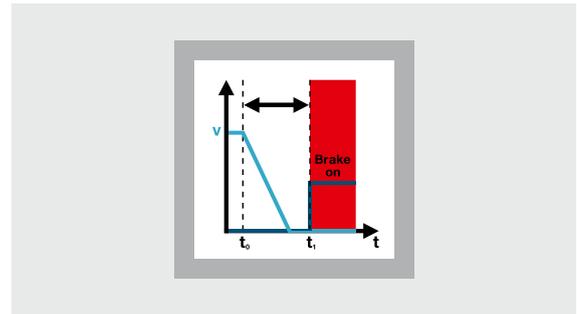
Safe brake functions

Safe brake control (SBC)

Safe brake control (SBC) supplies a safe output signal to drive an external mechanical brake. The brakes used must be “safety brakes”, in which a quiescent current operates against a spring. If the current flow is interrupted, the brake will engage. Control modules frequently include a power reduction feature when the brake is released to reduce energy consumption or brake heating. A safe brake test may be required to detect errors during operation, depending on the risk analysis.

Holding brakes and service brakes are often used on axes with suspended loads. Along with the brake, the brake drive is another key component in terms of the safety function. The safe brake

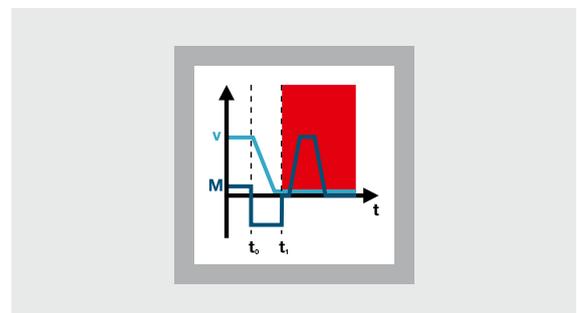
control (SBC) function is generally used to control the holding brake activated once an axis is at standstill.



Safe brake control

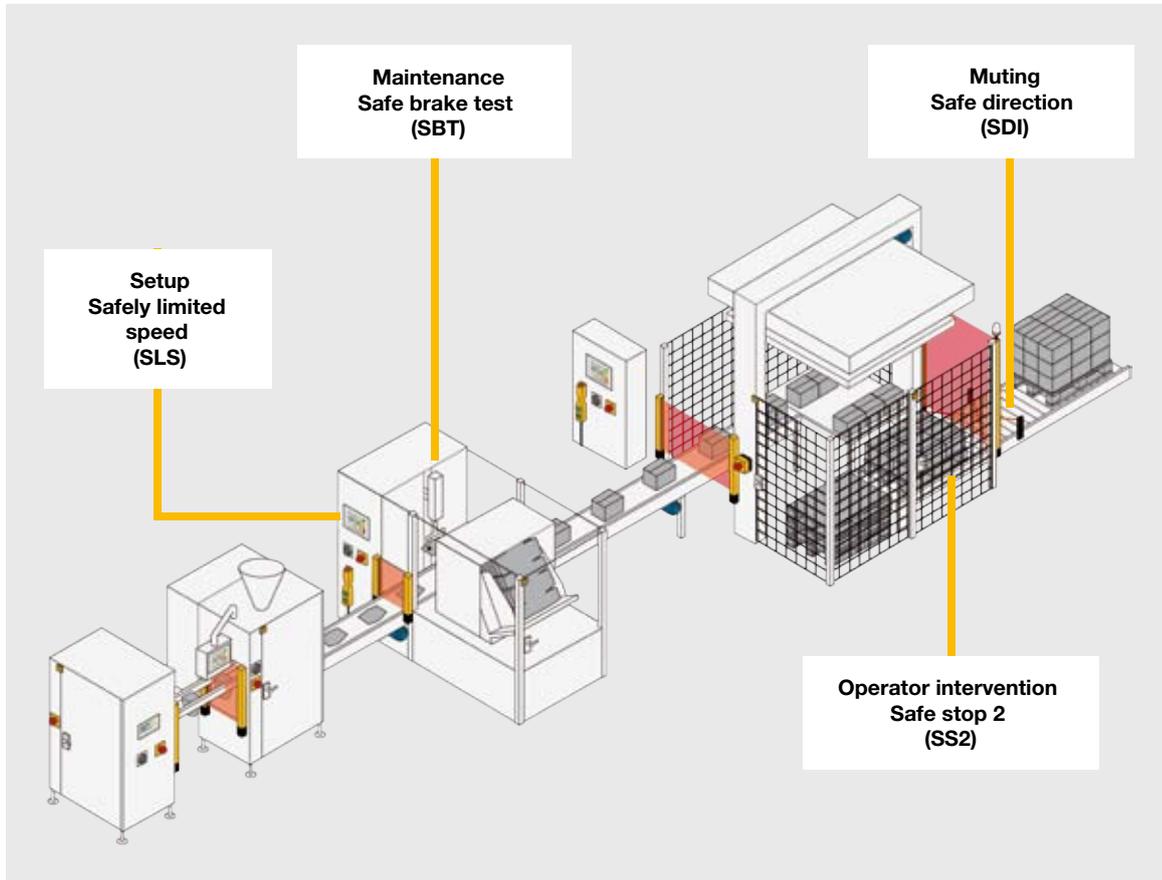
Safe brake test (SBT)

Using the safe brake test (SBT) function can significantly increase safety. In many cases, simply controlling a holding brake safely is not enough to make a vertical axis safe. If the wearing, mechanical part of the brake is not maintained regularly, it cannot be guaranteed that the holding brake will apply the designated braking action in the event of danger. The safe brake test (SBT) function provides an automatic test which replaces previous measures that could only be implemented through organisational and manual operations; if the result is negative, it can bring the plant to a standstill and signal an error. This reduces maintenance work considerably.



Safe brake test

▶ 6.4 Safety functions

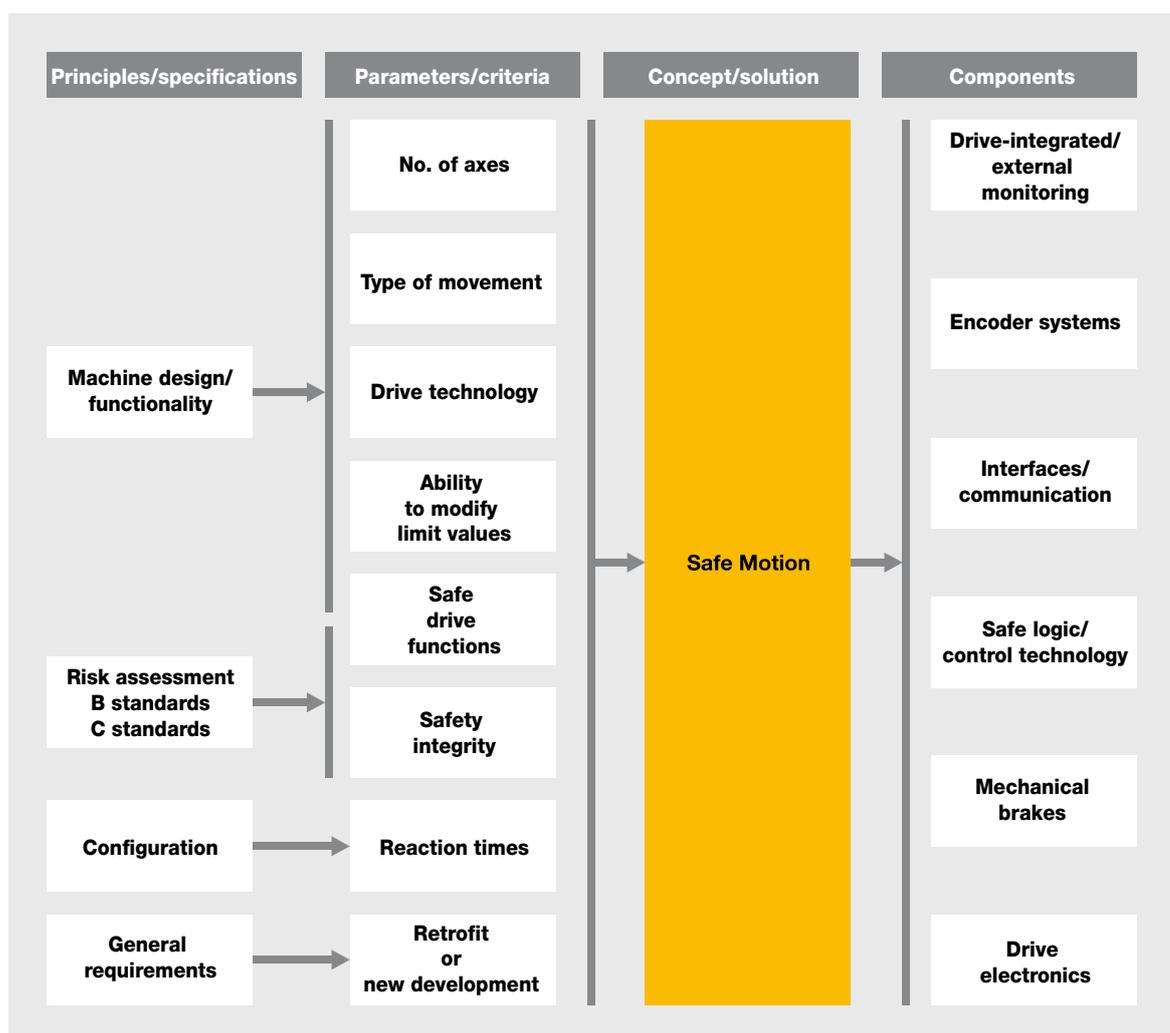


Safety functions using the example of a packaging machine.

▶ 6.5 System examination

Safe drive technology merges two issues, which individually already involve a high level of complexity. The challenge is to provide the user with transparent, comprehensible logic in the lifecycle of a safe motion application. The difficulty in configuring and selecting safe drive components is in translating the various influencing factors to the product requirements. Or

to put it another way: In selecting products for an optimum, safe drive solution, which parameters are to be derived from which specifications?



Procedure for configuring and selecting a safe drive solution.

▶ 6.5 System examination

The machine design and the functionality demanded by the end customer are essentially the factors that determine which drive technology will be used and how the machine will be operated in control technology terms. The resulting parameters are:

- ▶ How many drive axes are there?
- ▶ Does the system use servo amplifiers or frequency converters?
- ▶ Are the drives decentralised – i.e. outside the control cabinet?
- ▶ Which safe drive functions are required and how are the parameters to be set?
- ▶ Does the movement to be monitored involve an elliptical curve, synchronous drive axes or, in the simplest case, a single movement?

Specifications from the B and C standards and risk analyses will provide the safety integrity requirement (SIL and PL). These, of course, will also influence the required safety functions. The reaction times of the safe drive components are part of the overall machine design and must be fine-tuned as part of an iterative process. Factors such as stopping performance, safety distances, inertia of the moved mass or the reaction capability of the machine control system play a key role.

General requirements may be whether or not the machine is to be retrofitted with safe drive functions, for example. In some circumstances, existing components must continue to be used, a situation which will often favour an external safety solution. These criteria and parameters must be converted into a concept. The result is a safe drive solution, made up of standard market components.

6.5.1 Drive electronics

These days, modern frequency converters or servo amplifiers have an integrated safe shutdown path, through which the STO safety function can be performed. This shutdown path is generally accessible externally via a terminal pair and must be connected to 24 VDC. If the safety function is not in use, 24 VDC will be available permanently at the terminals. If the shutdown path is used as an STO or safe reset lock, the terminals must be connected to a safe output on a programmable safety system or safety relay. In this case, it is important to ensure that the test pulse on the safe output does not initiate the safety function. A countermeasure is to use an input filter with an appropriate time delay. Depending on the version, a feedback path is available for fault detection, to achieve greater safety integrity.

The benefits of a drive-integrated shutdown lie mainly in the

- ▶ Reduced wiring requirement
- ▶ Rapid restart, as the intermediate circuit remains charged
- ▶ Short reaction time (measured from the falling edge at the input to the shutdown of the optocoupler, the reaction time is in the millisecond range)

▶ 6.5 System examination

6.5.2 Motor

The relevant properties for the motor in terms of its use in safety-related systems are

- ▶ Type of movement (rotating, linear)
- ▶ Acceleration capability (inert asynchronous motor or air-borne linear drive)
- ▶ Integrated motor encoder
- ▶ Integrated holding brake incorporated into the safety concept

The motor's acceleration capability influences the system's maximum permitted overall reaction time. Highly dynamic linear motors have extremely low electrical time constants on the winding and a high overload capability, so that a multiple of the rated power is present in just a few milliseconds. Resolvers are widely used as motor encoders in servo drive technology. They are used in rotating motors and are both robust and economical. The measuring system provides an absolute position within a motor rotation, but has limited resolution due to the function principle. Only rarely can resolver signals be evaluated by safe monitoring components. For this reason, motor encoder systems with sine/cosine analogue tracks are preferable in safety-related applications with motion monitoring. Motor encoder systems with an all-digital interface can only be monitored using special manufacturer-specific safety components. Third party products cannot be connected.

6.5.3 Safe logic

Safety relays or programmable safety systems can perform the following tasks in systems with safe drive functions, depending on the application:

- ▶ Evaluation of sensors on safeguards
- ▶ Activation of safety functions
- ▶ Drive shutdown
- ▶ Evaluation of the status of safely monitored drive axes in a multi-axis system
- ▶ Establishing the plant's overall safety
- ▶ Specifying new limit values during operation
- ▶ Interface between the drive controller and the safety functions

The safe logic can be implemented either as separate, external components or as drive-integrated components. Safe logic is the interface between the sensors on the protection equipment and the safe monitoring unit. Drive-integrated solutions enable simple functions in single axis systems to be implemented economically. Sensors are connected directly on the drive and are evaluated. The limited number of safe interfaces makes cross-communication between the drives and complex logic links impossible. The cycle time of the safety control system must always be included in the assessment of the overall reaction time if pre-processing in safe logic is required in order to activate a safety function. Depending on the size of the user program, this ranges between 50 ... 200 ms and therefore dominates over the delay in the shutdown path. It's also necessary to consider a delay time on safe, digital inputs; this arises due to the input filters.

▶ 6.5 System examination

6.5.4 Safe braking

Mechanical brakes must be used if the output shafts on motors or gearboxes are affected by forces that would trigger movement when the motor was shut down. Example applications are vertical axes or motors with high inertia. The operation of vertical axes is a special case as far as safety technology is concerned. The failsafe principle – the removal of power to the drives in the event of an error – is generally applied in safety technology, but in this case it would not lead to a safe condition because falling loads present a hazard. Mechanical brakes are incorporated to rectify this; their functionality must be constantly verified using special proof tests. As with the encoder systems, various versions are available to fit the specific safety requirements. Dual channel capability can be implemented either through two independent brakes or through a brake with two separate brake circuits. The advantage of two separate brakes is that faults can be covered within the mechanical transmission elements between the drive and the process. The brake configuration depends largely on the machine design and the overall safety concept.

6.5.5 Motion monitoring

Motion monitoring has two main tasks: It must detect any violation of the limit values and then trigger an appropriate reaction function. It must also detect any potential errors on the encoder system and likewise trigger an appropriate error reaction function. Both functions are heavily linked to the availability of the drive system. Noisy signals or poorly tuned control loops can cause sensitive monitoring mechanisms to trigger reaction functions and therefore reduce plant availability. Proper screening of the motor and encoder cables is absolutely essential. The algorithms for the monitoring functions can be applied via hysteresis or filter settings. The reaction times for these components are in the millisecond range. Motion monitoring is available as both an external and a drive-integrated solution. An integrated solution has clear advantages over an external device in terms of wiring effort and convenience. Disadvantages are higher retrofitting costs for existing plants and dependence on the converter that is used. This means that the technical properties of the drive, as well as the interfaces and the performance of the safety functions, have to fit the application. With an external monitoring unit, safety functions can be implemented as standard on frequency converters and servo amplifiers of a different performance class or manufacturer.

▶ 6.5 System examination

6.5.6 Motion control

With the current state-of-the-art technology, motion control is a non-safety-related drive component. Depending on the task, the functions are either drive-integrated or are performed by an external control

system via fieldbus or drive bus. The classic allocation between the control systems depends on the required movement.

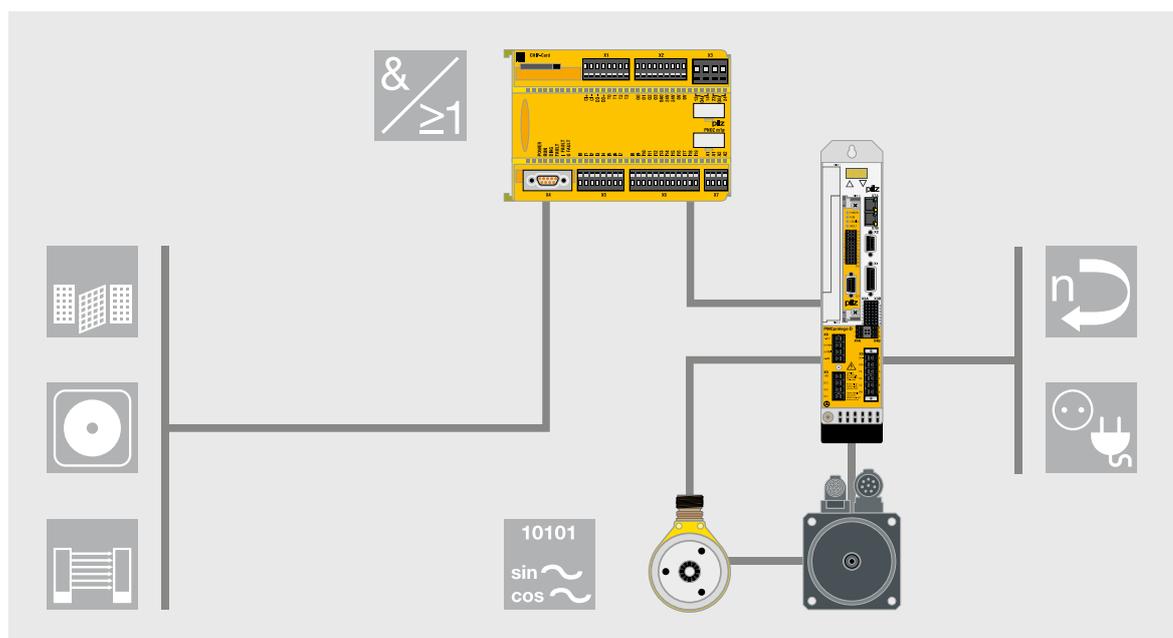
Movement	Controller	Safe motion monitoring
Positioning of a single axis	Positioning control system	Drive-integrated or external monitoring of single axis
Electronic cam disk (synchronous motion)	Motion control system	Limit value and monitoring must be examined for each drive axis. The status conditions of the individual axes are evaluated in central, safe logic.
Elliptical curve (resulting motion)	NC or RC control system	Safe, central calculation of the current position from the position of the individual axes.

6.5.7 Implementation examples

Servo converters with drive-integrated motion monitoring and safe pulse disabler for shutdown

Sensor evaluation is undertaken, for example, by a small, safety-related control system, which activates the safety functions in the drive via a safe

I/O interconnection. The servo motor has an integrated sine/cosine motor encoder for motor control and positioning. The reaction time before the safety function is activated is around 60 ms, the reaction time when limit values are violated is <10 ms.

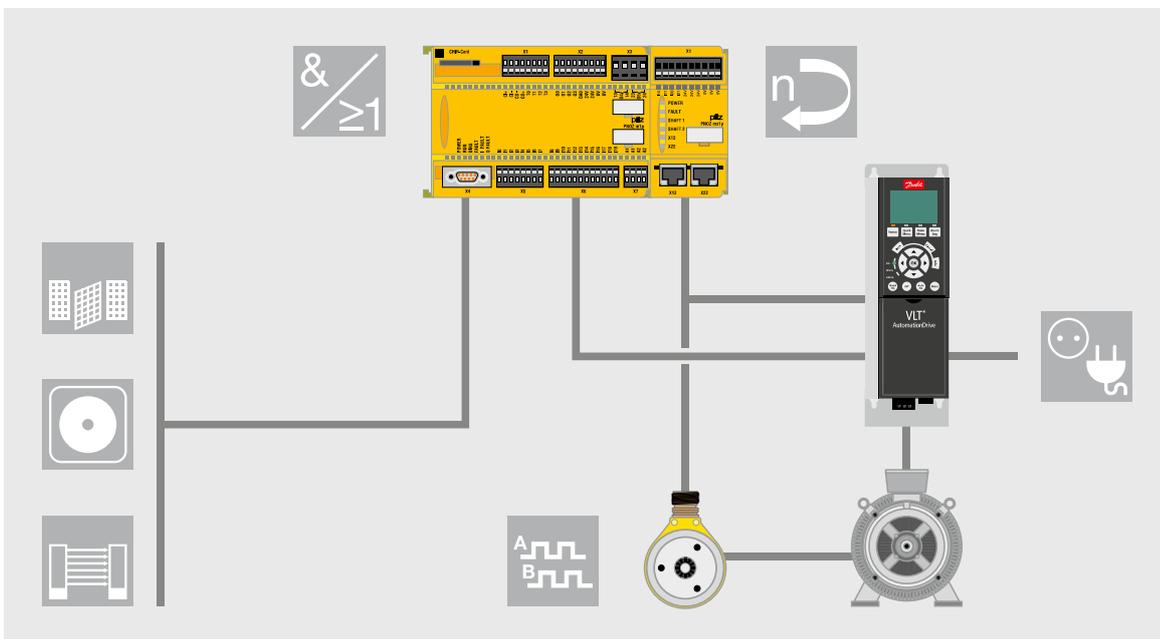


Implementation example with servo amplifier.

▶ 6.5 System examination

Safely monitored drive with frequency converter and asynchronous motor

An incremental encoder is used to detect motion. A safety relay or a small, safety-related control system with motion monitoring evaluates the sensor signals and triggers an STO function in the event of an error.



Implementation example with frequency converter.

▶ 6.6 Examples of safe motion

6.6.1 Performance level of safety functions

6.6.1.1 Normative basis

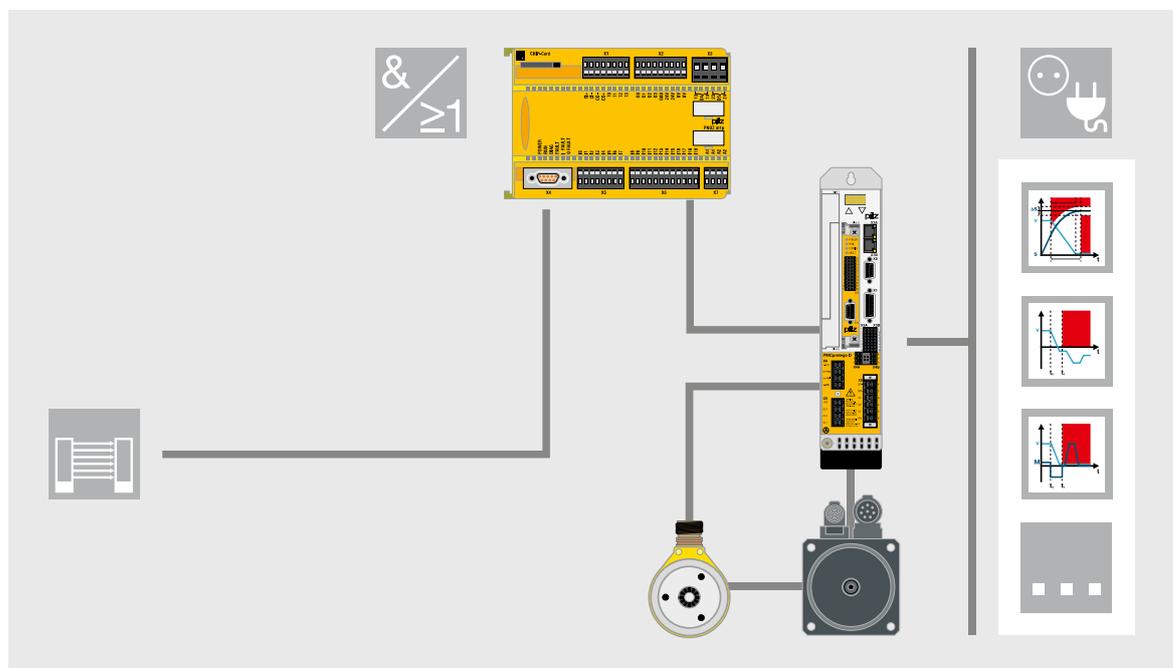
Several standards (generic safety standards and technical safety standards; type A and type B standards) are available for determining the safety level achieved by the safety-related section of a control system. EN ISO 13849-1 is generally applied in the engineering sector. For many machines, the safety level to be achieved can be taken from the respective machinery safety standards (type C standards); (e.g. presses → EN 692, EN 693; robots → EN ISO 10218-1, packaging machinery → EN 415). If there are no C standards for a product, the requirements can be taken from the A and B standards.

6.6.1.2 Safe stop function

The safety function “E-STOP when light curtain is interrupted” is addressed here by the example below; it illustrates a safe stop function for a motor-driven axis. The methodology described below is based on EN ISO 13849-1 and as such can only be applied if all the safety function subcomponents have their own performance level. Using the terminology of the standard, it is a series alignment of safety-related parts of a control system (SRP/CS).

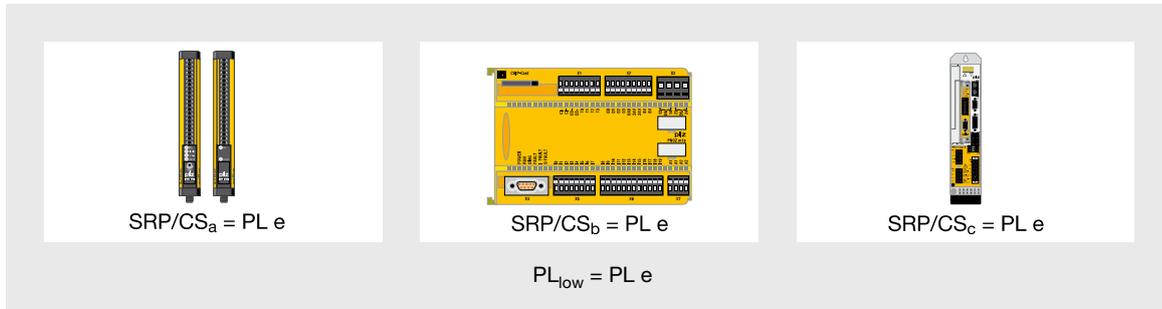
This example uses a light curtain, a configurable safety control system and a servo amplifier with integrated safety functions. A servo motor with feedback system is connected to the servo amplifier.

The risk analysis permits a stop category 1 for the axis.



Structure of the safety function.

▶ 6.6 Examples of safe motion



The block diagram shows the logical structure of the safety function, comprising the series alignment of the safety-related subcircuits.

Determination of the performance level for the overall circuit

EN ISO 13849-1: Table 11 – Calculation of PL for series connection of SRP/CS

PL_{low}	N_{low}	→	PL
a	> 3	→	None, not allowed
	≤ 3	→	a
b	> 2	→	a
	≤ 2	→	b
c	> 2	→	b
	≤ 2	→	c
d	> 3	→	c
	≤ 3	→	d
e	> 3	→	d
	≤ 3	→	e

Note: The values calculated for this look-up table are based on reliability values at the mid-point for each PL.

In the example of the safe stop function, all three components involved have performance level e. As a result, the lowest performance level of a safety-related subcircuit (SRP/CS) is also PL e. Using the standard's terminology, therefore, we have:

- ▶ 3 x SRP/CS each with PL e
- ▶ The lowest performance level of the 3 subcircuits (SRP/CS) = PL e and is assigned the parameter PL_{low}
- ▶ The lowest performance level occurs in 3 subcircuits and so the parameter $N_{low} = 3$

If you apply this information to Table 11 of the standard, the result for the example is an overall classification of PL e.

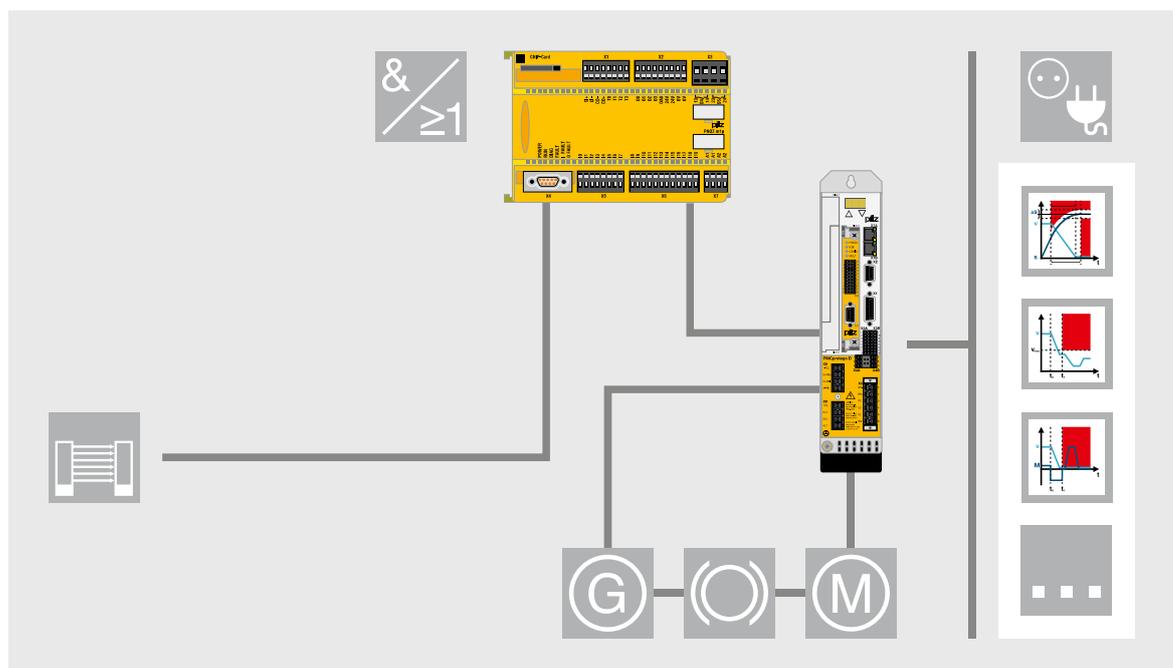
▶ 6.6 Examples of safe motion

6.6.1.3 Safe stop function on vertical axes

If you examine the potential risks on servo axes you'll see that a vertical axis is also a good example for increasing awareness of the mechatronic view. Removal of power is not enough to bring an axis to a safe condition. In many cases, the load's own weight is enough for the axis to fall. Mass and friction will determine the speed that occurs in the process. As part of the risk analysis, potential hazards are analysed in the various machine operating modes and as operators carry out their work. The required measures will then be derived from this analysis. With vertical axes, the measures that need to be taken will essentially depend on whether the

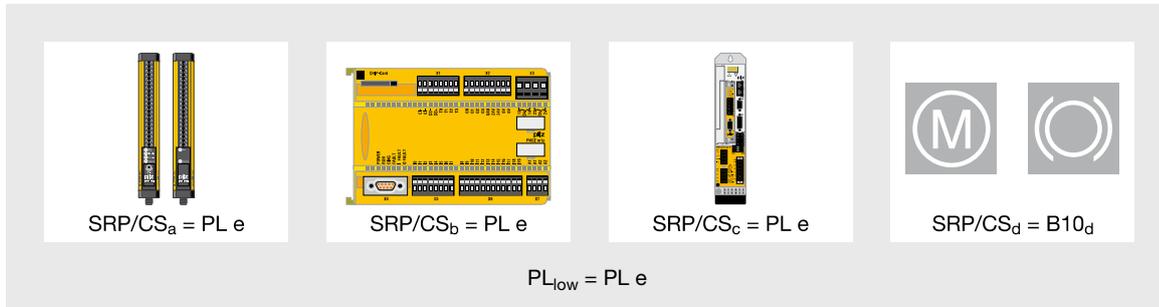
full body of the operator can pass below the vertical axis or whether just his arms and hands are positioned below the vertical axis. Another aspect is the frequency and duration of his stay in the danger zone. All these factors are added up to give the "performance level" that the safety functions must achieve.

Building on the "Safe stop function" example, a brake is added to the structure. Holding brakes and service brakes are both common.



Structure of the safety function.

▶ 6.6 Examples of safe motion



The block diagram shows the logical structure of the safety function, consisting of the series alignment of the safety-related subcircuits.

Determination of the performance level for the holding brake

Here the user of EN ISO 13849-1 is confronted with one of the positive approaches of this standard. The standard not only enables examination of the electrical part of the safety function, but also of the mechanical, hydraulic and pneumatic section.

However, the holding brake used in this example does not have a performance level, as this is only available for intelligent components. The brake manufacturer can only provide a B10_d value, as he does not know how exactly his components will be used in the application and so can only make a statement regarding the number of operations before a component failure. The design engineer constructing the safety-related part of the control system must now calculate the time to a dangerous failure of the component. The B10_d value is not the only consideration in this calculation; the mean time between two consecutive cycles is also a key factor which influences the MTTF_d value.

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

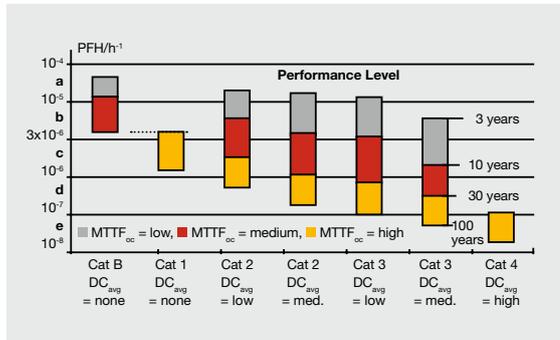
$$n_{op} = \frac{d_{op} \times h_{op} \times 3,600 \text{ s/h}}{t_{cycle}}$$

The following assumptions are made, based on the application of the component:

- ▶ h_{op} is the mean operating time in hours per day
- ▶ d_{op} is the mean operating time in days per year
- ▶ t_{cycle} is the mean time between the start of two consecutive cycles of the component (e.g. switching a valve) in seconds per cycle

Assuming that the calculation of the MTTF_d for the holding brake results in a value of > 100 years, this gives an MTTF_d classification of "HIGH". EN ISO 13849-1 provides a graph to make it easier to determine the performance level. To decipher the performance level from this graph the diagnostic coverage DC is required. To determine the level of diagnostic coverage it is important to know whether every conceivable error can be detected through tests. Based on this consideration, a high classification will be possible if a safe converter is used to drive the motor and the holding brake is always tested automatically before the danger zone is accessed. To do this, a torque is established with a factor of 1.3 to the brake's rated holding torque, before waiting for at least one second. If the axis holds its position during the whole test, it can be assumed that the holding brake is in good working order. On this basis, it is possible to define the diagnostic coverage at 99%.

▶ 6.6 Examples of safe motion



Graph to determine the PL in accordance with EN ISO 13849-1.

So we now have the following data:

- ▶ Category = 4
- ▶ $MTTF_d$ = high
- ▶ DC = high

If this data is applied to the graphic, PL e can be determined.

Determination of the performance level for the overall circuit

In the illustrated example of the safe stop function on a servo axis with holding brake, all four components involved have performance level e. As a result, the lowest performance level of a subcircuit (SRP/CS) is also PL e. Using the standard's terminology, therefore, we have:

- ▶ 4 x SRP/CS each with PL e
- ▶ The lowest performance level of the 4 subcircuits (SRP/CS) = PL e and is assigned the parameter PL_{low}
- ▶ The lowest performance level occurs in 4 subcircuits and so the parameter $N_{low} = 4$

If this information is applied to Table 11 of EN ISO 13849-1 for a simplified calculation, the result for the example is an overall classification of PL d. Unlike the example for the safe stop function (without brake), a reduction factor now applies: In accordance with EN/ISO 13849-1, the achieved performance level is reduced by one level if the overall circuit contains more than three subcircuits with PL_{low} . However, in this case, a detailed calculation using the achieved PFH_D values can certainly result in PL e. This is where software tools such as the PASCAL Safety Calculator come into their own.

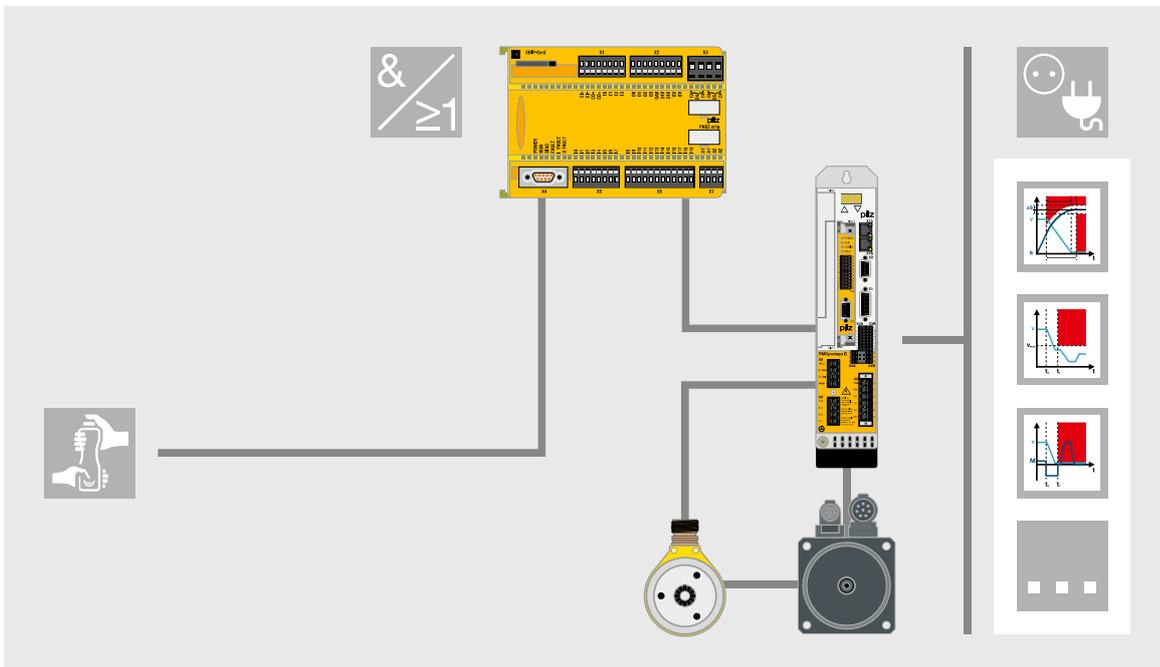


Safety Calculator PASCAL

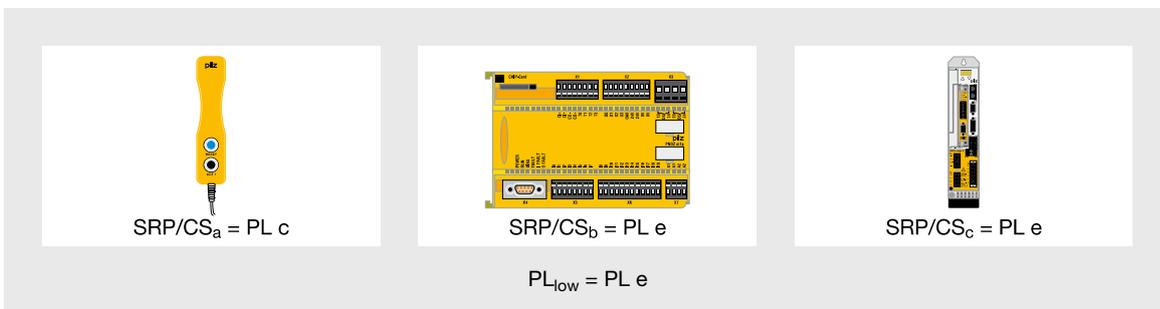
▶ 6.6 Examples of safe motion

6.6.1.4 Jog function with safely limited speed (SLS)

These days, jog functions can generally be carried out while guards are open thanks to the safely limited speed (SLS) function. The respective application will determine the type of increment that can be classified as non-hazardous. It may be helpful to consult EN 349 and EN 13855.



Structure of the safety function.



The block diagram shows the logical structure of the safety function, consisting of the series alignment of the safety-related subcircuits.

▶ 6.6 Examples of safe motion

Determination of the performance level for the overall circuit

In terms of structure, the jog function with safely limited speed is similar to the safe stop function described in section 7.6.1.2. The key difference lies in the pushbuttons used for the jog function and the impact this has on the calculation of the performance level. In EN ISO 13849-1, pushbuttons (enabling switches) are given a B_{10d} of 100,000. The time between two operations (cycles) is the key factor in calculating the $MTTF_d$.

Calculation formula for $MTTF_d$

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

$$n_{op} = \frac{d_{op} \times h_{op} \times 3,600 \text{ s/h}}{t_{cycle}}$$

The following assumptions are made, based on the application of the component:

- ▶ h_{op} is the mean operating time in hours per day
- ▶ d_{op} is the mean operating time in days per year
- ▶ t_{cycle} is the mean time between the start of two consecutive cycles of the component (e.g. switching a valve) in seconds per cycle

Assumptions:

- ▶ $B_{10d} = 100,000$
- ▶ $h_{op} = 16\text{h/day}$
- ▶ $d_{op} = 220\text{d/year}$

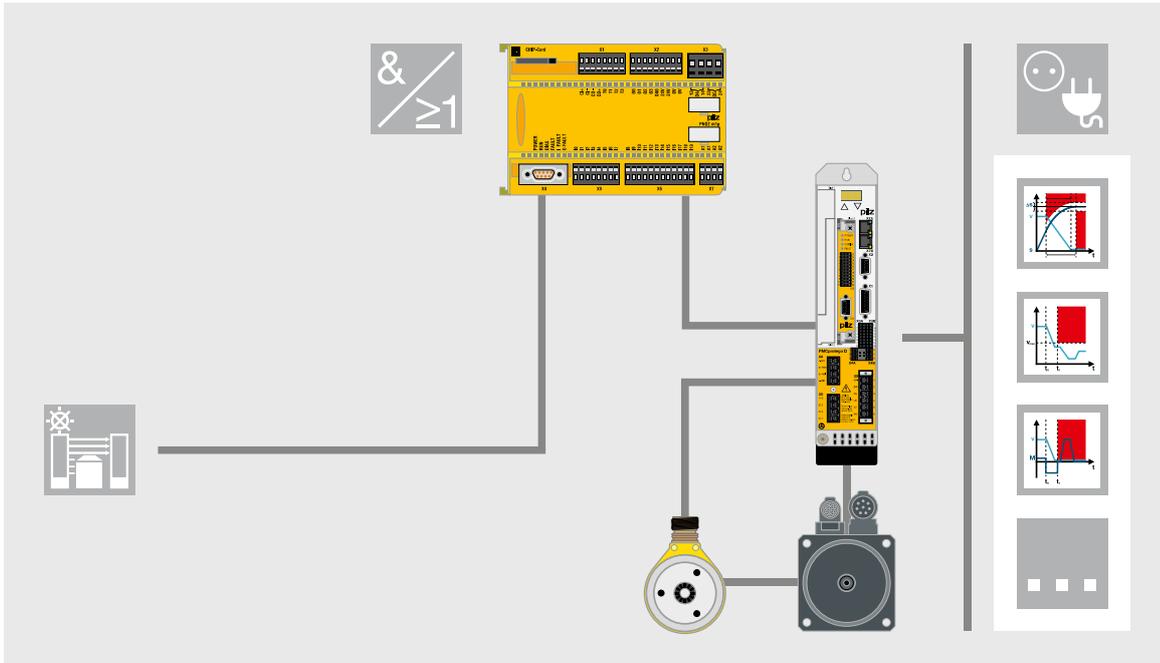
Calculation $MTTF_d$:

- ▶ $t_{cycle} = 5 \text{ s} \rightarrow MTTF_d = 0.395 \text{ years}$
- ▶ $t_{cycle} = 3,600 \text{ s} \rightarrow MTTF_d = 284.1 \text{ years}$

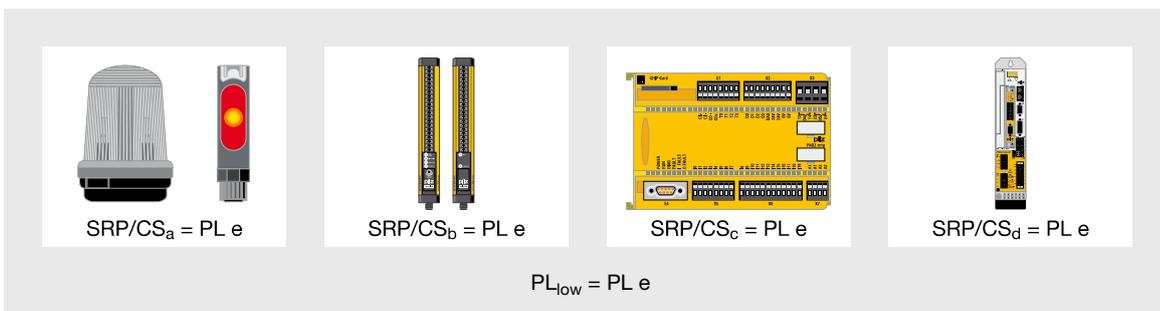
As shown in the example with cyclical operation in 5 s intervals, even in the best case it is only possible to achieve PL c with a B_{10d} value of 100,000. This demonstrates very clearly that the application range for wearing components has a direct influence on the calculation of the performance level and therefore affects the achievable safety level. The design engineer must therefore look very closely at the application range of his components in the respective application. Even if EN ISO 13849-1 states 100,000 cycles for B_{10d} , there may well be special components with a higher B_{10d} value. If an application uses a pushbutton as an E-STOP command device, it will certainly not be operated constantly at 5 second intervals. The situation is completely different if a pushbutton is used as a command device for cyclic initiation of a machine cycle and has to trigger a safe stop once released. The values stated in the example may cause a problem if a higher performance level is required.

▶ 6.6 Examples of safe motion

6.6.1.5 Muting with safe direction (SDI)



Structure of the safety function.



The block diagram shows the logical structure of the safety function, consisting of the series alignment of the safety-related subcircuits (SRP/CS).

In conjunction with light curtains and a muting circuit, the safe direction function (SDI) has a positive effect on safety because the respective direction of the drive axis is monitored during the muting phase and a safe shutdown occurs in the event of an error.

Determination of the performance level for the overall circuit

The performance level corresponds to the result from the example of the safe stop function.

▶ 6.6 Examples of safe motion

6.6.1.6 Motion monitoring with external devices

Drive-integrated motion monitoring is accompanied by external monitoring. In the simplest case, the drive has no safety function. A drive can be shut down in order to implement a safety function via conventional means, using contactors for example. However, today's drives often already have an STO function and can therefore implement a "safe stop". So an upstream safety relay can ensure that the hazardous movement is shut down simply and safely. Actual safety-related motion monitoring takes place in the external monitoring component, however.

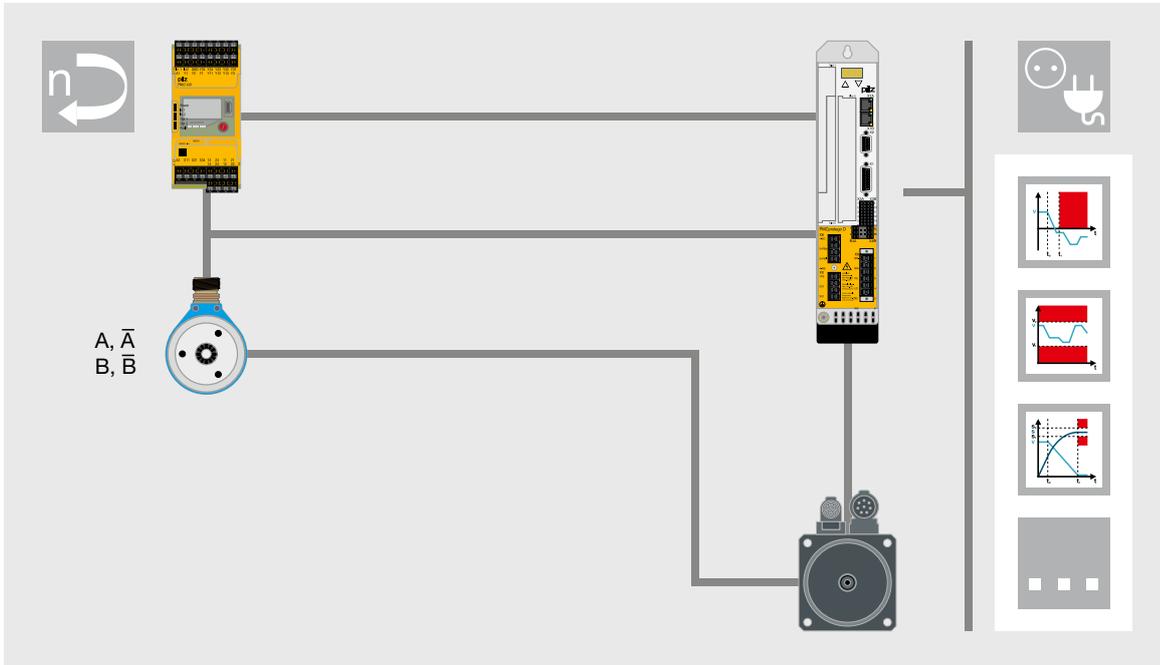
The task of the external devices is to detect motion. The safety characteristic data of the employed sensors, e.g. rotary encoders or proximity switches, is significant in determining the safety level that can be achieved. Different solutions to suit the various requirements are available to monitor movements with external monitoring devices. At the highest level it is necessary to distinguish between so-called standard encoders and "safe" encoders. When standard encoders are used, it is important to determine whether one or two encoders are required.

The following safety functions may be realised, for example, depending on the monitoring functions implemented in the external monitoring devices:

- ▶ Safely limited speed (SLS)
- ▶ Safe direction (SDI)
- ▶ Safe operating stop (SOS)
- ▶ Safe speed range (SSR)

The following examples illustrate potential types of motion monitoring using external devices. For the sake of clarity, the examples only illustrate those motion monitoring components with the task of monitoring motion sensors such as rotary encoders or proximity switches. The basic calculation method corresponds to the one illustrated in the previous examples.

▶ 6.6 Examples of safe motion



Motion monitoring with one standard encoder.

6.6.1.7 External motion monitoring with one standard encoder

In this example, one standard rotary encoder as sensor is responsible for motion detection. Various combinations are possible in conjunction with the drive controller. The hazardous function is shut down via an STO function available within the drive. If it is only the monitoring device that evaluates the encoder signals for the safety function, i.e. the drive controller does not use an encoder or only uses a separate encoder, a maximum of performance level PL c can be achieved. This requires an encoder with $MTTF_d = \text{high}$ and classification as a “well-tried component” or Category 1, or alternatively direct classification as PL c.

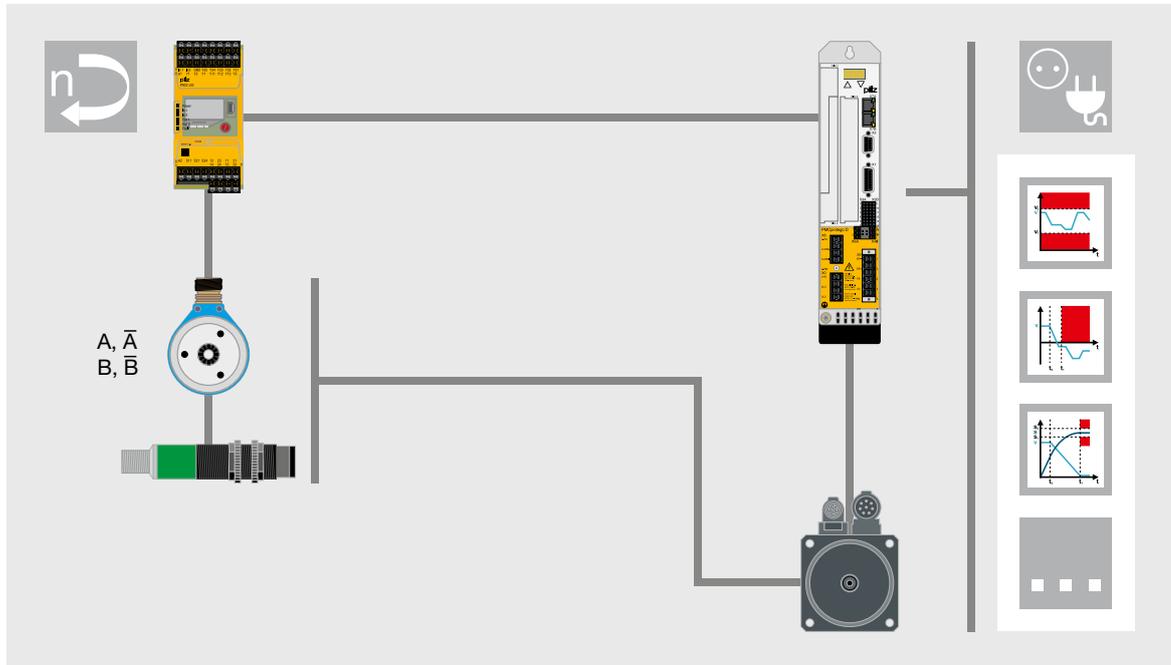
If the monitoring device evaluates the encoder signals while the drive controller for position control uses the same signals simultaneously, a performance level of up to PL d can be achieved. This requires an encoder with $MTTF_d = \text{medium/high}$. The drive controller acts as an additional diagnostic instance for the safety function through the appropriate parameterisation and activation of drag error detection (incl. shutdown). A pure frequency converter (FC) without control function cannot be used in this case.

The following safety functions are possible with the illustrated configuration:

- ▶ Safely limited speed (SLS)
- ▶ Safe direction (SDI)
- ▶ Safe operating stop (SOS)
- ▶ Safe speed range (SSR)

Note: The safety functions that can be realised depend on the monitoring functions implemented in the external monitoring device.

▶ 6.6 Examples of safe motion



Motion monitoring with redundant standard sensors.

6.6.1.8 External motion monitoring with standard encoder and proximity switch

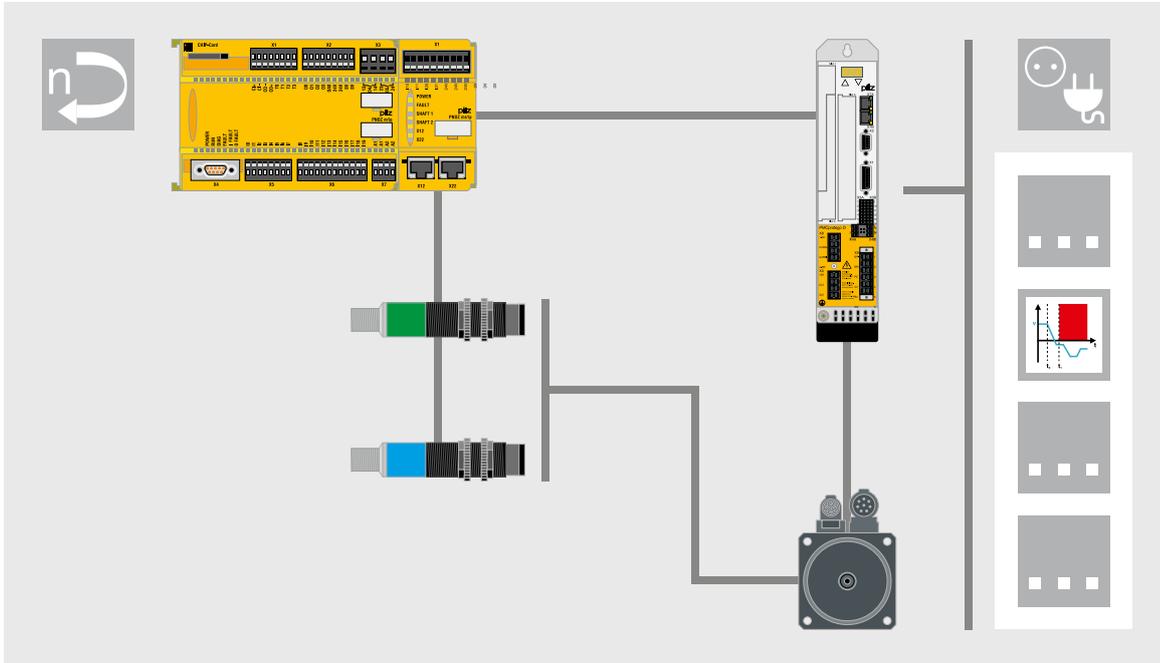
Generally speaking, two separate sensors for motion detection are required in order to achieve the highest safety level (PL e) with standard sensors. Depending on the external monitoring device, these may be two rotary encoders or, as shown in this example, one rotary encoder and an additional proximity switch. The corresponding values for $MTTF_d$ are required for the sensors. This enables the performance level to be calculated for the sensor subsystem, which consists of the encoder and proximity switch; this can then be used to calculate the performance level for the overall safety function. The hazardous function is shut down via an STO function available within the drive.

The encoder signals evaluated by the monitoring device for the safety function can also be used by the drive controller for speed and position control. However, this is not absolutely essential for the safety function. The following safety functions are possible with the illustrated configuration:

- ▶ Safely limited speed (SLS)
- ▶ Safe direction (SDI)
- ▶ Safe operating stop (SOS)
- ▶ Safe speed range (SSR)

Note: The safety functions that can be realised depend on the monitoring functions implemented in the external monitoring device.

▶ 6.6 Examples of safe motion



Motion monitoring with proximity switches.

6.6.1.9 External motion monitoring with two standard proximity switches

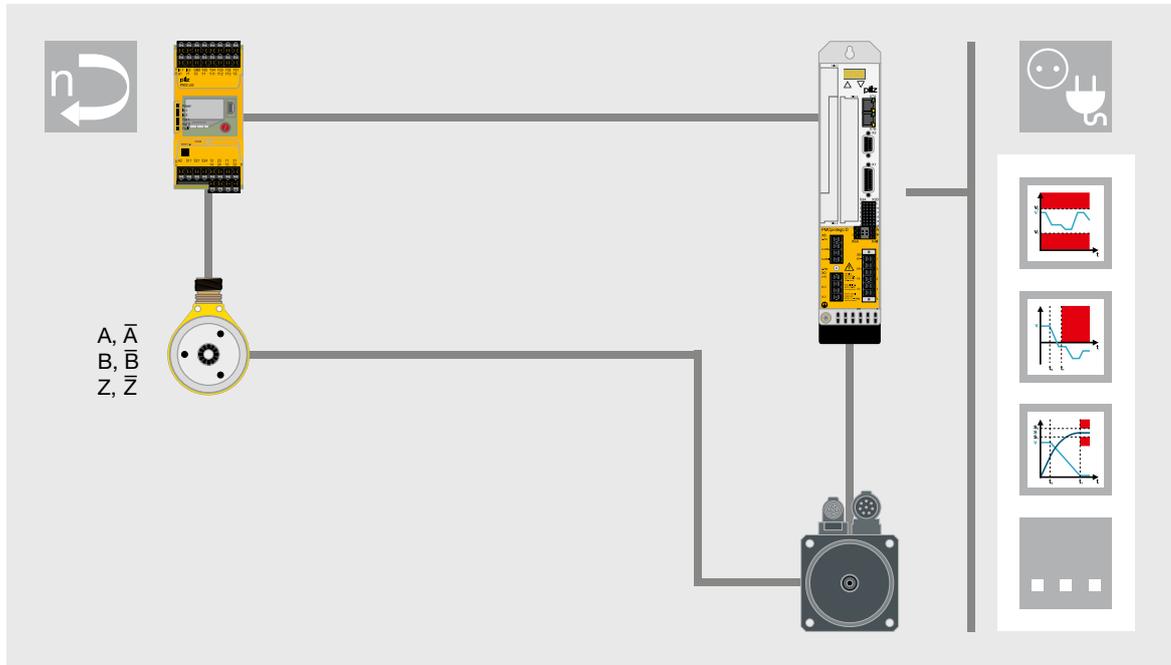
Without a rotary encoder, safety-related motion monitoring can still be implemented using standard sensors in the form of proximity switches, even up to the highest safety level (PL e). As in the previous example, two separate proximity switches are required for motion detection. If common cause failures (CCF), due to EMC for example, cannot be excluded or managed on both proximity switches, the use of diverse components from different manufacturers or of different types is recommended. The corresponding values for $MTTF_d$ are required for the proximity switches. This enables the performance level to be calculated for the sensor subsystem, which consists of the two proximity switches; this can then be used to calculate the performance level for the overall safety function. The hazardous function is shut down via an STO function available within the drive.

The following safety function is possible with the illustrated configuration:

- ▶ Safely limited speed (SLS)

Note: The safety functions that can be realised depend on the monitoring functions implemented in the external monitoring device.

▶ 6.6 Examples of safe motion



Motion monitoring with safe rotary encoder.

6.6.1.10 External motion monitoring with safe encoder

Manufacturers are increasingly offering “safe” encoders for motion monitoring tasks. These devices are designed specifically for use in safety functions and are certified accordingly. As a result, a performance level of PL d or PL e can be achieved, depending on the construction type. This is usually possible with just one encoder, i.e. there is no need for two devices, as is the case when standard components are used. However, safe encoders are not actually “safe” until they are combined with a safe monitoring device, because there are no diagnostic or feasibility tests implemented within the encoder. The use of safe encoders, therefore, requires detailed knowledge of the requirements for use in safety-related applications, as described by the manufacturer in the operating manual. The monitoring device must be able to meet these requirements exactly by performing the monitoring functions demanded by the device manufacturer.

One test that is often demanded, for example, is the absolute value check for sin/cos encoders: $\sin^2 + \cos^2 = 1$. If this check is not implemented within a monitoring device, the device cannot be used in combination with a safe encoder that requires such a check. To date there is still no uniform or even standardised interface for safe encoders, so the encoder manufacturers’ requirements for their products vary enormously. That’s why it is absolutely essential that the safe encoder and safe monitoring device are totally compatible. In this example, the hazardous movement is shut down via the STO function available within the drive. The following safety functions can be implemented with the illustrated configuration:

- ▶ Safely limited speed (SLS)
- ▶ Safe direction (SDI)
- ▶ Safe operating stop (SOS)
- ▶ Safe speed range (SSR)

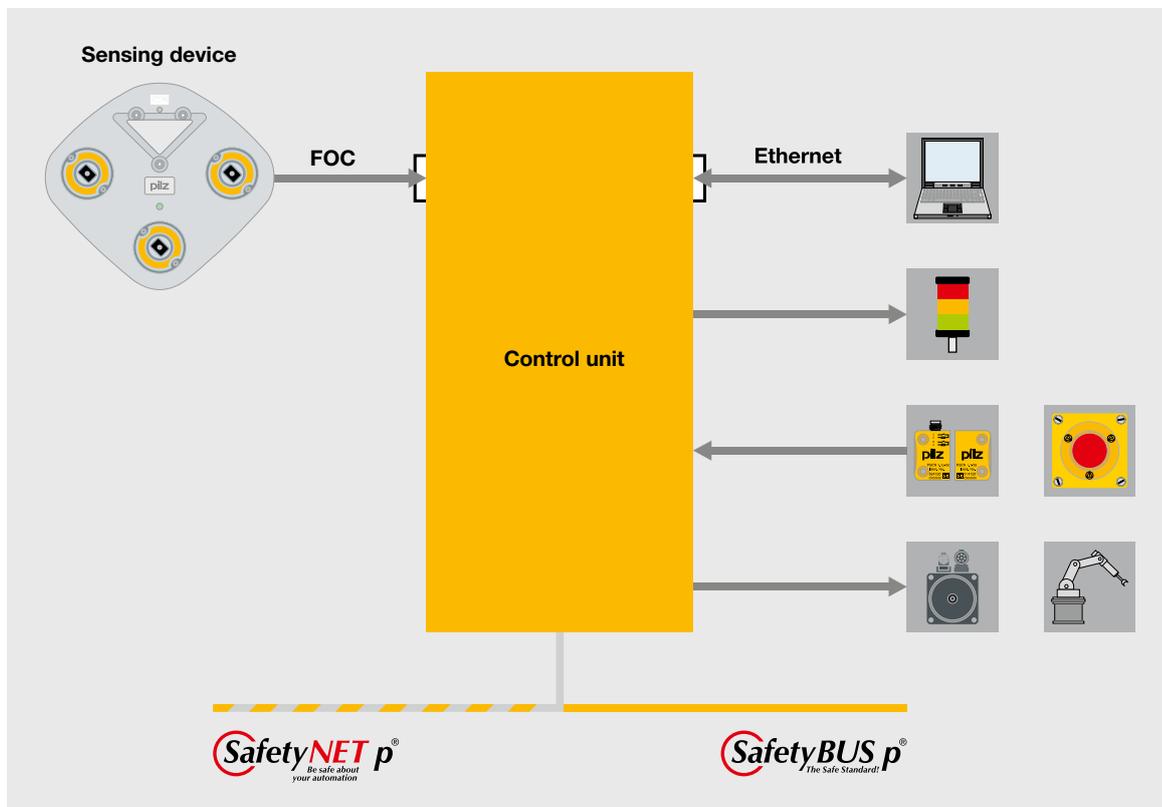
Note: Details of the safety functions that can be realised depend on the monitoring functions implemented in the external monitoring device.

▶ 6.6 Examples of safe motion

6.6.1.11 Safeguarding detection zones with a safe camera-based solution

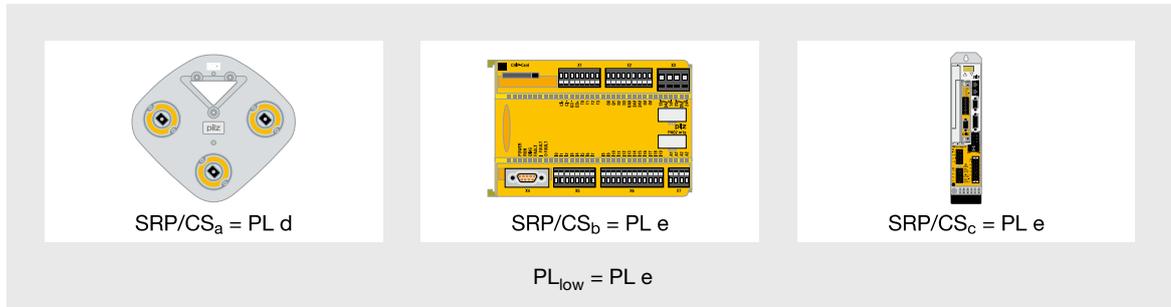
Until now, interaction between man and robot has largely been characterised by fixed safeguards. A modern camera-based solution offers a whole range of new options in this case. The detection zone covers all three dimensions; one single device

meets every requirement when accessing a danger zone and also provides protection against climbing over and crawling under the detection zone. The detection zones can be individually configured and can also enable the speed of the active axes in the monitored zone to be reduced if anyone approaches.



Structure of the safety function.

▶ 6.6 Examples of safe motion

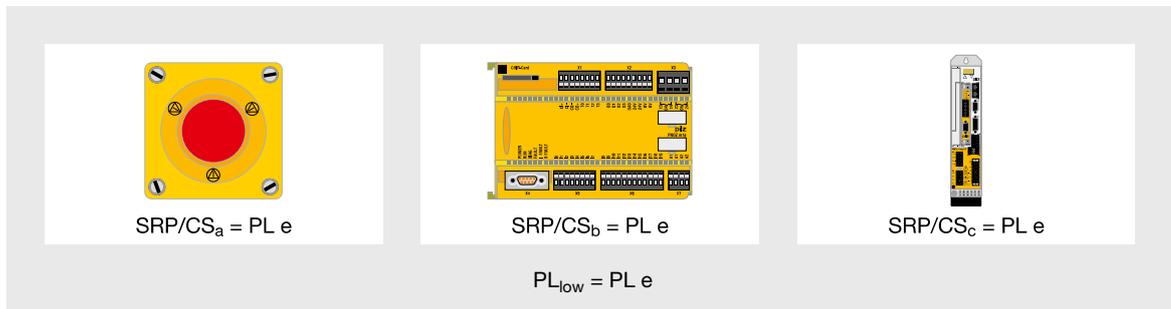


Block diagram of the safety functions.

Determination of the performance level for the overall circuit

The result is performance level d.

6.6.2 Reaction times of safety functions



Block diagram of the safety functions.

Several boundary conditions are involved in calculating a safety distance.

Determination of the reaction time in the case of external commands

If an E-STOP pushbutton acts upon an evaluation device, its reaction time is added to the reaction time of the drive-integrated safety function. It will also be necessary to add the time needed to bring an accelerated axis to standstill:

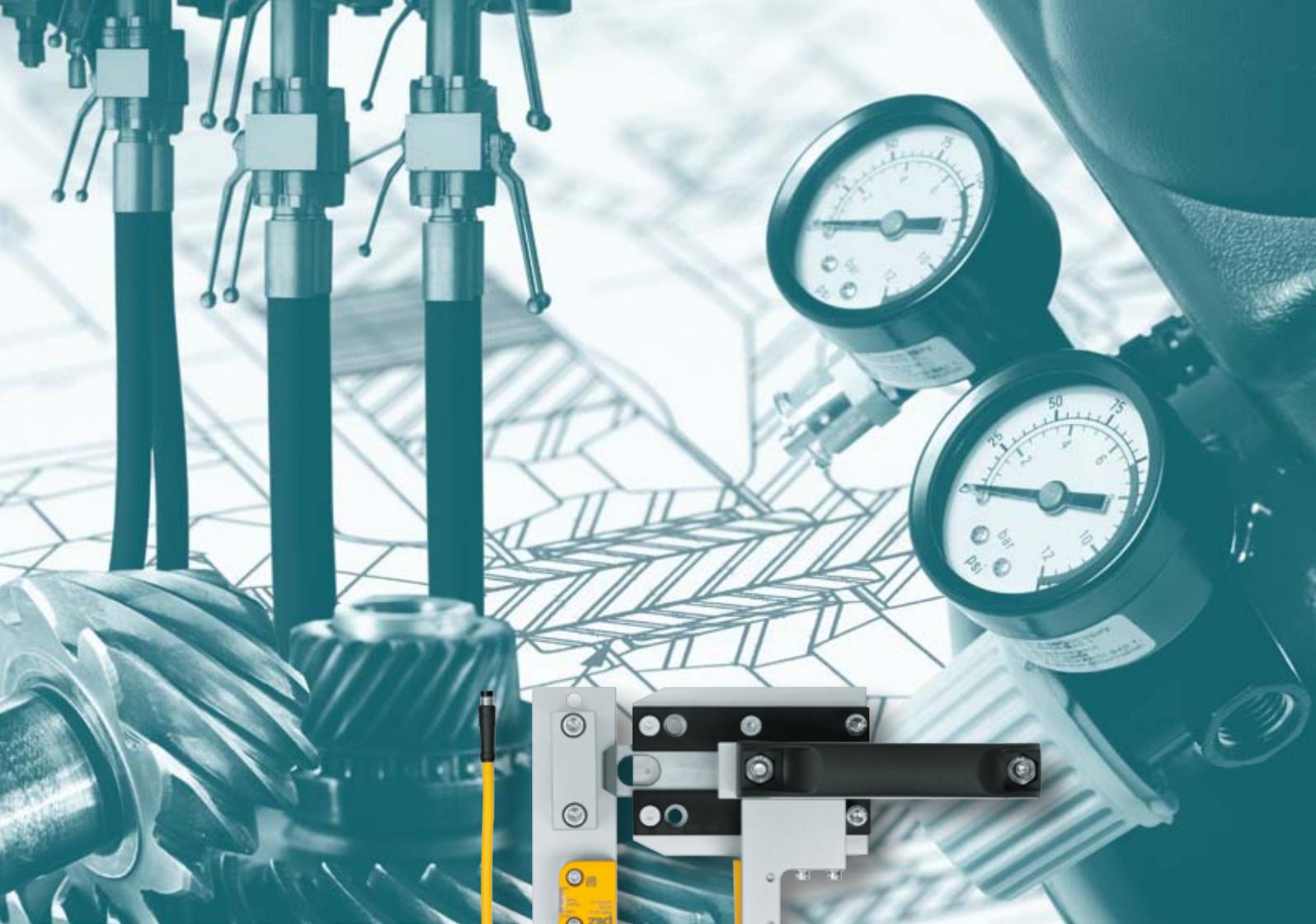
- ▶ $t_{\text{reac}} = t_{\text{multi}} + t_{\text{PMC}} + t_{\text{ramp}}$
- ▶ t_{multi} = Reaction time of the evaluation device is approx. 20 ms

- ▶ t_{PMC} = Reaction time of the drive-integrated safety functions to external signals is 6 ms
- ▶ t_{ramp} = Ramp time to standstill depends on the moved mass, speed and other application-dependent data

Determination of the reaction time when limit values are violated

If a monitoring circuit on a drive-integrated safety function is activated, it will be necessary to add the time needed to bring the accelerated axis to standstill.

- ▶ $t_{\text{reac}} = t_{\text{PMC}} + t_{\text{ramp}}$



7

**Mechanical,
pneumatic and
hydraulic design**

▶ 7 Mechanical, pneumatic and hydraulic design

Chapter	Content	Page
7	Mechanical, pneumatic and hydraulic design	7-3
7.1	Introduction to mechanical, pneumatic and hydraulic design	7-3
7.2	Mechanical design	7-4
7.2.1	Introduction	7-4
7.2.2	Danger, hazard, risk	7-5
7.2.3	Definition and implementation of safety measures	7-9
7.3	Pneumatic design	7-21
7.3.1	Introduction	7-21
7.3.2	Well-tried principles and protective measures	7-21
7.3.3	Circuit-based solutions	7-25
7.3.4	Stopping and braking	7-31
7.3.5	Circuit diagram and operating manual	7-33
7.4	Hydraulic design	7-35
7.4.1	Basic physical knowledge	7-35
7.4.2	Advantages of hydrostatic power transmission	7-35
7.4.3	Disadvantages of hydrostatic power transmission	7-35
7.4.4	Definitions	7-35
7.4.5	Relevant units	7-36
7.4.6	General hydraulic relationships	7-38
7.4.7	Structure of a hydraulic system	7-43
7.4.8	Simple hydraulic circuit, upward movement	7-43
7.4.9	Simple hydraulic circuit, downward movement	7-44
7.4.10	Simple hydraulic circuit, speed	7-44
7.4.11	Circuit diagram for simple hydraulic circuit	7-45
7.4.12	Two-cylinder control systems with electric valves	7-46
7.4.13	Two-cylinder control systems with sequence valves	7-47
7.4.14	Series circuit	7-48
7.4.15	Parallel circuit	7-48
7.4.16	Differential circuit	7-49
7.4.17	Speed control systems	7-50
7.4.18	Drive pumps, fixed pumps	7-51
7.4.19	Drive pumps, screw pumps	7-52
7.4.20	Drive pumps, vane pumps	7-53
7.5	Safety requirements on hydraulic circuits	7-54
7.5.1	Safety requirements in general	7-54
7.5.2	Concept and design	7-54
7.5.3	Additional safety requirements	7-54
7.5.4	Establishing compliance with the safety requirements	7-55
7.5.5	Safety-related parts of hydraulic control systems	7-56
7.5.6	Control systems in accordance with Category B, Performance Level a	7-57
7.5.7	Control systems in accordance with Category 1, Performance Level b	7-58
7.5.8	Control systems in accordance with Category 2, Performance Level b	7-59
7.5.9	Control systems in accordance with Category 3, Performance Level d	7-60
7.5.10	Control systems in accordance with Category 4, Performance Level e	7-61
7.5.11	Further example for control systems in accordance with Category 4	7-62

▶ 7.1 Introduction to mechanical, pneumatic and hydraulic design

The role of safety technology in the design of plant and machinery is becoming ever more significant. Although machinery may have already been fitted with a high level of safety, with rising demands on efficiency and productivity, safety technology continues to develop on an ongoing basis. The Machinery Directive also contributes in this regard. The following three sections deal with the mechanics, pneumatics and hydraulics. However, all three drive technologies should also always be considered in combination with the electrical design.

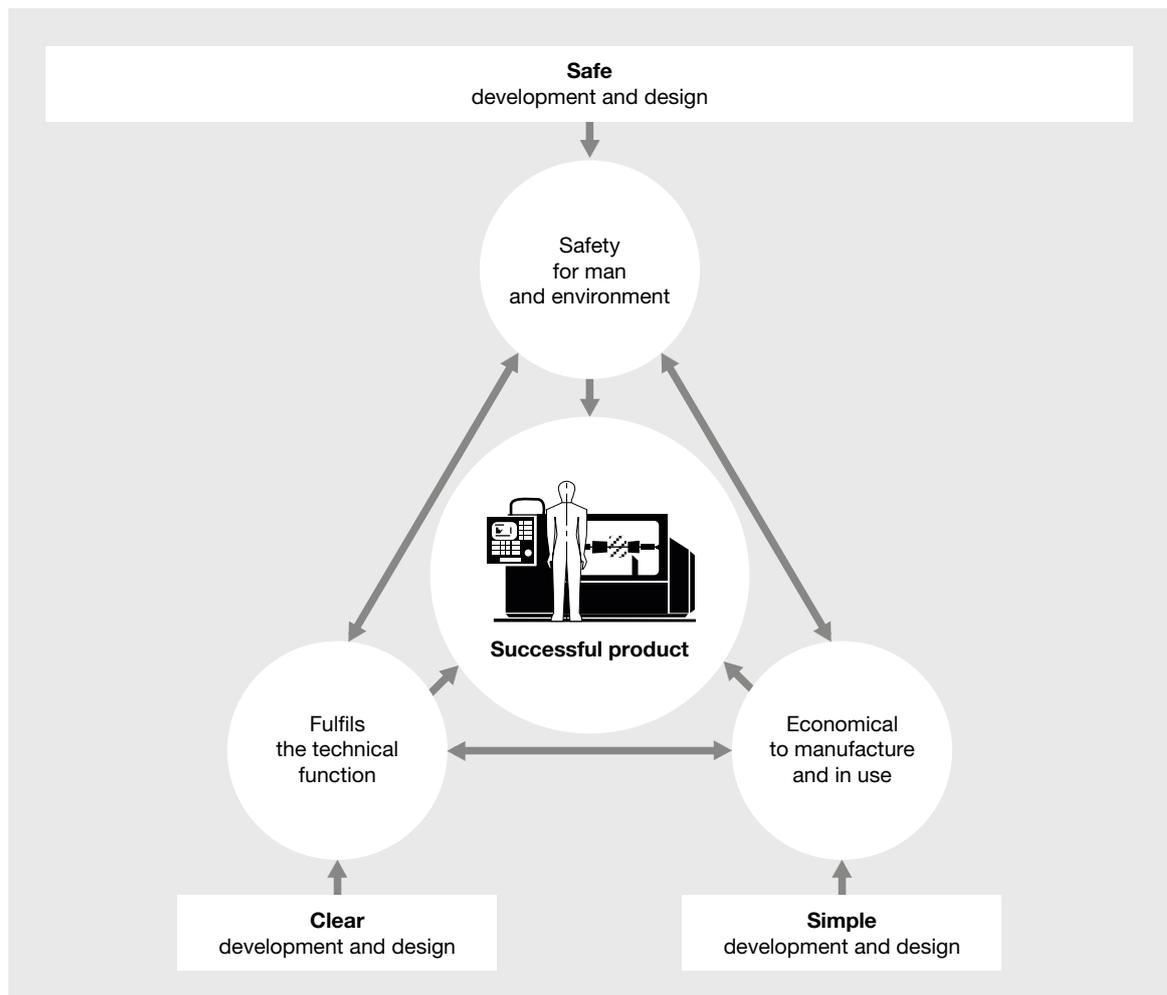
▶ 7.2 Mechanical design

7.2.1 Introduction

Engineers and designers have always done a good job. How else could you explain the remarkable level of safety on today's plant and machinery? The maelstrom surrounding the EC Machinery Directive (MD) has not actually been based on (safety) technology. It has been much more concerned with the fact that a member of the company's management team must use his good name to guarantee that the supplied machine actually has the necessary level of safety demanded and, what's more, that this can be proved legally (key words are documentation and operation manual). However, it's important to get one thing straight: Our machines are still not always perfect,

but they are continuously getting better. Evolution in safety technology does not mean the implementation of wholly new solutions; quite the opposite: Deficiencies provide the impetus for improvement and errors the premise for correction!

Regarding terminology: In general parlance, the distinction between reliability and safety is not always clear. That is because both terms have some things in common: They refer to future events and deal with probability. From the perspective of work safety and the associated safety-related design, a distinction should be made between the two terms, using exclusive definitions: If a component (incl. module, machine or plant) does not fulfil its intended function in compliance with



Ground rules for designing successful products.

▶ 7.2 Mechanical design

pre-defined boundary conditions, it is deemed to be unreliable. If a component (incl. module, machine or plant) causes an accident involving bodily harm, it is/was unsafe. The meaning of reliable and safe can be derived from the reverse implication. The logical consequence from an accident is that you can only sensibly speak of safety (or lack of safety) if all the relevant considerations of the technical systems and their design treat humans as an inextricable component of the work system, realistically, with all their deficiencies.

7.2.2 Danger, hazard, risk

Annex I of the EC Machinery Directive defines four mandatory steps as the basis for the design of safety-related machinery:

1. Systematically identify potential dangers in the design
2. Analyse hazardous situations when working with or on machinery (hazard analysis)
3. Estimate and evaluate the risks associated with the hazards
4. Implement and document all the safety measures necessary to manage the risk

Regarding terminology: Viewed objectively, dangers can be regarded as an energetic or material potential that exceeds human limits and can spontaneously lead to health impairments or injuries of varying degrees of severity.

Hazards arise as soon as there is the possibility of humans coinciding with danger in time and space, enabling an unwanted situation to arise. The effects of what happens as the hazard unfolds are subject to the relentless laws of nature.

The term risk requires a new mindset. It represents the consequences for man and the environment of hazards that occur with varying frequency. The consequences may have various degrees of severity. The level of risk is still determined by whether technical or organisational countermeasures can or cannot be implemented. Statements of risk are calculated prognoses of potential future events, in other words, the result of human considerations and not therefore the laws of nature playing out.

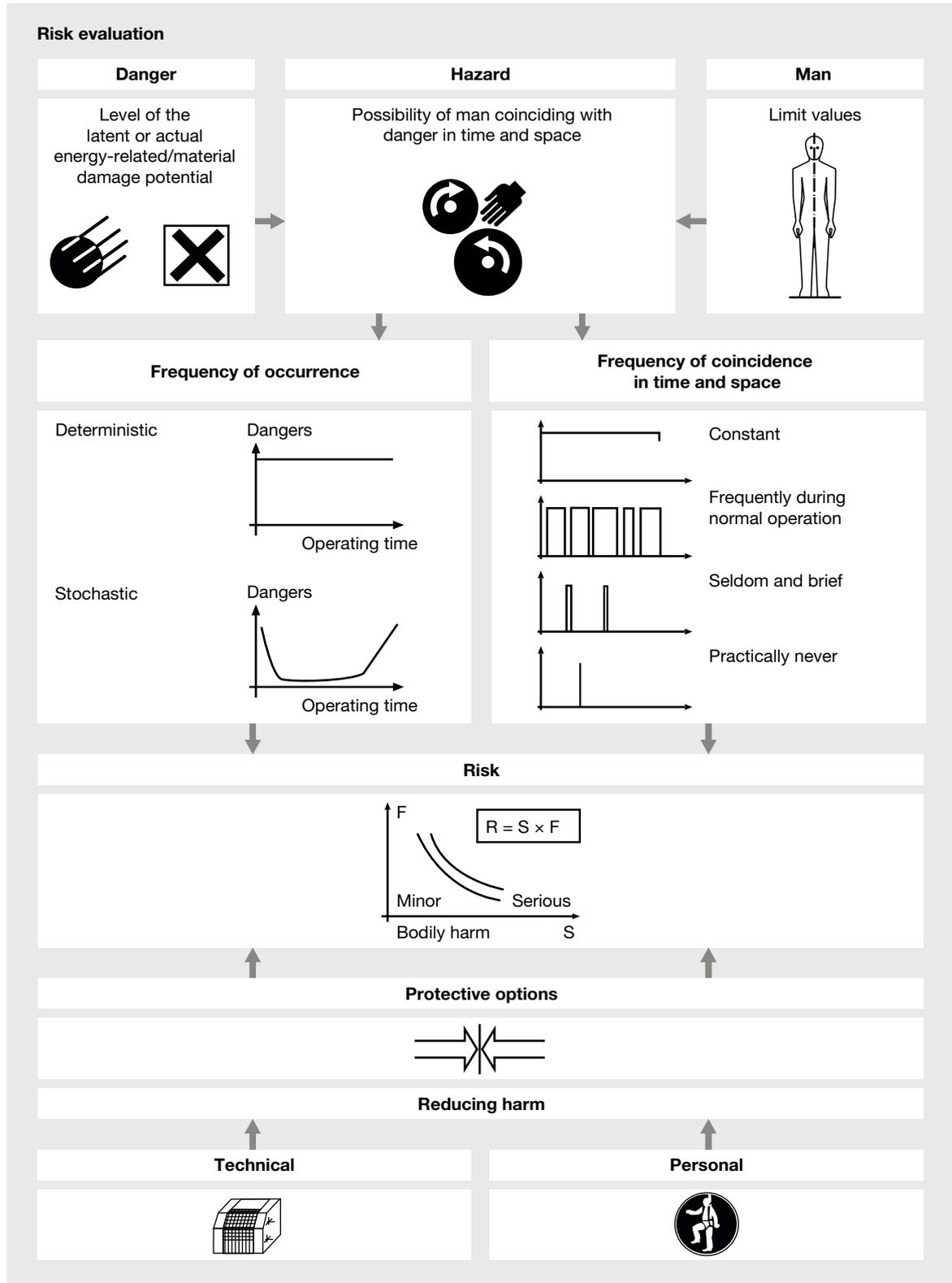
For design engineers it is important to know that the causes of danger lie in the effective parameters of material, energy and information. In other words, parameters they apply during the design process and which they can use to achieve a safe condition, via the same methods employed to design functional technical systems.

The hazard from materials may not only arise from their chemical or biological properties. They can also adversely affect humans on account of their property as space-filling matter (geometry) in the earth's gravitational field: Wherever the geometric layout of the machine results in forced postures or when heavy loads have to be carried or transported by hand (strain on the spine).

Energy: Every machine needs energy to perform its technological function. Any energy used to fulfil a work function can be hazardous to humans as soon as its impact is uncontrolled and exceeds certain energy densities.

Information: A poorly designed information flow between man and machine, including the boundary conditions, can trigger behaviours which can endanger the machine user and others. In this context, the basic information parameter implies that human safety in work systems depends on the natural laws of information processing and human behaviour. As the basic parameters of material, energy and information are used in machinery, dangers can only emanate from these parameters.

7.2 Mechanical design



Context of risk evaluation.

▶ 7.2 Mechanical design

Effective parameter	Effect	Examples		
		No.	3	4
Material 	Spatial disposition	1		Forced postures, unreachable function elements
	Physical stresses	2		Handling of loads, high operating forces, high cycle counts
	Physical influences	3		Air temperature, draught, air humidity, high or low pressure
	Biological influences	4		Fungal cultures, bacteria in inhaled air, contaminated germ-infested air filter
	Chemical influences	5		Corrosive, poisonous, harmful, irritant substances
	Thermal influences	6		High and low ambient and contact temperatures, fire
Energy 	Explosions	7		Chemical explosions (solid substances, vapours, gases), physical explosions
	Mechanical influences	8		Places where you can fall, danger sources, danger zones, collisions, impact points
	Noise, vibration	9		Sound emissions, hand vibration, whole body vibration
	Electrical influences	10		Electrostatic charges, body through-flow, arcing
	Electromagnetic fields	11		Electromagnetic fields, magnetic fields
	Radiation	12		Electromagnetic waves, IR/UV radiation, laser, ionising radiation
Information 	Presentation of information	13		Inadequate layout of notices, control elements; incompatibility
	Light conditions	14		Luminosity, glare, luminous colour, luminance distribution
	Psychomental stress	15		Unclear operating and work instructions, software ergonomics
	Organisational failings	16		Poorly thought-out, uncoordinated sequence of operations
	Hectic pace, stress, shock	17		Incorrect operation, panic reactions, mistakes

Dangers when dealing with machinery.

▶ 7.2 Mechanical design

7.2.2.1 Mechanical dangers

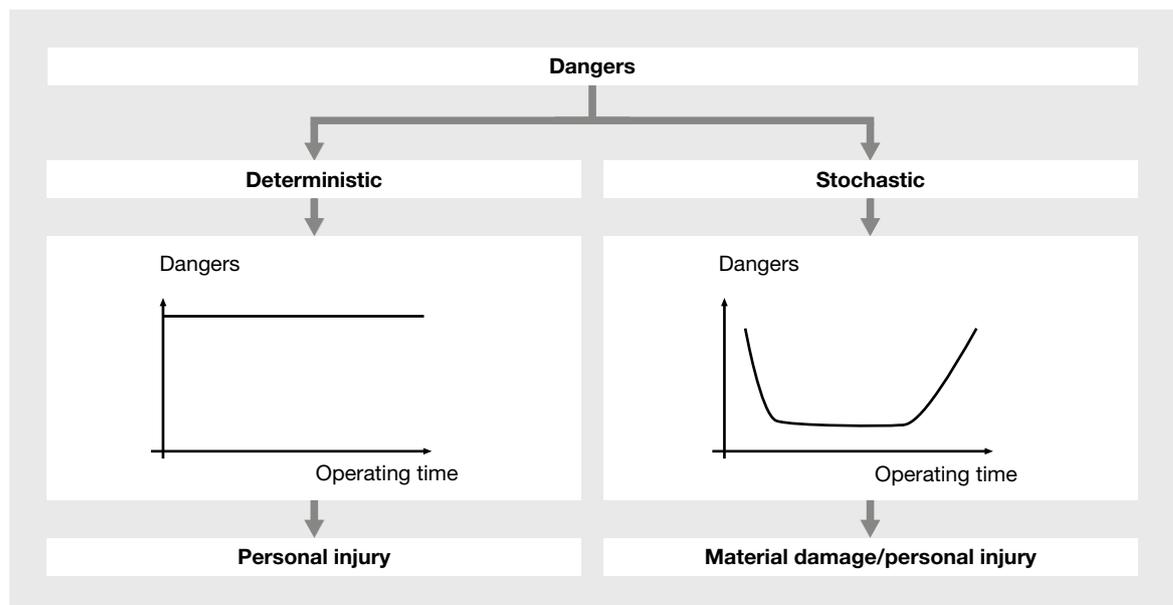
The essential distinguishing feature concerns the type of mechanical energy (kinetic, potential) and the question as to the basis of the energy (object or human) and which movements would precede a possible accident (kinematically based or free movements).

Hazards: Hazards occur when potential dangers and humans coincide in time and space. There are two types: stochastic (random) and deterministic (predetermined) hazards.

Deterministic hazards: These are rooted in the functional design of the machine, e.g. danger points which are a technical necessity, such as those on tools with set movements. Such hazards are latent throughout the whole of the machine's lifetime and have a consistently high level of probability. An accident at a danger point is therefore only a matter of time, unless design measures are used to counteract it. Deterministic, mechanical danger points are still the main focus for all machine

accidents, because their destructive impact is underestimated, both by design engineers and by those affected. Unlike stochastic dangers, with practice, danger points are visible to the naked eye of anyone with any sort of technical interest, whether in drawings, CAD designs or on finished machinery. It is really a benefit that today's design engineers can counteract these dangers using relatively simple means.

Stochastic hazards occur with a time-based probability during a machine's lifetime. They are normally visualised with the bathtub curve, although strictly speaking this only applies to a few modules or components; but when it does apply, the effect is sudden and surprising. It is rare for these hazards and their causes to be directly identifiable and, as is unfortunately almost always the case with spectacular accidents, they can hardly ever be reliably predicted.



Deterministic and stochastic dangers.

▶ 7.2 Mechanical design

7.2.2.2 Risk assessment

Today there are more than 80 risk assessment procedures on the market and in academia, and the trend is rising. However, none of them is (legally) binding. Although the Machinery Directive and harmonised machinery safety standards refer to some standards (EN ISO 13849, EN ISO 12100, IEC 61508/EN 62061), there may still be considerable difficulties implementing them in practice. And it's not all the fault of design engineers: With no relevant training, they are supposed to derive binding measures from multiple statements of probability for more events than are likely to occur. The following definition of technical risk is currently generally accepted:

Risk is not a law of nature, but a statement of probability (prognosis) regarding the impact of hazards on man and/or the environment under a defined set of circumstances. Risks are calculated from the frequency and severity of potential injury, damage to health or material damage, combined with the possibility or otherwise of technical, organisational or personal measures to avert or protect against the hazard. The result of the risk assessment ultimately determines the reliability requirements of the safety functions to be fulfilled by the safety-related parts of the control system. This also refers to the reliable performance of the guard function.

7.2.3 Definition and implementation of safety measures

Machine manufacturers are obliged only to supply safe products on the internal European market. For this reason, they must calculate all the hazards associated with the machine in advance and assess the resulting risks. With the knowledge gained from the hazard analysis and the risk assessment, manufacturers must design their machines in such a way that cannot be harmful either to users, other persons or the environment. In other words: the machines must be safe.

Many people like to use the term “safe”; after all, the feeling of safety is one of the most important basic human needs. Advertising and insurance industries, along with politicians, really understand how to address this basic need and exploit it for their own interests. In technology, safe is often taken to mean the fulfilment of a machine function over a fixed period. That really addresses reliability, however, so we need to be precise: In its true sense, safety is understood to be the absence of potential and real danger for man and the environment. Safety and reliability have many common features: Both describe a future machine behaviour and are therefore statements of probability.

The first commandment for safety-related design: All hazard types must be tackled within the design! The necessary design measures must counteract unforeseeable hazards, both stochastic and deterministic. The different modes of operation of both hazard types also require different design methods.

When selecting the design methods, the following should be noted:

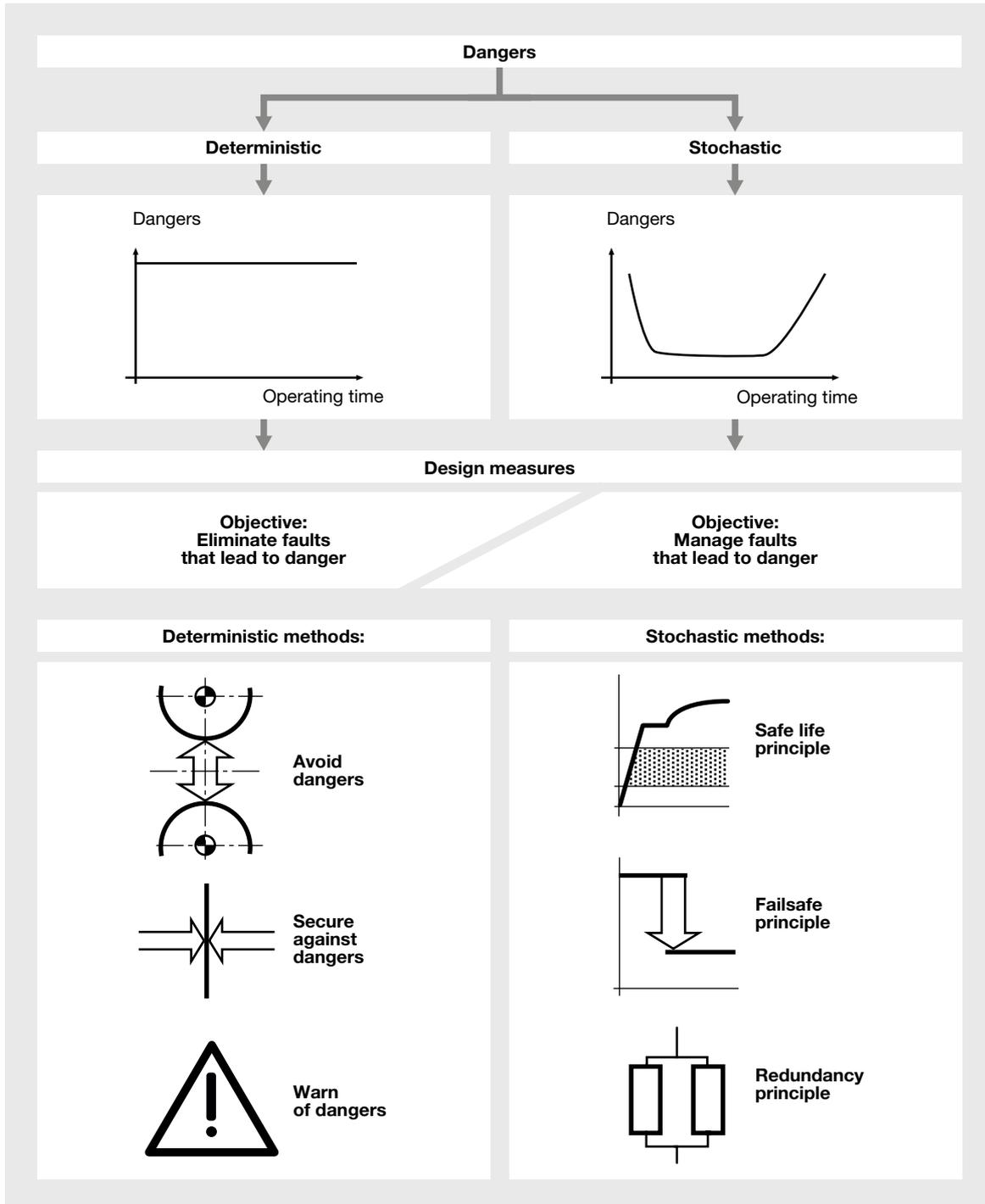
1. Design measures should always be used to reduce existing risks to such an extent that the achieved residual risk is tolerable to the individual and society (i.e. it may occur and must then be accepted).
2. As stochastic and deterministic hazards vary substantially, it is only logical that the measures taken to counteract them must also differ.

▶ 7.2 Mechanical design

Type of energy	Energy bearer	Movement	Graphic	Hazard due to
1	2	3	No. 4	5
Potential energy 	Objects 	Movement along fixed channels 	1 	Danger points on controlled moving parts: Danger is confined to a specific location.
Kinetic energy 			2 	
Potential energy 	People, parts of the body 	Free movement 	3 	Danger sources due to uncontrolled moving parts: Danger emanates from a specific location.
			4 	
Kinetic energy 	People, parts of the body 	Movement along fixed channels 	5 	Places where you can fall
			6 	Impact points
Kinetic energy 	People, parts of the body 	Movement along fixed channels 	7 	Inertia forces
			8 	

Basic mechanical hazards.

▶ 7.2 Mechanical design



Important design measures for avoiding danger.

▶ 7.2 Mechanical design

7.2.3.1 Design measures against stochastic hazards

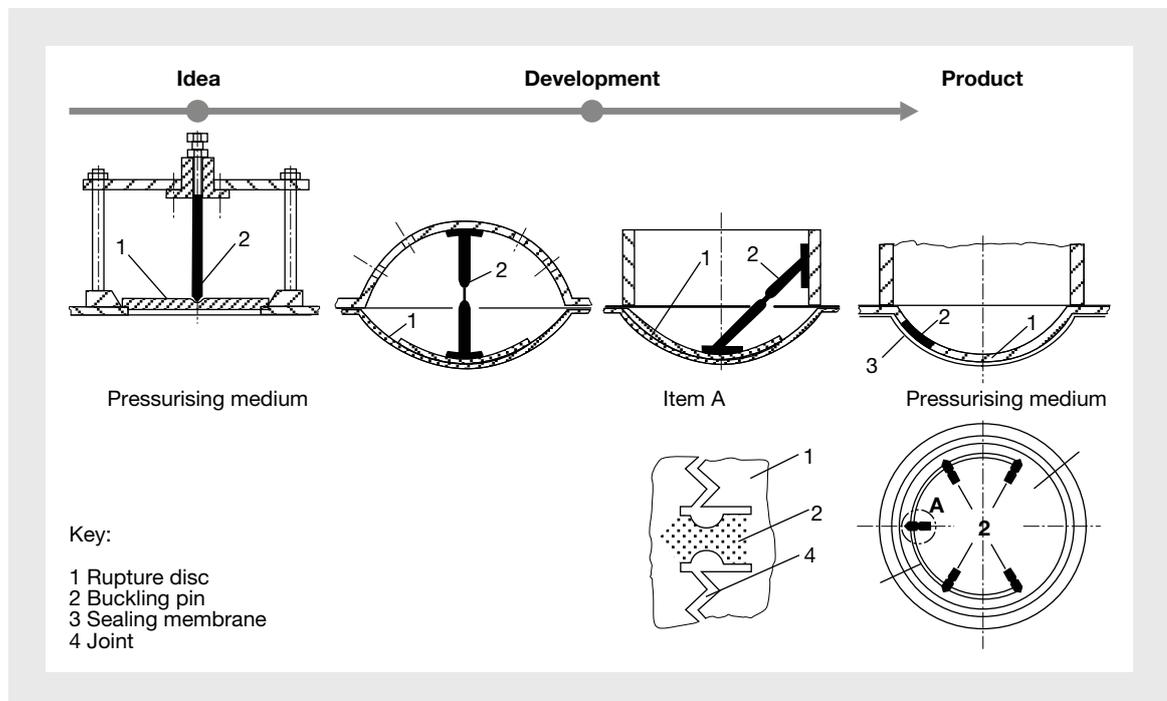
Stochastic hazards can be mainly attributed to component failures or software errors. Although they affect machine reliability, they may not necessarily have an adverse effect on human safety. The aim of targeted design measures is to increase the time-based probability that machines will fulfil their intended function within an agreed operating time and remain immune to random component failures. That way they can harm neither man nor the environment. The most well known design measures are:

- ▶ Safe life principle
- ▶ Failsafe principle
- ▶ Redundancy principle

Measures relating to the safe life principle start from the assumption that the machine is adequately dimensioned and designed according to its function, and as such will operate as intended during its warranted lifetime: without faults, failures or danger. This design principle is particularly significant on safety devices such as rupture discs, for example. The model shown below used the extremely reliable buckling bar principle.

Application of this principle assumes that:

1. All the stresses that act on the machine are known
2. The applied calculation methods and accepted material performance match reality
3. No influences other than those considered in the calculation will occur during the machine's lifetime

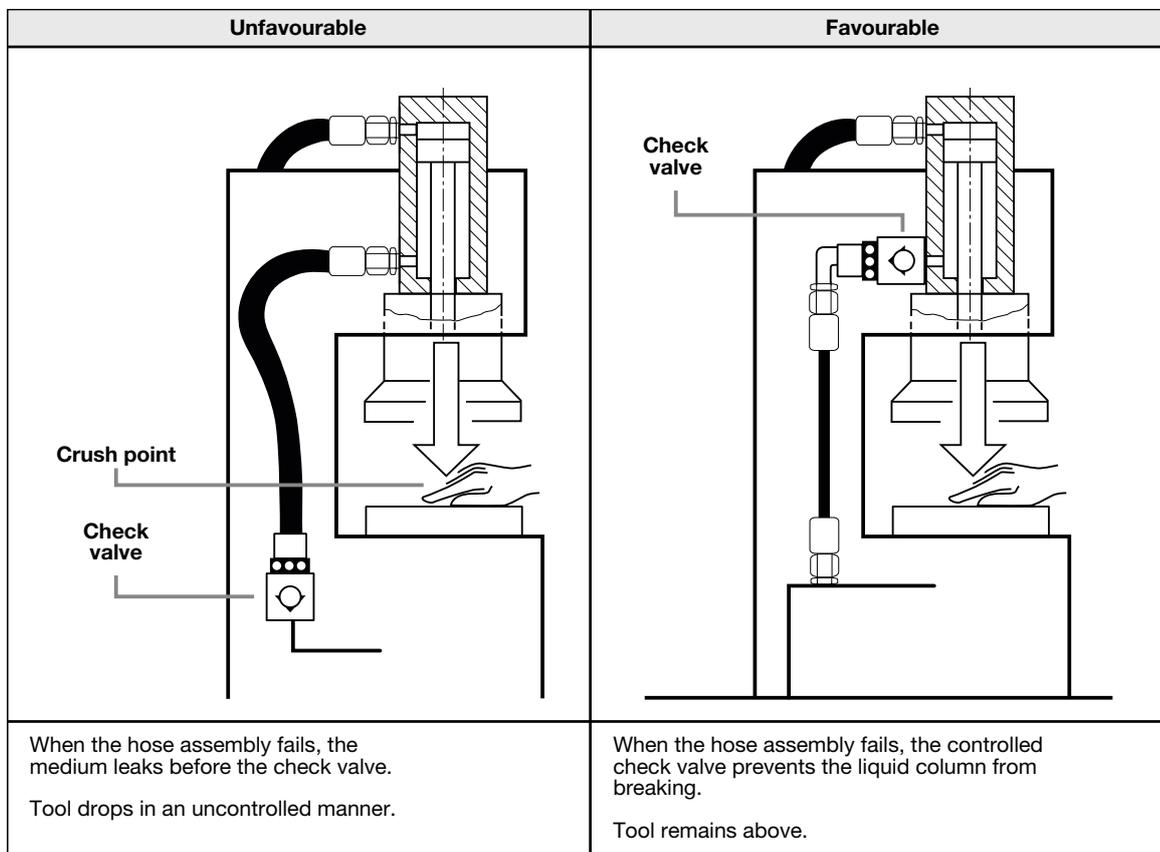


Non-fragmenting rupture disc (reverse buckling disc).

▶ 7.2 Mechanical design

In real life, none of these assumptions can be guaranteed. For this reason, it is advisable to take a different route. The failsafe principle knowingly permits errors. However, the systems are designed and constructed so that a safety-related crash does not lead into the abyss but stops at an agreed level. The systems react to faults in such a way that they “fail” to safety - although this only applies to known, identifiable and foreseeable faults. This assumes that energy for this function may be supplied within the system not just in case of emergency, but that sufficient energy is always stored in advance. This will be dissipated in the case of danger and the system transferred to a low-energy and therefore stable condition. Implementation of this principle often makes use of ever-present effects such as gravitational or frictional forces and the self-locking that can be achieved through these means.

In redundant systems, more components are provided to fulfil a function than are actually necessary. The assumption is as follows: If one of these components should malfunction or fail, the other will completely take over its function. The principle is to achieve the greatest possible reliability with a minimum of redundancy. As reasonable as this principle may be, it does have one important weakness: Experience shows that there are always situations, and always will be situations, in which all redundant components fail simultaneously due to a common cause failure. These situations are very difficult to predict and control through the design. Consistent but expensive diversity, particularly in terms of physical diversity, produces the best results.



Hose assembly with check valves.

▶ 7.2 Mechanical design

Redundancy	No.	Example	Explanation
Homogeneous	1		Duplication only increases safety when no systematic errors can occur, e.g. corrosion, material mix-up, which can render both safety devices ineffective simultaneously.
Diverse (components)	2		Diversity in the action principle of the safety device: Switching the action principle makes it unlikely that the independent safety devices, which operate to different principles and are made by different manufacturers, would fail simultaneously.
Diverse (process variables)	3		Diversity in the physical principle: Each of the diverse, controlled valves is activated by the control systems CS1/CS2, which react if a limit value on two process variables connected by a physical law (e.g. general equation of state) are exceeded.

Homogenous and diverse redundancy.

▶ 7.2 Mechanical design

7.2.3.2 Design measures against deterministic hazards

Deterministic hazards can be attributed to the functional design of the machinery, as required by technical necessity, and the employed procedures. Targeted design measures are intended to stop the possibility of latent dangers impacting on people. Three methods have been developed in the course of technical progress:

1. Indirect safety technology
2. Direct safety technology
3. Informative safety technology

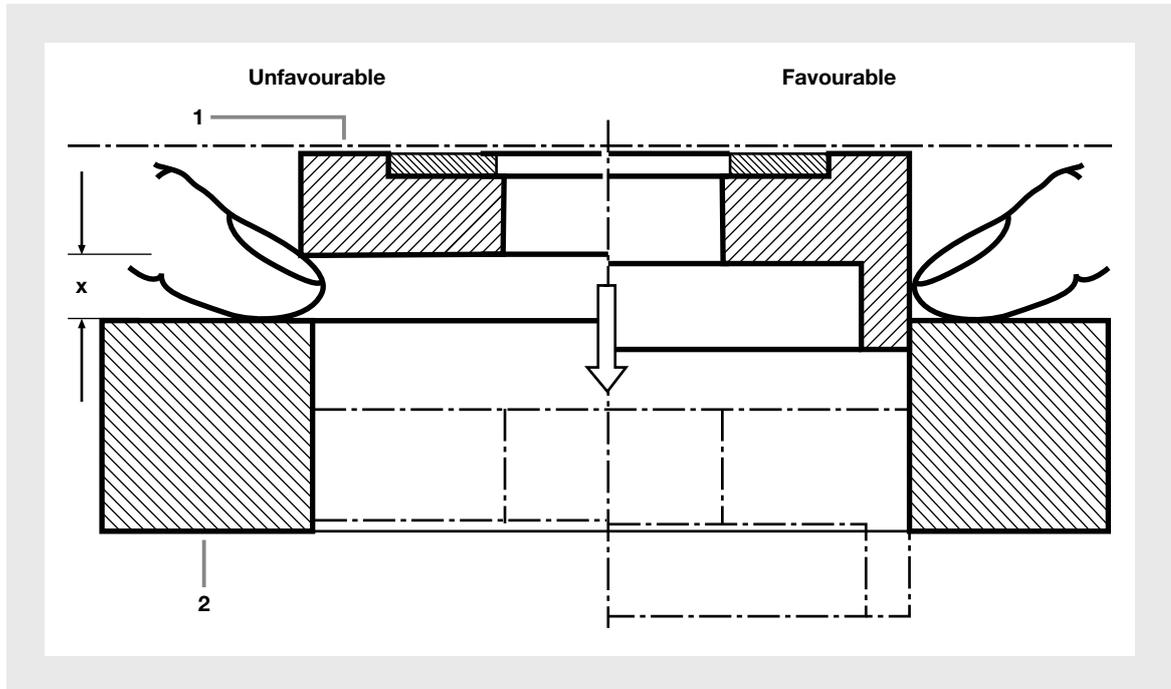
In contrast to the measures taken against stochastic hazards, which are fundamentally regarded as being of equal value, the EC Machinery Directive specifies the sequence and priority in which the respective measures against deterministic hazards should be applied:

1. Indirect
2. Direct
3. Informative

Safety technology methods			
Safety technology	Indirect	Direct	Informative
Action principle	Avoid dangers	Secure against dangers	Warn against dangers
Diagram			
EC Machinery Directive, EN ISO 12100	Eliminate or minimise dangers	Take the necessary protective measures when dangers cannot be eliminated	Instruct the user about the residual risks

Safety technology methods.

▶ 7.2 Mechanical design



Shearing hazard avoided by design.

7.2.3.2.1 Indirect safety technology

Methods using indirect safety technology attempt to configure components, machines and processes in such a way that they present no risk, or only a low, accepted risk to people. Geometric and energetic measures are available:

Geometric measures attempt to avoid the hazardous effect of danger points on moving machine parts by complying with standardised minimum distances to ensure that dangerous bottlenecks do not even arise, or by making such bottlenecks inaccessible by complying with safety distances.

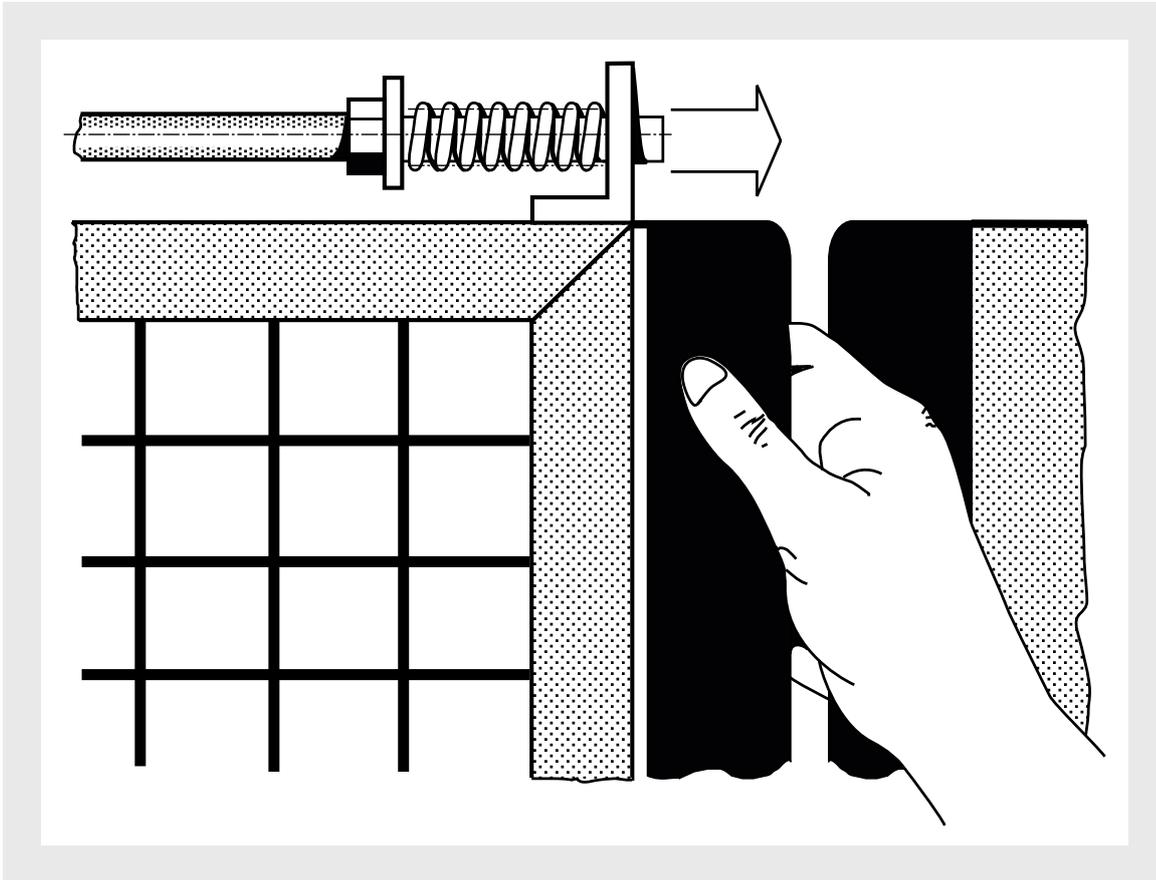
Energetic measures attempt to stop the hazard's underlying energy having a harmful effect on people, by:

- ▶ Limiting the effective energy
- ▶ Interrupting the flow of energy to people
- ▶ Targeted deformation of machine parts rather than the human body

The first measure attempts to limit the energies and forces that occur at a danger point, so that their impact remains below acceptable physiological values. Technically, however, such an energy level is generally only of limited use. The second measure prevents harmful impact on people by interrupting the flow of energy or forces towards the human body before the pain threshold is reached. The third measure reduces the rigidity of machine parts to such an extent that, if a danger point is accessed, machine rather than body parts are deformed.

Caution is required, however: Indirect safety technology is often portrayed as a “silver bullet”, but it cannot be applied on danger points with technological functions. Safeguards against these dangers should be provided via special measures such as protective devices, for example.

▶ 7.2 Mechanical design



Elastic closing edge on protective devices.

7.2.3.2.2 Direct safety technology

Components used in direct safety technology safeguard against dangers that are necessary to the machine function and therefore cannot be avoided. Protective devices are arranged between operator and danger, preventing the two coinciding in time and space. Guards or protective devices are used.

Guards, e.g. enclosures or covers, form impenetrable physical barriers and as such protect against entry or access to hazardous situations. They can also prevent operators being hit by objects ejected from the protected areas.

Although protective devices such as two-hand circuits or light beam devices do not prevent entry or access to hazardous situations, they do render them ineffective by influencing the process via the machine control system as soon as they are activated.

Ergonomic aspects decide on the manageability and therefore the acceptance of the protective devices. The most important ergonomic requirement is that the demands placed on operators during day-to-day handling of the protective device must be no more than necessary.

7.2 Mechanical design

Protection against	Breaking the cause and effect relationship	Effect via	Diagram	Description	Examples	Explanation
1	2	3	No. 4	5	6	7
Danger sources 	Space 	Static physical barriers 	1 	Fixed guard	Trap covers, protection structures on earth moving machinery (ROPS, FOPS)	Safeguards hold back the uncontrolled moving parts, absorb their kinetic energy and stop them reaching people.
			2 			
Danger points 	Space and time 	Mobile physical barriers 	3 	Impeding device	Finger impeder, hand impeder	Safeguards are kinematically connected to hazardous movements. They positively keep people away from danger zones.
			4 			
	Time 	Reliable control measures 	5 	Safeguard that binds you to a location	Enabling switch, hold-to-run control device, two-hand circuits	During the hazardous movement, safeguards bind people to a safe location, from which they cannot reach the danger points. If a person should leave the safe location, the hazardous movement is stopped.
			6 			

Basic types of protective device.

▶ 7.2 Mechanical design

7.2.3.2 Informative safety technology

As the final option in combating deterministic hazards, informative safety technology attempts to ensure that at-risk personnel observe safe work practices through targeted messages and information, using methods such as: Safety signs, safety guidelines in operating manuals, internal company instruction organised by the machine user etc. The effectiveness of this method varies from country to country. It can certainly enjoy considerable success in other cultures, but it should not necessarily be relied upon in European countries. Due to different mentalities among the population, priority must be given to technical protective measures that are activated automatically and prevent or safeguard against dangers.

It would be practically impossible to build a machine with an acceptable level of risk using only one of the design measures listed here. The various methods used in these measures must instead be co-ordinated to ensure they complement each other and are effective both functionally and overall. ¹⁾

¹⁾ Source: Neudörfer A.: *Konstruieren sicherheitsgerichteter Produkte [Design of safety-related products]*, 4th edition, Heidelberg, Berlin, New York et al, Springer, 2011

▶ 7.2 Mechanical design

Information parameters			Example	
Channel	Process	Means		
1	2	3	No.	4
Visual 	Static 	Text	1	Operating instructions
			2	
		Graphic symbol	3	Stop, halting a movement Rapid stop ISO 7000
		Safety mark	4	
		Marking	5	 Colour combination: Yellow-black (permanent danger) Red-white (temporary danger)
	Dynamic 	Light signals	6	
		Active diagrams	7	<ul style="list-style-type: none"> 1 • Main motor 2 • Infeed table open 3 • Cover open 4 • No compressed air 5 • Film broken 6 • Magazine empty
		Process visualisation, simulation	8	
Aural 		Acoustic signals	9	
Tactile 		Moving objects	10	Evasive safeguard

Means of informative safety technology

▶ 7.3 Pneumatic design

7.3.1 Introduction

Pneumatics ranks among the drive technologies in engineering, alongside electrics and hydraulics. To ensure that a machine can be operated safely, it is not enough to identify hazards and then pass this information to a control system or safety components. The drives must also be brought to a safe condition; only then is the machine safe.

7.3.2 Well-tried principles and protective measures

Safe pneumatics can be divided into two basic fields: Firstly, the basic and well-tried principles, as described in Annex B of DIN EN ISO 13 849-2, and secondly, the protective measures relevant for pneumatic drives. These include control technology solutions that move a cylinder in accordance with a desired behaviour.

7.3.2.1 Basic and well-tried principles

First let's look at some basic and well-tried principles of pneumatics. These include good compressed air treatment: Compressed air must be filtered and must be free of water and compressor oil. Poorly treated compressed air will cause elements to malfunction. Valves no longer switch and become stuck; cylinders may move unintentionally due to leakages. And there's the recurring question on whether or not to lubricate compressed air. The maxim here is: Lubricate once, lubricate forever. However, today's pneumatic components have lifetime lubrication and no longer need to be lubricated. If new components are built into old machines on which the compressed air is lubricated, the new parts will also be lubricated. In this case, select a lubricant that is valve-compatible. Only use a small amount of lubricant, for "overlubrication" will also lead to malfunctions.

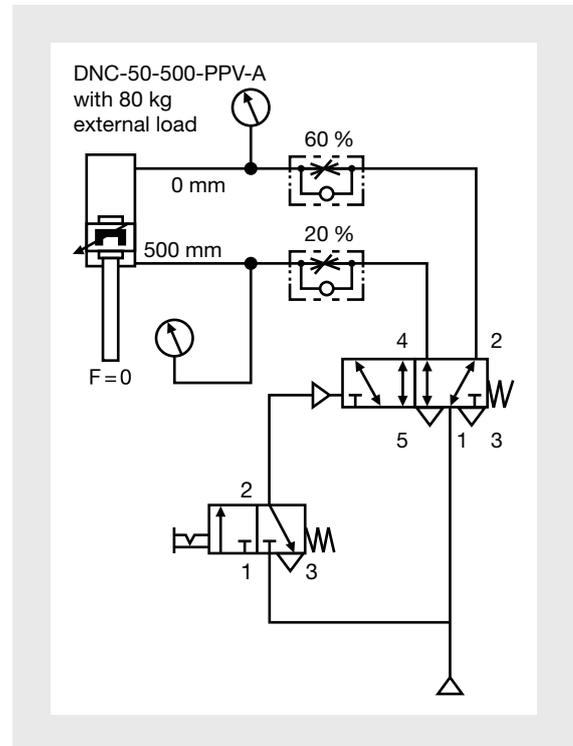
7.3.2.2 Selection and dimension

The pneumatic components should be selected and dimensioned to withstand the expected demands. Environmental conditions such as temperature, oils, acids, alkaline solutions and cleaning agents should be noted. A good safety-related circuit is worthless if aggressive cleaning agents soften the pneumatic hose. Pneumatic cylinders are normally calculated to apply the necessary force required within the machine. However, the calculation should also take account of kinetic energy. If a cylinder moves too quickly – applications frequently require high cycle counts – the energy with which a pneumatic cylinder travels to the end position will be correspondingly high. This will damage the cylinder in the long term.

▶ 7.3 Pneumatic design

7.3.2.3 Pressure limitation

Another basic principle is pressure limitation. A pressure relief valve is located on the air chamber behind the compressor and protects the air chamber from explosion. The machine has an integrated service unit, which regulates the operating pressure. If the setting for the operating pressure is turned up, the forces within the plant will increase, which can lead to an overload. Consequently, the machine operator should not be able to change the operating pressure without authorisation. It makes sense, therefore, to have a pressure relief valve in the service unit, protecting the machine from a dangerous failure of the pressure regulator. If there were any defect, the machine would face the full mains pressure. For this reason, further pressure limitation measures are required, which will concern the dimensioning of the cylinder. Where pneumatic cylinders are installed vertically, excess pressure arises on the cylinder due to the moving mass, the operating pressure and the surface difference. If this cylinder is then to be stopped pneumatically, e.g. by closing off the compressed air, pressure peaks of well over 30 bar are possible. In turn, this pressure will overload all the pneumatic components used in this part of the circuit.



Circuit diagram, pressure values (source: Festo)

Component description	Identifier	State variable	0 1 2 3 4 5 6 7 8 9 10
Cylinder, double-action	DNC-50-500-PPV-A	Travel mm	
Pressure gauge	Pressure up	Pressure bar	
Pressure gauge	Pressure down	Pressure bar	

Pressure values (source: Festo)

▶ 7.3 Pneumatic design

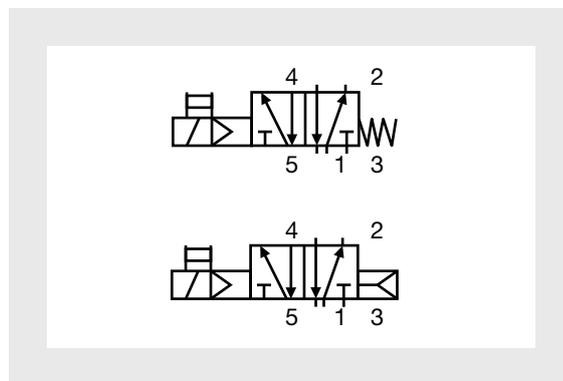
These pressure peaks can be reduced by installing a pressure regulator between the operating valve and the upper cylinder connection. In this case, the cylinder's downward movement is supported not with the normal operating pressure but with a pressure reduced to 2 bar. If the cylinder is subjected to very high pressure, no pressure is needed for the downward movement. In this case, a silencer is screwed into the upper cylinder connection. The cylinder can then be controlled with a 3/2 directional valve because the pressure is only needed for the upward movement.

7.3.2.4 Positioning of safeguards

Application in conjunction with a light beam device or two-hand circuit provides another reason for ensuring that the design of a pneumatic circuit is thorough and correct. In accordance with DIN EN ISO 13855 "Positioning of safeguards with respect to the approach speeds of parts of the human body", the stopping performance of a hazardous drive must be measured and the measurement used to determine the distance of the light beam device or two-hand circuit. The speed of a pneumatic cylinder depends not only on the operating pressure, mass and mounting position, but above all on the screw joints, hoses and valves that are used, along with their flow rates. If the latter is not calculated, the assembler will determine the machine's cycle counts and thereby the stopping performance for a light beam device, based on a greater or lesser degree of knowledge. If an operator then changes the hoses and screw joints, enabling a higher flow rate, he will be changing the stopping performance at the same time. The distance of the light beam device may no longer be sufficient for this drive; the risk of a hazardous incident would increase significantly. It is advisable, therefore, to make all the drive calculations in full and to include the values for hoses and screw joints in the circuit diagram. An indication that the information is "safety-related" also makes sense. A photograph during the acceptance test, showing exactly this layout, would also be a helpful guide in the event of any legal dispute.

7.3.2.5 Basic principle of mechanical springs or air springs

The mechanically well-tryed spring is another basic principle of safety technology, in mechanics as well as pneumatics and hydraulics. On valves with a mechanical spring, the valve's switching position is clearly defined if the control signal or even the compressed air supply is switched off. This is not the case on pulse valves (bistable valves with 2 coils). When selecting monostable valves it is worth paying particular attention to the return mode, for not only are there mechanical spring return valves but also air spring return valves. The diagram below shows two monostable valves. The upper valve has a mechanical spring, the lower valve has an air spring. The return mode is shown on the right-hand side of the valve. These are 5/2 directional valves with pilot control, manual override and electrical activation.

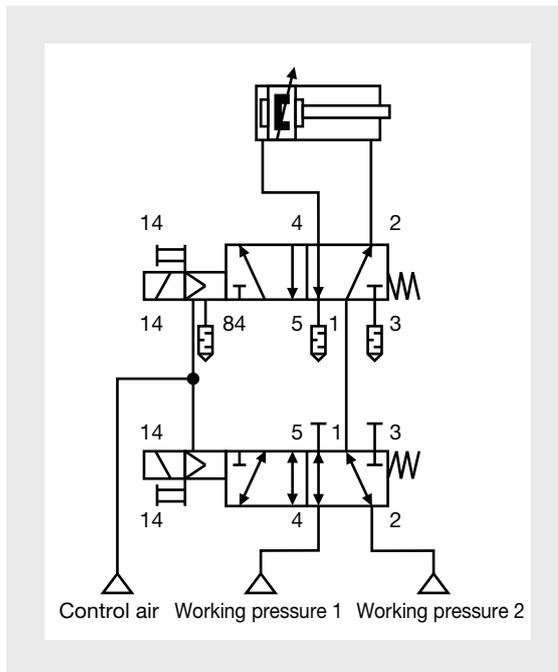


Monostable valves with mechanical/air spring
(source: Festo).

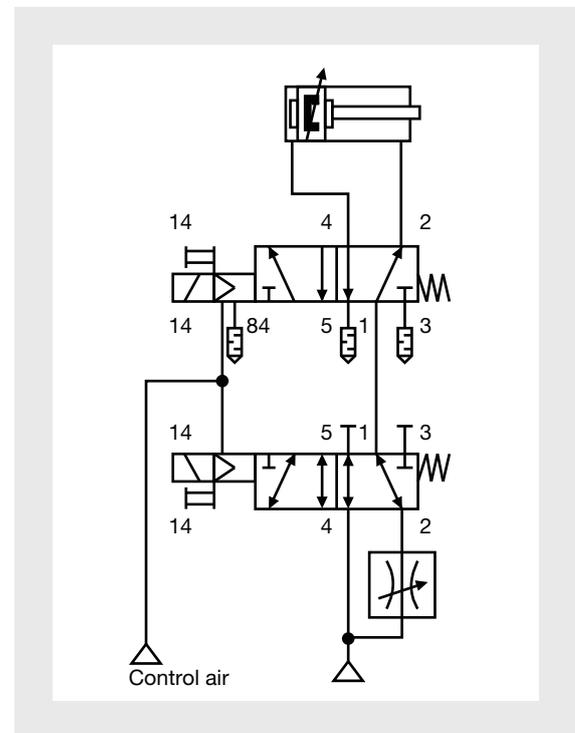
▶ 7.3 Pneumatic design

However, air-spring valves can only be reset if sufficient pressure is available for the air spring. The compressed air supply to the air springs can come from pressure port 1 or from a separate control air connection. Ultimately, this depends on the valve series. Specialists must clarify whether air-spring valves can be used in safety-related circuits, and under what conditions. Very close attention must therefore be paid to the design of the valve in pneumatic circuit diagrams.

Further safety principles in pneumatics concern the reduction of force and speed. These are mainly applied in set-up mode. Force is reduced by lowering the operating pressure for the cylinder. In pneumatics, speed is generated via the intensity of the flow rate. In both cases, the supply of pressure to the operating valve is simply switched. The risk assessment will determine whether this switchover needs to be single or dual channel.



Reduced force (source: Festo)



Reduced speed (source: Festo)

The circuit diagram for reduced speed only represents the principle. As the hoses and screw connections between the operating valve and the cylinder also affect the speed, reduced speed is generally achieved through valves that sit directly on the cylinder.

▶ 7.3 Pneumatic design

7.3.3 Circuit-based solutions

Having looked at some examples for basic and well-tried principles in pneumatics, let's look now at the actual protective measures. Protective measures for safety-related pneumatics describe circuit-based solutions. These include:

- ▶ Protection against unexpected start-up
- ▶ Ventilation and venting
- ▶ Braking movement
- ▶ Blocking movement
- ▶ Reversing movement
- ▶ Free movement option
- ▶ Balancing forces on the drive

Protection against unexpected start-up

In the first instance, a manual start-up valve on the service unit provides effective protection against unexpected start-up. With this manual valve, the maintenance engineer can vent the machine, using a padlock to protect against a restart. The next sensible measure is an electrical start-up valve, which can be activated via a higher level control system. This measure also includes a pressure sensor, which monitors the operating pressure. The control system detects any drop in pressure and consequently switches off all the outputs plus the soft start valve. As soon as the corresponding operating pressure has returned, the control system switches the compressed air back on and ventilates the machine and its drives.

The proper selection of operating valves is another effective protective measure. Valves with a separate control air supply cannot be switched without control air. As a result, valves would be prevented from switching in the event of an electrical fault. What's more, if the installed operating valves are closed in their rest position, there will be no cylinder movement when the machine is ventilated, as the compressed air is still unable to reach the cylinder. If the installed operating valves allow air to reach the cylinder when the compressed air is switched on, a slow build-up of pressure is generally desirable. A soft start valve can be used in this case. This valve will initially ventilate the machine slowly via a throttle point. The valve will not open fully until an operating pressure of 3 bar is present, for example. Only at this point will the entire operating pressure be available at full flow rate. So this valve can be used to perform slow, controlled cylinder movements in the initial ventilation phase. Should a hose be installed incorrectly, there would immediately be an audible hissing sound, but the hose would not thrash about forcefully, as it would if full pressure were applied.

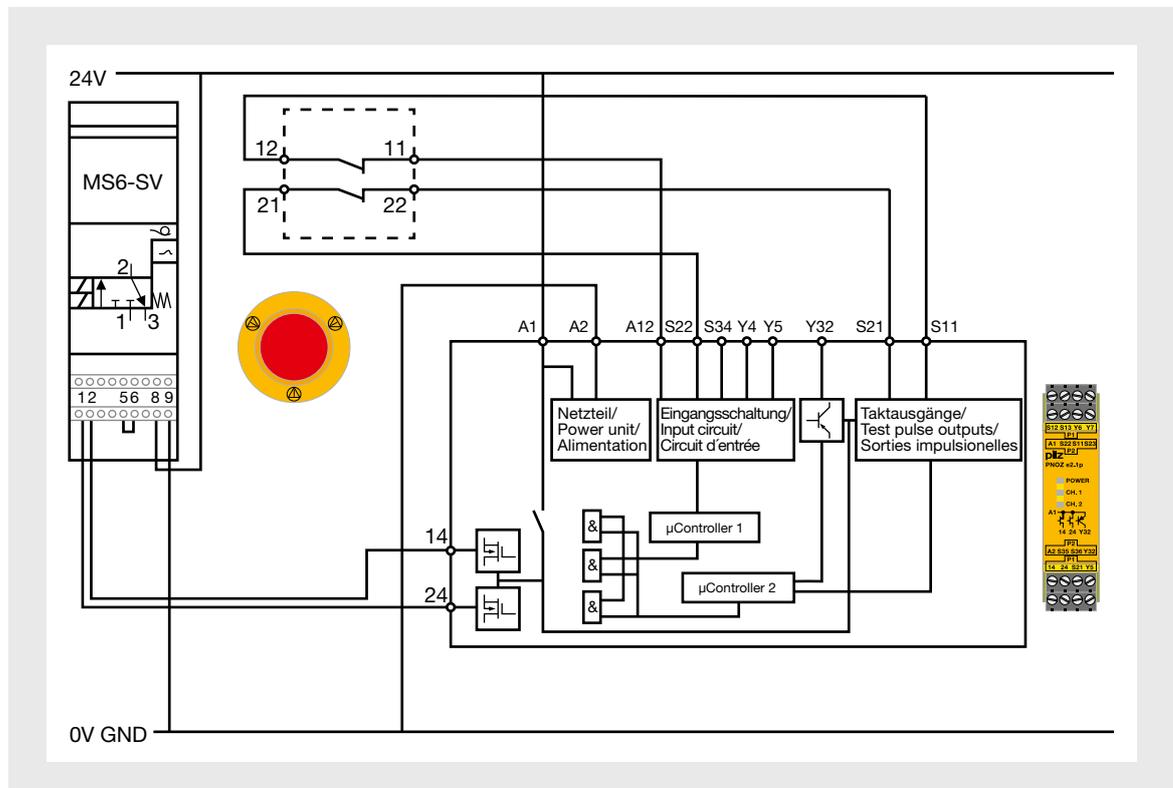
▶ 7.3 Pneumatic design

7.3.3.1 Venting

Venting is frequently used as a protective measure. It can be used when the cylinder presents no danger in a de-pressurised state. However, the respective mounting position and the mass at the cylinders must be taken into account. The concept of this measure is similar to that of removing power in the electrical field: The electrical voltage is simply switched off to avoid hazards from contact with electrical cables. The principle is exactly the same in the pneumatic field, for without power/compressed air, there's no danger. However, in safety technology it is always necessary to examine the mechanics which will ultimately have to perform the movements. If a vertically-installed cylinder is vented, the cylinder piston will obey inertia and move downwards. Additional protective measures must be considered for this exact scenario. In

industry, however, the practice of ventilating and venting is coming under increasingly critical scrutiny for quite different reasons: The procedure costs a lot of time and therefore money; productivity falls.

The fact that safety is the first priority is undisputed. A machine can certainly be ventilated and vented at performance level PL = "e". The soft start and exhaust valve MS6-SV is a safety component in accordance with the MD 2006/42 EC and meets performance level "e". It is an intrinsically safe, redundant, mechatronic system in accordance with the requirements of DIN EN ISO 13849-1. The pneumatic safety-related objective, i.e. safe venting, is guaranteed even if there is a fault in the valve (e.g. due to wear, contamination).



Schematic, safe ventilation and venting (source: Festo).

▶ 7.3 Pneumatic design

The schematic on page 8-26 shows a circuit with a dual-channel design for safe ventilation and venting. Two enable signals are sent from the electronic safety relay to pins 1 and 2 on the MS6-SV. An additional electronic safety relay would draw attention to any shorts between the two devices. As a result, performance level “e” can be achieved. The circuit diagram does not show the potential feedback from MS6-SV to the PNOZ. A volt-free contact, which is incorporated into the feedback loop, is available for this purpose. This enables the PNOZ to detect whether the MS6-SV is ready for operation.

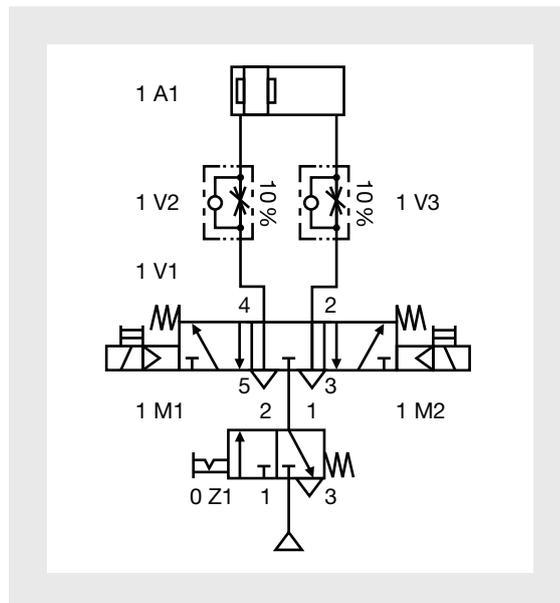


Festo MS6-SV (source: Festo)

Single-channel ventilation and venting is also possible, of course. Electropneumatic valves in the service unit fulfil this purpose, receiving their commands from the higher level control system or from a single-channel safety circuit. Venting can also be implemented via the operating valve 1 V1.

7.3.3.2 Normal operation

In normal operation, one of the two valve coils 1 M1 or 1 M2 is always under voltage. As a result the valve is switched. So the cylinder piston is either in one end position or moves from one end position to the other. The cylinder is vented when the operating valve is in its middle setting. This is the case when both coils are de-energised. The venting process on the operating valve is faster than venting via the service unit because the route for the compressed air is shorter and the pressure volume is lower. If venting is performed via the service unit, several cylinders will be vented and at the same time the pressure volume will be higher. There is another advantage to venting via the operating valve: Additional protective measures can easily be implemented in parallel on other cylinders, such as “reversing” for example.



Venting with 5/2 directional valve (source: Festo).

▶ 7.3 Pneumatic design

7.3.3.3 Reversing

“Reversing” as a protective measure is the right choice when the movement of the cylinder piston is dangerous in only one direction.

The monostable 5/2 directional valve, as shown in the diagram with 1 V1, needs an electrical control signal at the coil 1 M1 in order to switch the valve. The cylinder’s piston rod extends in sequence. If the coil is switched off, the control force on the left side of the valve will be missing. The mechanical spring on the right side can switch the valve back on; the piston rod continues to retract. In the normal machine cycle, the control system switches the valve coil on and off. A safety relay connected between the control system and the valve coil can also switch off the coil. In this case, it would be irrelevant whether the output on the control system (a non-safety-related PLC for example) is still switched on. Even if the electrical supply voltage should fail, the

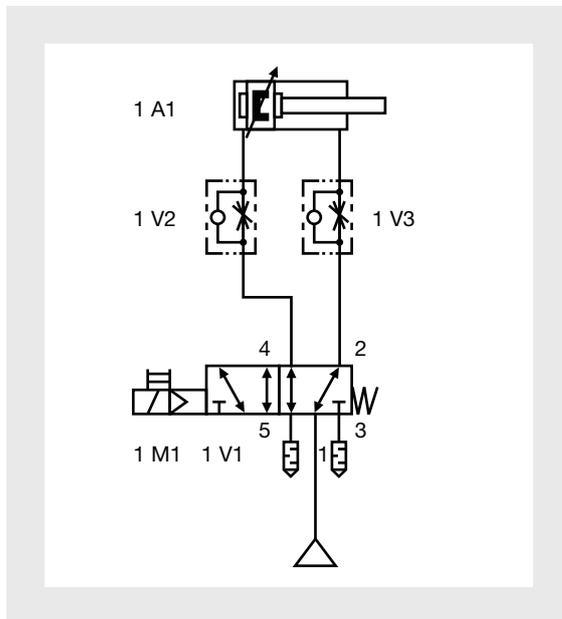
valve would be switched back to its home position. The piston rod cannot reverse until compressed air is returned. The emergency stop function therefore needs a stop category 1 for reversing. The compressed air will not be switched off until the cylinder has reached its safe end position. A stop category 0 switches off the compressed air supply immediately and cannot be used in this case because reversing would no longer be possible.

All pneumatic circuit diagrams must allow for a total failure of the compressed air supply. The electronic control system detects the failure of the compressed air: To ensure that the piston rod has sufficient air available to guarantee that the piston rod can reverse, a stored volume is arranged upstream of the operating valve. A check valve is connected upstream of the stored volume, to ensure that the stored air cannot discharge in the direction of the compressed air supply. As a result, the compressed air always flows in the direction of the cylinder.

7.3.3.4 Failure mode

When considering the failure mode of the operating valve, the following possibilities are conceivable:

- ▶ The valve does not switch, so the piston rod does not move either. There is no danger. There may be various causes. It may be that voltage is not reaching the valve coil, the valve may be defective. Sometimes the armature in the coil or the piston in the valve may stick.
- ▶ A different type of error occurs if the valve does not switch back. In this case, the piston rod continues to extend or remains extended. On the electrical side, a short may be the reason, or possibly the valve piston is hanging up. In any case, this is a dangerous failure.



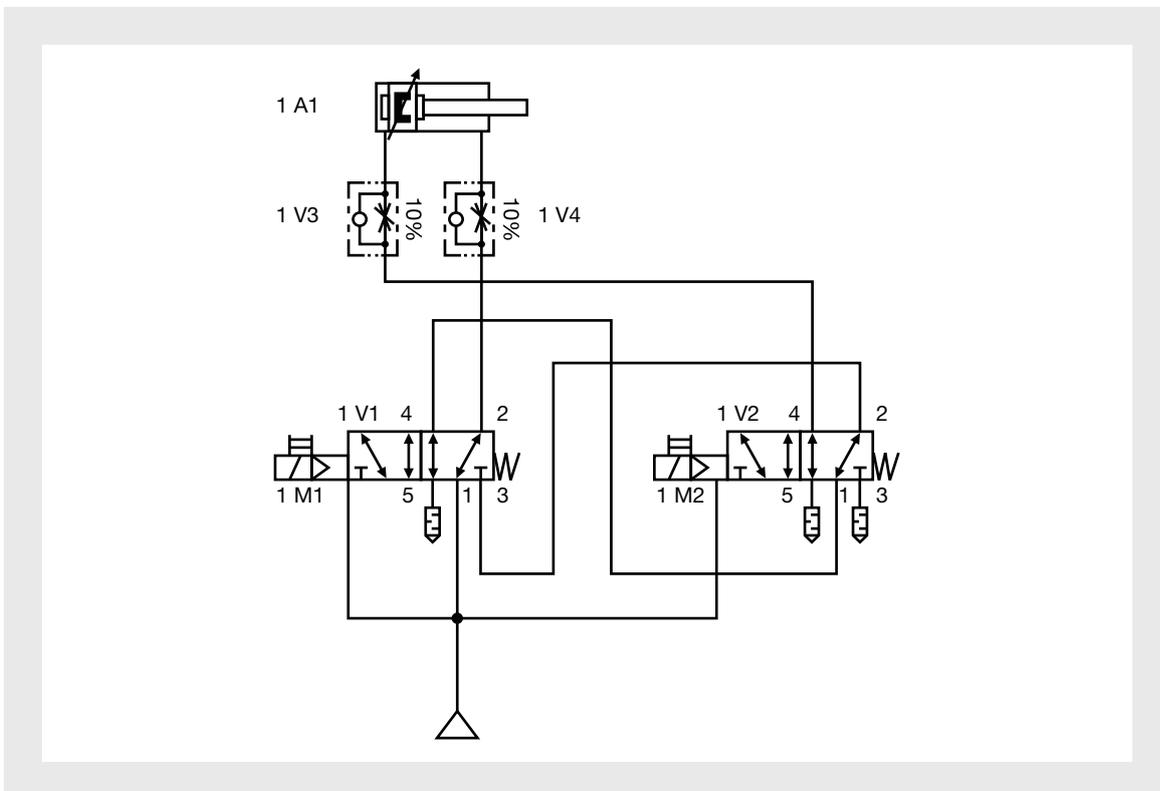
Single-channel reversing (source: Festo)

▶ 7.3 Pneumatic design

▶ Another error source lies exclusively within the valve: The valve piston remains stuck in an intermediate position. To be able to describe this fault more specifically, you need to be familiar with the internal design of the valve. The question is, when the valve piston is in the intermediate position, are all the valve's connections blocked off or interlinked? If all the connections are blocked off, compressed air can no longer flow through the valve. If the cylinder piston is extended, compressed air would no longer flow in, but neither would any air flow out of the cylinder. This would represent a dangerous failure of the valve. If all the valve's connections are interlinked, the cylinder would possibly not be completely de-pressurised, but its force would be substantially reduced. Ultimately, the cylinder's mounting position and the mass to be moved would need to be considered in order to estimate the danger.

It is clear that single-channel systems will fail in the event of a dangerous failure of one component in the safety chain. As a result, they can only be used when the risk is low. For greater risks, dual-channel systems should always be selected.

On a dual-channel system, both operating valves 1 V1 and 1 V2 must be switched to enable the piston rod to extend. If one valve fails to switch, the piston rod will not extend. If both valves have switched and one valve switches off, because the cable to the coil is broken for example, the piston rod will retract, even if the other valve is still switched. If one of the two valves becomes stuck in the switched position but the other valve can still be switched, the piston rod will either extend or retract, depending on how the functioning valve is connected. This is called single fault tolerance, as a dangerous failure does not lead to the loss of the safety function.



Dual-channel reversing (source: Festo)

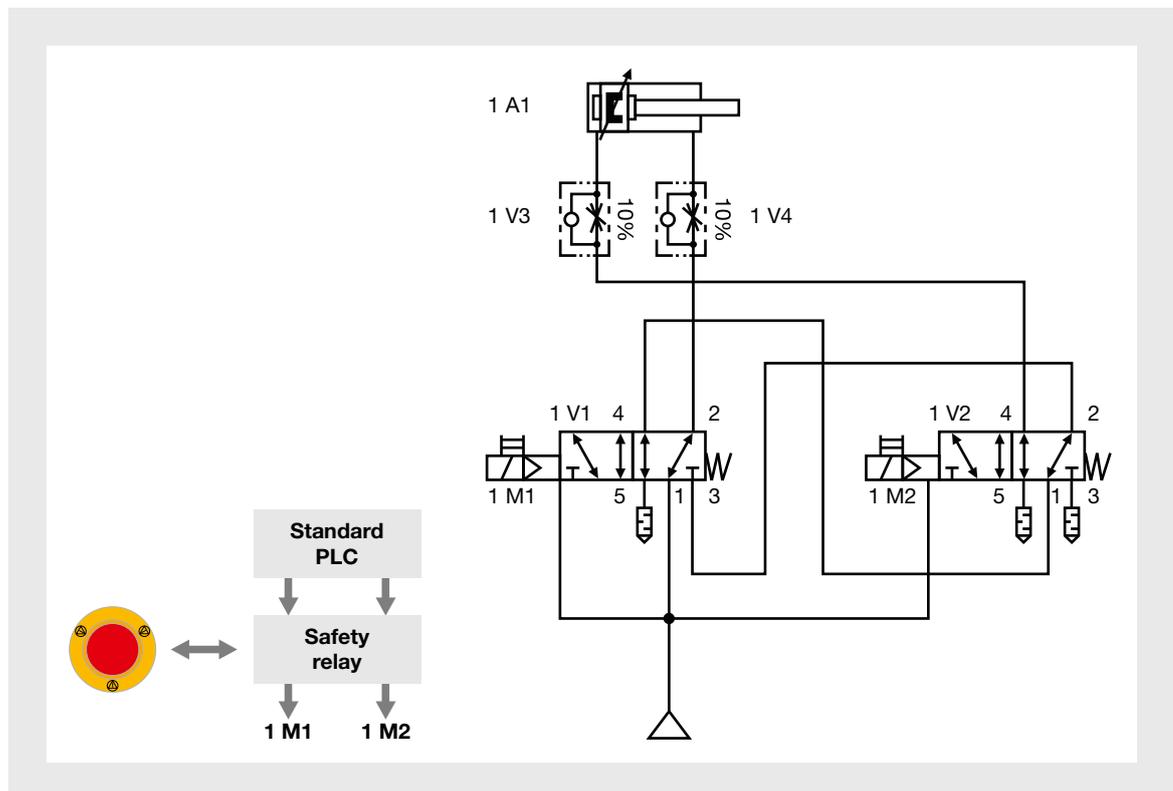
▶ 7.3 Pneumatic design

How do you detect a dangerous failure on a valve? Valves with integrated switching position sensing offer one possibility. These valves have an integrated sensor in the body of the valve, which senses the switching position of the valve piston. A diagnostic coverage of 99% can be applied when calculating the performance level for this valve. Pressure sensors on either of the two valve outputs are another possibility. When a signal changes at the valve coil, the signal at the sensor must change within a very short time, in which case the valve, sensor and wiring are all in order. This applies for the pressure sensor as well as the sensor integrated within the valve.

A third possibility is provided by valve diagnostics, which make use of the sensors that are normally installed on the cylinder to sense the cylinder's switching position. This demands some skill from the programmer, however. The cylinder's piston rod is in the rear end position; the sensor registers this position. Initially, only one operating valve is switched, so the piston rod is not yet permitted to

leave the end position. The piston rod may only leave the end position once the second valve is switched. If the piston rod were to extend even as the first valve was switched, this would indicate that the second valve was already switched. A fault would therefore be present. The other operating valve must not be switched until the next cycle; this is the only way to detect a dangerous failure of the second valve. It is important to check all sensors for a signal change, for only a signal change confirms that the sensor and wiring are operating correctly. The example below illustrates the interaction between pneumatics and electrical engineering.

A standard PLC controls the normal machine cycle. As the cylinder is categorised as a dangerous drive, a risk analysis resulted in a dual-channel design for controlling the cylinder. If a dual-channel safety switch acts upon a dual-channel safety relay, the safety relay will switch off the coils on both valves 1 V1 and 1 V2 if the safety switch is operated. The PLC needs a signal so that it can also



Interaction between electrical engineering and pneumatics (source: Festo).

► 7.3 Pneumatic design

switch off the outputs to the coils. The safety function impacts upon the PLC, therefore. A performance level of “d” to “e” can be achieved, depending on the diagnostics. The valves will require a diagnostic coverage of 99 % for PL = “e”.

7.3.4 Stopping and braking

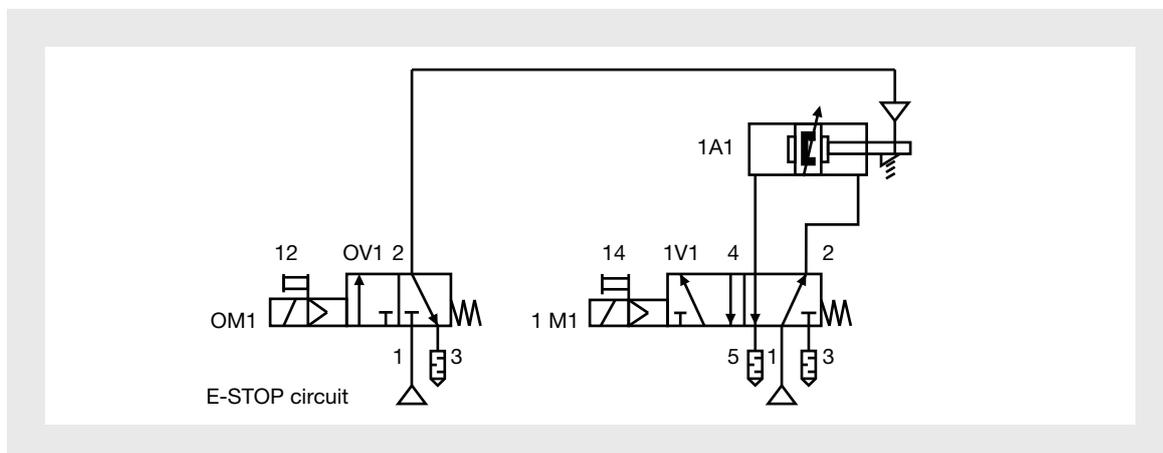
Another protective measure is to stop or brake a movement. The intended use and application must be clarified quite specifically in advance. The clamping cartridge is a holding brake; its sole purpose is to clamp the piston rod once it has already stopped. A service brake can absorb kinetic energy, so a moving piston rod can be decelerated using a service brake.

Clamping cartridge

A clamping cartridge is used when a vertically installed cylinder is to be held at an end position in order to stop any further downward movement of the piston rod in the event of a compressed air failure. It is important that the clamping cartridge does not close until the piston rod is at the end position and has come to a stop. If a cylinder with a service brake is used instead of a clamping cartridge, the movement can be stopped at any time. But what happens if the piston rod is in an intermediate position between the two end positions as the brake is opened? If the cylinder is installed vertically and is de-pressurised, the piston rod will move downwards with its mass. This generally means danger. Admittedly, this danger would no longer exist with a horizontal installation. If the cylinder still contained compressed air and the piston rod happened to be in an intermediate position, a hazardous movement would still occur as the brake was opened. One side of the cylinder is ventilated, the other side is vented. “Pre-vented” systems generate very high acceleration values and speeds. 3/2 directional valves provide an elegant solution in this case.



Cylinder with clamping cartridge (source: Festo)



Cylinder with clamping cartridge and monostable 5/2 directional valve (source: Festo).

▶ 7.3 Pneumatic design

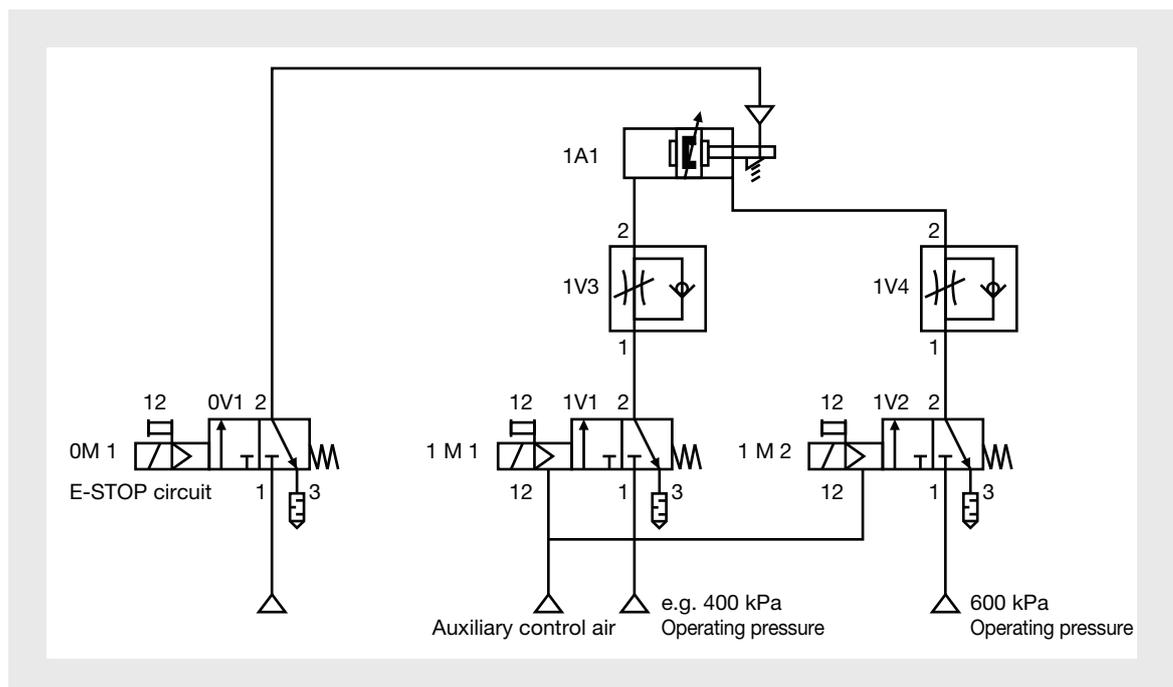
4 switch variants are possible with two 3/2 directional valves: The cylinder is de-pressurised on both sides when both valves are switched off (as shown in the circuit diagram). If both valves are switched, the cylinder is ventilated on both sides. Forces need to be balanced on the valve piston to ensure that the piston rod remains stationary as the brake is opened. This requires different operating pressures on the two 3/2 directional valves. The values that are required here depend on the mounting position and the mass at the piston rod. Once the brake is

open, one of the two valves 1 V1 or 1 V2 switches off; the piston rod moves slowly in the required direction. Two throttle check valves 1 V3 and 1 V4 are responsible for the slow movement. These valves are incorporated as exhaust throttles in order to restrict the compressed air flowing from the cylinder. Exhaust throttles are only effective if there is air in the cylinder, which is another reason why it should be ventilated before the brake is opened.

In this context, we are reminded once again of the correct design of the pneumatic drives, as described previously under the basic and well-tried principles. For the design is especially significant for the brake. It is commonly believed that a compressed air signal achieves a higher speed in a thin hose than it does in a thick hose. The lower volume is generally given as the reason. However, the flow behaviour within the hose has a much greater significance, as the following graphic shows.

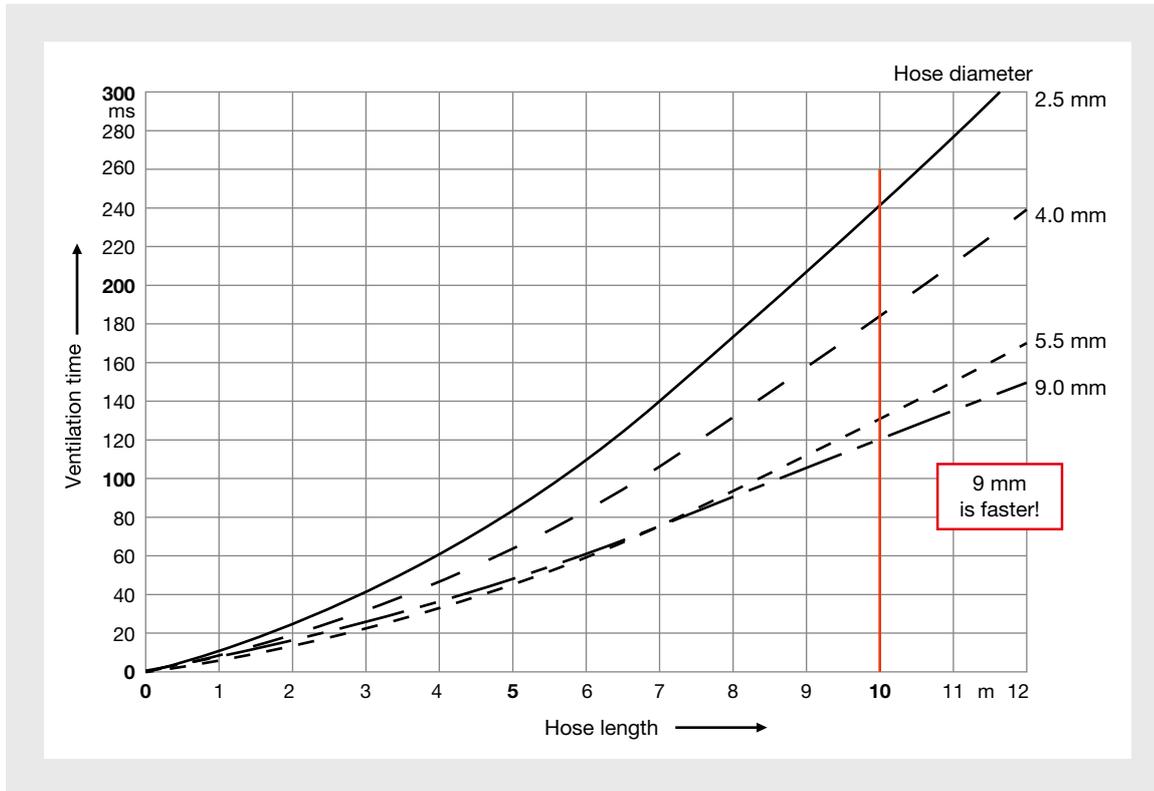


Cylinder with brake (source: Festo)



Cylinder with brake (source: Festo)

► 7.3 Pneumatic design



Ventilation time based on hose length and diameter at 6 bar (600 kPa) (source: Festo).

The ventilation time rises as the length of the hose increases; the increase is more pronounced on thin hoses than on thick ones. The behaviour when venting is the same, so the brake's reaction time depends on the hose. With a long, thin hose, the brake activates later than with a short, thick hose. For this reason, it is always beneficial to locate the shift valve directly on the brake. The brake closes when the pressure drops below approx. 3.5 bar. So when the compressed air drops below the set operating pressure, the brake reacts more quickly. However, care needs to be taken if the machine operator can adjust the operating pressure on the machine himself. If the operating pressure is increased, the venting time will also be extended. The brake will react later, the stopping performance will be longer. Brakes and clamping cartridges are zero fault tolerant, in other words, they can fail. Just like on a car, a brake is subject to constant wear. For this reason, it must be tested at appropriate intervals. For further details on the design and testing of the brake please refer to the operating

manual or consult the manufacturer. The influence of hose length and diameter is also important for the cylinder speed. The shorter and thicker the hose, the faster the cylinder, the higher the kinetic energy and the longer the stopping distance. This is important in connection with light beam devices, etc. and the required distance from the danger point.

7.3.5 Circuit diagram and operating manual

To conclude, some thoughts on pneumatic circuit diagrams: Annex 7 of the Machinery Directive calls for instructions. These instructions should provide all persons working on the machine with all the information necessary to perform their work safely. For maintenance engineers this means access to complete, accurate circuit diagrams that match the machine. They must be able to locate the components they see on the circuit diagram on the machine, otherwise it is impossible to work safely. Connection designations should be included in the circuit diagram; the hose connections should

▶ 7.3 Pneumatic design

be made accordingly. Components should be identified and the connections named. These markings should be identifiable over the whole of the machine's service life. It makes sense for safety-related components to be identified on the circuit diagrams. As such, the maintenance engineer will recognise the special significance of these components. The correct connection designations should be stated alongside the component designations. If hoses are connected incorrectly because the connection designations are incorrect, the piston rod will suddenly extend rather than retract when the valve is activated electrically.

Under what conditions is a circuit diagram drawn and viewed? All drives and valves are shown in their home position; compressed air is present, even if the start-up valve on the service unit is shown in the off position. The home position is the position of the drives before automatic mode is started and is different from the machine's initial position. On a vertically installed cylinder the piston rod is extended, while on this cylinder the piston rod is retracted in the home position. Before starting automatic mode, the control engineer must first bring the drives in the initial position. With the exception of mechanical directly actuated limit switches, all valves are shown in the non-actuated condition. On monostable valves and middle-setting valves, this switch setting is defined by the mechanical spring.

The circuit diagram display starts at the bottom left with the service unit or pressure source and continues towards the top right. However, when drafting or planning the circuit diagram, you should start at the top with the drives and only draw the service unit at the end. Before the design engineer starts to think about the control valves for the cylinders, he needs to be clear about the mounting position, the behaviour in the event of a power failure and subsequent restoration (pneumatics and electrics), the necessary protective measures, plus the control and stop category. The frequently fixed allocation of 5/2 directional valves to double-acting cylinders generally leads to a vain attempt to provide individual cylinders with reasonable, effective and above all low-priced safety circuits.

Only when all the requirements of the cylinder have been defined can thoughts turn to the service unit. The cylinders may require different operating pressures, in which case several pressure regulators will need to be used. In the event of an emergency stop, only one part of the compressed air should switch off, while in another part of the machine, full pressure should still be available. Valve terminals require a separate control air supply, for which the service unit must offer an appropriate solution. Once these aspects have been considered, a service unit can often look quite different to the one that was originally planned. This is a disadvantage if the service unit has already been ordered at an early stage: The additional parts that are needed will have to be selected, ordered and installed and the necessary modifications will be complex, costing even more time and money. Information regarding hose colours and hose cross sections, screw joints and hose numbers help to provide clarity during assembly and when troubleshooting. Clarity is always a plus for safety and speed; DIN ISO 1219, DIN ISO 5599 and DIN EN 81346-1 are standards dealing with the generation of circuit diagrams and graphic symbols.

In pneumatics, is safety technology more difficult than the electrical technology? Essentially no. The basic principles and concepts are the same or similar. Compressed air as a medium is different; to many people it's new and unfamiliar. As with electrical drives, mechanics must also be considered in pneumatics. An electric motor does not operate through its shaft alone; extensive mechanics generally follow to a greater or lesser extent, as is the case with pneumatics. The information in this chapter, with its examples, ideas and suggestions, is simply an initial introduction to the subject of "safety and pneumatic design" and is certainly not sufficient to guarantee safe operation of a plant or machine.

▶ 7.4 Hydraulic design

7.4.1 Basic physical knowledge

In hydraulics the talk is of hydrodynamic energy transfer, e.g. a pump transfers mechanical energy to the oil and flow energy is used to drive a turbine wheel, for example.

7.4.2 Advantages of hydrostatic energy transfer

The following advantages play a role in hydrostatic energy transfer:

- ▶ Transfer of high forces and powers in the smallest possible space
- ▶ Sensitive, infinitely variable control of speeds
- ▶ Smooth speed control under load, within a large setting range
- ▶ Large transmission range on drives
- ▶ Quiet operation, fast, smooth reversal of motion
- ▶ Simple, safe overload protection
- ▶ High switch-off accuracy when stopping the operating component.
- ▶ Long service life and low plant maintenance as the sliding components are automatically lubricated by the hydraulic fluid

7.4.3 Disadvantages of hydrostatic energy transfer

The following disadvantages should be mentioned:

- ▶ Operation accuracy changes in the event of oil viscosity fluctuations due to temperature variation
- ▶ Sealing problems, particularly when there are high system pressures and temperatures
- ▶ Air dissolves in hydraulic fluid. Air bubbles are created when the pressure drops, adversely affecting control accuracy
- ▶ Hydraulic fluids are channelled in a loop with cooler and filter

7.4.4 Definitions

- ▶ Fluid power: The means whereby signals and energy can be transmitted, controlled and distributed using a pressurised fluid or gas as the medium
- ▶ System: Arrangement of interconnected components that transmits and controls fluid power energy
- ▶ Component: An individual unit (e.g. cylinder) comprising one or more parts designed to be a functional part of a fluid power system
- ▶ Hydraulics: Science and technology which deals with the use of a liquid as the pressure medium
- ▶ Maximum working pressure: The highest pressure at which a system is intended to operate in steady-state conditions
- ▶ Rated pressure: The highest pressure at which the component is intended to operate for a number of repetitions sufficient to assure adequate service life
- ▶ Control device: A device that provides an input signal to an operating device (switch)
- ▶ Operating device: Device that provides an output signal to a component (solenoid)
- ▶ Piping: Any combination of fittings, couplings or connectors with pipes, hoses or tubes, which allows fluid flow between components

▶ 7.4 Hydraulic design

7.4.5 Relevant units

Size	Unit	Symbol	Relationship
Lengths	Micrometre	μm	$1 \mu\text{m} = 0.001 \text{ mm}$
	Millimetre	mm	$1 \text{ mm} = 0.1 \text{ cm} = 0.01 \text{ dm} = 0.001 \text{ m}$
	Centimetre	cm	$1 \text{ cm} = 10 \text{ mm} = 10,000 \mu\text{m}$
	Decimetre	dm	$1 \text{ dm} = 10 \text{ cm} = 10 \text{ mm} = 100,000 \mu\text{m}$
	Metre	m	$1 \text{ m} = 10 \text{ dm} = 100 \text{ cm} = 1,000 \text{ mm} = 1,000,000 \mu\text{m}$
	Kilometre	km	$1 \text{ km} = 1,000 \text{ m} = 100,000 \text{ cm} = 1,000,000 \text{ mm}$
Areas	Square centimetre	cm^2	$1 \text{ cm}^2 = 100 \text{ mm}^2$
	Square decimetre	dm^2	$1 \text{ dm}^2 = 100 \text{ mm}^2 = 10,000 \text{ cm}^2$
	Square metre	m^2	$1 \text{ mm}^2 = 100 \text{ dm}^2 = 10,000 \text{ cm}^2 = 1,000,000 \text{ mm}^2$
	Ar	a	$1 \text{ a} = 100 \text{ m}^2$
	Hectare	ha	$1 \text{ ha} = 100 \text{ a} = 10,000 \text{ m}^2$
	Square kilometre	km^2	$1 \text{ km}^2 = 100 \text{ ha} = 10,000 \text{ a} = 1,000,000 \text{ m}^2$
Volume	Cubic centimetre	cm^3	$1 \text{ cm}^3 = 1,000 \text{ mm}^3 = 1 \text{ ml} = 0.001 \text{ l}$
	Cubic decimetre	dm^3	$1 \text{ dm}^3 = 1,000 \text{ cm}^3 = 1,000,000 \text{ mm}^3$
	Cubic metre	m^3	$1 \text{ m}^3 = 1,000 \text{ dm}^3 = 1,000,000 \text{ cm}^3$
	Millilitre	ml	$1 \text{ ml} = 0.001 \text{ l} = 1 \text{ cm}^3$
	Litre	l	$1 \text{ l} = 1,000 \text{ ml} = 1 \text{ dm}^3$
	Hectolitre	hl	$1 \text{ hl} = 100 \text{ l} = 100 \text{ dm}^3$
Density	Gram/ Cubic centimetre	$\frac{\text{g}}{\text{cm}^3}$	$1 \frac{\text{g}}{\text{cm}^3} = 1 \frac{\text{kg}}{\text{dm}^3} = 1 \frac{\text{t}}{\text{m}^3} = 1 \frac{\text{g}}{\text{ml}}$
Force/ Weight force	Newton	N	$1 \text{ N} = 1 \frac{\text{kg} \times \text{m}}{\text{s}^2} = 1 \frac{\text{J}}{\text{m}}$
			$1 \text{ daN} = 10 \text{ N}$
Torque	Newton metre	Nm	$1 \text{ Nm} / 1 \text{ J}$
Pressure	Pascal	Pa	$1 \text{ Pa} = 1 \text{ N/m}^2 = 0.01 \text{ mbar} = \frac{1 \text{ kg}}{\text{m} \times \text{s}^2}$
	Bar	Bar	$1 \text{ bar} = 10 \frac{\text{N}}{\text{cm}^2} = 100,000 \frac{\text{N}}{\text{m}^2} = 10^5 \text{ Pa}$
	$\text{psi} = \frac{\text{pound}}{\text{inch}^2}$	Psi	$1 \text{ psi} = 0.06895 \text{ bar}$
	$\frac{\text{kp}}{\text{cm}^2}$		$1 \frac{\text{kp}}{\text{cm}^2} = 0.981 \text{ bar}$
Mass	Milligram	mg	$1 \text{ mg} = 0.001 \text{ g}$
	Gram	g	$1 \text{ g} = 1,000 \text{ mg}$
	Kilogram	kg	$1 \text{ kg} = 1,000 \text{ g} = 1,000,000 \text{ mg}$
	Tonne	t	$1 \text{ t} = 1,000 \text{ kg} = 1,000,000 \text{ g}$
	Megagram	Mg	$1 \text{ Mg} = 1 \text{ t}$

▶ 7.4 Hydraulic design

Size	Unit	Symbol	Relationship
Acceleration	Metre/square second	$\frac{m}{s^2}$	$1 \frac{m}{s^2} = 1 \frac{N}{kg}$ $1 g = 9.81 m/s^2$
	Angular speed	One/second	$\frac{1}{s}$
Power	Watt	W	$1 W = 1 \frac{Nm}{s} = 1 \frac{J}{s} = 1 \frac{kg \times m}{s^2} \times \frac{m}{s}$
	Newton metre/second	Nm/s	
	Joule/second	J/s	
Work/energy, heat	Watt second	Ws	$1 Ws = 1 Nm = 1 \frac{kg \times m}{s^2} \times m = 1 J$
	Newton metre	Nm	
	Joule	J	
	Kilowatt hour	kWh	$1 kWh = 1000 Wh = 1000 \times 3600 Ws = 3.6 \times 10^6 Ws$ $= 3.6 \times 10^3 kJ = 3600 kJ = 3.6 MJ$
	Kilojoule	kJ	
	Megajoule	MJ	
Mechanical stress	Newton/square millimetre	$\frac{N}{mm^2}$	$1 \frac{N}{mm^2} = 10 bar = 1 MPa$
Plane angle	Second	''	$1'' = 1'/60$
	Minute	'	$1' = 60''$
	Degree	°	$1^\circ = 60' = 3600'' = \frac{\pi}{180^\circ} rad$
	Radian	rad	$1 rad = 1m/m = 57.2957^\circ$ $1 rad = 180^\circ/\pi$
Rotational speed	One/second	1/s	$\frac{1}{s} = s^{-1} = 60 min^{-1}$
	One/minute	1/min	$\frac{1}{min} = min^{-1} = \frac{1}{60 s}$

▶ 7.4 Hydraulic design

7.4.6 General hydraulic relationships

7.4.6.1 Pressure, absolute pressure and overpressure

Pressure p is the force applied to a unit area, also called pressure for short. The amount of pressure at any point is irrespective of the position. The unit of measurement for pressure is defined with PASCAL using the base units of the International System of Units: kilogram, metre and second.

Absolute pressure: The absolute pressure scale starts at $P_{abs} = 0$, as absolute pressure is the zero pressure of a vacuum.

Overpressure: The difference between absolute pressure and the existing atmospheric pressure P_{amb} is called overpressure.

7.4.6.2 Pascal's law

Pascal's law is the basic law of hydrostatics and applies to incompressible fluids at rest:

Pressure exerted anywhere in a confined fluid is transmitted equally to the internal wall of the container and to the fluid.

7.4.6.3 Gravitational pressure

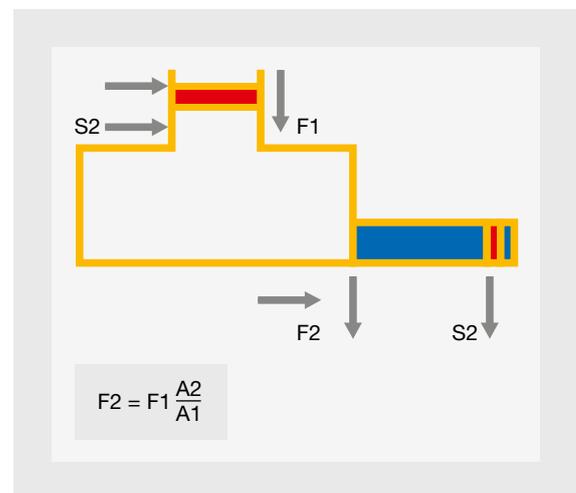
The pressure generated in the fluid by gravity alone is determined by

$$P_h = \rho \times g \times h$$

When designing hydraulic systems it is necessary to check whether the gravitational pressure is of any notable size compared with the pressures occurring within the system. Generally the gravitational pressure is not of any note because it is often less than the required system pressure.

7.4.6.4 Force and path transmission

The principle of force and path transmission can be best explained using the example of an hydraulic press: In accordance with Pascal's law, the pressure generated by the force F_1 is transmitted equally to all parts of the fluid and to the area A_2 . This gives:

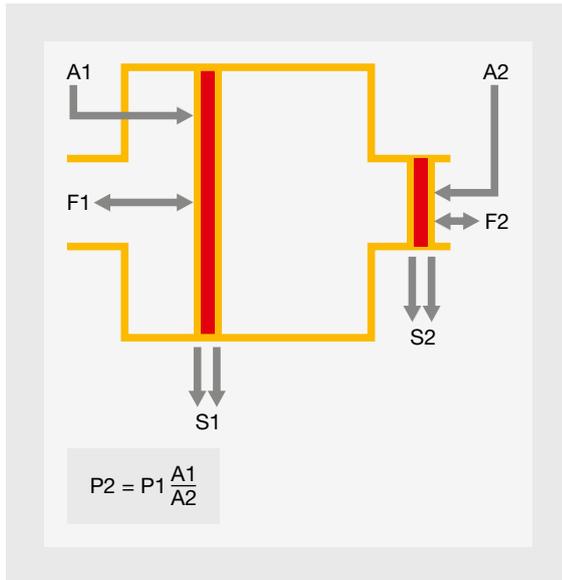


In this way, it is possible to illustrate the principle of force transmission: For example, if the area A_2 is ten times greater than the area A_1 ($A_2 = 10 \cdot A_1$), the force F_1 will also be transmitted at ten times its value.

▶ 7.4 Hydraulic design

7.4.6.5 Pressure transmission

The principle of pressure transmission:



If, for example, the area A_1 is twice the size of area A_2 ($A_1 = 2 \cdot A_2$), the pressure P_1 will be transmitted at double its value.

7.4.6.6 Hydraulic work

On the hydraulic press, if piston 1 is moved downwards along the path S_1 with the area A_1 and force F_1 , the hydraulic work executed in the process is W_1 . The hydraulic work executed at piston 2 A_2 during this process is W_2 .

7.4.6.7 Volumetric efficiency factor

This takes into account the volumetric losses resulting from leakage flows. The hydraulic-mechanical efficiency factor gauges the losses resulting from flow losses and sliding machine parts.

7.4.6.8 Continuity equation

Assumption: A fluid flows through a tube with various cross sectional areas. As no fluid is lost between the various cross sectional areas, the following applies for the mass flows that stream through these areas:

$$A_1 \times V_1 = A_2 \times V_2 = A_3 \times V_3 = \text{const.}$$

7.4.6.9 Bernoulli's equation

Bernoulli's equation is a special case derived from the familiar Navier-Stokes equation from fluid mechanics, which apply to three-dimensional viscous flows. The equation for the energy form is:

$$\frac{V^2}{2} + \delta \times Z + \frac{p}{\zeta} = \text{const.}$$

7.4.6.10 Flow forms

Laminar or turbulent flow forms occur in the tubes of hydraulic systems. With a laminar flow, the fluid particles move in orderly, separate layers, which is why we talk of a flow direction. The flow lines run in parallel to the tube axis. With a turbulent flow, the fluid no longer moves in orderly layers.

The main axial flow is now superimposed on all points through random longitudinal and transverse movements, that result in a disturbed flow. The flow is thereby mixed. The transition from a laminar to a turbulent flow occurs in straight tubes with a circular cross section when the critical REYNOLDS NUMBER $Re_{crit} = 2320$

$$v_{crit} = \frac{Re_{crit} \times \nu}{d}$$

▶ 7.4 Hydraulic design

7.4.6.11 Viscosity

A surface-mounted plate with an area A is moved at constant speed V on a fluid layer with a defined height h . The force F is required to maintain the movement. If the layer thickness A is not too great, a linear velocity gradient develops between the plate and the bottom of the fluid.

The law discovered by Newton

$$\frac{F}{A} = \tau = \eta \times \frac{dv}{dz}$$

is known as Newton's law of friction.

τ stands for the friction shear stress and η for the dynamic viscosity of the fluid, which as a property represents a measurement for the internal friction, which makes it more difficult for the fluid particles to move. The energy expended in moving the particles is converted into heat. The definition of the viscosity used in hydraulics:

$$\eta = N \times \frac{s}{m^2} \quad \nu = \frac{\eta}{\zeta}$$

7.4.6.12 Pressure losses in tubes, fittings and valves

When fluid flow is friction-free, the total energy comprising pressure energy, kinetic and potential energy is constant. With real fluid flows (subjected to friction), due to the influence of the viscosity, part of the flow energy is converted into thermal energy, which cannot be utilised technically and is therefore associated with flow loss. Only pressure energy can be affected by losses due to frictional influences. Considerable pressure losses occur in fittings (tube bends, tube branches, extensions, narrowings) due to frictional influences. The calculated resistance coefficient is used for the numeric simulation.

7.4.6.13 Cavitation

Cavitation describes the formation of bubbles (air and steam bubbles) on bottlenecks in hydraulic components due to pressure drops and the sudden breakdown of these bubbles once the bottleneck is passed. A distinction is made between two types of cavitation: Air bubble cavitation and steam bubble cavitation. Both types of cavitation have similarly negative effects on the components in hydraulic systems.

7.4.6.14 Air bubble cavitation

One property of fluids is the ability to dissolve gases. In this context, we talk of the gas dissolving capacity of fluids. Hydraulic oils in particular contain air in a dissolved state. As well as being present in a dissolved state, air can also occur as air bubbles within the oil. This happens when the oil's static pressure on-site drops to the dissolved gas pressure and therefore the oil's capacity to absorb air is exhausted.

7.4.6.15 Steam bubble cavitation

This occurs when steam bubbles are formed in the oil because the static pressure drops to or below the steam pressure of the oil. Here too, the pressure drops due to the increased flow rates present at bottlenecks in hydraulic components.

▶ 7.4 Hydraulic design

7.4.6.16 Hydro pumps

At the heart of any hydraulic system is the hydro pump. The mechanical energy fed via its drive shaft, generally through an electric motor, is needed to increase the energy or pressure of the oil flowing through the pump and to cover all the losses that occur within the pump. The energy of the flow rate leaving the pump's pressure port, also known as hydrostatic energy, is then available to operate hydraulic applications. Hydro systems generally require high pressures at low flow rates; only in rare cases are these greater than 300 l/min. For this reason, centrifugal pumps are not suitable for this type of application. Hydro pumps operate in accordance with the displacement principle, like

radial piston pumps for example. This system is based on the reducing and expanding space. The displacement volume, also known as stroke volume, is understood to be the volume of oil delivered when a pump rotates.

On hydro pumps, the distinction is made between constant and variable pumps. On constant pumps, the displacement volume V_i cannot be varied. On variable pumps, the displacement volume V_i is a changeable variable and is dependent on the volume setting. The theoretical flow rate of the pump is calculated by multiplying the displacement volume by the pump speed.

Piston pressure force

Graphic	Equation/equation conversion	Formula symbol/units
	$F = 10 \times p \times A$ $F = p \times A \times \eta \times 10$ $A = \frac{d^2 \times \pi}{4}$ $A = \sqrt{\frac{4 \times F \times 0,1}{\pi \times p}}$ $p = 0,1 \times \frac{4 \times F}{\pi \times d^2}$	<p>F = Piston pressure force [N] p = Hydraulic pressure [bar] A = Piston area [cm²] d = Piston diameter [cm] η = Cylinder efficiency factor</p>

Piston forces

Graphic	Equation/equation conversion	Formula symbol/units
	$F = P_e \times A \times 10$ $F = P_e \times A \times \eta \times 10$ $A = \frac{d^2 \times \pi}{4}$ <p>A for circular ring area:</p> $A = \frac{(D - d^2) \times \pi}{4}$	<p>F = Piston pressure force [N] P_e = Excess pressure on the piston [bar] A = Effective piston area [cm²] d = Piston diameter [cm] η = Cylinder efficiency factor</p>

▶ 7.4 Hydraulic design

Piston forces

Graphic	Equation/equation conversion	Formula symbol/units
	$\frac{F_1}{A_1} = \frac{F_2}{A_2}$ $F_1 \times s_1 = F_2 \times s_2$ $\varphi = \frac{F_1}{F_2} = \frac{A_1}{A_2} = \frac{s_2}{s_1}$	<p>F_1 = Force on the pump piston [N] F_2 = Force on the working piston [N] A_1 = Area of pump piston [cm²] A_2 = Area of working piston [cm²] s_1 = Travel of pump piston [cm] s_2 = Travel of working piston [cm] φ = Transmission ratio</p>

Continuity equation

Graphic	Equation/equation conversion	Formula symbol/units
	$Q_1 = Q_2$ $Q_1 = A_1 \times v_1$ $Q_2 = A_2 \times v_2$ $A_1 \times v_1 = A_2 \times v_2$	<p>$Q_{1,2}$ = Volume flow rates [cm³/s, dm³/s, m³/s] $A_{1,2}$ = Cross-sectional areas [cm², dm², m²] $v_{1,2}$ = Flow speeds [cm/s, dm/s, m/s]</p>

Piston speed

Graphic	Equation/equation conversion	Formula symbol/units
	$v_1 = \frac{Q_1}{A_1}$ $v_2 = \frac{Q_2}{A_2}$ $A_1 = \frac{d^2 \times \pi}{4}$ $A_2 = \frac{(D^2 - d^2) \times \pi}{4}$	<p>$v_{1,2}$ = Piston speed [cm/s] $Q_{1,2}$ = Volume flow rate [cm³/s] A_1 = Effective piston area (circle) [cm²] A_2 = Effective piston area (ring) [cm²]</p>

Pressure intensifier

Graphic	Equation/equation conversion	Formula symbol/units
	$p_1 \times A_1 = p_2 \times A_2$	<p>p_1 = Pressure in the small cylinder [bar] A_1 = Piston area [cm²] p_2 = Pressure on the large cylinder [bar] A_2 = Piston area [cm²]</p>

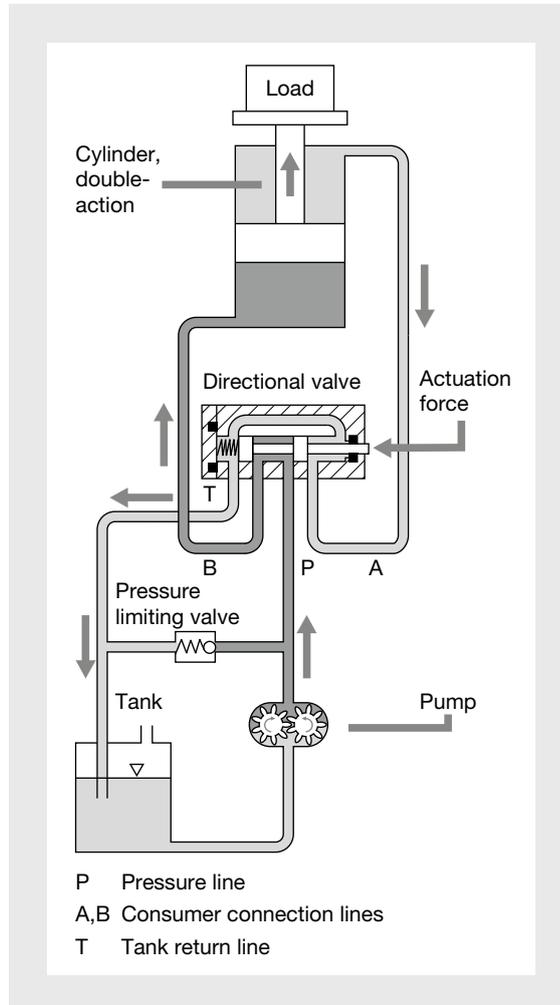
▶ 7.4 Hydraulic design

7.4.7 Structure of a hydraulic system

The hydraulic circuit diagram shows the structure of a hydraulic circuit. The individual hydraulic devices are represented by standardised symbols and are interconnected through pipelines. The diagrams that follow illustrate simple hydraulic circuits. In this case, the devices are not represented by standardised symbols but are shown schematically to identify their mode of operation. The pump sucks the hydraulic oil from the container and pushes it into the pipeline system containing the built-in devices. The oil flows from P to B through a directional valve in the hydro cylinder. The piston (with tool) creates resistance for the oil. The pressure rises in the power section between the pump and piston until the piston force is sufficient to overcome the load and the piston moves.

7.4.8 Simple hydraulic circuit, upward movement

The directional valve is held in position by any amount of force. The piston travels to the top end position. The displaced oil flows through the directional valve from A to T, back to the tank. The directional valve therefore controls the direction of the oil flow. To ensure that the system is protected from excessive loads (pressures), a pressure relief valve is installed in the pressure line, after the pump. If the set pressure is exceeded, the valve will open and the remaining oil will flow into the tank. The pressure will not increase any further.

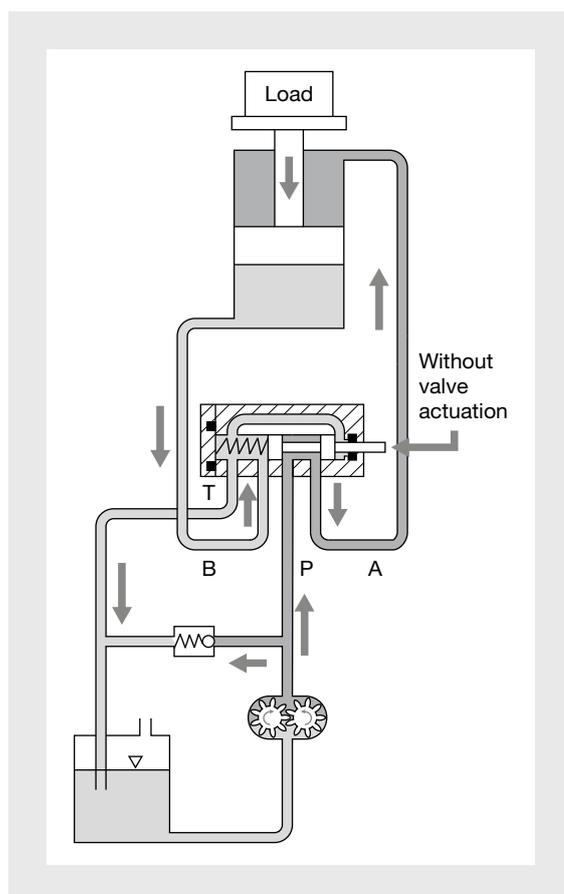


Structure of a hydraulic system.

▶ 7.4 Hydraulic design

7.4.9 Simple hydraulic circuit, downward movement

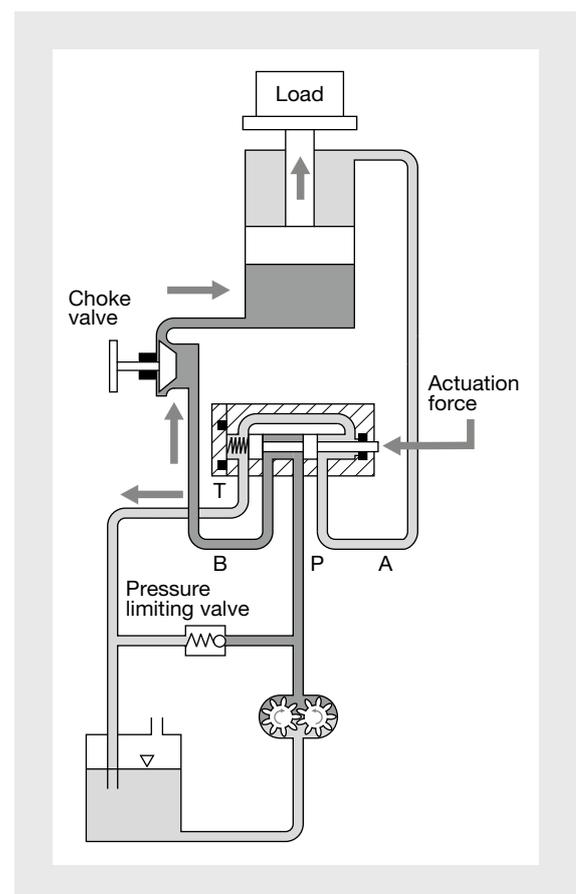
When the piston reaches the top end position, the actuation force is removed and the directional valve is reset via spring force. Now the oil flows from P to A to the rod side of the piston. The piston moves towards the bottom end position, the displaced oil flows through the directional valve from B to T, back to the tank. Switching the directional valve in the piston end positions enables the piston to continuously move back and forth.



Downward movement on a simple hydraulic circuit.

7.4.10 Simple hydraulic circuit, speed

If it's necessary to control not only the direction of the piston but also the speed, the amount of oil flowing in and out of the cylinder will need to be varied. This can be done using a choke valve: For example, if the valve cross section is reduced, less oil will flow into the cylinder over a defined unit of time. The oil flow is less than before it was choked, so the piston speed will also be slower, in accordance with the continuity equation. In other words, the piston speed is proportional to the oil flow. So the speed is controlled by controlling the oil flow.

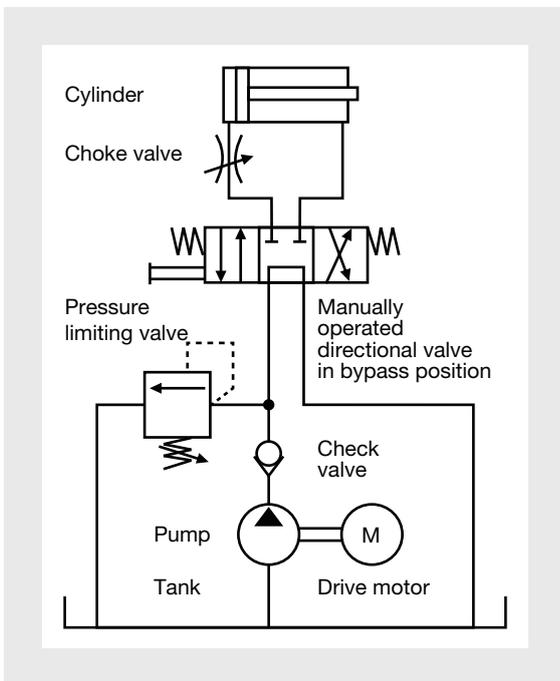


Speed control on an individual hydraulic circuit.

▶ 7.4 Hydraulic design

7.4.11 Circuit diagram for a simple hydraulic circuit

The hydraulic process described above is illustrated below as a hydraulic circuit diagram. The directional valve is manually operated; when unoperated it is held in the spring-centred middle position by spring force.



Circuit diagram for a simple hydraulic circuit

▶ 7.4 Hydraulic design

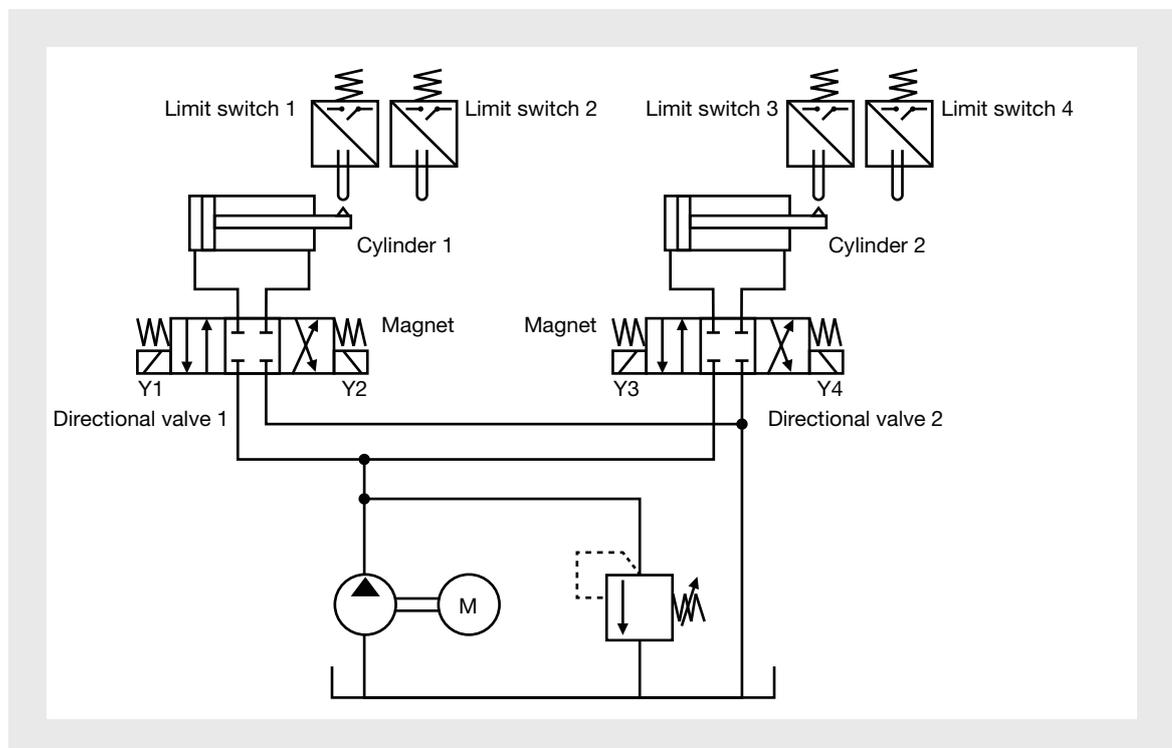
7.4.12 Two cylinder control systems with electric valves

If two or more cylinders are to be used on a hydraulic system, various requirements can be associated with their use, and these can be implemented using various circuit types:

- ▶ Sequential circuits
- ▶ Synchronous circuits
- ▶ Series circuits
- ▶ Parallel circuits

The diagram below shows a sequential circuit (sequential circuit with limit switches and solenoid valves): In the version with limit switches, the limit switches actuate the piston rods, based on the path (the electrics are not shown):

1. Start: Solenoid Y1 is energised, directional valve 1 to the right, piston on cylinder 1 to the right.
2. Limit switch 2 actuated: Solenoid Y1 de-energised, solenoid Y3 energised, directional valve 2 to the right, piston on cylinder 2 to the right
3. Limit switch 4 actuated: Solenoid Y3 de-energised, solenoid Y2 energised, directional valve 1 to the left, piston on cylinder 2 to the left
4. Limit switch 1 actuated: Solenoid Y2 de-energised, solenoid Y4 energised, directional valve 2 to the left, piston on cylinder 2 to the left
5. Limit switch 3 actuated: Solenoid Y4 de-energised, solenoid Y1 energised, directional valve 1 to the right, piston on cylinder 1 to the right



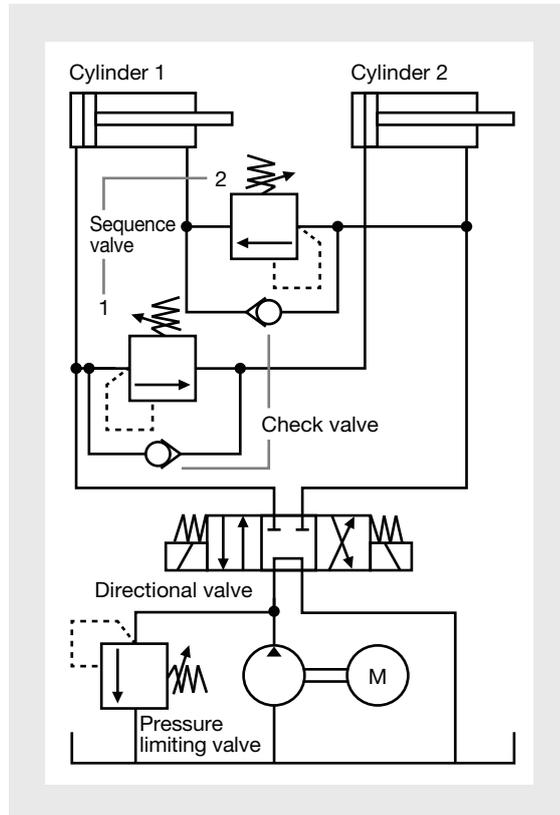
Circuit diagram for two cylinder control systems with electric valves.

▶ 7.4 Hydraulic design

7.4.13 Two cylinder control systems with sequence valves

Sequence valves 1 and 2 are pressure valves which open at a certain pressure, which can be selected. They close again when the pressure drops. This results in the following motion sequence:

1. Start: Left directional valve is activated, the piston side of cylinder 1 is pressurised, the cylinder extends. When the piston stops, the pressure rises above the value set on the pressure limiting valve; sequence valve 2 opens.
2. The pressure flows into cylinder 2; this cylinder also extends.
3. Right directional valve is activated, the rod side of cylinder 2 is pressurised, the cylinder retracts. When the piston stops, the pressure rises above the value set on the pressure limiting valve; sequence valve 1 opens.
4. As a result, cylinder 1 receives flow. The piston also retracts.
5. The switchover of the directional valve is activated via limit switches.



Circuit diagram for two cylinder control systems with sequence valves.

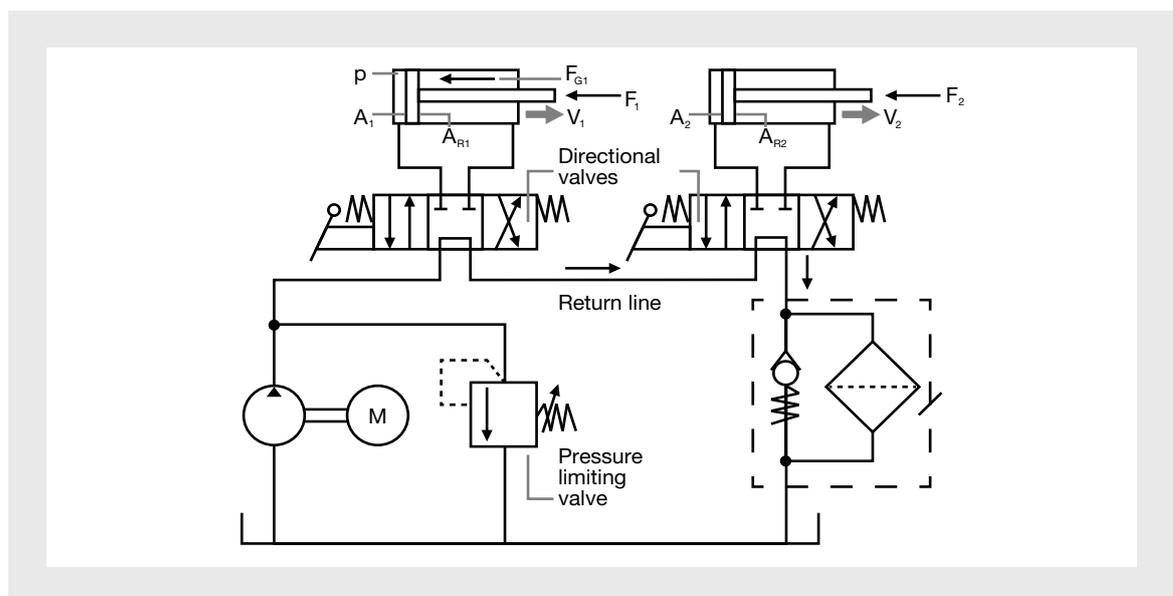
▶ 7.4 Hydraulic design

7.4.14 Series circuit

A series circuit is implemented as with valves connected in series. The return line is not guided back into the tank, as with a single circuit, but to the directional valve on the second cylinder. If both cylinders are operated simultaneously in this type of circuit, the piston force and piston speed will influence each other. The result is the following relationships: System pressure p , which acts upon the piston area of cylinder 1, must be large enough not only to generate its own lifting force F_1 but also to overcome the counteracting force F_{G1} , generated by cylinder 2. This counteracting force comes from the fact the oil pressure needed to operate cylinder 2 in turn acts upon the piston ring area of cylinder 1. The ring area of cylinder 1 displaces the oil and conveys it to cylinder 2. Its speed depends therefore on the return flow rate from cylinder 1. The relationship between the extending speed of cylinder 1 and the extending speed of cylinder 2 is the same as the relationship between the piston area of cylinder 2 and the ring area of cylinder 1.

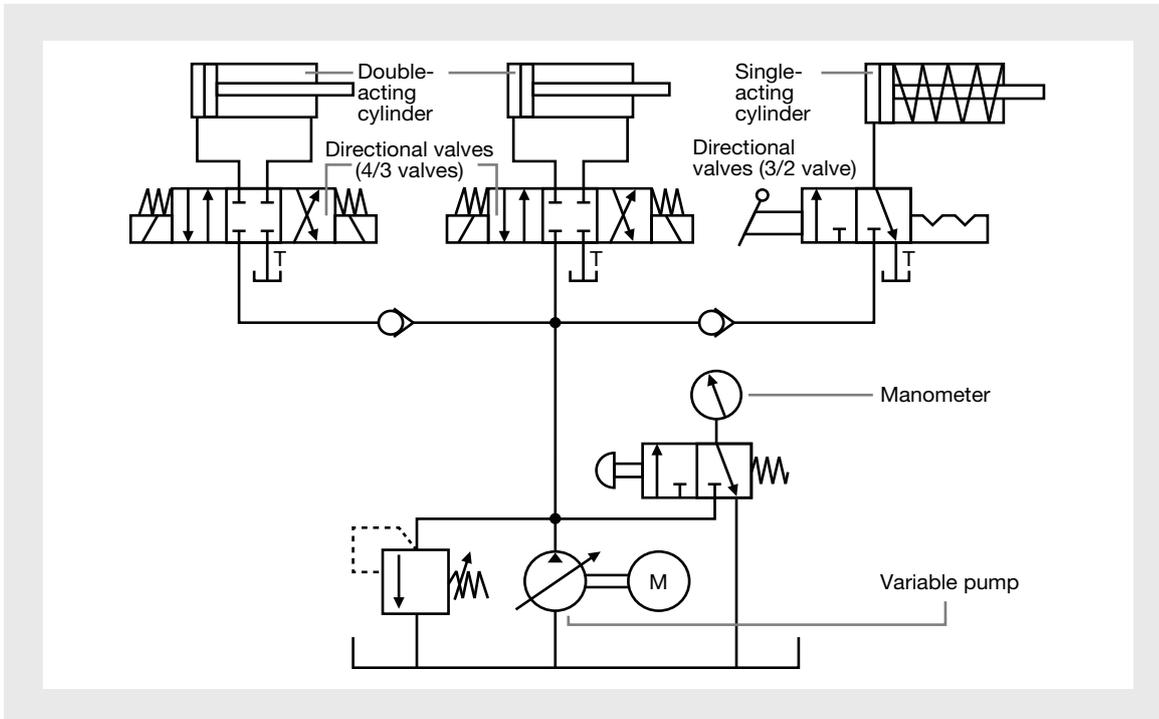
7.4.15 Parallel circuit

In contrast to a series circuit, with a parallel circuit there is no mutual influencing when all the cylinders operate simultaneously. Oil is supplied via a branch pipe line. The system pressure set at the pressure limiting valve prevails as far as the directional valves. With a parallel circuit, sufficient fluid must be available to maintain the necessary system pressure if the cylinders are to be extended simultaneously. If the pump conveys too little fluid, the cylinder with the lowest operating resistance will extend first. If it is in the end position, the pressure continues to rise until it is sufficient for the next cylinder. So the extension of the cylinders depends on the necessary operating pressure.



Circuit diagram for a series circuit

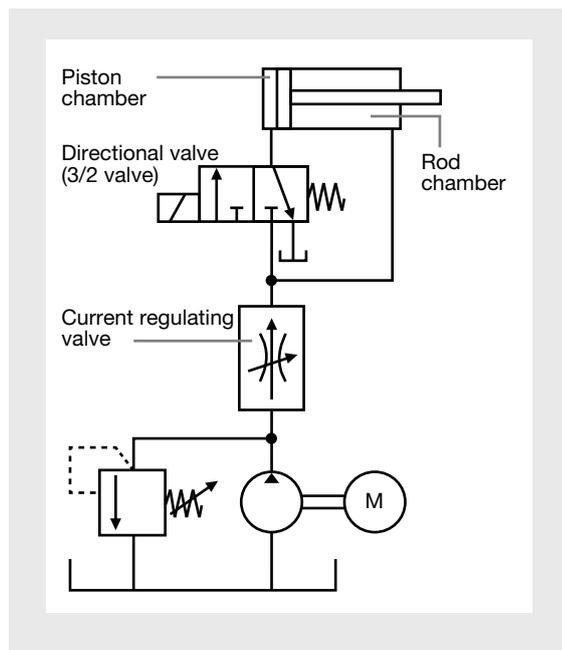
▶ 7.4 Hydraulic design



Circuit diagram for a parallel circuit

7.4.16 Differential circuit

The rod chamber is constantly under pressure, the piston chamber is connected to a directional valve. This circuit is called a differential circuit because the force acted upon the piston rod is expressed as a ratio of piston area to rod area. The differential circuit is used when the piston must be hydraulically clamped and the pump must be as small as possible. If the piston extends via the directional valve, the fluid dispersed from the ring area will be combined with the pump flow ahead of the directional valve and will be fed back to the piston side of the cylinder. With this circuit, the force exerted by the piston rod is calculated from the product of pressure times rod area.



Circuit diagram for a differential circuit

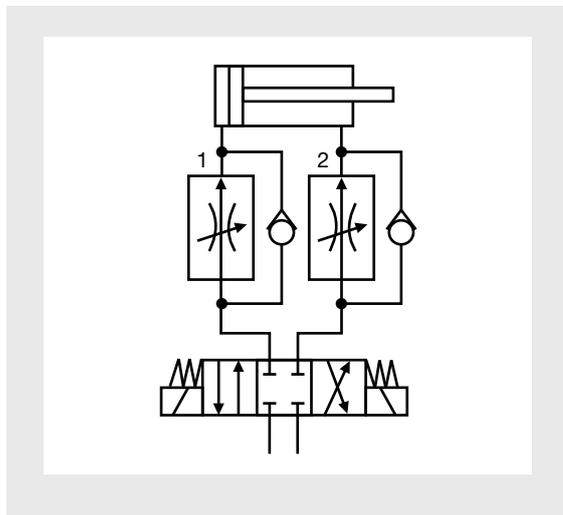
▶ 7.4 Hydraulic design

7.4.17 Speed control systems

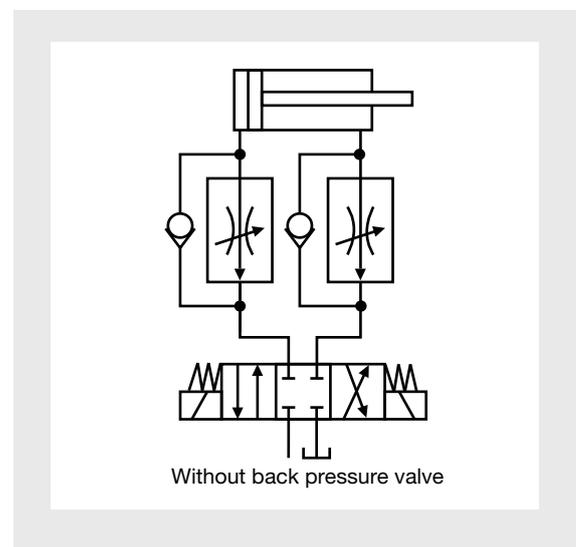
Flow control valves are used for speed control. Flow valves are choke valves or flow control valves. There are two options: primary or secondary control.

Primary control: With primary control, the flow valve sits in the inlet between the directional valve and the cylinder. It controls the inflowing hydraulic fluid. The graphic symbol shows a two-way flow control valve. A check valve is connected in parallel, which blocks the inflow but lets the return flow through. As a result, the fluid flows through the flow valve only on the infeed and not on the return. Only the piston's extension speed is controlled in this case. Two flow control valves must be installed if the retract speed is also to be controlled. The disadvantage of primary control is that the piston jumps if the operating resistance suddenly drops. A back pressure valve can prevent this.

Secondary control: With secondary control, the flow valve sits in the outlet between the directional valve and the cylinder. As such, it controls the return flow. The graphic symbol shows a two-way flow control valve. A check valve is connected in parallel, which blocks the outflow but lets the return flow through. As a result, the fluid flows through the flow valve only on the infeed and not on the return. Only the piston's extension speed is controlled in this case. Two flow control valves must be installed if the retract speed is also to be controlled. Secondary control does not have the disadvantage that the piston can jump.

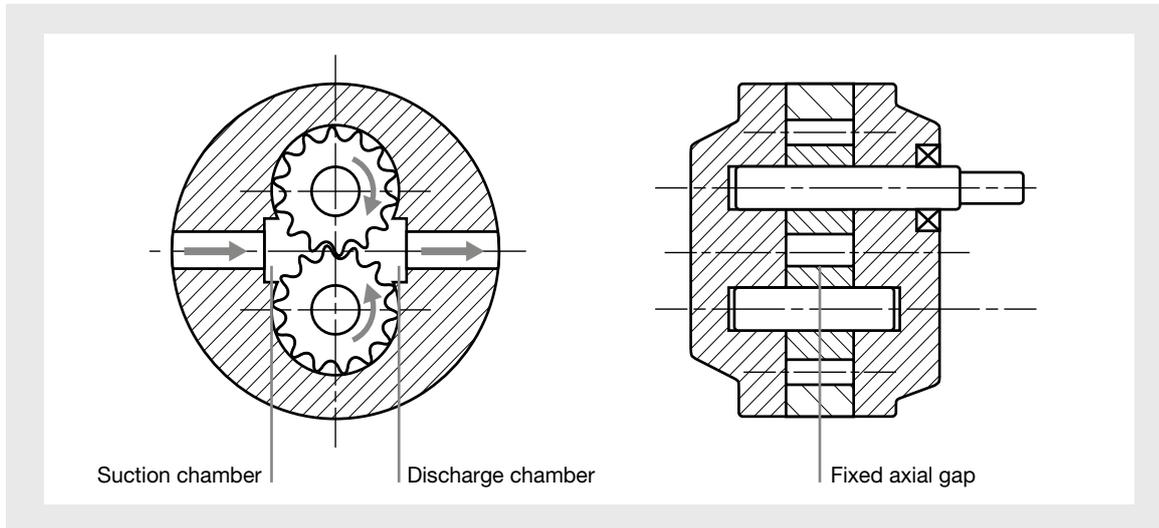


Circuit diagram for primary control



Circuit diagram for secondary control

▶ 7.4 Hydraulic design

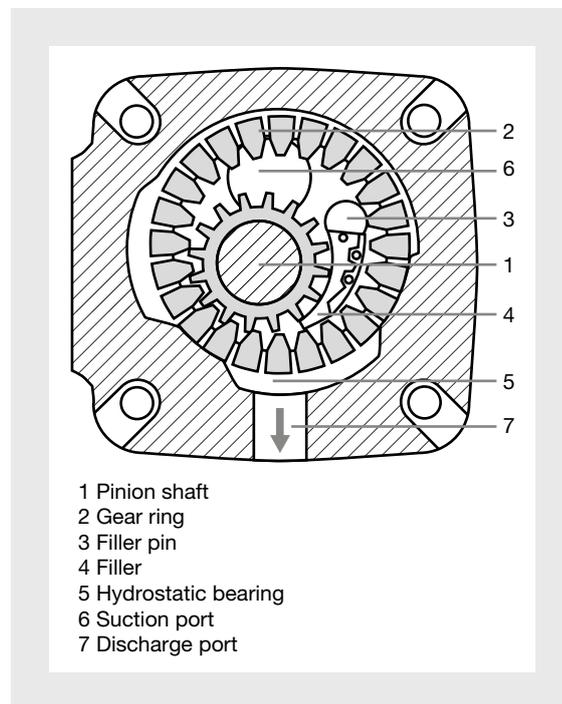


Externally toothed gear pumps

7.4.18 Drive pumps, fixed pumps

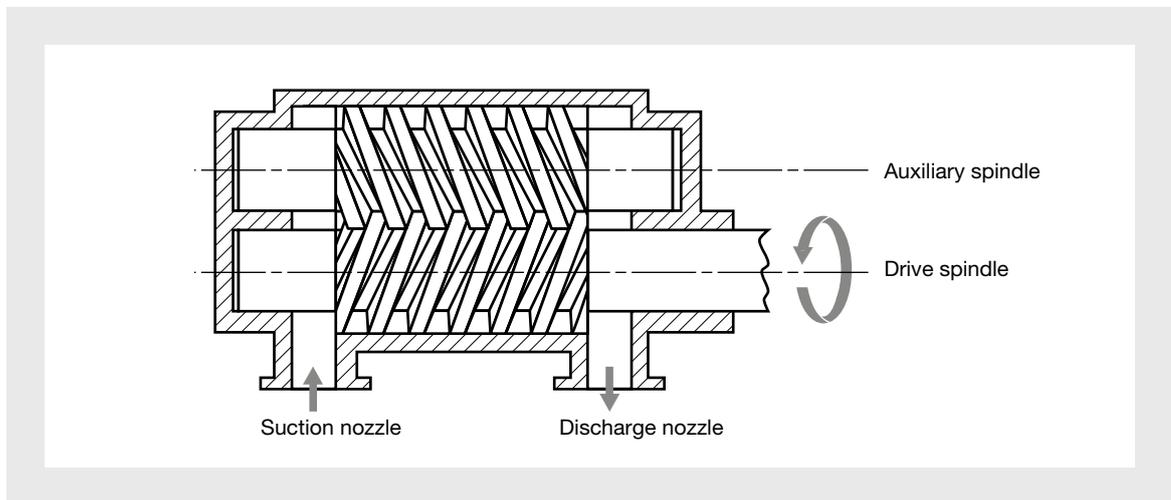
On fixed pumps, the displacement volume cannot be changed. The principle: The fluid conveyed from the suction side to the discharge side is displaced alternately from the gaps through the interlocking cogs. Advantages: Low-cost standard pump with high efficiency factor, which can be connected to other pumps working to the same principle. Disadvantages: High noise level. Application: In open circuits in industrial applications

Internally toothed gear pumps: A driven pinion shaft (1) carries a toothed wheel (2). The principle: The tooth chambers are filled on the suction side, the filler separates the suction and discharge zone on the discharge side. On the discharge side, the oil is displaced through the gear ring. Advantages: Low-noise standard pump with high efficiency factor, which can be connected to other pumps working to the same principle, lower noise level. Disadvantages: More expensive than the traditional gear pump. Application: In open circuits in industrial applications, where quiet running is an important requirement.



Internally toothed gear pumps

▶ 7.4 Hydraulic design



Screw pump

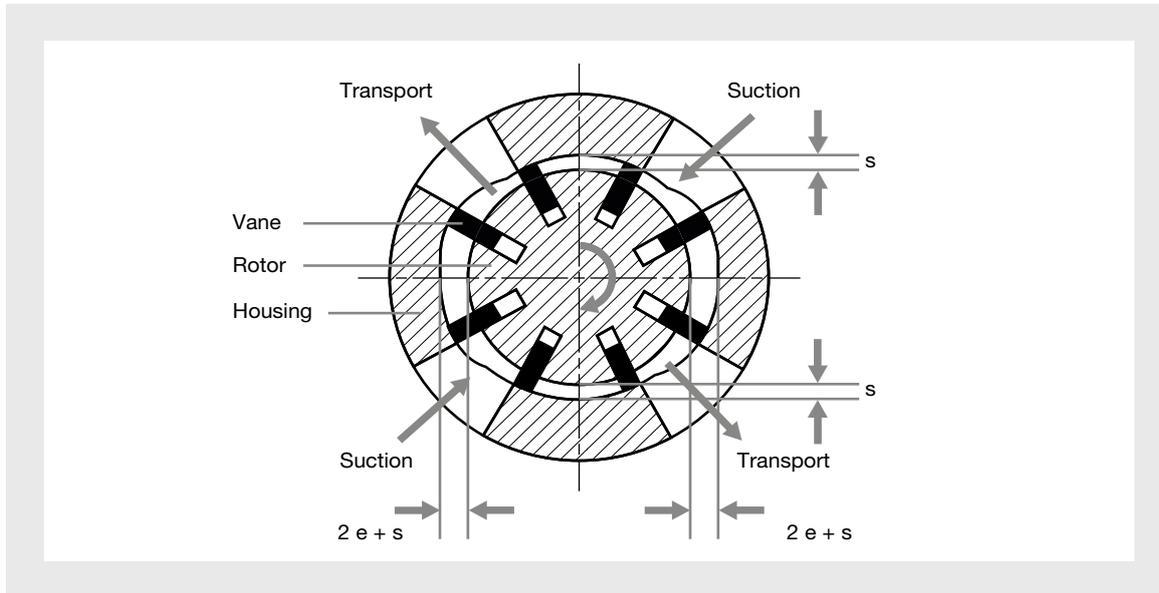
7.4.19 Drive pumps, screw pumps

Two spindles driven jointly. The principle: The meshing spindles form oil chambers within the housing, which are moved from the suction to the pressure nozzle as the spindles rotate.

Advantages: Pulse-free flow rate, low noise level.

Disadvantages: Relatively low efficiency factor due to high volumetric losses, so high oil viscosity is required. Application: In open circuits in industry; for example, on precision machines and in the lift industry. High volume flows.

▶ 7.4 Hydraulic design



Drive pump with vane cells.

7.4.20 Drive pumps, vane pumps

Moving vanes in the slots on the rotor. The principle: The moving vanes located in the slots on the rotor are pressed against the housing wall by centrifugal force and pressure. The cell size increases in conjunction with the suction port and reduces in conjunction with the discharge port. Advantages: Pulse-free flow rate, low noise level, can be flanged to multi-flow pumps. Disadvantages: Low efficiency factor as gear pumps, more sensitive to dirt. Application: In open circuits in industry; for example, on precision machines with low pressure.

▶ 7.5 Safety requirements on hydraulic circuits

7.5.1 Safety requirements in general

When designing hydraulic systems for machinery, all the intended operating states and applications must be taken into account. To determine the hazards, a risk assessment must be carried out in accordance with EN ISO 12100, 2007. As far as is practicable, all identified risks should be designed out of the system where possible. Where this is impossible, appropriate safeguards should be provided.

7.5.2 Concept and design

All system components should be selected in such a way that they guarantee safety during operation and operate within the limits defined in the design.

- ▶ All parts of the system must be designed to withstand pressures corresponding to the maximum operating pressure of the system or any other component; if not, further protective measures should be put in place.
- ▶ Preferred safeguards against excess pressure are one or more pressure limiting valves, which restrict pressure in all parts of the system.
- ▶ Systems should be designed, built and configured to minimise pressure surges and pressure increases. A pressure surge and increased pressure must not give rise to any hazard.

7.5.3 Additional safety requirements

Leakages:

- ▶ Must not give rise to any hazard

Energy supply:

- ▶ The electrical or hydraulic energy supply must not cause a hazard
- ▶ Switching the energy supply on or off
- ▶ Energy reduction
- ▶ Failure and/or restoration of energy

Unexpected start-up:

- ▶ The system is to be designed in such a way that, when the pressurised medium is completely isolated, an unexpected restart is prevented.
- ▶ Mechanical interlock on stop valves in the stop position, plus removal of pressure
- ▶ Isolation from the electrical supply (EN 60204-1)

Mechanical movements:

- ▶ Must not lead to a situation in which persons are endangered, whether intentionally or unintentionally

Low-noise design:

- ▶ Compliance with EN ISO 11688-1 is essential

Operating temperatures:

- ▶ The temperature of the pressure medium must not exceed the maximum operating temperature stated as the limit value for all the system's components.

Operating pressure range:

- ▶ Must be complied with

▶ 7.5 Safety requirements on hydraulic circuits

Couplings or fastenings:

- ▶ Drive couplings and fastenings must be capable of withstanding the maximum torque under all operating conditions on a sustained basis.

Speed:

- ▶ The speed must not exceed the maximum value stated in the manufacturer's documentation.

Lift stops:

- ▶ Appropriate means should be used to secure adjustable lift stops.

Valves with defined switching position:

- ▶ Any drive that must maintain its position or adopt a specific failsafe position in the event of a control failure must be controlled by a valve which guarantees a defined switching position, either via a spring pre-load or an interlocking device.

Hydraulic systems with hydraulic accumulator:

- ▶ Hydraulic systems with hydraulic accumulators are used to automatically relieve the storage fluid pressure or to safely shut off the hydraulic accumulator. Hydraulic accumulators and the associated pressurised components must operate within the specified limits, temperatures and environmental conditions.

7.5.4 Establishing compliance with the safety requirements

As a hydraulic system is generally not a complete machine, many test procedures cannot be carried out until the hydraulic system is incorporated into a machine. See below, from DIN EN 982 clause 6:

Clause 6: Inspection

The systems and their components shall be verified by inspecting their identification in comparison to the system specifications. In addition, the connection of components on the hydraulic system shall be inspected to verify its compliance with the circuit diagram.

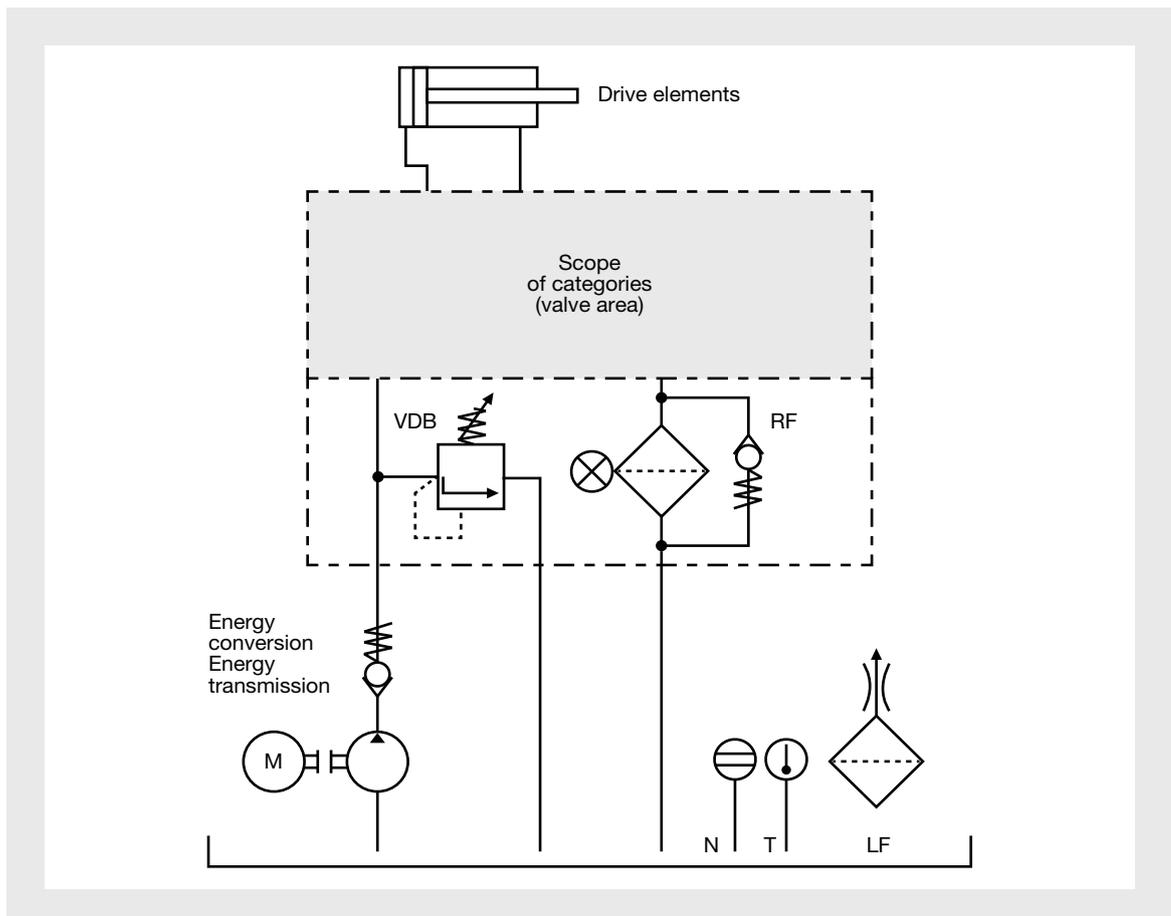
Clause 6.2: Testing

The following tests shall be conducted to determine compliance with the applicable safety requirements.

- ▶ *Operational tests to prove the correct operation of the system and all safety devices.*
- ▶ *Pressure tests to test each part of the system at the maximum working pressure which may be sustained under all conditions of intended use.*

Important: Measurable leakage is defined as slight wetting insufficient to form a drop.

▶ 7.5 Safety requirements on hydraulic circuits



Fluid power system

7.5.5 Safety-related parts of hydraulic control systems

On fluid power systems, any valves that control hazardous movements or conditions should be regarded as safety-related parts of the control system. On hydraulic systems, measures taken within the system to limit pressure (VDB) and to filtrate the hydraulic fluid (RF) should also be taken into account, although these components are not directly control components.

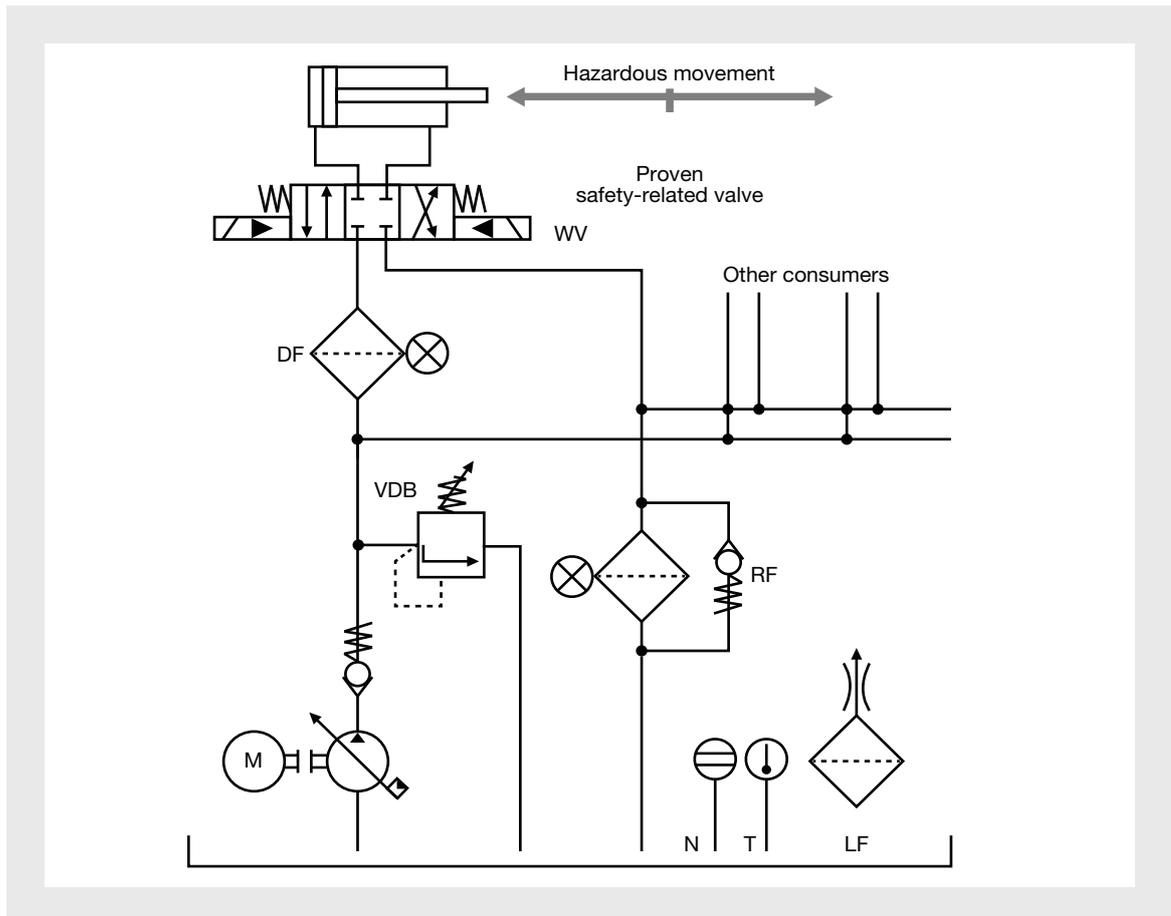
▶ 7.5 Safety requirements on hydraulic circuits

7.5.6 Control systems in accordance with Category B, Performance Level a

Category B is the basic category; its requirements apply to all other categories. These requirements also incorporate the basic safety principles. The basic safety principles which are particularly relevant and specific for fluid power systems are:

- ▶ De-energisation principle
(positive signal for starting)
- ▶ Management of energy changes,
failure and restoration of energy
- ▶ Pressure limitation within the system
- ▶ Selection of an appropriate hydraulic fluid
- ▶ Filtration of the pressure medium
- ▶ Avoidance of contamination
- ▶ Isolation of energy supply
- ▶ All the valves listed in the relevant standards
can be selected for all of the above components.
- ▶ They must comply with the basic requirements
for shock, temperature, pressure, viscosity etc.
- ▶ Compliance with the basic safety principles
requires that the safety-related switch position
for these valves must be achieved when the
control signal is removed (effective springs)
- ▶ The basic safety principles also refer to the
pressure medium. The type and state are highly
significant.
- ▶ Sufficient filtration of the pressure medium
- ▶ On Category B control systems, it must be
accepted that a component failure can lead to
the loss of the safety function

▶ 7.5 Safety requirements on hydraulic circuits



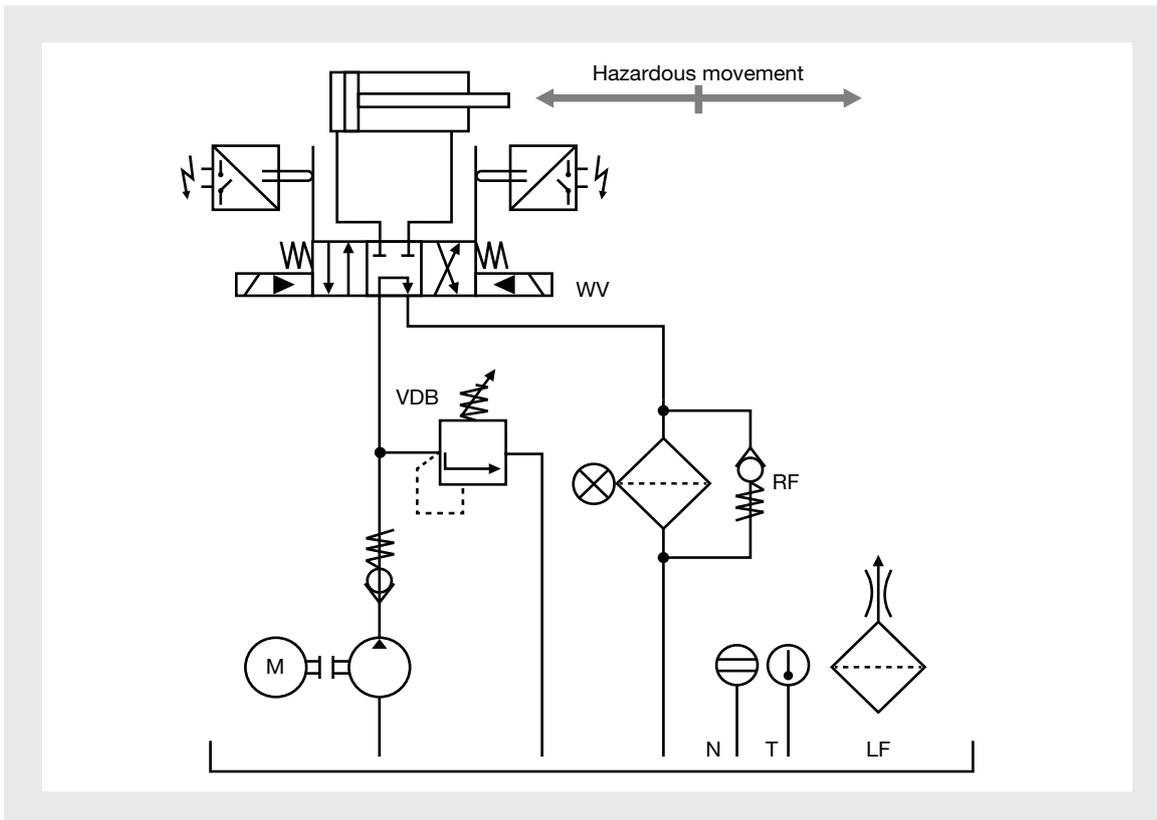
Example of hydraulic circuit (Cat 1, PL b)

7.5.7 Control systems in accordance with Category 1, Performance Level b

In addition to the requirements from Category B, Category 1 control systems must be designed and constructed using well-tried safety principles and well-tried components. Generally well-tried principles are:

- ▶ Torque/force limitation (reduced pressure)
- ▶ Reduced speed (reduced flow rate)
- ▶ Over-dimensioning
- ▶ Travel limiting jog mode
- ▶ Sufficient positive overlapping in piston valves
- ▶ Positive force (positive mechanical action)
- ▶ Targeted selection of materials and material pairings
- ▶ Expose safety-related springs to at least 10% above the endurance limit based on 10^7 duty cycles

▶ 7.5 Safety requirements on hydraulic circuits



Example of hydraulic circuit (Cat 2, PL b)

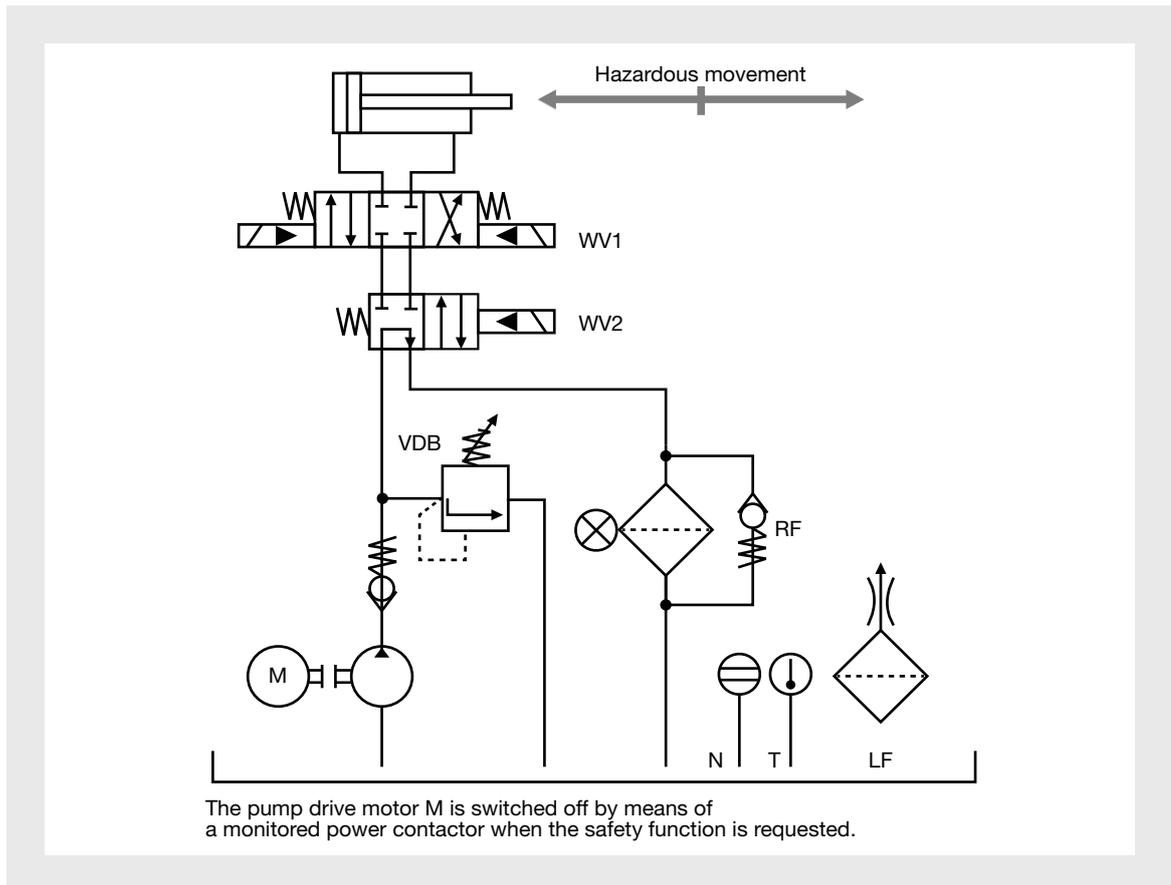
7.5.8 Control systems in accordance with Category 2, Performance Level b

In addition to the requirements from Category B and the use of well-tried safety principles, Category 2 control systems must be designed so that their safety functions are checked at suitable intervals by the machine control system.

Only one directional valve controls the hazardous movement. The electrical machine control system must test the valve's safety function as part of each cycle and on each machine start-up. The failure of

a directional valve must not be able to influence the test function. Conversely, if the test function should fail, this must not affect the reliability of the directional valve. Two position switches detect each time the valve's sliding piston moves away from its safety-related middle setting. If the machine control system detects a failure in a directional valve, it immediately triggers a machine shutdown.

▶ 7.5 Safety requirements on hydraulic circuits



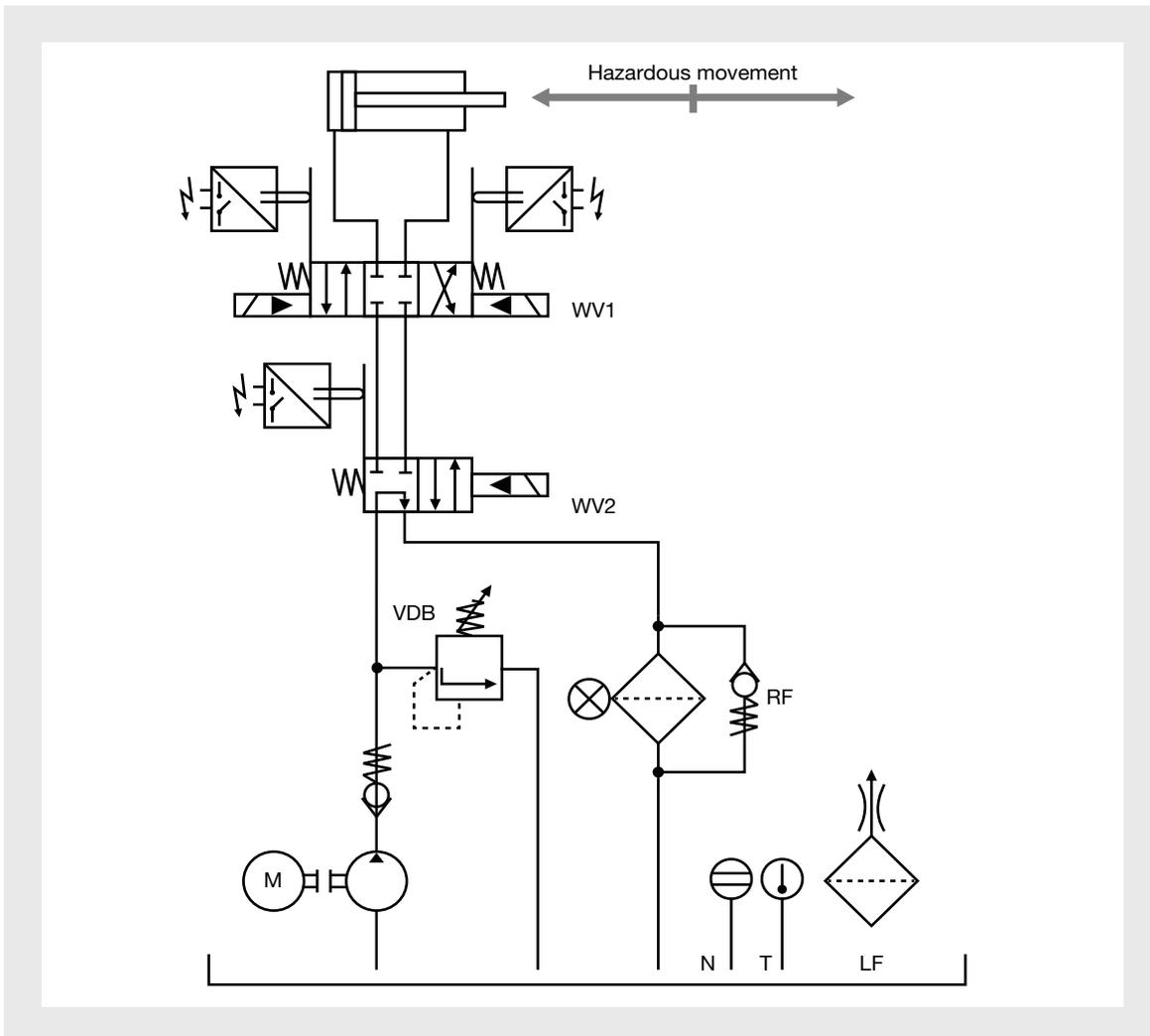
Example of hydraulic circuit (Cat 3, PL d)

7.5.9 Control systems in accordance with Category 3, Performance Level d

In addition to the requirements from Category B and the use of well-tried safety principles, Category 3 control systems must be designed so that a single fault not leads to the loss of the safety function.

Safety-related control of the hazardous movement is via the directional valve WW1, which switches as part of each cycle, and via the pressure valve WW2. The additional shutdown of the pump drive motor is not absolutely necessary. The movement of the valve sliding piston from the safety-related mid-setting is not polled in this case, the pressure valve is switched on redundantly. This provides single fault tolerance.

▶ 7.5 Safety requirements on hydraulic circuits



Example of hydraulic circuit (Cat 4, PL e)

7.5.10 Control systems in accordance with Category 4, Performance Level e

In addition to the requirements from Category B and the use of well-tried safety principles, Category 4 control systems must be designed so that a single fault does not lead to the loss of the safety function. The objective of safety concepts is for a single fault to be detected at or before the next demand upon the safety function.

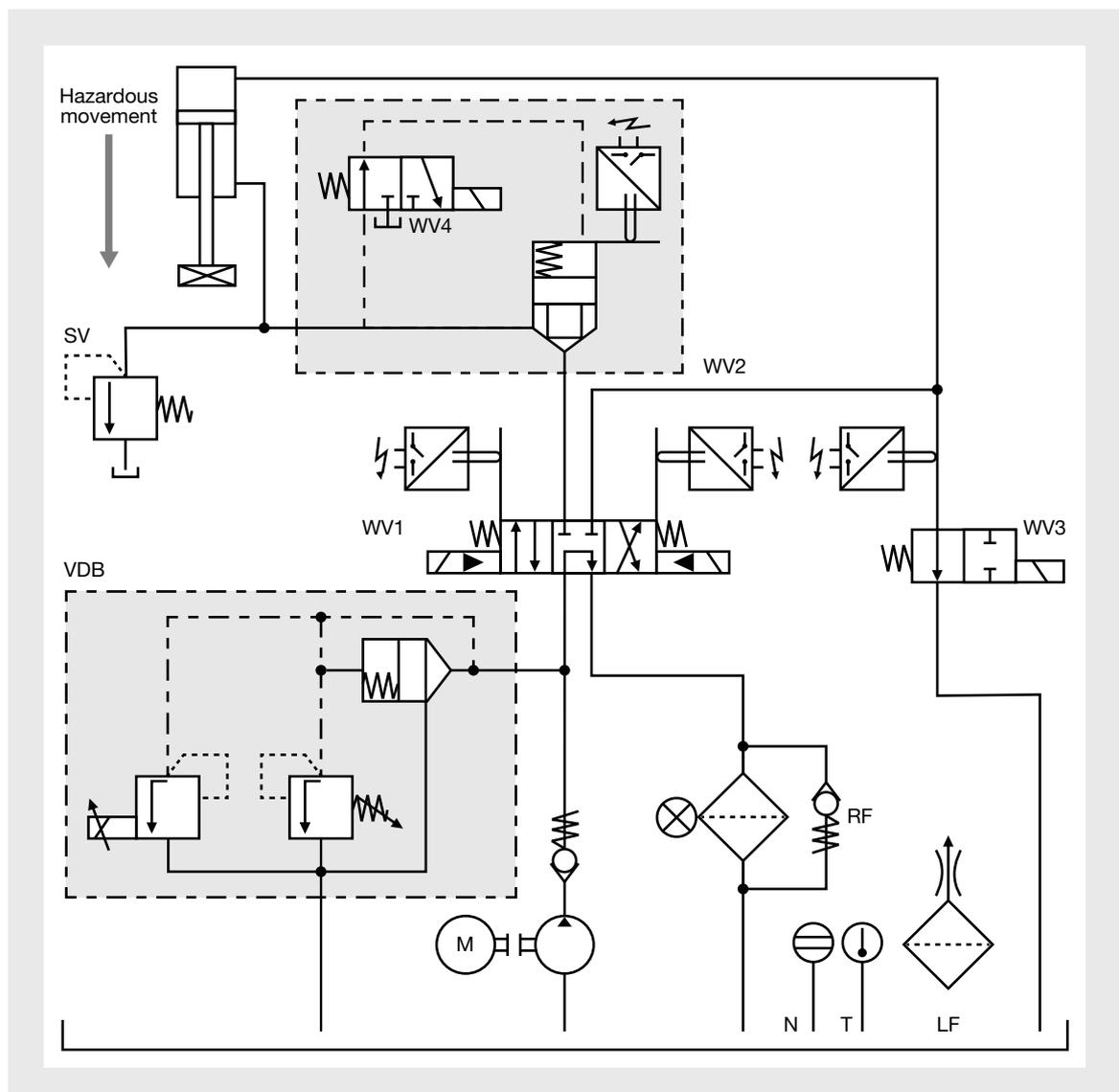
Two valves control the hazardous movement. Each valve is able to shut down the hazardous movement on its own, so single fault tolerance is provided. Both valves are also equipped with electrical position monitoring. This ensures that all possible single faults are detected early by the control system.

▶ 7.5 Safety requirements on hydraulic circuits

7.5.11 Further example for control systems in accordance with Category 4, Performance Level e

In this hydraulic control system, only the downward movement is monitored in terms of safety (compare hydraulic press). Two electrically monitored valves WV1 and WV3 control the build-up of pressure on the upper side of the piston; valves WV2 and WV1

are responsible for reducing the pressure. Valves WV1, WV2, WV3 are equipped with electrical position monitoring. Working in conjunction with the control system, this guarantees that all faults are detected. By monitoring the main stage of valve WV2, any failure in the pilot valve WV4 will be detected at the same time. The pressure limiting valve VDB is designed as an electrically adjustable pressure valve with a pressure limiting function.



Example of hydraulic circuit (Cat 4, PL e)



8

Appendix

▶ 8 Appendix

Chapter	Contents	Page
8	Appendix	8-3
8.1	Index	8-3
8.2	Exclusion of liability	8-15

▶ 8.1 Index

▶ Tags, 0-9

1999/5/EC 2-16
 2001/95/EC 2-16
 2003/10/EC 2-16
 2004/108/EC 2-16
 2006/42/EC 2-5, 2-16, 2-17, 3-4
 2006/95/EC 2-16
 3 contactor combination 4-3, 4-6
 89/686/EEC 2-16
 β factor 2-33
 λD 2-34
 λDD 2-26
 λDtotal 2-26

▶ A

ABNT NBR/IEC 61058-1 2-43
 ABNT NBR/IEC 61058-2-1 2-43
 Absence of feedback 4-22
 Absolute pressure 7-38
 Access 2-7, 3-3, 3-4, 3-5, 3-8, 3-9, 3-11,
 3-17, 3-19, 3-20, 6-17, 6-31, 6-41, 7-17
 Access to the danger zone 3-11, 3-19
 Accident insurance law (UVG) 2-59
 Accreditation Directive 765/2008/EC 2-55
 Active optoelectronic protective devices 3-17
 Actuator 4-3, 4-4, 4-6, 4-28, 5-13, 6-4
 Adjustable guards restricting access 3-5
 Air bubble cavitation 7-40
 Air springs 7-23, 7-24
 Analogue processing 4-12, 4-20
 Annex I 2-10, 2-12
 Annex II B 2-10
 Annex IV 2-10
 Annex IX 2-11
 Annex VI 2-10
 Annex VII 2-11
 Annex VIII 2-11
 Annex X 2-11
 ANSI (American National
 Standards Institute) 2-15, 2-42, 2-45
 ANSI standards 2-42
 Anthropometric data 2-30
 Application area 2-6, 2-17,
 2-24, 2-31, 2-35
 Application blocks 4-11, 4-12, 4-16, 4-18, 4-19
 Application layer 5-14, 5-17, 5-18
 Approach speed 2-19, 2-30, 3-7, 3-17, 7-23
 Argentine Institute of
 Standardization and Certification (IRAM) 2-43
 AS4024.1 2-45

Assembled machinery 2-7
 Assembly instructions 2-10, 2-14
 Assembly of machines 2-6
 Assessment 2-26, 2-33, 2-46, 7-5
 Assessment procedures 2-11
 Associação Brasileira
 de Normas Técnicas (ABNT) 2-43
 Asynchronous motor 6-24, 6-27
 ATEX 4-10
 Austrian Standards Institute (ÖNorm) 2-18
 Authorised representative 2-6, 2-54
 Automatic 4-17
 Automation technology 4-11, 4-22, 4-29,
 4-31, 4-37, 5-7, 5-13
 Avoiding danger 7-11
 Axes 4-20, 4-37, 6-7, 6-14, 6-16,
 6-17, 6-18, 6-20, 6-26, 6-41

▶ B

B and C standards 6-23
 B10d 2-25, 2-33, 2-47, 6-31, 6-34
 Basic Drive Module (BDM) 6-10
 Basic physical knowledge 7-35
 Bernoulli's equation 7-39
 BG 2-8, 4-11, 4-31, 5-9
 BGIA 2-33, 3-25
 BGIA Dokument GS-ET-26 2-23
 Block diagram 6-29, 6-31, 6-33, 6-35, 6-42
 Block properties 4-12
 bmwfi 2-57
 Body measurements 2-19
 Bottom-up 2-49
 Brake 6-20, 6-25, 6-30, 6-31, 7-31, 7-32, 7-33
 Brake test 6-20
 Braking 6-15, 6-16, 6-18, 7-1, 7-25, 7-31
 Braking ramp 6-15, 6-16
 British Standard (BS) 2-18
 Broken shearpin 4-17
 Bus scan time 5-13, 5-14
 Bus systems 4-4, 4-21, 4-22, 4-29,
 5-4, 5-5, 5-11, 5-13, 6-9

▶ C

Calculation tool 2-24, 2-54
 Calibration reports 2-58
 Camshaft: 4-17, 4-32, 4-33
 CAN 5-7, 5-17
 CAN communication standard 5-7
 CANopen 5-9, 5-14, 5-17, 5-18, 6-7
 CANopen standard 5-17

▶ 8.1 Index

- Category 2-27, 2-28, 3-22, 4-20, 6-6, 6-12,
6-15, 6-32, 6-37, 7-57, 7-58, 7-59,
7-60, 7-61, 7-63
- Category
Category 1, Performance Level b 7-58
Category 2, Performance Level b 7-59
Category 3, Performance Level d 7-60
Category 4, Performance Level e 7-61
- Cavitation 7-40
Cavitation types 7-40
CCC certification 2-44
CCF factor 2-26
CCOHS (Canadian Centre
for Occupational Health and Safety) 2-42
CDCN 5-18
CE certification process 2-7
CE mark 2-5, 2-10, 2-11, 2-15
CE-marking 2-5, 2-6, 2-7, 2-10,
2-12, 2-15, 2-17, 3-24
CEN 2-18, 2-28
CENELEC 2-18
Check list of manipulation incentives 3-25
Check valve 7-13, 7-28, 7-32, 7-50
Circuit diagram 4-11, 7-22, 7-23, 7-27, 7-32,
7-33, 7-34, 7-43, 7-45, 7-46,
7-47, 7-48, 7-49, 7-50, 7-55
Circuit-based solutions 7-25
Clamping cartridge 7-31, 7-33
CLC/TS 61496-2:2006 2-20, 2-39, 3-7
CLC/TS 61496-3:2008 2-20, 2-39, 3-7
CNC 4-28
Commissioning 2-10, 4-6, 6-9
Common cause factor 2-33
Communauté Européenne 2-5
Communication error 5-3, 5-7
Communication functions 5-4
Communication media 5-9
Communication standard 5-7
Communications hierarchy 5-15
Competent persons 2-59
Complete drive module (CDM) 6-10
Conduct contrary to safety 3-31
Configurable safety relays 4-4, 4-11, 4-13,
4-16, 4-20, 4-26
Configuration 2-27, 3-19, 6-22, 6-25,
7-23, 7-32, 7-33, 7-38, 7-54
Configuration tools 4-11
Conformity 2-5, 2-7, 2-12,
2-14, 2-16, 2-55
Conformity assessment procedures 2-17
- Connecting 4-3, 4-7
Connection designation 7-33, 7-34
Connection logic 4-8
Constant pump 7-41, 7-51
Contact-based technology 4-9, 4-13
Continuity equation 7-39, 7-42, 7-44
Control (SRP/CS) 6-28
Control circuit plans 2-14
Control system 2-20, 2-31, 2-35, 2-46,
3-12, 4-21, 4-22, 4-25, 4-28,
4-30, 5-13, 5-19, 6-11
Control technology 4-3, 4-22, 4-24,
4-29, 4-30, 7-34
Control valve 4-20
Control variable 6-5, 6-6
Controlled braking 6-15
Controlled loop status 6-17
Controlled stop 6-12, 6-14, 6-15, 6-16
Controller inhibit 3-23
Controller release 6-5, 6-6
Controlling valves 4-33
Converter 3-23, 6-4, 6-5,
6-6, 6-25, 6-31
Counter No. 5-19
Couplings or fastenings 7-55
CRC 5-19
Cross muting 4-16
Crushing 2-19, 3-7
CSA (Canadian Standards Association) 2-42
Cycle initiation 4-17
Cycles 6-31
Cyclical data channel 5-17, 5-18
- ▶ **D**
- DACH 2-57
Daisy chain wiring 5-16
DAkKS (German Accreditation Body) 1-3, 2-54,
2-57, 2-58, 2-59, 2-60
Dangers 2-14, 3-3, 3-8, 3-24,
3-27, 3-30, 4-7, 4-31, 6-30,
7-5, 7-7, 7-8, 7-9, 7-10,
7-12, 7-15, 7-16, 7-17,
7-19, 7-21, 7-26, 7-54
DAP 2-57
Data exchange 4-13
Data security mechanism 5-4
DC value 2-26, 2-49
DC_{avg} 2-26
Decentralised safety technology 5-3
Declaration of conformity 2-5, 2-6, 2-10,

▶ 8.1 Index

- 2-11, 2-14, 2-15, 2-54
- Declaration of incorporation2-10, 2-14
- Declaration of no objection 2-44
- Defeating safeguards 3-25
- Design error 3-29
- Design of safeguards 3-12
- Design principles 2-21
- Detection of shorts across contacts 4-21
- Deterministic dangers 7-8, 7-9, 7-15, 7-19
- Diagnostic capability 4-6
- Diagnostic coverage (DC).....2-26, 2-27,
6-31, 7-30, 7-31
- Diagnostic data 4-13
- Diagnostic purposes 4-4
- Differential circuit 7-49
- DIN 2-18
- DIN EN 982 clause 6 7-55
- DIN EN ISO 17020..... 1-3, 2-54, 2-59
- Direction of approach 2-30
- Direction of rotation 6-7, 6-35
- Directives 2-3, 2-4, 2-5, 2-12, 2-15, 2-16,
2-42, 2-43, 2-45, 2-54
- Directives and laws in America 2-42
- Directives and laws in Asia 2-43
- Directives and laws in Oceania 2-45
- Distance monitoring 4-32
- DKD 2-57
- Documentation 2-7, 2-14, 2-46,
2-51, 3-14, 7-4, 7-5
- Domestic law 2-3
- Doors 2-19
- d_{op} 6-31, 6-34
- Downward movement 7-44
- Drag error detection 6-37
- Drive 3-12, 3-23, 6-4, 6-12, 6-15, 6-18, 6-19,
6-24, 6-25, 6-26, 6-27, 6-36, 6-37,
6-38, 6-39, 6-40, 7-4, 7-23, 7-30, 7-35
- Drive bus 6-9, 6-26
- Drive components 6-22, 6-23
- Drive electronics 6-4, 6-23
- Drive environment 4-20
- Drive pump 7-51, 7-52, 7-53
- Drive system 4-21, 6-3, 6-4, 6-6,
6-10, 6-11, 6-12, 6-25
- Drive technology 3-23, 4-37, 6-6,
6-15, 6-16, 6-22, 6-23, 7-3
- Drive-integrated monitoring 6-26, 6-36
- Drive-integrated safety 3-23, 4-36, 6-3, 6-13
- Drive-integrated safety technology 6-3, 6-19
- Drive-integrated solution 6-6, 6-12, 6-19, 6-25
- Duration of exposure to hazard 2-25
- ▶ **E**
- EC declaration of conformity 2-10, 2-15, 2-17
- Electrical codes (NEC) 2-42
- Electrical safety 2-35
- Electronic cam disk (synchronous motion) 6-26
- Electronic safety relays 3-21, 4-6, 4-9
- Electronics 1-3, 2-18, 4-37
- Electrosensitive protective equipment 2-20,
2-39, 3-7, 3-17
- Elliptical curve (resulting motion) 6-26
- EMC directive 2-16
- EMC load 5-9
- EMC requirements 2-20, 2-38
- Emergency stop ... 4-3, 4-4, 4-6, 4-7, 4-9, 4-20, 4-29
- Emergency stop devices 6-34
- EN 1005-1 to -4:2008 2-19
- EN 1005-5:2007 2-19
- EN 1010 3-26
- EN 1037 3-23
- EN 1037:2008 2-19
- EN 1050 2-20, 2-21
- EN 1088 3-11
- EN 1088:2007 2-19, 2-39
- EN 12453:2000 2-19
- EN 292 2-19, 2-21
- EN 349:1995+A2:2008 3-7
- EN 349:2008 2-19
- EN 415 6-28
- EN 547-1 to -3:2008 2-19
- EN 574:2008 2-19
- EN 60204-1 2-35, 2-42, 6-12
- EN 60204-1:2007 2-35
- EN 60204-1:2010 2-20
- EN 60947-5-1:2009 2-20
- EN 60947-5-2:2008 2-20
- EN 60947-5-3:2007 2-20
- EN 60947-5-4:2003 2-20
- EN 60947-5-5:2006 2-20
- EN 60947-5-6:2001 2-20
- EN 60947-5-7:2003 2-20
- EN 60947-5-8:2007 2-20
- EN 60947-5-9:2008 2-20
- EN 61326-3 parts 1+2:2008 2-20, 2-38
- EN 61496-1:2010 2-20, 2-39, 3-7
- EN 61496-3:2003 2-20, 2-39, 3-7
- EN 61508 2-18, 2-20, 2-23, 2-31, 2-35,
2-36, 2-37, 2-40, 2-46
- EN 61508 Parts 1-7:2010 2-20

▶ 8.1 Index

EN 61511 Parts 1-3:2004	2-20	European co-operation for Accreditation (EA)....	2-57
EN 61784-3:2010	2-20, 2-23	European Union.....	2-3, 2-4
EN 61800.....	6-10, 6-11	Evaluation logic	4-4
EN 61800-5-2:2007	2-20, 2-39, 2-40	Ex area.....	4-10
EN 62061.....	2-31, 2-35, 2-51, 3-11	Ex area II (1)GD [EEx ia] IIB/IIC.....	4-10
EN 62061:2005.....	2-31	Examples of safe motion.....	6-28
EN 62061:2010.....	2-20	Excess pressure	7-22, 7-38
EN 692.....	6-28	Excessive functionality	3-29
EN 693.....	6-28	Exhaust throttles	7-32
EN 953.....	3-9, 3-30	Exposition.....	2-24, 3-11
EN 953:1997+A1:2009	3-7	External commands	6-42
EN 953:2009.....	2-19	External motion monitoring	
EN 999.....	2-19, 2-30, 3-7	with one standard encoder.....	6-37
EN ISO 10218-1	6-28	External motion monitoring	
EN ISO 11161:2010.....	2-19, 2-41	with safe encoder	6-40
EN ISO 12100:2010.....	2-19, 2-21	External motion monitoring with	
EN ISO 12100-1 and 2	2-19, 2-21	standard encoder and proximity switch.....	6-38
EN ISO 12100-1:2009	2-21	External motion monitoring with	
EN ISO 12100-2:2009	2-21	two standard proximity switches.....	6-39
EN ISO 13849-1	2-19, 2-21, 2-23, 2-24, 2-25, 2-26, 2-27, 2-28, 2-29, 2-31, 2-35, 2-40, 2-46, 2-47, 2-51, 2-53, 2-54, 3-12, 6-12, 6-28, 6-29, 6-31, 6-32, 6-34		
EN ISO 13849-1:2008	2-25, 2-28, 2-29		
EN ISO 13849-1:2009	2-19		
EN ISO 13849-2:2008	2-19		
EN ISO 13855.....	2-30, 3-16, 3-17, 3-18, 3-19, 6-33		
EN ISO 13855:2010.....	2-19, 2-30, 3-7		
EN ISO 13857:2008.....	2-19, 2-30, 3-7		
EN ISO 14121-1:2007	2-20, 2-21		
EN/IEC 61508.....	6-7, 6-10, 6-11		
EN/IEC 61800-5-2	6-3, 6-6		
Enable principle.....	4-24, 4-25		
Enable switch	4-7, 6-34		
Encoder cable	4-20, 6-25		
Encoder signal.....	4-20, 6-7, 6-37, 6-38		
Encoder systems.....	6-7, 6-8, 6-19, 6-25		
Encroachment from behind	3-19, 3-21		
Energy supply.....	3-23, 4-3, 6-5, 6-6, 6-30, 7-54		
Environmental requirements.....	2-52		
EPDM	3-21		
Error reaction function.....	6-25		
Error state.....	4-13		
ESPE	3-17, 3-18, 3-21		
Ethernet.....	4-22, 5-13, 5-14, 5-15		
Ethernet communication system.....	5-13		
Ethernet OSI Layer	5-14		
Ethernet technology	5-14		
Ethernet/IP	5-9		
Ethernet-based fieldbus system	5-13		
		▶ F	
		Failsafe	7-12
		Failsafe control system.....	4-24
		Failsafe principle	6-3, 6-25
		Failure mode.....	7-28
		Fault rectification procedure.....	3-27
		Fault simulation (safety check).....	2-54
		Fault tolerance.....	2-34
		Feasibility tests.....	6-7
		Fibre-optic (FO) communication.....	5-9
		Fibre-optic cable	5-9, 5-12
		Fibre-optic communication	5-9
		Fibre-optic routers.....	5-9
		Fieldbus	2-20, 2-23, 4-13, 4-24, 4-25, 5-6, 5-11, 5-13, 5-16, 6-7, 6-9
		Fieldbus communication	5-6
		Fieldbus modules	4-13
		Fieldbus standard.....	5-17
		Fieldbus system	5-6, 5-13, 5-20
		Fire Codes (NFPA)	2-42
		Fittings.....	7-40
		Fixed guards.....	3-8, 3-12
		Flow	7-50
		Flow forms.....	7-39
		Fluid power system	7-35, 7-56
		Force and path transmission.....	7-38
		Freedom of movement.....	2-17
		Frequency converter	5-14, 6-4, 6-23, 6-27, 6-37
		Frequency of the	
		exposure to the hazard.....	2-25, 2-32

▶ 8.1 Index

Friction shear stress	7-40	IEC 61508	2-36, 4-37, 7-9
Function blocks	4-26, 4-34	IEC TR 62061-1:2009	2-20
Function test	2-52, 2-54, 3-11, 7-55	IEC/TR 62685:2010	2-20, 2-23
Functional safeguard	3-23	IEC/TS 62046:2008	2-20, 2-39
Functional safety	1-3, 2-20, 2-24, 2-31, 2-35, 2-40, 6-3, 6-10	IL (Instruction List)	4-21
▶ G		Immunity requirements	2-38
Generic safety standards and technical safety standards	6-28	Import	2-7
German Institute for Standardization (DIN)	2-18	Incomplete machinery	2-10
GOST-R certification	2-43	Incorrect message sequence	5-4
Gravitational pressure	7-38	Increase productivity	4-22
Guard locking	3-5, 3-9, 3-12	Incremental encoder	6-27
Guards	3-4, 3-5, 3-6, 3-7, 3-8, 3-9, 3-12, 3-29, 7-17	Indicative safety technology	3-3, 7-15, 7-19
▶ H		Indirect safety technology	7-15, 7-16
Harmonisation	2-3, 2-4, 2-18, 2-43	Indirect safety technology	7-15, 7-17
Harmonised standard	2-4, 2-46	Industrial communication networks	2-20, 2-23
Hazard	2-14, 2-16, 3-8, 3-16, 3-17, 3-23, 4-3, 6-18, 6-19, 6-25, 7-5, 7-54	Industrial Safety and Health Law	2-44
Hazard assessment	2-52	Industrial Safety and Health Law	2-44
Health and safety requirements	2-12, 2-14, 2-17	Input device	4-20, 6-7, 6-8, 6-36, 6-37, 6-38, 6-40
Health and safety requirements	2-12, 2-14, 2-17	Input devices	2-39, 3-12, 3-20, 3-21, 4-4, 4-16, 4-32, 5-13, 6-24, 6-26, 6-36, 6-37, 6-38, 6-39, 7-30
High Demand Mode	2-31	Inputs/outputs	4-11, 4-21
High-end safety solutions	6-3	Installation	4-7, 5-13
Holding and service brakes	6-20, 6-30	Installation process	4-7
Holding brake	6-20, 6-24, 6-31, 6-32, 7-31	Institute for Standardization	2-18
h_{op}	6-31, 6-34	Instituto Argentino	2-43
Hose colours	7-34	Instituto Nacional	2-43
Hose cross sections	7-34	Integrated fault detection	3-14
Hose numbers	7-34	Integrated safe shutdown path	6-14, 6-23
Hydraulic accumulator	7-55	Interfaces/communication	6-22
Hydraulic circuit	7-43, 7-44, 7-45	Interlock	3-4, 3-5, 3-9, 3-26, 3-29, 3-31, 4-29, 7-54
Hydraulic control systems	7-56, 7-62	Interlocking concept for special operating modes	3-27
Hydraulic fluid filtration (RF)	7-56	Interlocking device	2-19, 2-39, 3-5, 3-7, 3-11
Hydraulic system	7-43	Intermediate circuit	6-5, 6-6, 6-23
Hydraulic systems with hydraulic accumulator	7-55	International Accreditation Forum (IAF)	2-57
Hydraulic work	7-39	International Electrotechnical Commission (IEC)	2-18, 2-45
Hydraulics	2-35, 4-29, 7-3, 7-21, 7-23, 7-35, 7-40	International Laboratory Accreditation Cooperation (ILAC)	2-57
Hydro pumps	7-41	International Organization for Standardization (ISO)	2-18, 2-45
Hydrostatic power transmission	7-35	Inverted rectifier	6-5, 6-6
▶ I		I_s	3-16
I/O interconnection	6-9, 6-26	I_{Smax}	3-16
IEC 60204-1	6-14, 6-15, 6-16	$I_{Smax(i)}$	3-16
IEC 61131	4-26	ISO 14118:2000	2-19
IEC 61495-2:2006	2-20, 2-39, 3-7	ISO 14119	2-19, 2-39
		ISO 15189	2-58

▶ 8.1 Index

ISO TR 23849:2010	2-20	Manual start-up valve	7-25
ISO/IEC 17020	2-58	Manual valve	7-25
ISO/IEC 17025	2-58	Manufacturer	2-3, 2-4, 2-5, 2-6, 2-7, 2-10, 2-12, 2-14, 2-23, 2-35, 2-40, 3-24, 3-26, 3-28, 3-29, 4-11, 6-11, 6-25, 6-31, 6-39, 6-40, 7-9, 7-33
ISO/OSI reference model	5-15	Manufacturer's declaration	2-10
▶ J		Manufacturing process	2-53, 4-31, 6-11
JIS standards (Japan Industrial Standards)	2-44	Marking	7-33
Jog function	6-18, 6-33, 6-34	Master/slave system	5-13
Jog mode	6-3, 6-18, 7-58	Measurements	2-54, 2-58, 5-13
▶ L		Mechanical dangers	7-8, 7-10
Laser scanners	2-39, 3-21, 4-10, 4-16	Mechanical movement	6-7
Law of friction	7-40	Mechanical spring	7-23, 7-28, 7-34
LD (Ladder Logic/Ladder Diagram)	4-21	Mechanics	2-18, 2-35, 4-37, 7-3, 7-23, 7-26, 7-34
Leakages	7-21, 7-54	Mechatronic units	4-30, 5-20
Lifecycle	1-3, 2-35, 2-40, 6-22	Message Channel	5-18
Lifecycle phases	2-14	Message corruption	5-4
Lift stops	7-55	Message delay	5-4
Light barrier	2-39, 2-54, 3-6, 3-8, 4-6, 4-16, 4-17, 7-17, 7-23	Message insertion	5-4
Light curtain	2-39, 2-54, 3-19, 4-6, 5-7, 5-11	Message loss	5-4
Limbs	2-19, 2-30, 3-7	Message repetition	5-3, 5-4
Limit value	4-20, 6-3, 6-9, 6-12, 6-15, 6-16, 6-17, 6-18, 6-19, 6-24, 6-25, 6-36, 7-5, 7-54	Microprocessor technology	4-6, 4-9
Limit value violation	6-12, 6-19, 6-42	Minimum distances	2-19, 3-7, 3-19, 7-16
Low Demand Mode	2-31	Minimum speed	6-18
Low voltage directive	2-12, 2-16	MLA = Multilateral Recognition Arrangement ...	2-57
Low-noise design	7-54	Modification	5-8
▶ M		Modular machine design	5-20
MAC-Frames	5-14	Modularisation	4-28, 4-30
Machine availability	6-6	Monitored disconnection	4-4, 4-10
Machine cycle	6-34	Monitoring function	4-4, 4-22, 4-29, 6-16, 6-18, 6-25, 6-36, 6-37, 6-38, 6-39, 6-40
Machinery	2-5, 2-6, 2-7, 2-8, 2-10, 2-12, 2-14, 2-15, 2-28, 2-29, 2-44, 2-46, 2-47, 2-48, 2-49, 2-51, 2-52, 2-54, 3-3, 3-4, 3-5, 3-6, 3-11, 3-12, 3-13, 3-16, 3-17, 3-19, 3-21, 3-26, 3-28, 3-29, 3-31, 4-3, 4-4, 4-6, 4-7, 4-22, 4-30, 4-37, 6-7, 6-9, 6-23, 6-25, 6-30, 7-4, 7-5, 7-8, 7-9, 7-12, 7-17, 7-19, 7-21, 7-22, 7-25, 7-26, 7-33, 7-34, 7-55, 7-59	Monitoring obligation	3-29
Machinery Directive	1-3, 2-5, 2-6, 2-7, 2-8, 2-10, 2-11, 2-12, 2-14, 2-15, 2-16, 2-17, 2-19, 2-24, 2-29, 2-31, 2-60, 3-4, 3-7, 3-24, 3-28, 3-31, 7-4, 7-5, 7-9, 7-15, 7-33	Motion	4-28, 4-29, 4-30
Mains contactor	6-5	Motion control	3-23, 6-4, 6-26
Mandatory certification	2-44	Motion control system	6-26
Manipulation of safeguards	3-24	Motion generation	6-4, 6-12
Manual controls	3-22, 3-26	Motion monitoring	6-24, 6-25, 6-26, 6-27, 6-36, 6-37, 6-38, 6-39, 6-40
		Motion monitoring with external devices	6-36
		Motor	6-3, 6-4, 6-5, 6-6, 6-7, 6-9, 6-10, 6-12, 6-14, 6-15, 6-16, 6-17, 6-19, 6-24, 6-25, 6-31
		Motor contactor	6-5, 6-6
		Motor current	6-19
		Motor feedback	6-7
		Movable guards	2-19, 3-5, 3-7, 3-12, 3-14, 3-16
		Movable safeguards	4-4

▶ 8.1 Index

- MRA = Mutual Recognition Agreement..... 2-57
 MS6-SV 7-26, 7-27
 MSCN (Message Channel) 5-18
 MTTFd – Mean time to dangerous failure 2-25
 Multi-master bus system..... 5-13, 5-14
 Multi-turn encoder..... 6-7
 Muting 3-20, 6-35
 Muting function 3-20, 4-10, 4-16
 Muting lamp 4-16, 4-17
- ▶ **N**
- N/C contacts 3-13, 6-6
 National Standards Institute (INN)..... 2-43
 Navier-Stokes equation 7-39
 NC control system..... 6-26
 NFFA (National Fire Protection Association)..... 2-42
 NFFA 79 2-41, 2-42
 NFFA 79:2008 2-41
 NFFA 79:2009 2-20
 Noise Directive 2-16
 Non-safety-related communication function..... 5-4
 Normal mode..... 3-11, 3-29, 7-27
 Normally energised mode 7-57
 Normally open principle 3-21
 Notified body..... 2-17, 2-43, 2-44
- ▶ **O**
- Occupational Health and Safety Act (OH&S – Gesetz über Arbeits- und Gesundheitsschutz)..... 2-45
 OD – Ordinary Device..... 5-16
 Official Journal of the EU..... 2-3, 2-4, 2-28
 Oil flow control 7-44
 Old machine 2-7
 Open circuit 4-4, 4-37, 6-12, 7-16
 Opening frequency 3-11, 3-30
 Operating manual..... 2-6, 2-14, 2-54, 3-3, 3-24, 3-27, 7-4, 7-19, 7-33
 Operating mode selection 4-33
 Operating pressure..... 7-22, 7-23, 7-24, 7-25, 7-33, 7-35, 7-54, 7-55
 Operating pressure range..... 7-54
 Operating temperatures 7-54
 Operator 2-6, 2-41, 2-44, 2-52, 2-54, 3-28, 3-29, 4-7, 7-23
 Optocoupler 6-5, 6-6, 6-23
 OSHA standards..... 2-42
 OSI reference model..... 5-15, 5-18
 OSSD..... 3-14, 3-16
- Overall circuit..... 6-29, 6-32, 6-34, 6-35, 6-42
 Overrun..... 6-3, 6-19, 6-23, 7-23, 7-33, 7-60
 Own use 2-7
- ▶ **P**
- Packet Identifier 5-19
 Parallel circuit 7-46, 7-48, 7-49
 Parameter tool..... 4-12
 Parameters S, F and P 2-29
 Particularly hazardous machinery 2-10
 Partly completed machinery..... 2-10
 Partly completed machinery..... 2-10
 Parts of the body..... 2-19, 2-30, 3-7, 3-17, 7-16
 PAScal Safety Calculator..... 2-24, 2-31, 2-50, 2-54, 6-32
 Passport to Europe 2-5
 PDS/Safety-Related (SR)..... 6-10
 Peak current IS..... 3-16
 Pendulum movement 4-32
 Performance Level 2-24, 2-26, 2-47, 2-51, 2-54, 3-12, 4-20, 6-28, 6-29, 6-30, 6-31, 6-32, 6-34, 6-35, 6-37, 6-38, 7-26, 7-27, 7-30, 7-31, 7-57, 7-58, 7-59, 7-60, 7-61, 7-62
 Performance Levels PLr 2-24, 2-25, 2-28, 2-47, 2-50
 Personal Protective Equipment Directive..... 2-16
 PFD (Probability of failure on low demand)..... 2-31
 PFHD 2-34, 6-32
 Physical performance..... 2-19
 PID (Packet Identifier)..... 5-19
 Piston forces 7-41, 7-42
 Piston pressure force 7-41
 Piston speed 7-42, 7-44, 7-88
 PL 2-25, 2-26, 2-28, 2-49, 3-14, 6-29, 6-32, 6-37, 6-38, 6-39, 6-40, 7-26, 7-31, 7-58, 7-59, 7-60, 7-61, 7-62
 PL e 3-14, 6-38, 6-39, 6-40, 7-62, 7-62
 PL graph..... 2-25, 2-28, 6-32
 Placing on the market 2-17
 PLC..... 4-21, 4-34
 PMCprotego DS 4-36
 Pneumatic components 7-21, 7-22
 Pneumatic system..... 2-35, 4-29, 7-3, 7-21, 7-23, 7-24, 7-25, 7-26, 7-30, 7-34
 PNOZ..... 4-3, 7-27
 PNOZelog..... 4-9
 PNOZmulti 3-23, 4-4, 4-33, 4-30
 PNOZsigma 4-6
 Polling..... 5-7
 Position monitoring 4-4, 4-20, 6-19

▶ 8.1 Index

- Position window 6-12, 6-17, 6-19
- Positioning.....6-26
- Positioning control.....6-26
- Possibility of avoidance.....2-25
- Possibility of defeat2-39, 3-19
- Power contactor.....4-4, 7-60
- Power drive system (PDS).....6-10
- Press applications4-17
- Press safety valve.....4-17
- Press stroke.....4-32
- Pressure3-25, 3-29, 7-22, 7-24, 7-25, 7-33,
7-34, 7-35, 7-38, 7-39, 7-40, 7-41, 7-43,
7-47, 7-48, 7-49, 7-53, 7-54, 7-57, 7-58
- Pressure drops7-40
- Pressure intensifier7-42
- Pressure limitation.....7-22, 7-56, 7-57, 7-62
- Pressure limitation in the system (VDB).....7-56
- Pressure losses7-40
- Pressure relief valve.....7-43
- Pressure sensitive mats.....3-19, 3-21
- Pressure source.....7-34
- Pressure transmission7-39
- Pressure values7-22
- Presumption of conformity2-3, 2-4,
2-24, 2-28, 2-31
- Primary control7-50
- Problems due to EMC5-4
- Procedures used to attach
and monitor safeguards3-30
- Process data object5-17, 5-18
- Process data objects (PDOs)5-17
- Product liability2-29
- Product monitoring.....3-29
- Product Safety Directive.....2-16
- Product standards.....2-28, 2-39
- Profibus DP5-9
- Programmable logic control system (PLC).....4-3
- Protective device.....2-39, 3-5, 3-8, 3-9,
3-11, 3-12, 3-17, 3-19, 3-26,
3-30, 3-31, 7-17
- Protective devices3-5, 3-7, 3-8, 7-17
- Proximity switches3-14
- PSSu multi.....4-34
- Publisher/subscriber principle.....5-16
- ▶ **Q**
- Quality assurance.....2-58, 2-60
- Quiet running.....7-51
- ▶ **R**
- Radio Equipment Directive.....2-16
- Range monitoring4-20
- Rated holding torque.....6-31
- RC control6-26
- Reaction function6-19, 6-25
- Reaction times.....4-22, 5-8, 5-9, 6-3,
6-15, 6-16, 6-23, 6-25, 6-42
- Real-time communication5-16
- Reduction factor.....6-32
- Redundancy3-14, 5-3, 5-5, 7-12, 7-13, 7-14
- Redundant design4-6
- Reed contacts3-16
- Reference variable.....6-5, 6-6
- Relay circuits4-3
- Relay technology.....4-4, 4-6
- Relays.....2-53, 3-16, 4-3, 4-6
- Required characteristics
of guards and protection devices.....3-4
- Requirement manual2-7
- Residual risk2-14, 3-28, 3-29, 7-9
- Resistance coefficient7-40
- Restart.....3-19, 3-23, 4-12, 6-6,
6-14, 6-23, 7-54
- Retrofit.....6-25
- REYNOLDS NUMBER.....7-39
- RFID.....3-14
- Ring area7-48, 7-49
- Risk.....2-14, 2-25, 2-32, 3-5, 3-28, 3-30, 3-31,
4-3, 7-5, 7-9, 7-19, 7-23, 7-29
- Risk analysis.....2-13, 2-14, 2-21, 2-24, 2-32, 2-44,
6-11, 6-18, 6-20, 6-23, 6-28, 6-30, 7-30
- Risk assessment2-10, 2-12, 2-13, 2-20, 2-21,
2-46, 2-47, 2-54, 3-12, 7-9, 7-24
- Risk assessment in accordance
with EN 62061, EN ISO 13849-13-12
- Risk evaluation2-19, 2-21, 2-24, 2-28, 2-29,
2-32, 2-34, 2-40, 3-18, 3-24, 7-6, 7-9, 7-54
- Risk factors2-21
- Risk graph2-24, 2-25, 2-29, 2-31, 2-32
- Risk minimisation2-21, 2-46
- Risk reduction2-19, 2-21, 2-22, 4-4
- Root Device.....5-16
- Rotary encoder.....5-14, 6-6, 6-7, 6-36,
6-37, 6-38, 6-39, 6-40
- Rotation direction monitoring4-33
- Rotational speed2-20, 2-40, 4-4,
4-10, 4-12, 4-20, 6-10, 6-12,
7-37, 7-41, 7-55, 7-58

▶ 8.1 Index

R_{Pmin}	3-16	Safe stop 1 (SS1).....	6-7, 6-12, 6-14, 6-16
RSA	2-18	Safe stop 2 (SS2).....	6-12, 6-16, 6-17
$R_{Smin(0)}$	3-16	Safe stop function	6-14, 6-19, 6-28, 6-32, 6-35
RTFL (Real Time Frame Line)	5-14, 5-15, 5-16	Safe stop function on vertical axes	6-30
RTFN (Real Time Frame Network).....	5-14, 5-15	Safe torque off (STO).....	6-12, 6-14
Rule breach	3-27	Safe torque range (STR)	6-19
Run	2-41, 3-3, 3-11, 3-23, 5-18, 6-9, 6-12, 6-14 6-16, 6-17, 6-20, 6-24, 6-25, 7-34, 7-41, 7-54	Safeguarding detection zones with a safe camera-based solution	6-41
Run monitoring.....	4-17	Safely limited acceleration (SLA).....	6-17
▶ S		Safely limited increment (SLI).....	6-19
$S = (K \times T)$	3-16	Safely limited position (SLP).....	6-19
$S = (K \times T) + C$	3-19	Safely limited speed (SLS).....	6-18, 6-19, 6-33, 6-34, 6-36, 6-37, 6-38, 6-39, 6-40
$S = K * (t1 + t2) + C$	3-17	Safely limited torque (SLT).....	6-19
Sabotage	3-26	Safely reduced speed.....	6-3, 6-18
Safe absolute position.....	6-7	Safety and Health Organisation).....	2-42
Safe acceleration range (SAR).....	6-17	Safety chain.....	4-4, 6-13, 7-29
Safe analogue processing.....	4-20	Safety characteristic data.....	6-36
Safe brake control (SBC).....	6-20	Safety component	2-6, 2-11, 2-53, 7-21, 7-26
Safe brake function	6-20	Safety control systems	2-35, 4-4, 4-21, 4-24, 4-26, 4-31, 4-32, 4-33, 4-34, 4-36, 4-37, 5-7, 5-9, 6-3, 6-24
Safe brake test (SBT).....	6-20	Safety distance.....	3-6, 3-16, 3-17, 3-18, 3-19, 6-42
Safe braking	6-25	Safety fence	3-6, 3-16, 3-19
Safe cam (SCA)	6-19	Safety functions.....	2-23, 2-24, 2-28, 2-31, 2-39, 2-40, 2-47, 2-48, 2-49, 2-50, 2-51, 2-52, 2-54, 3-12, 4-3, 4-4, 4-6, 4-9, 4-11, 4-20, 4-21, 4-25, 4-32, 4-33, 4-37, 5-17, 6-3, 6-6, 6-7, 6-10, 6-11, 6-12, 6-13, 6-14, 6-15, 6-16, 6-17, 6-18, 6-19, 6-20, 6-21, 6-23, 6-24, 6-25, 6-26, 6-28, 6-29, 6-30, 6-31, 6-33, 6-35, 6-36, 6-37, 6-38, 6-39, 6-40, 6-41, 6-42, 7-9, 7-29, 7-31, 7-57, 7-59, 7-61
Safe camera systems	2-39, 2-60, 3-17, 3-21, 6-3	Safety gate	2-60, 3-9, 3-12, 3-13, 3-14, 3-16, 4-6, 4-7, 4-9, 4-12, 4-20, 4-29, 4-33, 4-37, 5-11, 6-3
Safe camera-based solution	6-36	Safety guidelines	7-19
Safe communication	4-13, 5-8, 5-9, 5-18, 5-19	Safety integrity	6-8, 6-11, 6-13, 6-23
Safe condition	6-3	Safety Integrity Level (SIL).....	2-32, 2-47, 2-51
Safe control systems.....	4-26, 6-9	Safety lockout	6-16
Safe control technology	4-3, 4-29	Safety objectives	2-3, 2-4, 2-49, 7-26
Safe decentralisation.....	4-24	Safety principles.....	2-23, 2-48, 2-53, 7-24, 7-57, 4-58, 7-59, 7-60, 7-61
Safe direction (SDI).....	6-19, 6-36, 6-37, 6-38, 6-40	Safety relays.....	2-35, 3-16, 3-20, 3-21, 4-3, 4-4, 4-6, 4-7, 4-8, 4-9, 4-10, 4-11, 4-12, 4-13, 4-16, 4-20, 4-26, 6-24
Safe direction (SDI).....	6-35		
Safe drive function	6-3		
Safe encoder	6-8, 6-40		
Safe life principle	7-12		
Safe limit value specification	6-9		
Safe logic.....	6-24		
Safe motion	6-3, 6-22		
Safe motion	6-3		
Safe motion control	3-23, 6-4		
Safe motion function	6-17		
Safe motion monitoring	6-9, 6-26		
Safe operating stop (SOS).....	6-16, 6-17, 6-36, 6-37, 6-38, 6-40		
Safe reset lock.....	6-14, 6-23		
Safe Service Data Objects	5-18		
Safe speed monitoring (SSM).....	6-19		
Safe speed range (SSR)	6-18, 6-36, 6-37, 6-38, 6-40		

▶ 8.1 Index

- Safety requirements2-17, 2-51,
4-13, 6-12, 6-25, 7-54, 7-55
- Safety switches with
integrated fault detection3-14
- SafetyBUS p..... 5-3, 5-5, 5-6, 5-7, 5-8,
5-9, 5-10, 5-11, 5-12
- SafetyBUS p system description5-7
- SafetyNET p 5-3, 5-4, 5-13, 5-14,
5-15, 5-16, 5-17, 5-18,
5-19, 5-20, 6-7
- Safety-related communication 5-3, 5-8,
5-9, 5-13, 5-18
- Safety-related communication function5-4
- Safety-related message5-4, 5-5
- Schematic7-26, 7-27
- Screw joints.....7-23, 7-34
- Screw pump7-52
- SDO (service data objects).....5-17
- Secondary control7-50
- Sector standard..... 2-25, 2-31, 2-35,
2-38, 2-46, 6-11
- Segmented shutdowns3-26
- Selectable operating modes and times4-6
- Semiconductor outputs.....4-4, 4-6
- Sensor subsystem.....6-38, 6-39
- Sequence valve7-47
- Sequential muting4-16
- Series connection..... 3-12, 3-13, 6-28,
6-29, 6-31, 6-33, 6-35
- Series connection.....3-9, 3-16, 7-46, 7-48
- Service data objects.....5-17
- Service unit.....7-22, 7-25, 7-27, 7-34
- Servo amplifiers..... 6-4, 6-12, 6-14,
6-15, 6-23, 6-26, 6-28
- Servo and frequency converter6-11
- Servo converter6-25, 6-26
- Servo presses.....4-32
- Setpoint specification.....6-6
- Set-up Mode4-17, 6-18, 6-19, 7-24
- Severity of injury.....2-25
- SFF2-34
- Shutdown 1-3, 3-20, 3-23, 4-3, 4-31,
4-36, 6-3, 6-17, 6-18,
6-24, 7-60
- Shutdown path 6-4, 6-5, 6-6, 6-14, 6-23, 6-24
- Signal flow path.....3-28
- Significant change.....2-8
- Significant change.....2-8
- Sin/cos encoders: $\sin^2+\cos^2=1$ 6-40
- Sine/cosine motor encoder6-24, 6-26
- Single axis6-26
- Single Stroke4-17
- Sistema.....2-54
- Slide stroke.....4-32
- Software tool4-11
- SPDO.....5-18, 5-19
- Specifications.....2-14, 2-49
- Speed control.....7-44, 7-50
- Speed monitoring3-23
- Speed threshold6-17
- SRCF2-49
- SSDOs (Safe Service Data Objects).....5-18
- Standard communication5-8
- Standard encoder..... 4-20, 6-8, 6-36, 6-37, 6-38
- Standard ISO 90012-58
- Standard sensors6-38 6-39
- Standards 1-3, 2-3, 2-4, 2-12,
2-14, 2-16, 2-17, 2-18, 2-19, 2-21,
2-28, 2-29, 2-38, 2-39, 2-42, 2-43,
2-45, 2-46, 2-51, 2-55, 2-58, 3-7,
3-9, 4-4, 4-31, 4-37, 5-8, 6-28, 7-9,
7-34, 7-57
- Standards Australia2-45
- Standards for dimensioning of guards3-7
- Standards for guards3-7
- Standards for the design of
protective devices or electrosensitive
protective equipment3-7
- Standstill..... 4-20, 6-3, 6-12, 6-16, 6-20, 6-42
- Standstill detection6-15, 6-16
- Standstill position6-16, 6-17
- Standstill threshold6-12
- Statistical methods.....2-24, 2-31
- Steam bubble cavitation7-40
- Stochastic dangers 7-8, 7-9, 7-10, 7-12, 7-15
- Stop 3-5, 3-12, 4-4, 6-12, 6-14,
6-15, 6-16, 6-20
- Stop category.....6-12, 7-28
- Stop function6-12, 6-14, 6-19, 6-28,
6-29, 6-30, 6-32, 6-34, 6-35
- Stop functions6-12
- Stopping7-31
- Structural components.....5-7
- Structural methods.....2-24, 2-31
- Subscriber5-16
- Suspended loads6-20
- SWISS INSPECTION2-57
- Switching position sensing.....7-30

▶ 8.1 Index

- Synchronisation 6-16
 Synchronous circuits 7-46
 System category 2-26
 System examination 2-25, 2-33, 6-22
- ▶ **T**
- T1 mission time 2-34, 3-17
 T2 diagnostic test interval 2-34, 3-17
 t_{cycle} 6-42
 Technical documentation 2-14
 Technical specification 2-14
 Telegram 5-3, 5-4, 5-7, 5-8, 5-18
 Telegram structure 5-19
 Terminal voltage 6-5
 Test results 2-14, 2-49
 TGA/DATECH 2-57
 Throttle check valves 7-32
 Time delay 6-15, 6-16
 Timeout 5-4
 t_{multi} 6-42
 T_m Mission time 4-27
 Toothed gear pumps 7-51, 7-53
 Top-down 2-49
 Topology 5-14
 Torque measuring system 6-19
 Torque monitoring 4-37
 trampe 6-42
 Transition periods 2-3, 2-28, 2-35
 TRBS 1203 2-59
 $t_{\text{reac}} = t_{\text{multi}} + t_{\text{PMC}} + t_{\text{ramp}}$ 6-42
 $t_{\text{reac}} = t_{\text{PMC}} + t_{\text{ramp}}$ 6-42
 TÜV 4-11, 4-31, 5-9
 Two-cylinder control systems
 with electric valves 7-46
 Two-hand 4-6
 Two-hand control device 3-22
 Two-hand relays 2-19, 3-19, 3-22, 7-17
 Type C 2-59
 Type-examination 2-17, 2-2-43
- ▶ **U**
- UDP/IP-based communication 5-14, 5-15
 UL 2-18
 Unexpected start-up 2-19, 3-12, 3-23,
 6-14, 7-25, 7-54
 Unintended restart 3-23
 Upgrade 2-8, 7-34
 UPmax 3-16
 Upward movement 7-43
- ▶ **V**
- Validation 2-19, 2-24, 2-31, 2-46,
 2-47, 2-48, 2-49, 2-50, 2-51,
 2-52, 2-53, 2-54, 3-12
 Validation of safety functions 2-24, 2-31,
 2-50, 2-51
 Valve cross section 7-44
 Valves with defined switching position 7-55
 Vane pumps 7-53
 Variable pump 7-41
 Ventilation time 7-33
 Venting 7-25, 7-26, 7-27, 7-33
 Vertical axes 6-14, 6-25, 6-30
 Viscosity 7-40, 7-57
 Visualisation 4-28, 4-30
 V-Model 2-51
 Volumetric efficiency factor 7-39
- ▶ **W**
- Walking and hand speed 3-17, 3-19
 Wireless and antenna technology 5-10
 Wireless communication 5-10
 Wiring requirement 4-7, 4-8, 4-9, 4-13,
 6-12, 6-23, 6-25

8.2 Exclusion of liability

Our safety compendium has been compiled with great care. It contains information about our company and our products. All statements are made in accordance with the current status of technology and to the best of our knowledge and belief. While every effort has been made to ensure the information provided is accurate, we cannot accept liability for the accuracy and entirety of the information provided, except in the case of gross negligence. In particular, it should be noted that statements do not have the legal quality of assurances or assured properties. We are grateful for any feedback on the contents.

All rights to this safety compendium are reserved by Pilz GmbH & Co. KG. We reserve the right to amend specifications without prior notice. Copies may be made for internal purposes. The names of products, goods and technologies used in this manual are trademarks of the respective companies.

© 2013 by Pilz GmbH & Co. KG, Ostfildern
4., revised and expanded edition

Item no.: 775 740
8-8-2-0-100,2013-12 Printed in Germany

► Support

Technical support is available from Pilz round the clock.

Americas

Brazil
+55 11 97569-2804

Canada
+1 888-315-PILZ (315-7459)

Mexico
+52 55 5572 1300

USA (toll-free)
+1 877-PILZUSA (745-9872)

Asia

China
+86 21 60880878-216

Japan
+81 45 471-2281

South Korea
+82 31 450 0680

Australia

+61 3 95446300

Europe

Austria
+43 1 7986263-0

Belgium, Luxembourg
+32 9 3217575

France
+33 3 88104000

Germany
+49 711 3409-444

Ireland
+353 21 4804983

Italy
+39 0362 1826711

Scandinavia

+45 74436332

Spain

+34 938497433

Switzerland

+41 62 88979-30

The Netherlands

+31 347 320477

Turkey

+90 216 5775552

United Kingdom

+44 1536 462203

You can reach our international hotline on:

+49 711 3409-444
support@pilz.com

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.



Presented by:



Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Germany
Tel.: +49 711 3409-0
Fax: +49 711 3409-133
info@pilz.com
www.pilz.com

