

Friedrich Adams / Frank Schmidt (Editors)

## **Best of MRL-News\***

New information on  
"Safety of Machinery and Machine Control Systems"

\* and other Schmersal/Elan publications



**SCHMERSAL**





---

## **Liability**

The information and recommendations in this book are provided to the best of our knowledge and in good faith. Nevertheless they do not absolve you from your responsibility to check and weigh up different aspects. With the exception of any opposing and compelling statutory provisions, we shall assume no liability for any errors and misunderstandings arising from the presentation.

---

Editors:

Friedrich Adams, Frank Schmidt

on behalf of:

K.A. Schmersal GmbH

Safety at work Switching Systems

Möddinghofe 30

D-42279 Wuppertal

Tel.: +49 (0)202 6474-0

Fax: +49 (0)202 6464-100

E-Mail: [info@schmersal.com](mailto:info@schmersal.com)

Internet: [www.schmersal.com](http://www.schmersal.com)

Responsible person under German Press Law (ViSdP):

Friedrich Adams, K.A. Schmersal Holding GmbH & Co. KG, Möddinghofe 30, D-42279 Wuppertal

Tel.: +49 (0)178 6474-051

Typesetting:

flick-werk, Gladenbach

Printer:

WD print + medien, Wetzlar

ISBN: **9783926617-43-9**

First print run 2,500 copies, April 2011



Friedrich Adams / Frank Schmidt (Editors)

***Best of MRL-News\****

**\* and other Schmersal/Elan publications**

---

New information on  
“Safety of Machinery and Machine Control Systems”

---



# Contents

<b>I</b>	<b>Foreword</b> Thomas Ruhs	<b>9</b>
<b>II</b>	<b>Foreword by the editors</b>	<b>11</b>
	<b>Chapter 1: Legal bases of machinery safety in Europe and elsewhere</b>	<b>13</b>
	1.1 European Union (EU) directives framework	15
	1.2 The new EC Machinery Directive 2006/42/EC (MD)	21
	1.3 Further information and interpretation assistance on the Machinery Directive 2006/42/EC	41
	1.4 EC Machinery Directive – Excursus (1): Proof of conformity using a quality assurance system in accordance with Annex X of MD 2006/42/EC	45
	1.5 EC Machinery Directive – Excursus (2): Keyword “The documentation officer”“	51
	1.6 Excursus (3): Current and ongoing borderline questions of European and German machinery legislation [1] – Modifications vs. significant modifications to machinery – Machinery (complete machinery) – Used machinery	53
	1.7 Future changes in the Directives of the European Union (EU)	61
	1.8 Comparison: with the non-European requirements placed on machinery safety [1]	65
	<b>Chapter 2: New requirements placed on safety-related parts of control systems (replacement of EN 954-1 and standard successor EN ISO 13849-1:2006/2008)</b>	<b>75</b>
	2.1 EN ISO 13849-1: New category principle for machine safety	77
	2.2 New requirements placed on the design of safety-related parts of machine control systems	81
	2.3 The practical implementation of EN ISO 13849-1:2008 (2006) – Part 1: Further information and assistance – Part 2: Borderline issues – Part 3: Additional new requirements	93
	<b>Chapter 3: Safety-related issues with cross-cutting significance</b>	<b>109</b>
	3.1 Risk assessment and the safe design of machinery	111
	3.2 Protective devices for machines	127
	3.3 Manipulation of protective devices	133
	3.4 Risk: unexpected start-up	147
	3.5 New standard EN EN ISO 11 161: Safety of integrated manufacturing systems	153
	<b>Chapter 4: Technological development of safety components – illustrated using the example of the Schmersal range</b>	<b>161</b>
<b>III</b>	<b>Index</b>	<b>187</b>



# Foreword

Dear Schmersal customer,  
Dear Elan customer,

For many years we have been providing you with ongoing and up-to-date new information in our company magazine *MRL-NEWS* and our other publications about the safety of machinery and machine control systems, whether this information be of a legal, normative or other practical nature.

Through this and other measures such as the new Safety Consulting service, the tec.nicum and the CE network, the Schmersal Group wishes to underline its special claim to competency, going beyond being merely a manufacturer of safety-related components, albeit a very efficient one. Rather, we aim to be your preferred contact partner in all matters concerning functional machine safety, one that is able to provide you with background knowledge and additional information as well as practical tips and problem-solving individual consultancy services in a qualified manner in addition to an attractive product range.

If one considers the new EC Machinery Directive, the replacement of EN 954-1:1996 and its successor EN ISO 13849-1:2008 (2006) as well as the other amendments to standards and current questions, we have all had to contend with a great deal of change recently in the area of functional machine safety.


For this reason we have summarised the most important changes and topical issues for you in this *BEST OF ...* book. It is divided into the following chapters:

1. Current legal bases of machinery safety in Europe and elsewhere;
2. New requirements placed on the design of safety-related parts of control systems (replacement of EN 954-1 and standard successor EN ISO 13849-1:2008/2006);
3. Other topical or new tasks and issues concerning machinery safety;
4. Technological developments in the field of safety components.

In the book you can find updated articles from the *MRL-NEWS* and other Schmersal/Elan publications that have been written by well-known external experts and by our own colleagues. Once again it provides you with a summarising overview, an update and, hopefully, numerous useful suggestions on the subject of safe machinery that you can make use of for your work.

Wuppertal/Wettenberg, December 2010

With best regards,



Thomas Ruhs  
Managing Director  
K.A. Schmersal GmbH





## Foreword by the editors

Despite the diverse statutory and normative regulations for machinery safety which we discuss in this publication and others, designers and developers will repeatedly be faced with borderline issues and grey areas when it comes to practical implementation. In such cases a further directive would be helpful, one that we, on the basis of many years of experience and with a certain degree of irony, would like to name "Directive on the application of good common sense".

While this may not exist either as a legal or a standard document, there has been something with similar content since time immemorial. In philosophy this is called the "Golden Rule".

Ever since the 17th century, the "Golden Rule" (Latin *regula aurea*) has described time-honoured and widespread principles of a practical ethical code which regulates social behaviour simply on the basis of reciprocity, frequently formulated in an authoritative manner. This is illustrated by the following example: "Do unto others as you would have them do unto you!" The source was often the bible. The famous saying "Do not do unto others what you do not want them to do unto you" came from the positive translation of Tobias 4:15 in the 1545 Lutheran bible. Similarly negatively or positively formulated mnemonics and doctrines were already being handed down in religious texts from China, India, Persia, Ancient Egypt and Greece in the 7th century b.c. (Text: WIKIPEDIA).

In other words: in the case of borderline and grey areas, always ask yourself whether, with a clear conscience, you would allow those dearest to you – your partner or your children – to work on this machine. If you can answer this question in the affirmative, you will almost certainly not make any wrong decisions.

Having said this, you can always fall back on Immanuel Kant's (1724–1804) famous categorical imperative: "Live your life as though your every act were to become a universal law."

On this note we hope you find this book interesting.



**Fig. 1** Golden Rule mosaic from a painting by Norman Rockwell, which has been at the UN headquarters in New York City since 1985. Inscription: "Do unto others as you would have them do unto you".

We would also like to thank those whose assistance behind the scenes has considerably contributed to the success of this book publication.

Wuppertal/Wettenberg, December 2010

Frank Schmidt  
Head of Standards, Committee and Association  
Work, K.A. Schmersal GmbH

Friedrich Adams  
Head of Schmersal tec.nicum  
K.A. Schmersal Holding GmbH & Co. KG





*Chapter 1:*

***Legal bases of machinery safety in Europe  
and elsewhere***



# European Union (EU) directives framework



The information below is designed to promote better understanding of this book and in particular of the following article “The new Machinery Directive 2006/42/EC”.

A directive is a legal act from the European Union that is directed at the governments of EU Member States and which obliges them to transpose a directive into the respective national law within a specific period of time. As such the term “directive” is somewhat confusing if one takes this as something uncertain, non-binding or optional. In actual fact it concerns legal regulations whose implementation is mandatory without any “ifs and buts”. As such one could also simplify matters by referring to a kind of indirect law or European legislation (see also the background information on “European legislation” below).

When we realise the number of issues for which there are now EU directives, we could come to the conclusion that a major part of everyday life today, whether this concerns professional or person life, is defined by such EU legal acts.

The binding obligation on Member States to transpose directives into national law is derived from the European Treaties, the most recent version of which is the Lisbon Treaty dated November 2009.

## Technical work equipment

With regard to technical work equipment, a distinction must be made between two types of directive:

- a) So-called domestic market directives in accordance with Article 114 of the Lisbon Treaty (formerly Article 95)
- b) So-called occupational health and safety directives in accordance with Article 153 of the Lisbon Treaty (formerly Article 137).

With respect to a): with relation to the requirements placed on occupational health and safety, domestic market directives regulate the (minimum) requirements for products that are marketed for the first time in the European internal

market (irrespective of whether they have been manufactured here or externally, whether they are sold, leased or provided in any other manner and irrespective of whether they are manufactured for the market or – although this differs from directive to directive – for own use).

The objective of the domestic market directives is the free movement of goods for the products concerned at a very high safety level. Directives of this kind, which also include the Machinery Directive for example, must be transposed into the national law of Member States with their content unaltered (1 : 1).

For example, in Germany this transposition generally takes place under the umbrella of the Equipment and Product Safety Act (Geräte- und Produktsicherheitsgesetz – GPSG) by ordinance (MD 2006/42/EC becomes the machinery ordinance) but also sometimes within the framework of independent laws. Examples here are the EMVG (the German act dealing with the area of “electromagnetic compatibility”) or the MPG (the German Medical Device Act).

With respect to b): by contrast, occupational health and safety directives regulate the relationships between employers and employees and define minimum standards for the respective area. One example relates to workplaces which can in some cases also include machinery. In this case the emphasis is on the “workplace”, however (briefing, maintenance, inspection, environmental and ambient conditions etc.).

A typical example in this context is the so-called Use of Work Equipment Directive that has been transposed into national law in Germany via the Employment Protection Act (ArbSchG) and the German Ordinance on Industrial Health and Safety (BetrSichV). Today one can also find the term “Work Equipment Safety Directive” in place of the term Use of Work Equipment Directive [1]. Unlike domestic market directives, Member States can go beyond minimum requirements in the case of occupational health and safety directives.

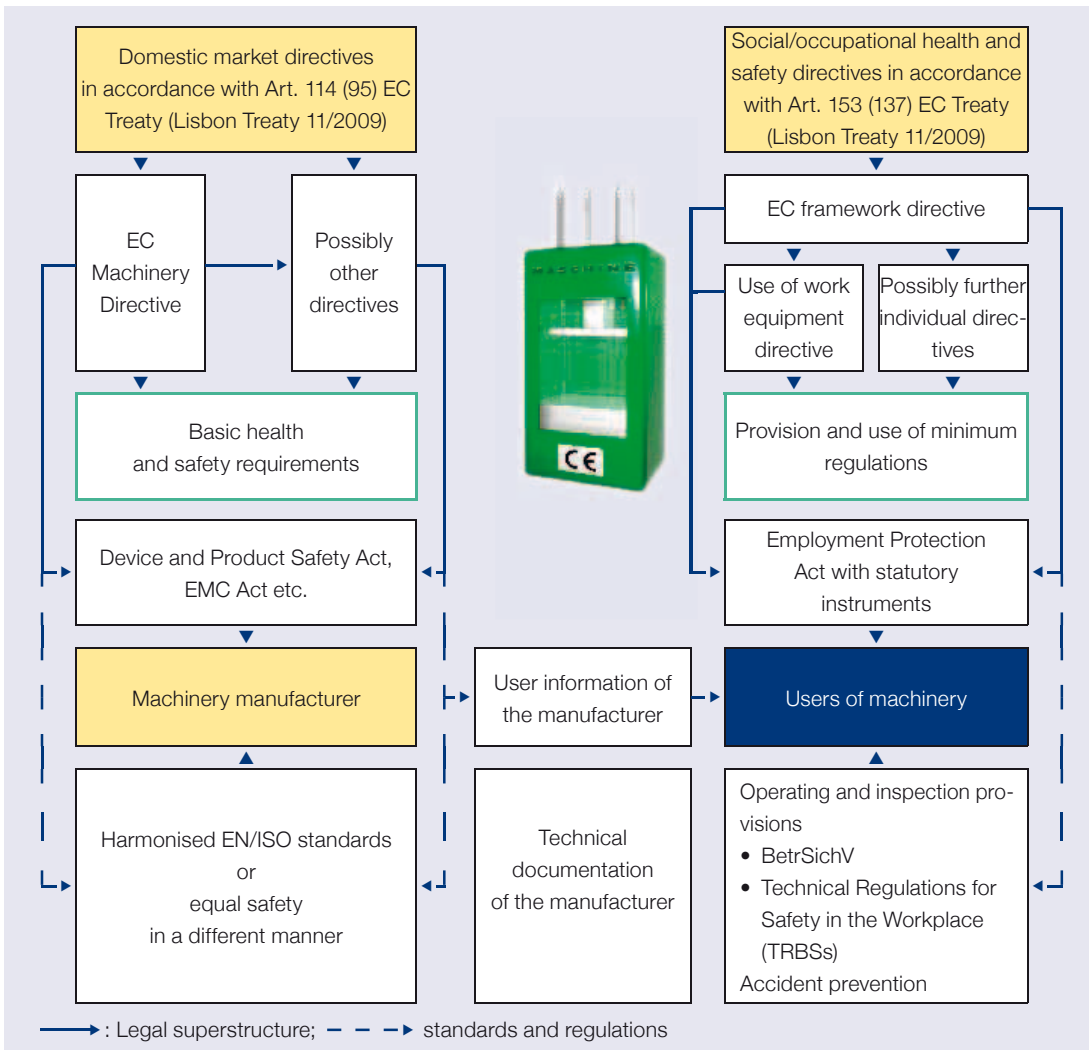


Fig. 1 European and national legal bases for safe machinery [2]

**Feature: New Approach and harmonised standards and regulations**

Something that both types of directives now have in common is that they stipulate their respective protective goals in a relatively abstract way, so that the interpretation and precise specification of the protective goals, in other words the practical and detailed transposition, is left to harmonised European standards (in case of domestic market directives) or national regulations of the Member States (in the case of occupational health and safety directives).

This kind of division of labour between the legislator and standard setter has existed since 1985 and is frequently described as the “New Approach”, and the corresponding directives as “New Approach directives”.

The advantage of taking these standards and regulations into consideration when applying directives is the so-called presumption of conformity. This means that, in a reversal of the burden of proof, authorities must presume that the statutory protective goals have been correctly transposed. However, there is no mandatory application of those harmonised standards and regulations; rather the reversal of the burden of proof then no longer applies, i.e. the person responsible must be able to demonstrate that his individual approach is at least as good as the harmonised standards and regulations. In this case the harmonised standards and regulations therefore serve as a benchmark.

If one looks at developments in industrial accidents in the EU area, one has to acknowledge

that EU directives have without doubt contributed significantly to reducing accidents.

**Background information:**

**European legislation [2]**

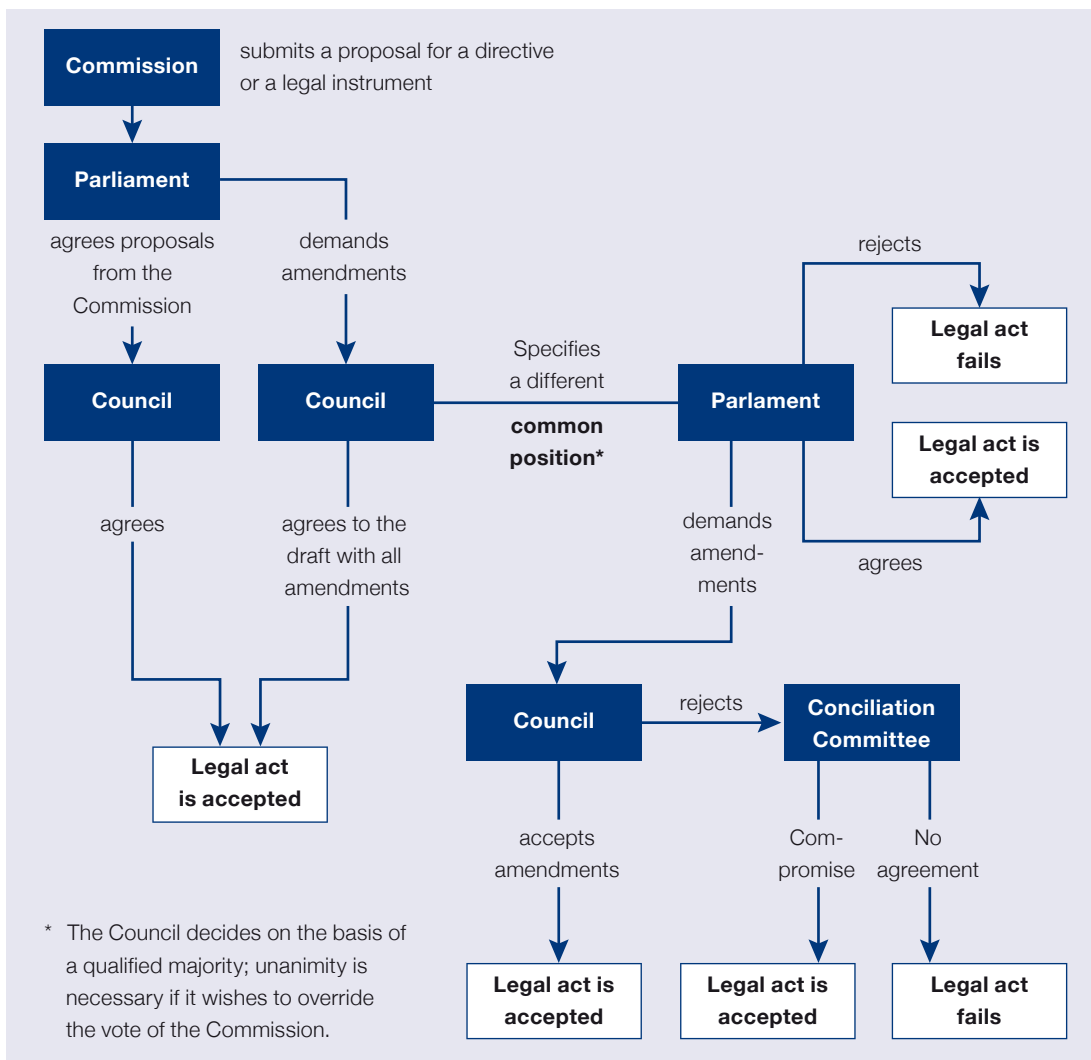
Through its “legislation”, the EU intervenes ever more frequently in the political and economic life of Member States and their citizens. A distinction must be made between four types of European **legal acts** here:

- Regulations (EC) enacted by the EU are generally applicable and are directly binding law in all Member States.
- EU directives stipulate goals that all Member States must comply with; however, it is up to individual states as to how they transpose the directives into their national law.

- Decisions are directed at the government of a Member State, a company or private individuals.
- Finally EU bodies can also submit recommendations or comments without legally binding effect.

There is no uniform procedure for the conclusion of EU legislative acts (regulations and directives). Which procedural path is taken and what say the European Parliament is given will depend on the policy area about which the decision is being taken.

As a result, the European legislation channel is cumbersome and difficult to understand. The Amsterdam and Nice reforms attempted to go some way to rectifying this: they extended the co-



**Fig. 2** European legislation: codecision procedure pursuant to Article 251 of the EC Treaty [3]





References and footnotes:

- [1] The term “Work Equipment Safety Directive” is also used today in place of the term “Use of Work Equipment Directive”. The correct title of Directive 2009/104/EC is actually “Directive on the Minimum Safety and Health Requirements for the Use of Work Equipment by Workers at Work”. The term “Use of Work Equipment Directive” became established for its predecessor 89/655/EEC and subsequent supplements, but is clearly no longer used consistently for the codified 2009/104/EC version. We nevertheless keep to the former shorter term in the following. The above directive is a separate directive within the meaning of 89/391/EEC, the so-called health and safety at work framework directive for the implementation of measures to improve health and safety protection of workers at work. Other separate directives deal with workshops, potentially explosive atmospheres (1999/92/EC), substances etc. In Great Britain this subject is introduced under the abbreviation PUWER (meaning “Provisions on Use of Work Equipment Regulations”).
- [2] **Reudenbach/Hüning:**  
Journal series “Sichere Maschinen in Europa”; Teil 1: Europäische und nationale Grundlagen; July 2009;  
ISBN 978-3-941441-17-0
- [3] Source: Zahlenbilder  
Die Europäische Union – Entwicklung, Ziele, Institutionen im Schaubild. 3rd edition, 2005, 64 pages, 61 ZAHLENBILDER, paperback Erich Schmidt Verlag,  
ISBN: 3503087230
- [4] The explanations are based on the EU Treaty status before Lisbon. May be updated.



# The new EC Machinery Directive 2006/42/EC (MD)

L 157/24

EN

Official Journal of the European Union

9.6.2006

**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)**  
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION

(4) In order to ensure legal certainty for this Directive and the concept of machinery should be defined as precisely as possible.

*The following information is based on lectures at Schmersal/Elan events given by Alois Hüning (Technical Supervisor [TAP] of the Metal and Mechanical Engineering Employer's Liability Insurance Association and head of the specialist "Machinery Safety" department). Previously Mr. Hüning was delegated to the Federal Ministry of Labour to participate on the part of Germany in the composition of the new MD, and was therefore able to add profound professional and material knowledge in his presentation on the subject.*

*The extension of the MD in the meantime to include pesticide application machines (Directive 2009/127/EC) is not included in the following presentation.*

The new MD 2006/42/EC [1] was published in the Official Journal of the European Community on 09.06.2006, i.e. a 24-month implementation period (plus additional 14 days, something whose logic is difficult for outsiders to understand but which is connected to EU "rules") started as from this date. During this period the individual Member States had to transpose the contents of the new Directive into their national law [2, 3]. This was followed by an 18-month informative transition period which meant that one could prepare for the new directive, but could only apply it as from 29.12.2009 [4]. The earlier version of the MD 98/37/EC remained valid until 28.12.2009.

It was clear to every practitioner that the coming into force of the new MD without a transitional

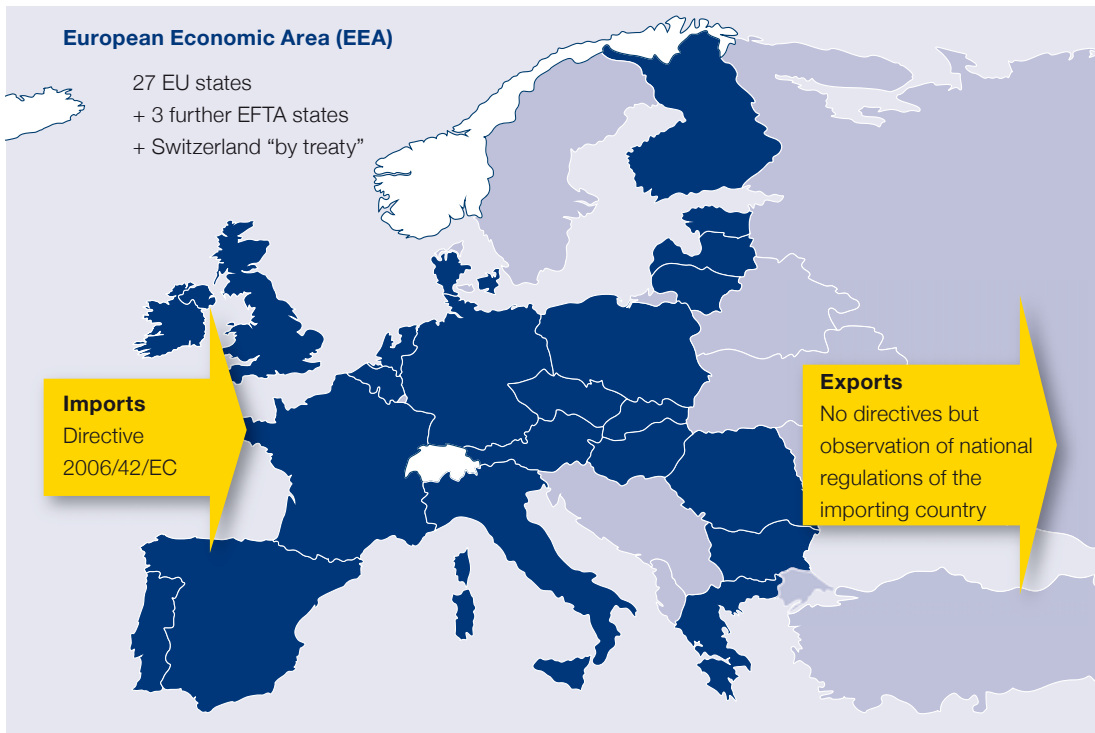
period would be associated with certain difficulties with respect to implementation, however despite this they somehow came to terms with this surprising fixed date arrangement. For example it was interpreted that Annex I could be applied in advance and that it was permitted to issue 2 EC declarations of conformity (1 × based on the "old" and 1 × based on the "new" MD) if in the case of standard products it was not possible to control precisely when they were marketed (before or after 28.12.2009).

## **Background**

The new version of the MD was inspired by the so-called "Molitor Report" under the heading "Lessons learned!"; this report on sensible adjustments to the legal and administrative regulations of the EU was prepared by a group of independent experts. The report from this group of experts is known by those in relevant circles as the "Molitor Report" (named after the chairman of the group of experts, Bernhard Molitor, a former high-ranking employee in the German Federal Ministry of Economic Affairs).

In September 1994 this group was appointed by the European Commission to examine the impact of Community and national legislation on employment and competitiveness with respect to possible relaxation and, above all, simplification. The group was composed of experts from the most diverse areas (including industry, trade unions and public administration).

Those in the group were unanimously of the



**Fig. 1** EU and European Economic Area

opinion that tightening or simplifying the Directive would considerably increase its applicability. This would likewise also lead to a further increase in safety at work.

**Spatial scope**

The new Directive is effective in all Member States of the European Community, i.e. in 27 states (if this includes the accession of Rumania and Bulgaria from 2007) as well as in Switzerland (via bilateral agreements between Switzerland and the EU) as well as in Iceland, Liechtenstein and Norway (the so-called remaining EFTA states). Together the community of these 31 European states is referred to as the EEA (European Economic Area). Recently the spatial scope has been expanded to include Turkey that has similarly introduced the MD into its national legislation.

**Editorial scope**

A comparison between the number of articles and annexes in the old and new MD shows that the scope is nominally greater. In future there will be 29 articles instead of the current 16, while the number of annexes increases from 9 to 12.

It is important to emphasise, however, that the

	From 2004	From 2007
Belgium	Poland	Rumania
Denmark	Czech Republic	Bulgaria
Greece	Hungary	
Spain	Slovenia	
France	Slovakia	
Ireland	Latvia	
Italy	Lithuania	
Luxembourg	Estonia	
Portugal	Malta	
UK	Cyprus	
Finland		
Austria		
Sweden		
Netherlands		
Germany		

**Fig. 2** The 27 EU Member States

majority of these additions are for the purpose of clarification and to create new options. For those who want precise information, Annex XII of the MD contains a so-called correlation table.

## Scope of issues covered

Under the aspect of the legislative system, in future there will only be machinery and partly completed machinery and consistent with this, also only two declarations: firstly the EC Declaration of Conformity in accordance with MD Annex II A and the so-called Declaration of Incorporation in accordance with MD Annex II B.

**Company letterhead**  
(Company name and full address)

**EC Declaration of Conformity in accordance with EC Machinery Directive 2006/42/EC, Annex II A**

**We hereby declare that the *CNC lathe***  
(designation of the machinery)

Model: *MD* Serial No.: *1234*  
Year of construction: *2009*

**complies with the following pertinent provisions:**  
Machinery Directive (2006/42/EG)  
EMC Directive (2004/108/EG)

**Fig. 3** Annex II A of the EC Machinery Directive: Example of a Declaration of Conformity (extract)

**Company letterhead**  
(Company name and full address)

**Declaration of incorporation in accordance with EC Machinery Directive 2006/42/EC, Annex II B**

**We hereby declare that the partly completed machinery**

Model: *Gantry loader MD* Serial No.: *1234*  
Year of construction: *2009*

**– complies with the basic requirements\* of**  
(\* see Annex for which requirements have been satisfied)

**insofar as this is possible from the scope of delivery,**  
Machinery Directive (2006/42/EG)  
EMC Directive (2004/108/EG)

**Fig. 4** Annex II B of the EC Machinery Directive: Example of a Declaration of Incorporation (extract)

An EC Declaration of Conformity for machinery in accordance with Annex II A must in future also be submitted for products that in an everyday sense are not machines but which fall within the scope of the MD, e.g. safety components etc. (see loc cit.). This leads to talk of “legally defined machinery”. By contrast the Declaration of Incorporation for partly completed machinery in accordance with Annex II B replaces the previous manufacturer’s declaration (see loc cit).

You may be surprised to see that the Low Voltage Directive is missing from the directives applied in the two excerpts of declarations provided (as shown in Figures 3 and 4). This directive no longer needs to be listed in future because the protective objectives of electrical safety are contained in MD Annex I. The declaration of conformity for having satisfied MD requirements therefore automatically encompasses this protective objective.

### Abstract definitions of machinery

In principle the abstract definition of machinery remains (see Article 1), however the description of *at least one moving component linked to an assembly of parts* which are joined together for a specific application now applies to the presence of a **drive system** (not human or animal effort).

The choice of the term “drive system” is intended in particular to achieve improved delineation to bagatelle products (the example that the author of this article likes to cite is that of the “mouse trap” machine).

Two further special cases are dealt with within the framework of the abstract definition, namely that machinery is likewise legally machinery

- If the only missing components are those added on site or used to connect it to sources of energy and motion on site or
- It only becomes fully functional if mounted on a means of transport or installed in a building or structure.

### Machinery and interchangeable equipment

The following are also included under the term machinery:

- An assembly of machines (so-called machinery systems) arranged so they function as an integral whole and
- Interchangeable equipment.

### Summary (1)

- Machinery: An assembly fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves and which are joined for a specific application.
- Machinery as referred to above, missing only the components to connect it on site or to sources of energy and motion.
- Machinery as referred to above, able to function as it stands only if mounted on a means of transport or installed in a building or structure.
- An assembly of machines arranged so they function as an integral whole (loc cit).
- Interchangeable equipment
- ...

**Fig. 5** Definition of “Machinery” in accordance with MD Article 2 (1)

See page 55 for further information on the subject of “machine assemblies”.

### In future, treated in the same way as “machinery”: products that were previously classified as a “special position”

Also to be recognised as “machinery” within the new MD in future in the uniform EC Declaration of Conformity in accordance with Annex II A are products that today are dealt with separately or only marginally (i.e. are not explicitly mentioned in Article 1). The MD provisions will in future also apply to these products without restriction and with all formal and substantial duties as they do to complete machinery.

Affected by this are (see loc cit.) firstly safety components, and secondly other specifically named mechanical engineering products (products that extend beyond the abstract MD definition or which deviate from it). These concern the following:

- Lifting equipment whose source of motion is the direct deployment of human effort and
- Lifting accessories including slings, chains, ropes and webbing separately placed on the market for this purpose.

This can be considered as clarification because these products were also included in the earlier MD. Clearly, however, misunderstandings and cases of ignorance occur repeatedly in this connection.

In spite of this, it has now been (finally) clarified that the “full MD programme” also applies to these products, e.g. an EC Declaration of Conformity must be issued in accordance with MD Annex II A and the associated conditions (protection targets in accordance with MD Annex I, Technical Documentation etc.) must be complied with.

### Summary (2)

- Lifting equipment whose source of motion is direct human effort
- Safety components that guarantee the safety function and which are placed on the market separately.
- Lifting accessories
- “Chains, ropes, belts” for lifting purposes as part of lifting machinery and lifting accessories which are placed on the market separately.
- ...

**Fig. 6** Definition of “Machinery” in accordance with MD Article 2 (2)

### Other changes in scope

This refers to the following:

- a) Complete reconfiguration of the subject of “partly completed machinery”
- b) The extension of the MD to building site and/or goods lifts
- c) A more specific delineation to the Low Voltage Directive
- d) Clarifications and extensions with respect to the list of exclusions.

With respect to a): Specific regulations on the subject of “partly completed machinery” eliminate a frequently complained of weakness in the former MD where this issue had practically been ignored. For detailed information on this see loc cit.

With respect to b): Due to the fact that an

amendment was made to the application area in Article 24 of the Lift Directive 95/16/EC, in future construction site lifts fall within the application scope of the Machinery Directive. Until now construction site lifts had been left out of both the Machinery Directive and the Lift Directive and were therefore subject exclusively to national legislation.



They have now been completely integrated into the new Machinery Directive and must comply with all requirements applicable to machinery. The result of this is that all machines on the construction site that satisfy the same purpose as construction site lifts, e.g. material hoists, now fall within the application scope of the Machinery Directive.

New to the MD application area in this context in future will then also be stair lifts and similar (to transport people and goods) if they are moved at a maximum speed of 1.6 m/min.

With respect to c): Excluded from the application area in future are the following named electrical and electronic products insofar as they fall within the Low Voltage Directive:

- Household appliances;
- Audio and video equipment;
- Information technology equipment;
- Ordinary office machinery;
- Low voltage switchgear and control gear;
- Electric motors.

With respect to d): Essentially the familiar exclusions remain (as shown in Figure 7). However there are some products that are given new (more precise) wording in the list of exclusions or products to which special regulations apply. Since these are “special interest products”, anybody interested can refer to specialist literature.

By contrast, “machinery for research purposes” has been newly incorporated in the list of exclusions. It is important to emphasise in this connection that with regard to this type of machinery firstly the criterion of temporary use applies, and that secondly despite this, basic safety-related requirements as derived from other statutory provisions apply as far as possible. As such the actual advantage of excluding machinery for research purposes lies rather in the fact that the formal MD obligations do not apply.

#### Exceptions to the application area

- Safety components as spare parts when supplied by the original manufacturer
- Machinery for nuclear use
- Firearms apart from captive-bolt pistols
- Tractors and other vehicles used in agriculture or forestry that fall within 2003/37/EC
- Offshore plants and seagoing vessels
- Hoisting plants
- Stage lifts as passenger lifts
- Machinery for research purposes and temporary use in the laboratory
- Switching and control devices, transformers for high voltage
- Special devices for markets and amusement parks
- ...

**Fig. 7** Areas excepted in accordance with MD Article 1 (examples)

#### Summary and interfaces of the MD approach

Compared to the 98/37/EC version of the MD and the interpretation of it, the amendments introduced do not actually signify anything that is fundamentally new.

There are, however, a few new interface definitions:



- The first is the place where the machinery is erected, i.e. in future the person responsible for the MD must give thought to which interfaces must be taken into consideration for example in relation to structural prerequisites etc. to ensure safe use of a machine or safe machine operation.
- Also to be taken into consideration as an additional interface definition is the fact that a product that falls within the scope of the MD always remains an MD product even if subsequent use should fall within a different directive (*once Machinery Directive, always Machinery Directive!*). This applies for example to automatic revolving doors which in future will remain subject to the more stringent requirements of the MD and no longer get “submerged” in the Construction Products Directive.

### Party completed machinery

The former and unsatisfactory process of the manufacturer’s declaration in accordance with MD Article 4 (2) will be replaced by the new regulations (*relating to machinery into which the partly completed machinery is to be installed which can then only be commissioned when it corresponds to requirements of the Machinery Directive*). The terms part machine, machinery not ready for use (not operational) or partly completed machinery – the term that has now been adopted in the new MD – have become established for machinery that is not complete.

They concern mechanical engineering products for which the three of four features (depending on the counting method used) that define machinery (see loc cit) do not apply completely but rather only in part. A drive system or a gantry loader designated for installation, and even a robot whose fencing is missing and therefore cannot be operated safely, are partly completed machinery in this sense.

Firstly the definition for partly completed machinery has been substantially improved in that the new MD sticks closely to the definition of “completed machinery”.

According to the definition, partly completed machinery, unlike completed machinery, has not been assembled to the extent that it can carry out a specific function including its safe handling and safe operation. In these cases it is up to



© 2008 REIS ROBOTICS  
Reis GmbH & Co. KG Maschinenfabrik

**Fig. 8** Examples of partly completed machinery

the next value creation stage to manufacture a complete and safe machine that complies with all MD requirements. Conscious downgrading of machinery to partly completed machinery to save on protective devices and safety technology is a legal violation, however (see also the MD 2006/42/EC Guide in this connection).

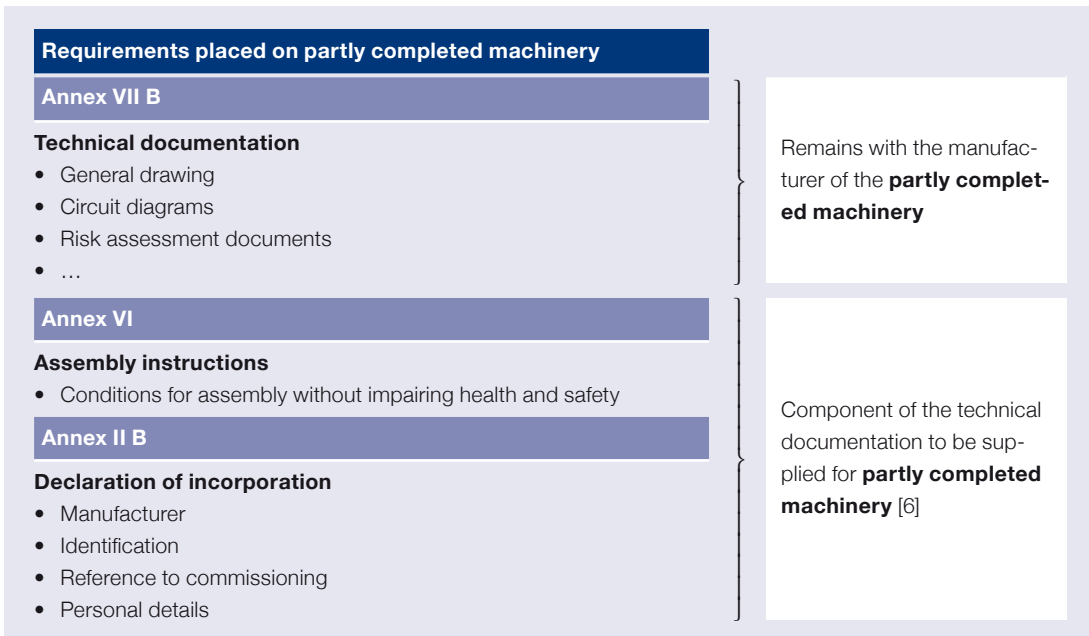
If until now it has formally the case that the manufacturer of partly completed machinery or the authorised representative [5] was absolved from all further MD obligations (apart from the completion of the so-called manufacturer’s declaration with putting into service reservation which is to be discontinued in future), he will now have to deal with concrete obligations. While submitting the manufacturer’s declaration in the past also did not mean that the manufacturer concerned moved in a legal vacuum, it was all rather “nebulous”.

It is an inevitable consequence of the new MD regulation that in some cases the new regulation may involve considerably more work.

Various separate regulations stipulate that partly completed machinery must also be as “safe” as possible and that the manufacturer is subject to corresponding documentation and declaration duties to this extent. In future no more voluntary or individual contractual regulations will be required.

In future the manufacturer of partly completed machinery must prepare:

1. a technical documentation;
2. submit assembly instructions for the partly completed machinery [6]; and



**Fig. 9** Procedure for partly completed machinery in accordance with MD Article 13

3. submit a so-called Declaration of Incorporation [6].



Partly completed machinery receives no CE label under Article 16 of the MD!

**With respect to 1):**

The scope and content of the technical documents to be prepared are defined in MD Annex VII B. The above figure shows the scope of these documents (= Section B), also compared to the technical documents for machinery (= Section A).

An assembly which is almost machinery but which cannot itself satisfy any specific function. A drive system represents partly completed machinery. Partly completed machinery is only intended to be installed in other machinery or in other partly completed machinery or equipment or to be joined to it in order to form machinery within the meaning of this Directive.

**Fig. 10** Legal definition of “partly completed machinery”

Partly completed machinery subject to the Machinery Directive is a product intended to form machinery that is in the scope of the Machinery Directive after incorporation.

“An assembly which is almost machinery” means that partly completed machinery is a product that is similar to machinery in the strict sense referred in Article 1 (1) (a), that is to say, an assembly consisting of linked parts or components at least one of which moves, but which lacks some elements necessary to perform its specific application. Partly completed machinery must thus undergo further construction in order to become final machinery that can perform its specific application.

...

Machinery that can in itself perform its specific application but which only lacks the necessary protective means or safety components is not to be considered as partly completed machinery.

Since partly completed machinery is “almost machinery”, it is to be distinguished from machinery components that are not subject to the Machinery Directive as such. Machinery components can usually be integrated into a wide range of categories of machinery with different applications.

**Fig. 11** Extract of comment in the 2006/42/EC MD Guide (Article 46)

## MD Annex VII (Technical documents)

### A. Technical documents for machinery

### B. Specific technical documents for partly completed machinery

- Manufacturer:**
- Assess
  - Guarantee
  - Documents available

#### The technical documents include:

##### Part A

##### Part B

- A complete plan of the (partly completed) machinery and control system plans
- A list
  - of the basic requirements of this Directive
  - of standards and
  - of other technical specifications that have been taken into consideration when designing the machinery

##### • Risk assessment

- Operating manual
- Copy of the EC declaration of conformity
- Declaration of incorporation and assembly instructions
- ...

- Assembly instructions
- Series production: setting out the internal measures for warranties
- ...

#### Documents to be kept for at least 10 years after manufacture

**Fig. 12** Manufacturer obligation: preparation of specific technical documents for partly completed machinery in accordance with MD Annex VII Part B. Compared to the requirements for complete machinery in accordance with Part A of Annex VII, it can be seen that the future requirements placed on manufacturers of partly completed machinery only differ gradually. See in particular the item on “Risk assessment”.

The rule for the technical documents according to MD Annex VII B is also that they – in the same way as the documents for completed machinery – need not be supplied automatically. Rather, here too, individual contractual regulation is needed between the manufacturer and his customer if this is required.

The scope of the documentation to be prepared (risk assessment, consideration of the protection objectives in accordance with Annex I etc.) makes it clear that comparable obligations apply to a manufacturer of partly completed machinery as to a complete manufacturer.

Which safety-related requirements a manufac-

turer can comply with in their entirety or which requirements he can only partly comply with or cannot comply with at all because they are in the nature of the situation, will certainly initially lead to grey areas and interface problems. In conjunction with this it should also be considered that, with a few exceptions, there is an absence of interpreting harmonised EU standards in this area.

#### **With respect to 2):**

While the assembly instructions for partly completed machinery are somewhat different to the operating manual for a machine as they are essentially limited to the “assembly” life cycle phase, there are also a few other problems. If



**Addition/excuse:**

If a manufacturer manufactures partly completed machinery in series, the requirement for a QA system within the meaning of Annex VIII applies.

No detailed discussion of the general requirement for a QA system in accordance with MD Annex VIII will be entered into here (as shown in Figure 15) because today it is natural for a company that wishes to survive on the market to use such a system. ISO 9001 is not necessarily meant. However it makes sense for QA processes in an enterprise to be in accordance with it and to be specified in writing.

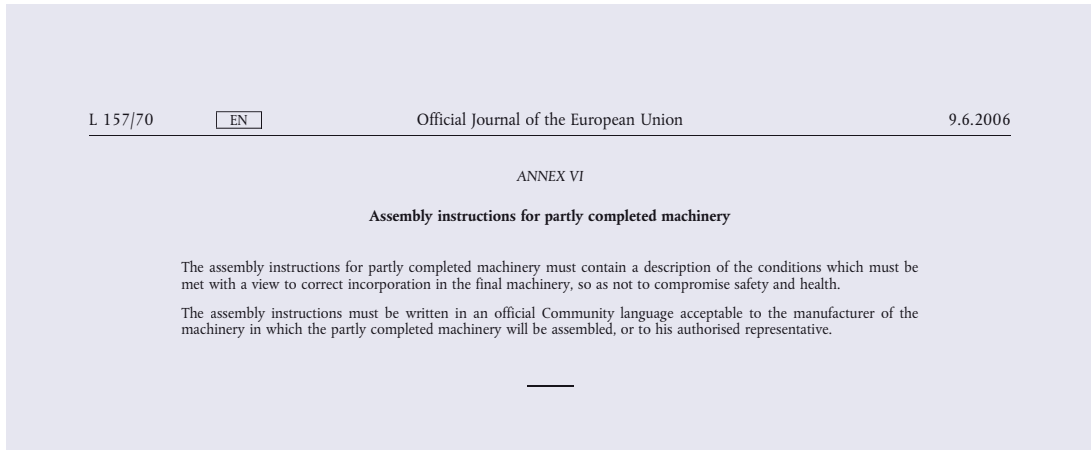
**Safety components**

In principle the definition for safety components remains the same but in a form adapted

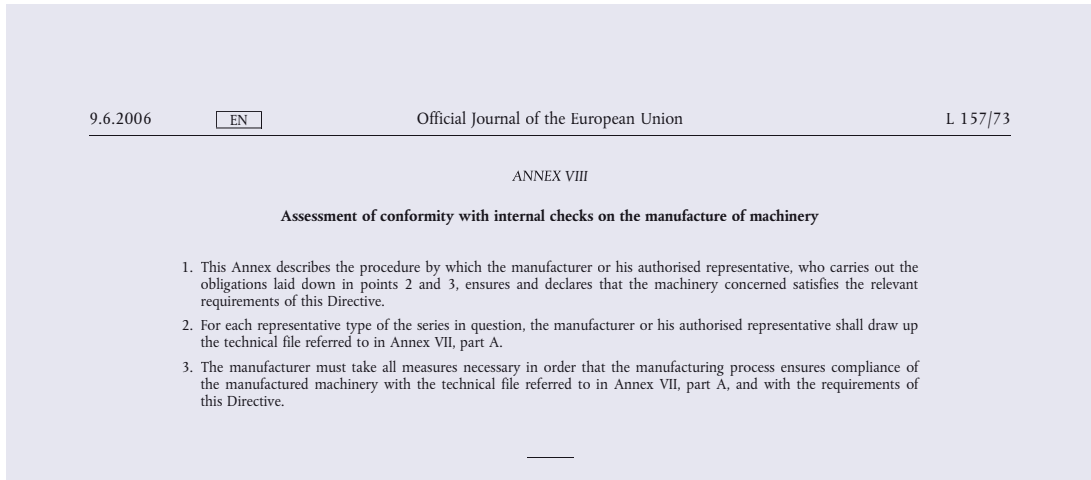
to technological development that also includes “hybrid” products. In addition to the other MD obligations which also had to be taken into consideration in the past, there will in future be an obligation with respect to safety components – because these are legally equivalent to a machine in the new MD – to provide an operating manual in the language(s) of the country using them.

Furthermore so-called logic units to guarantee safety functions (that is controllers with safety functions, see loc cit) in future fundamentally “migrate” to Annex IV.

With regard to safety components, there is also an informative Annex V with an exemplary list of safety components. While no explicit new obli-



**Fig. 14** Annex VI: Assembly instructions for partly completed machinery



**Fig. 15** Annex VIII: Assessment of conformity with internal checks on the manufacture of machinery and where applicable partly completed machinery



**Fig. 16** Examples of safety components from the Schmersal product range

gations result from this (from Annex V, which can continue to change in future), what is counted as a safety component may still come as a surprise to some manufacturers. For example the following will in future fall within the term of a safety component:

- Discharge systems for potentially dangerous electrostatic charge; or
- Systems and equipment to reduce vibration or noise emissions.

### Responsibilities

In terms of content, nothing has actually changed. There continues to be a distinction between a manufacturer based in the EU (EEA) and, for example, an authorised representative who is based (established) in the EU (EEA) working for a third country machinery manufacturer who may be responsible for observing the MD obligations. In addition a declaration of conformity or incorporation can also be issued directly by the manufacturer if he is not based in the EU or in the EEA [5].

As previously the rule in case of doubt where it is not possible to identify the person legally responsible is that the company placing the machinery on the market or which has put it into service is considered to be manufacturer.

There are also the familiar special cases, so according to the MD the person responsible in future is also the person who

- manufacturers machinery for own use;
- makes substantial changes to machinery;
- assembles machinery to machinery systems;

### The following are responsible for conformity to the directive:

- Manufacturer in the direct sense (authorised representative)
- Somebody putting together machinery or parts of machinery
- Somebody manufacturing machinery for own use
- Somebody importing machinery from non-EEA States
- Somebody who operates machinery (becomes the manufacturer) if he himself:
  - converts machinery (**substantial** alteration)
  - compiles systems
  - completes machinery
- Somebody who **substantially** alters machinery through additions or rebuilding
- Somebody who **substantially** alters used machinery and then passes it on to others

**Fig. 17** Unaltered responsibilities

- places used machinery from third party states on the market.

The continued incorporation of these special cases in the MD field of application is therefore guaranteed also to produce surprises in the future.

See page 53 and 57 for more information on the subject of “significant changes” and used machinery.

Two new MD requirements are integrated in connection with the question of responsibility even if this does not precisely suit the systematic description set out:

### “CE-attendant”

With respect to declarations in future (in the EC declaration of conformity for machinery and in the declaration of incorporation for partly completed machinery) one person resident in the Community must also be named who is authorised to compile the technical documents according to Annex VII.

## ANNEX II

## Declarations

## 1. CONTENT

## A. EC DECLARATION OF CONFORMITY OF THE MACHINERY

This declaration and translations thereof must be drawn up under the same conditions as the instructions (see Annex I, section 1.7.4.1(a) and (b)), and must be typewritten or else handwritten in capital letters.

This declaration relates exclusively to the machinery in the state in which it was placed on the market, and excludes components which are added and/or operations carried out subsequently by the final user.

The EC declaration of conformity must contain the following particulars:

1. business name and full address of the manufacturer and, where appropriate, his authorised representative;
2. name and address of the person authorised to compile the technical file, who must be established in the Community;

3. description and identification of the machinery, including generic denomination, function, model number and commercial name;

4. statement that the machinery fulfils all the relevant provisions of the Directive.

## B. DECLARATION OF INCORPORATION OF PARTLY COMPLETED MACHINERY

This declaration and translations thereof must be drawn up under the same conditions as the instructions (see Annex I, section 1.7.4.1(a) and (b)), and must be typewritten or else handwritten in capital letters.

The declaration of incorporation must contain the following particulars:

1. business name and full address of the manufacturer of the partly completed machinery and, where appropriate, his authorised representative;
2. name and address of the person authorised to compile the relevant technical documentation, who must be established in the Community;

3. description and identification of the partly completed machinery including generic denomination, model number and commercial name;

4. statement that the partly completed machinery fulfils all the relevant provisions of the Directive.

Fig. 18 Greater market surveillance

We have termed this the “CE-attendant”, others refer to the person as the documentation officer or similar. Ultimately it is up to individual companies how they deal with this requirement in organisational and competency terms. What is important is satisfying the legal implication and nominating a qualified contact (see loc cit).

See page 51 for further information on the subject of “CE-attendant”.

There are also no changes in the overall responsibility of the person signing declarations who can additionally double up as the “CE-attendant”, but it is emphasised also with reference to greater market surveillance in the future (see loc cit) that the new MD places greater weight on the subject of “responsible perception of obligations”.

### Greater market surveillance

This uncomfortable subject (due to little implementation and impact) is taken up by the new MD. Compared to the current MD it expands the area of market surveillance and regulates tasks more precisely in Article 4, especially obliging Member States to create more effective structures.

It is therefore possible to hope that future “black sheep” will have less opportunity to distort com-

petition and endanger life and limb with deficient designs.

### Duty to provide effective market surveillance

- Setting up and naming competent bodies
- Checking machinery and partly completed machinery
- Information to the Commission and Member States regarding organisation and authorisations



Fig. 19 Unchanged responsibilities for market

### Demarcation to other (domestic market) directives

There is a change and a clarification in conjunction with this:

- The change results from the fact that the protective objectives of the Low Voltage Directive have been expressly incorporated in Annex I of the new MD (see Section 1.5.1), so that the listing of Directive 2006/95/EC in both product conformity declarations will in future not be applicable (can be dispensed with).
- The clarification, termed the “MD specific hazard (sub)exclusion” also helps with the interpretation of alternative or cumulative use of



### Examples of directives that deal with hazards in a more specific manner:

- Directive 94/9/EC (ATEX Directive)
- Directive 2000/14/EC (Outdoor Directive)
- Directive 2004/18/EC (EMC Directive)

### Examples of such directives are as follows:

By contrast other directives regulate product groups more precisely. It may also be possible here that a hazard is not even present for a product or that the risk is so low that a lower protective level is appropriate for this hazard. Article 3 would also apply in such a case. The hazard would be recorded “more precisely”.

- Directive 93/42/EEC (Medical Devices Directive)
- Directive 88/378/EEG (Toy Directive)
- Directive 95/16/EC (Lift Directive)
- Directive 2000/9/EC (Cableways for the carriage of passengers)
- Directive 97/23/EC (Pressure Equipment Directive)

**Fig. 20** Demarcation to other (internal market) directives

other EC directives (completely or partially) if these record hazards more specifically or “precisely”. The MD then does not apply (no longer applies) to this degree).

The manufacturer must therefore establish which directives apply to his machines. For this reason he must check whether the machinery:

1. Falls within the Machinery Directive;
2. Is subject to a different directive according to Article 4, e.g. Building Products, Medicinal Devices, Toys or Lifts;
3. Is also affected by another directive that is applicable at the same time for individual hazards or assemblies e.g. pressure equipment, electromagnetic compatibility or sound emissions.

#### Conformity assessment procedure

- Where products do not fall within MD Annex IV (list of so-called especially hazardous machinery), there are virtually no changes to the conformity assessment procedure (for products not included in Annex IV).

This means that nothing has changed with respect to manufacturers taking self-responsibility for placing MD products on the market.

It is true that these products are also now formally obliged to undergo internal production checks by the manufacturer in accordance with MD Annex VIII. However the very general requirements set out here do not amount to

anything that a qualified manufacturer does not already do.

- An exception to the previous manufacturer's responsibility when placing safety components on the market merely concerns the so-called logic units for safety functions that in future also fall within MD Annex IV.

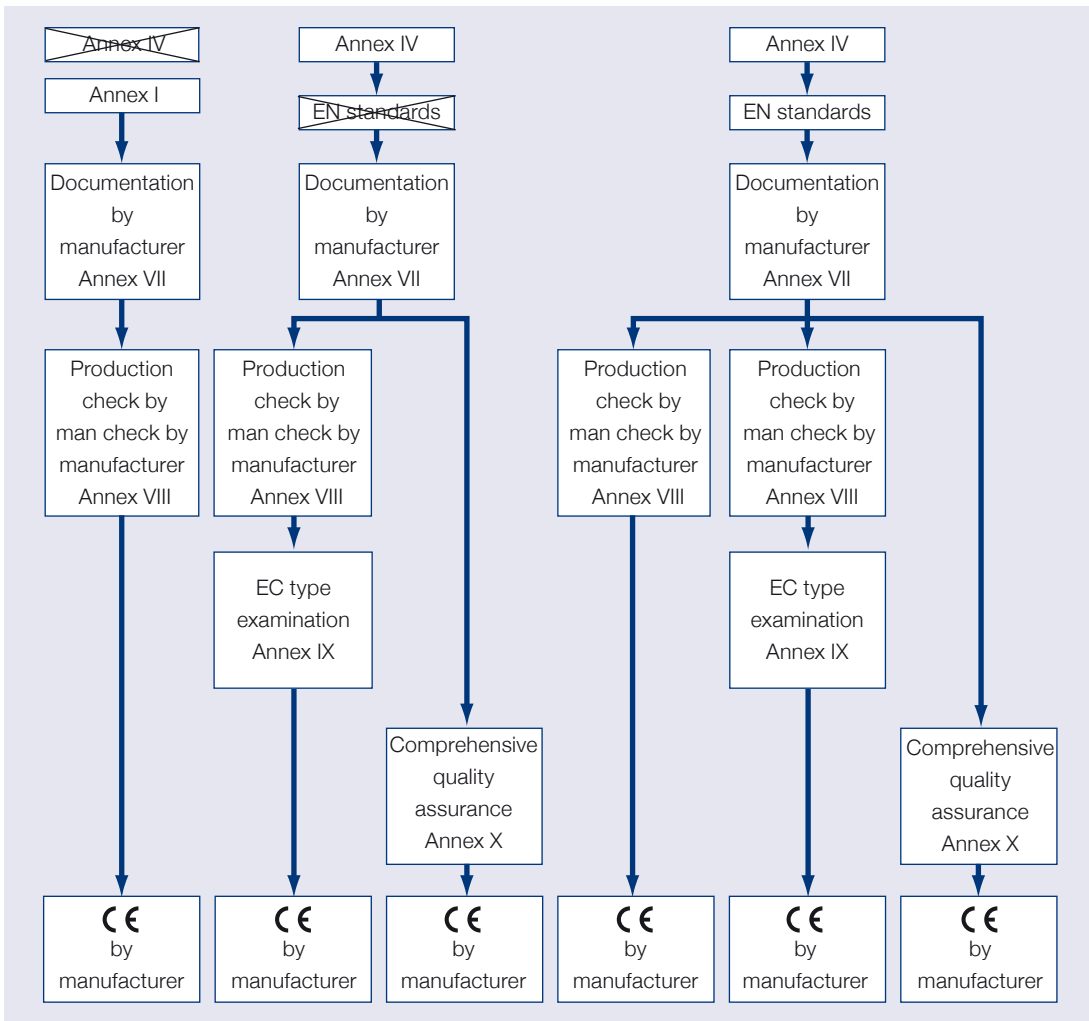
By contrast, the list of machinery in Annex IV remains unchanged apart from some changes in wording.

- If the objective of the German (and other) negotiating delegations was to completely get rid of MD Annex IV (because of the dubiousness of the claims that these concern particularly hazardous machinery), then it has not been possible to achieve this objective.

On the other hand the previously obligatory requirement to engage a notified body and the obligation to conduct an EC type examination for the Annex IV products concerned may be handled considerably more flexibly in future.

#### NEW Annex IV procedure

- Depending on whether or not there is a harmonised EN standard under the umbrella of the MD for the product concerned (there are now 35 of the 37 EN standards required) there will in future be up to two other conformity assessment procedures to choose from as an alternative to the EC type examination:



**Fig. 21** Conformity assessment procedure in accordance with MD Article 12

- Option 1: Internal production check by the manufacturer in accordance with MD Annex VIII, e.g. with the manufacturer taking direct responsibility (see loc cit) or
- Option 2: Comprehensive quality assurance by the manufacturer in accordance with MD Annex X (see loc cit) or
- Option 3 (as previously): EC type examination in accordance with MD Annex IX.

In exceptional cases where no harmonised EN standard exists for the product concerned, Option 1 is removed from the choices available, i.e. options are then limited to options 2 and 3.

In return the possibilities in future for documentation (specifications) to be deposited at or

checked by a notified body will no longer apply to Annex IV products.

Even if selection between all three options is treated equally for Annex IV products where harmonised standards are available for them, in practice this is influenced by the acceptance question, particularly with reference to Option 1 (the manufacturer's self-responsibility). It will be necessary to wait and see how the market reacts here, especially in countries with particularly defined Annex IV affinity as is the case in some European and Asian countries.

#### **Comprehensive quality assurance in accordance with Annex X**

This new option for Annex IV products should represent a considerable simplification especially for manufacturers of unique products, special

machinery and bespoke designs for customers and also be of particular economic significance when it comes to the “time to market” issues.

The QA system addressed in Annex X originates from Council Decision 93/465/EEC and corresponds to the so-called H Module (not “H +” or “H a”, which also provides for design examination).

Annex X essentially describes a QA system as also used in the ISO 9000 et seq. series of standards, however there are two principal differences.

The first difference concerns greater incorporation of the product design and specification in QA-related processes. Therefore it not only deals with the production quality, but also the safety-related quality of the design.

The second difference is examination of the QA system by a so-called Notified Body).

See page 45 for further information on the subject of “NEW Annex IV procedures”.

### Internal production checks in accordance with Annex VIII

By contrast the procedure for internal production checks set out in Annex VIII merely concerns the manufacturer’s general obligation to be responsible for taking all requisite measures to ensure that products comply with technical documents and satisfy the requirements of the MD.

### ANNEX I: ESSENTIAL HEALTH AND SAFETY REQUIREMENTS RELATING TO THE DESIGN AND CONSTRUCTION OF MACHINERY

This most significant safety-related MD section remains largely unchanged apart from different numbering, from changes in wording signifying adjustment to EN ISO 12100 [7], and from changes of details.

The unchanged continuation of Annex I can be considered as a result of a “political” determination (not to go deeply into the substance of this annex).

In spite Annex I contains a few interesting changes and new slants in detail. An extract with ex-

ceptions to the generally unchanged MD can be found in Figure 22.

#### Basic requirements

- Annex I corresponds to the old Annex I in terms of numbering and content
- The new Annex I has, however, been adapted to the terminology in DIN EN ISO 12100
- Risk analysis becomes risk assessment
- 1.1.6: Ergonomics is now regulated in greater detail
- 1.2.1 and 1.2.7 have been combined in 1.2.1: “Safety and reliability of control systems”
- 1.2.5: Selection of the control or operating modes has been extended (process observation)
- 1.4: Requirements placed on protective devices have been adapted to the reality today with respect to terms and content (Types A and B no longer apply)
- 1.7 – Information: new in parts (operating manual, labelling of machinery etc.)
- 1.8 – ...

Fig. 22 Annex of the EC Machinery Directive (amendments)

#### In detail:

- First the subject of “risk assessment” (a term taken from EN ISO 12100-1/-2 and EN ISO 14121-1) assumes much greater weight in the new MD. While the 98/37/EC version has until now only used the term “risk analysis” (and this only in one sentence), the requirements now are set out much more comprehensibly and specifically. One could refer to it as the key issue in machinery safety.

See page 111 for further information on the subject of “risk assessment”.

- In addition the principles of safety integration (Section 1.1.2) introduce the concept of reasonably foreseeable misuse, i.e. machinery must be designed and constructed so that no

person is subjected to danger from this point of view.

Even if it is not possible to analyse here whether consideration of reasonably foreseeable misuse constitutes a “tougher” requirement than the current MD requirement [8], it is recommended that the person responsible for the MD examines internal communication and reporting paths, also with respect to the development of case law. In practice this means close or even closer feedback from sales staff, service technicians and other colleagues “on the front” should be ensured. Using their information it is possible to accommodate the requirement of taking reasonably foreseeable misuse into consideration, whether using technical measures or using warning safety technology (keyword: operating manual).

- Another element of the new MD may flow into this consideration which is the strength of advertising statements made in sales literature, on the internet etc. and during sales meetings (see Section 1.7.4.3. in this respect). As obvious as it may sound, one should only ever make promises that can actually be kept.

### Details of ergonomic requirements

A further change in Annex 1 (Section 1.1.6) concerns greater details on ergonomic principles for machinery (see also Figure 23).

With respect to this it can be expected that this new weighting afforded to the area of “ergonomics” will also be reflected in additional requirements for future C standards.

### NEW": legalisation of the “process observation” operating mode

If any significant change can be highlighted in the new MD and its Annex I, then this concerns Section 1.2.5 (Operation of machinery without effective protective devices). The adding of a specific passage does not, however, amount to legalisation of the disputed “process observation” operating mode.

Until now it has required a special legal mnemonic (a position shared in particular by the German employer’s liability insurance associations) to implement this operating mode which is of special significance to special NC and CNC-

### The ergonomic principles have been set out in greater detail:

- Adaptation to different body size, physical strength and stamina of the operator
- Sufficient freedom of movement for the operator
- Prevention of a working rhythm dictated by the machinery
- Prevention of observation activities requiring continuous attentiveness
- The adaptation of the man/machinery interface to the anticipated characteristics of the operating staff

Fig. 23 Annex I of the EC Machinery Directive (ergonomics)

controlled applications and for integrated production systems.

It still applies that machinery operation without effective protective devices is linked to four cumulative requirements (as shown in Figure 24).

In future deviation from this will be possible, i.e. not all four conditions must be satisfied simultaneously if this requirement

- Is not operationally applicable and
- There is an essential technological need to deviate from it.

As shown in Figure 25.

To put it plainly this means that, where necessary, machinery can also operate at higher speeds (i.e. “necessary for the process”) in line with other safety-related measures where protective devices for automatic operating mode have been lifted.

CAUTION: The “process observation” mode will still continue to be an exceptional operating mode in the future, and strict requirements will apply to it (examination of necessity on a case by case basis, technical measures with PL “d” CC 3 quality in accordance with EN ISO 13849-1:2008 (2006), appropriately qualified and trained operating personnel etc.). It can be

## Operating modes (process observation)

The following **four prerequisites specified in the Directive** must be complied with in order to be allowed to operate machinery when there are no effective protective devices:

- Other control or operating modes are not possible (example: automatic control system is blocked)
- Hazardous movements can only be operated when controls are actuated (example: enabling devices with automatic resetting)
- Dangerous functions can only be operated under more stringent safety conditions and hazards resulting from command chains are shut down (example: reduced speeds or outputs)
- Sensors that can trigger dangerous functions through intended or unintended impact are blocked (example: starting up of chip conveyors)

**Fig. 24** Annex I of the EC Machinery Directive (Section 1.2.5)

regarded as a compromise for the special operation of machinery if it could be expected that protective devices would otherwise be manipulated in order for the operator to be able to carry out necessary work.

### Other changes in Annex I

Other changes in Annex I: MD Annex I also contains a range of further smaller amendments affecting individual safety aspects that are not of general significance (with the exception of the following section on “operating manual”).



## Operating modes (process observation)

However if these cannot be applied for operational reasons and if there is an **urgent technical need**, the procedure in future can be as follows:

- If these four prerequisites are not satisfied simultaneously then the control or operating mode selector switch must trigger other protective measures that are designed and created such that a safe working area is guaranteed.

**Fig. 25** Annex I of the EC Machinery Directive (NEW Section 1.2.5)

Where they are included in the general section of Annex I, amendments of this nature are set out in note form in the box on page 38.

### Instructions (operating manual)

There are two main new points of general and partial significance under this heading (MD Annex I, Section 1.7.4).

- In general the rule in future is that two sets of the operating manual must be provided. The first are the so-called original instructions and the second are a translated version in the language(s) of the country in which the machinery is used which must bear the title “translation of the original instructions”.

Against the background that there are now 23 official EU languages, the point of the above distinction is to differentiate the manufacturer's legal responsibility for the operating manual.

While this applies without restriction to the original instructions, responsibility for the translation is limited, i.e. the manufacturer need not be held responsible for translation mistakes as long as sufficient care has been taken in the translation e.g. in selection of the translator.

**CAUTION:** This interpretation is not undisputed!

The MD does not stipulate whether instructions can also be supplied in the form of electronic data carriers. However according to the current EU interpretation this is possible and, with a correspondingly updated interpretation expected, this will remain so. What is not ex-

## Instruction manual

Due to the changed terminology for “**Machinery**”, considerably more products will in future also require an operating manual.

In detail this affects the following:

- Safety components
- Lifting accessories
- Chains, ropes and webbing
- Removable drive shafts

In addition the requirements on the content of the operating manual have been made more precise and expanded to include the following information:

- EC declaration of conformity or document with comparable content;
- Warning signs where misuse has been shown to occur;
- Details on residual risks that remain;
- Instructions for the protective measures to be taken by the operating company, including the personal protective equipment to be provided;
- Stability requirements for the machinery in all phases of life;
- Information on sound emissions from the machinery.

**Fig. 26** Annex I of the Machinery Directive

pected, by contrast, is that a download possibility from the internet will be regarded as equivalent.

- Something that is only of significance to certain manufacturers, however, is that an operating manual must now also be provided for these mechanical engineering products due to the extension of the concept of “machinery” in MD Article 1 (as shown in Figure 26).





## List of more minor changes [10]

### 1.1.5 Design of the machinery with respect to use

There is a new requirement to preclude involuntary changes to position and hazards caused by a lack of stability if the machinery is used in accordance with the operating manual.

### 1.1.7 Work positions

A general requirement applying to all machinery has now emerged from the requirement formerly only specified in Section 3 (... specific hazards due to the mobility of machinery – 3.2.1 Driving position).

### 1.1.8 Seating

Here too a general requirement applying to all machinery has now emerged from the requirement formerly only specified in Section 3 (... specific hazards due to the mobility of machinery – 3.2.2 Seating).

### 1.2.1 Safety and reliability of control systems

There is a new requirement for wireless control systems (radio control systems) to automatically shut down when the correct signals are not received.

### 1.2.4.2 Operational stop

Directive 98/37/EC stipulated that the power supply to the actuators must always be interrupted after a stop condition.

If, for operational reasons, a stop condition is necessary while maintaining the power supply to the actuators, then this state must be monitored. Unlike the *Normal stop* (see 1.2.4.3), the power supply to the actuators is not interrupted during an operational stop.

In this case, however, additional measures to prevent the machinery starting up unexpectedly are required, e.g. standstill monitoring.

### 1.2.6 Failure of the power supply

A new addition is that the parameters of the machinery may not be allowed to change in an uncontrolled manner during interruptions to the power supply if such an uncontrolled change could lead to dangerous situations.

### 1.3.8.1 Moving transition parts

### 1.3.8.2 Moving parts involved in the process

Some of the changes to both sections also results from the amendment to Section 1.4.2.2 in Annex I (q.v.). There is a new requirement to use a risk assessment on a protective device to decide whether guard locking is necessary. In the case of protective devices to prevent risks from moving parts within the meaning of Section 1.3.8.1, in future interlocks with guard locking, may additionally be necessary (something that had previously not been formulated in this way), whereas these can be dispensed with under certain conditions for protective devices within the meaning of 1.3.8.2 (similarly not previously formulated in this way) (i.e. depending on risk assessment, devices without guard locking can also be used).

### 1.3.9 Risks of uncontrolled movements

Parts of machinery may not move in an uncontrolled manner without actuation of an operating element.

### 1.4.2.1 Fixed guards

A new addition is that when the protective device has been removed, the fixing systems must remain attached to this or to the machinery.

### 1.4.2.2 Interlocking movable guards

Classification of the interlocking guards according to Type A and B is no longer necessary and will be replaced by requirements placed on the interlocking guards that are designed with or without a guard locking device.

### 1.5.8 Noise

An addition is that it must be possible to assess the level of noise emission by referring to comparative data for similar machinery.

### 1.5.9 Vibrations

As with Section 1.5.8 “Noise”, the reference to comparative emission data is added to the previous requirement to minimise levels.

### 1.5.15 Risk of slipping, tripping or falling

An addition is that, where necessary, handholds must be present on machinery. They must be fixed relative to the user and enable them to maintain their stability.

### 1.5.16 Lightning

Machinery in need of protection against the effects of lightning while being used must be fitted with a corresponding earthing system.

### 1.7.1 Information and warnings on the machinery



This provision has been included now.

Information and warnings on machinery must be provided on the machinery in an easily understandable form, preferably using symbols or pictograms. Any written information and warnings must be expressed in an official Community language of the Member State in which the machinery has been placed on the market.

Another new aspect is that, on request, this information may also be provided in any other official Community language understood by the operators.

#### 1.7.1.1 Information and information devices

A new addition is that visual display units or other interactive means of communication between the operator and machinery must be easily understood and easy to use.

### Summary

This is an overview of the fundamental new requirements in the 2006/42/EC Machinery Directive. In the meantime a range of extensive information has appeared on the subject, including the publication of books by Alois Hüning [11].

### Bibliography:

[1] Complete download e.g. from [www.schmersal.com](http://www.schmersal.com) or “google” “2006/42/EC”

[2] In the following this transposition into national law will be left on side, i.e. for simplification purposes reference will always be to the MD directly, skipping over the (legally more correct) transposition into national law.

[3] For example the MD in Germany has been transposed within the framework of the 9th GPSGV (9<sup>th</sup> Ordinance on the Product and Safety Act).

[4] There are a few exceptions to products to which the date of “29.12.2009” does not apply, for example captive bolt pistols, tractors etc.

[5] In the following and for reasons of simplification, the authorised representative who is resident (established) in the EU (in the EEA) or the authorised representative who acts explicitly on behalf of an EEA manufacturer will also be referred to as “manufacturer” as long as the manufacturer concerned is not resident in the territory.

[6] To be supplied by the manufacturer of partly completed machinery.

[7] In future risk analyses etc. will replace risk analyses with reference to the aspect of adaptation to EN ISO 12 100.

[8] According to sensible assessment of the anticipated use of the machinery.

[9] For further details, see “Guide to implementation of directives based on new approach and global approach” (93/465/EEC).

[10] Without any claim to completeness. There is also no analysis of additional requirements for specific machinery and for specific hazards (Annex II, Sections 2 et seq.). Detailed presentation in the “team of authors: the new EC Machinery Directive” – see No. 11 of the bibliography.

[11] **Hüning/Kirchberg/Schulze:** Die neue EG-Maschinenrichtlinie. 2009, Bundesanzeiger Verlagsges. mbH, Köln. ISBN 978-3-89817-798-6



# Further information and interpretation assistance on the Machinery Directive 2006/42/EC

Irrespective of technical books and other literature that have since appeared in great number on the subject of the “New Machinery Directive 2006/42/EC”, we would like to make reference in the following to two free publications which have been directly or indirectly initiated by the EU Commission.

## Synopsis of MD 2006/42/EC vs. 98/37/EC

This publication entitled “The new Machinery Directive – A tool to uncover the changes introduced by the revised directory” was published by the Commission for Occupational Health and Safety and Standardization (KAN) (Download: [www.kan.de/uploads/tx\\_kekandocs/Beri40e.pdf](http://www.kan.de/uploads/tx_kekandocs/Beri40e.pdf)).

This is essentially an article and paragraph comparison of the “old” and the “new” Machinery Directive, particularly of the basic safety and health protection requirements. It also contains a selection of views on the articles and annexes of the new legislative text. New texts, deleted texts and editorial text changes are highlighted in col-

ANNEX I		
Directive 2006/42/EC ("new" directive)	Directive 98/37/EC ("old" directive)	Comments
Particular attention must be given to the following points: <ul style="list-style-type: none"> <li>the machinery must not start unexpectedly,</li> <li>the parameters of the machinery must not change in an uncontrolled way, where such change may lead to hazardous situations,</li> <li>the machinery must not be prevented from stopping if the stop command has already been given,</li> <li>no moving part of the machinery or piece held by the machinery must fall or be ejected,</li> <li>automatic or manual stopping of the moving parts, whatever they may be, must be unimpeded,</li> <li>the protective devices must remain fully effective or give a stop command,</li> <li>the safety-related parts of the control system must apply in a coherent way to the whole of an assembly of machinery and/or partly completed machinery.</li> </ul> <p>For cable-less control, an automatic stop must be activated when correct control signals are not received, including loss of communication.</p>	Text from 1.2.2. In particular: <ul style="list-style-type: none"> <li>the machinery must not start unexpectedly,</li> <li>the machinery must not be prevented from stopping if the command has already been given,</li> <li>no moving part of the machinery or piece held by the machinery must fall or be ejected,</li> <li>automatic or manual stopping of the moving parts, whatever they may be, must be unimpeded,</li> <li>the protection devices must remain fully effective.</li> </ul>	Prevention of unexpected start-up is dealt with in EN 1037:1996. EN ISO 12100-2:2003 clause 4.11.1 mentions the uncontrolled speed change as one typical example of hazardous machine behaviour. In 98/37/EC the requirement concerning unexpected start-up was placed in EN ISO 1.2.7. Failure of the control circuit, therefore unexpected start-up was considered only as a consequence of such a failure. Now, with the migration of the requirements from old 1.2.7 to new 1.2.1, the new directive aims at preventing unexpected start-up resulting from any cause associated with the design of the control system (including, of course, the behaviour in case of failure).  The directive text could be misunderstood here. This requirement does not apply to "fully completed machinery" alone, but to "assemblies of machinery and/or partly completed machinery".  This new requirement is equivalent to the provisions of EN ISO 12100-2, 4.11.8 (principles relating to manual control, hyphen 1). It should be compared with the requirements concerning remote-controlled machinery, inserted among the requirements concerning the handling function, in 3.3.3 of the new directive.
1.2.2. Control devices Control devices must be: <ul style="list-style-type: none"> <li>clearly visible and identifiable, using pictograms where appropriate,</li> <li>positioned in such a way as to be safely operated without hesitation or loss of time and without ambiguity,</li> <li>designed in such a way that the movement of the control device is consistent with its effect,</li> </ul>	1.2.2. Control devices Control devices must be: <ul style="list-style-type: none"> <li>clearly visible and identifiable and appropriately marked where necessary,</li> <li>positioned for safe operation without hesitation or loss of time, and without ambiguity,</li> <li>designed so that the movement of the control is consistent with its effect,</li> </ul>	In all Annex I, the generic term "control" has been changed with "control device" or "control system" according to its intended meaning. In 1.2.2, "Control device" and "control" are to be considered synonyms.
<b>new text</b>	<b>deleted text</b>	not having undergone formal changes
		not copied from another part of the "old" directive

Fig. 2 Example of a page from the KAN publication “The new Machinery Directive”



Fig. 1 Title page of the KAN publication “The new Machinery Directive”

our. There is also an additional column for brief comments.

## Guide to MD 2006/42/EC

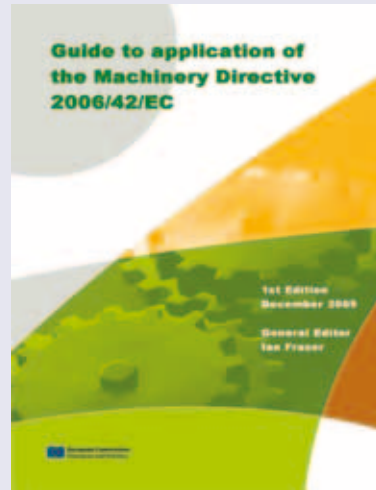
Just in time for the coming into force of the new Machinery Directive 2006/42/EC on 29.12.2009, a Guide (now in its second edition) also appeared with explanations and further information. The publisher is the “Enterprise and Industry” Department of the European Commission. The document was prepared by a group of representatives from the Member States.

Even if the Guide is not a legally binding text, it is an excellent aid in the interpretation of MD 2006/42/EC – if only in view of the competence and expertise of the authors involved (as shown in Figure 3).

The Guide is currently available as PDF document in English. Work is in progress on a German translation and translations into other languages as well. Download: see page 43.

The Guide has been prepared with the help of an Editorial Group [1]. The Commission wishes to warmly thank the members of the Editorial Group both for the huge amount of work they have carried out as well as for the efficient, constructive and cooperative spirit in which the drafts have been prepared. In parallel to the work of the Editorial Group, a Machinery Core Group established by ORGALIME, including representatives of the main sectors of machinery manufacturing, has provided invaluable input from the industry. The drafts prepared by the Editorial Group have been submitted to the Member States and stakeholders for comments. The Commission would also like to thank all those who have made comments. We have tried to take them into account as far as possible.

Of course, the Commission takes full responsibility for the content of the Guide. Readers are invited to communicate any corrections or comments on this 1st Edition of the Guide [2] so that they can be taken into account in preparing the 2nd Edition.



Brussels, December 2009                      The General Editor, Ian Fraser

- 1] The following people have taken part in the work of the Editorial Group:  
Lennart Ahnström, Emilio Borzelli, Robert Chudzik, Roberto Cianotti, Mike Dodds, Cosette Dussaughey, Marcel Dutrieux, Pascal Etienne, Ludwig Finkeldei, Tuiri Kerttula, Thomas Kraus, Partrick Kurtz, Wolfgang Lentsch, Göran Lundmark, Phil Papard, Boguslaw Piasecki, Marc Schulze, Katri Tytykoski, Gustaaf Vandegaer, Henk van Eeden, Richard Wilson, Jürg Zwicky.
- [2] Corrections, comments and suggestions for improvement should be addressed to: [ian.fraser@ec.europa.eu](mailto:ian.fraser@ec.europa.eu)

**Fig. 3** The Guide to MD 2006/42/EG

The Guide comprises 389 pages and refers to the normative part of the new MD 2006/42/EC and the Annexes I to XII.

The Guide is structured such that the individual articles, sections and sub-sections of the Di-

rective (in red boxes) are cited individually and the corresponding comments (marked by §) given – with cross-references where applicable (see example in Figure 4). These are accompanied by very helpful diagrams (see example in Figure 5).

(3) Member States are responsible for ensuring the health and safety on their territory of persons. In particular of workers and consumers and, where appropriate, of domestic animals and goods, notably in relation to the risks arising out of the use of machinery.

**§ 6 Health and safety**

The protection of health and safety is both a fundamental duty and a prerogative of the Member States. Since the Machinery Directive harmonises the health and safety requirements for the design and construction of machinery at Community level, the responsibility of Member States to protect health and safety of people with regard to the risks associated with machinery implies, ensuring that the requirements of the Machinery Directive are correctly applied.

**Fig. 4** Example of a comment in the Guide to application of the Machinery Directive

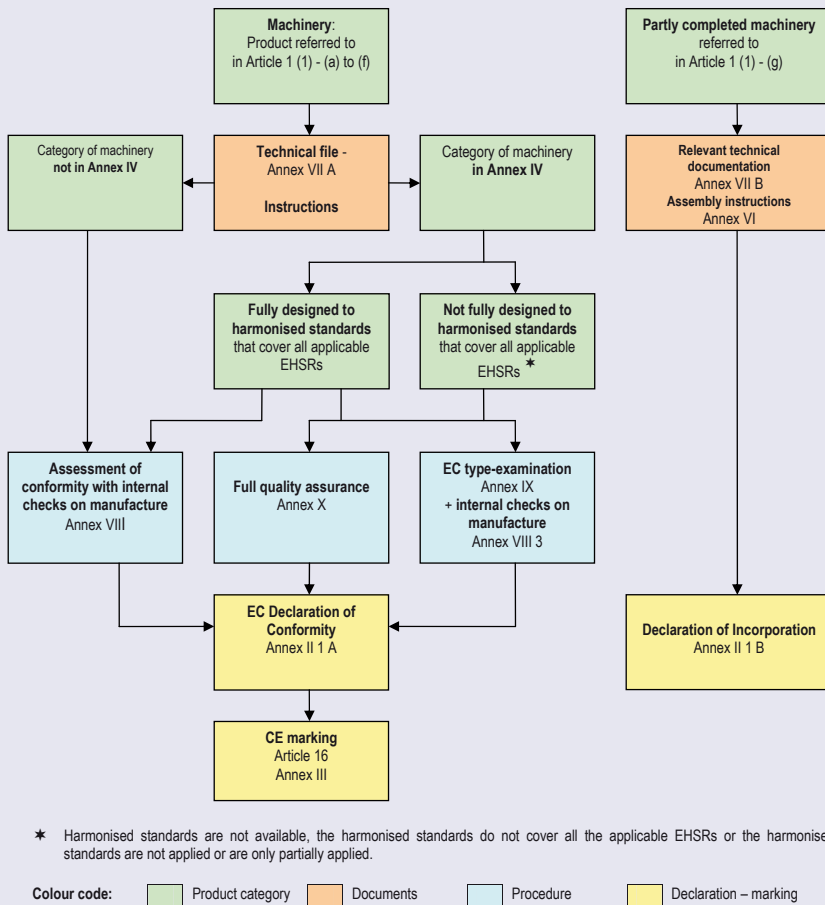
The Guide is therefore an extremely useful reference work if anything is unclear or doubtful.

The following diagram is an example of the very helpful diagrams in the Guide to application of

the Machinery Directive 2006/42/EC. It shows the requisite conformity assessment procedure depending on the existence of a completed or partly completed machine, whether it falls within the scope of the MD Annex IV and if so which op-

**§132 Diagram of the procedures for the placing on the market of machinery and partly completed machinery**

The following diagram summarises the procedures set out in Article 12 and 13:



**Fig. 5** Example of a diagram in the Guide to application of the Machinery Directive 2006/42/EC

tions are available to the manufacturer to satisfy the additional requirements.

If you are interested in the “Guide to application of Machine Directive 2006/42/EC“, please go to our Schmersal Homepage for downloading: [www.schmersal.com](http://www.schmersal.com) → Safety standards.



# Proof of conformity using a quality assurance system in accordance with Annex X of the Machinery Directive 2006/42/EC

L 157/6

EN

Official Journal of the European Union

9.6.2006

## ANNEX X

### Full quality assurance

This Annex describes the conformity assessment of machinery referred to in Annex IX, manufactured using a full quality assurance system, and the procedure whereby a notified body assesses and approves the quality system and monitors its application.

1. The manufacturer must operate an approved quality system for design, manufacture, final inspection and testing, as specified in point 2, and shall be subject to the surveillance referred to in point 3.

While the proof of conformity with the requirements of the Machinery Directive is usually provided by the manufacturer for the placing on the market or commissioning of new machinery, there are also exceptions to this rule. These are the so-called Annex IV machinery which has special hazard potential in the view of the legislator. The proof of conformity for this group of machinery used to be provided according to the “old” Machinery Directive by an additional EC prototype test which was performed by an authorised test office (a so-called notified body).

According to the new Machinery Directive 2006/42/EC, the procedure of “full quality assurance” under Annex X will exist in future for Annex IV products as an alternative to the EC prototype test. This procedure also requires the support and approval of a notified body. Article 12 (3) letter c and Article 12 (4) letter b in the normative part of the new Machinery Directive are pertinent here.

In theory a manufacturer could place Annex IV products on the market on his own responsibility if he had an internal production control system (i.e. a usual quality assurance system) and if the respective product has been designed and constructed exclusively making reference to a C standard (a machinery safety standard). This would therefore be a third alternative. However, if there is no C standard or if it is not applied fully – with all its cross references – there is also no alternative 3. The question is whether alternative 3 will be accepted by the market anyway because it is accustomed to having an external test office for these products.

### The future importance of Annex X

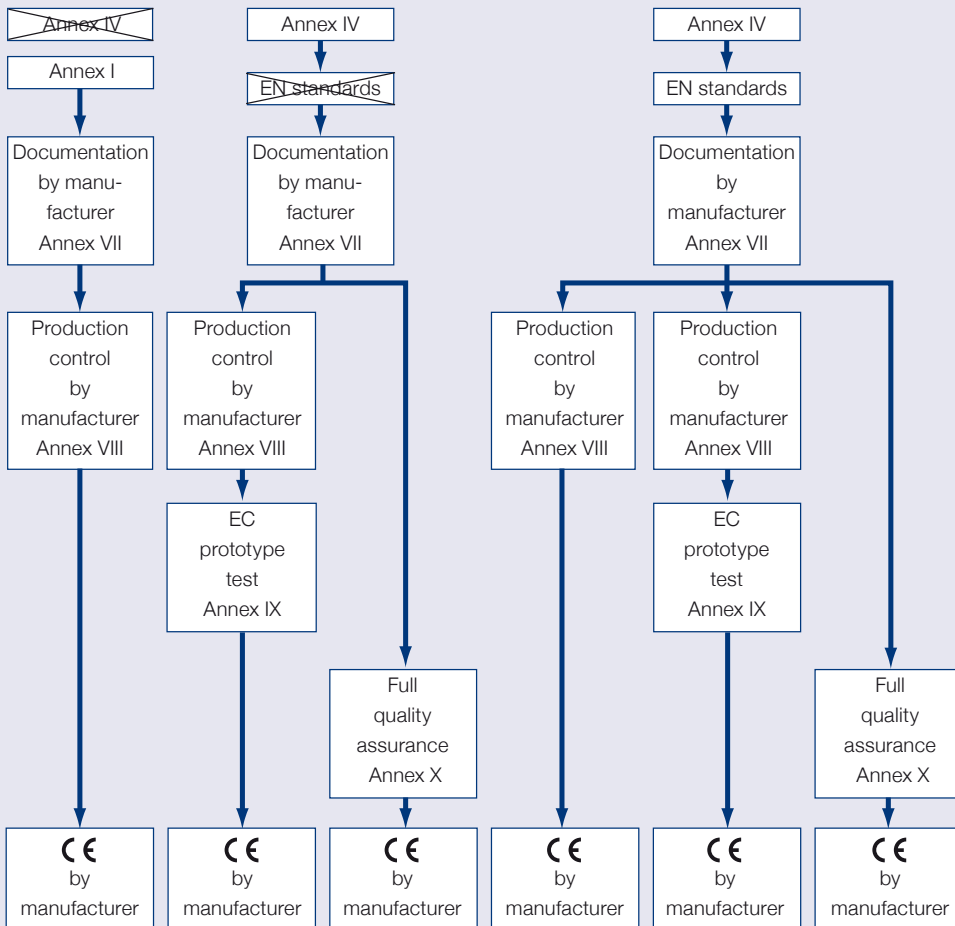
It can be expected that great use will be made of the new procedure set out in Annex X of the Machinery Directive 2006/42/EC particularly if manufacturers offer not only standard products but many application- and customer-specific product versions. The aspects that would speak in favour of the Annex X procedure are then essentially “time to market” and “customer-oriented flexibility”.

Manufacturers of safety components will also use the new procedure. The Schmersal Group will probably be one of the first companies in the industry to have this new quality assurance system and to already have had it assessed and approved by the TÜV Rheinland Technical Inspectorate (TÜV Rheinland).

For us, one of the main reasons for this additional effort is that in future more and more safety components will fall within Annex IV of MD 2006/42/EC compared to the case with Annex IV of the “old” MD 98/37/EC.

While the actual machinery part of Annex IV has more or less remained unchanged, i.e. differences between MD 98/37/EC and MD 2006/42/EC essentially refer to wording only, there has been an important extension to safety components in that all logic units to ensure safety functions [1] will in future fall under within this Annex with the resultant special requirements on placing on the market.

The safety components which have so far been covered by Annex IV remain unaltered.



**Fig. 1** Conformity assessment procedure according to Machinery Directive 2006/42/EC

**Example: Schmersal (hybrid handling)**

In future we will be subjecting safety-related devices and systems (safety components) to prototype tests. In the past this was frequently voluntary and was only required by law in exceptional cases; in future this situation will then be reversed although this will hardly make no difference in practical terms. This difference was not therefore our main motivation to introduce the new quality assurance system set out in MD Annex X.

Rather, we decided in favour of the additional option, i.e. of avoiding a mandatory EC prototype test, so that this is not performed – as is our concern – to the detriment of customer-oriented flexible readiness to supply. Otherwise we would

have had to always first await the “EC prototype test certificate” document before we could sample new versions or even market them.

**What does a quality assurance system according to Annex X mean?**

In addition to the description in Annex X of MD 2006/42/EC itself, this system – referred to as QAS in the following – is described in the so-called module paper of the EC as module H (see Blue Guide: “Guide to implementation of directives based on the New Approach and the Global Approach”; published by the European Commission).

Annex X and module H extend beyond the EN ISO 9001. The following differences exist [2] :

- The QAS assesses the safety-related design quality higher than the production quality.
- The QAS must guarantee the compliance of the machinery with the provisions of the Machinery Directive.
- The examination of the QAS must be made by a conformity assessment office (“notified body”). Under certain circumstances this may mean that companies may have to cooperate in this area with a different certifier than for the certification of their company under DIN EN ISO 9001.

**DIN EN ISO 9001 – not a complete substitute**  
 QM documentation in accordance with DIN EN ISO 9001 is not adequate to document the QAS. The QAS documentation must enable a notified body to assess on application for the approval of a QAS whether it is suitable to guarantee the compliance of the machinery manufacturer with the provisions of the Machinery Directive on a lasting basis. The following are also required:

- The competence and powers of the managerial staff in matters concerning the design and production quality must be described.
- The design examination and verification procedures, processes and systematic measures used in the design of machinery must be described.
- The standards used for the construction of machinery must be stated.
- Evidence must be provided that the product satisfies the requirements of the Machinery Directive.

The QM officer is given extended responsibility with respect to the coordination and monitoring of the QAS. In addition to updating documentation his main task is to coordinate with company management to maintain the approved QA system. If the notified body determines that this has not been maintained, it must revoke the approval granted. The company is then not allowed to place any more products of the product category concerned on the European market.



If the QAS procedure has been used for a product according to Annex X, the CE labelling must also bear the ID number of the notified body.



**Fig. 2** Products which in future fall within the scope of Annex IV (see paragraph 21): logic units with safety function. This change represents an essential extension to Annex IV safety components (see also loc. cit.)

**Which safety components will fall within Annex IV in future?**

Reference is made here to a proposal of the Institute for Occupational Safety and Health (BGIA) of the German Social Accident Insurance with a list of examples in accordance with Fig. 4.

## Logic units to ensure safety functions

On 29 December 2009, application of the new Machinery Directive 2006/42/EC [1] becomes mandatory. The differences between the former and the new Machinery Directives are described in a number of publications, for example in [2]. This article deals solely with one amendment which concerns “logic units to ensure safety functions”. These products are now stated in Annex IV of the new Machinery Directive. It lists products which owing to their function are a source of particularly high hazard. Accordingly, stricter requirements apply to the conformity assessment method. The components affected and the possible assessment methods are stated below.

### 1 What products are described as “logic units to ensure safety functions”?

Products are affected by this new provision if

a) they are safety components (see below) and are therefore governed by the Machinery Directive

and

**Fig. 3** BGIA proposal on the subject of safety components

No.	Component	Logic unit to ensure safety functions [3] in accordance with the Machinery Directive, Annex IV, Point 21	
1	Position switch with positive opening	no	Does not perform logic operations for the control of safety functions.
2	Proximity switch for safety functions [4]; also referred to as PDF-X according to DIN EN 60947-5-3	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
3	Guard locking to DIN EN 1088/DIN EN 14 119 (for protection of persons)	no	Does not perform logic operations for the control of safety functions.
4	Guard locking for safety functions for protection of persons [4], e.g. electromagnetic guard locking	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
5	Trapped-key interlocking system for safety functions [4]; in the form of a complete system only, not of individual components	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
7	Position sensor for safety functions [4], e.g. rotary encoder, length measuring device	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.

**Fig. 4** Components for safety functions



No.	Component	Logic unit to ensure safety functions [3] in accordance with the Machinery Directive, Annex IV, Point 21	
9	Protective device for indirect detection of the presence of persons, for example by the use of RFID transponders	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
10	Protective device for the detection and de-activation of possible hazards (not a warning system only), such as the detection of hazards presented by laser radiation by active laser guards	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
12	Emergency stop device	no	Does not perform logic operations for the control of safety functions.
13	Control device for enabling devices (enabling control)	no	Does not perform logic operations for the control of safety functions.
14	Safety switch gear [4], for example for the monitoring of speed, protective doors, emergency-stop, two-hand control, enabling device; note: may be part of a portable control station	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
15	Safety PLC [4]	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
16	Relay/contactor relay with mechanically linked contacts	no	Does not perform logic operations for the control of safety functions.
17	Contactors with mirror contacts	no	Does not perform logic operations for the control of safety functions.
18	Contactors monitoring module	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
19	Power Drive System with integrated safety functions [4]	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
20	Time delay element for safety functions [4]	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
21	Under-voltage release for a mains disconnecting device, intended for use in safety functions (for example to provide protection against restarting following power restoration)	no	Does not perform logic operations for the control of safety functions.
22	Braking unit, for example for woodworking machines	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
23	Component for the logical processing of safety-related signals of safety bus systems [4]; excluding components to be applied in "black channels" according to DIN EN 61 784-3 (black channel: communication channel without available evidence of design of validation according to IEC 61 508)	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.

**Fig. 4** Components for safety functions

No.	Component	Logic unit to ensure safety functions [3] in accordance with the Machinery Directive, Annex IV, Point 21	
24	Brake assembly for the protection of persons, for example to keep up gravity loaded axis	no	Does not perform logic operations for the control of safety functions.
25	Combination of valves, for example a safety valve block for presses	yes	Performs logic operations for generation of the output signal, and is intended for use within safety functions.
26	Valve with additional means for failure detection intended for the control of dangerous movements on machinery	no	Does not perform logic operations for the control of safety functions.
27	Equipment for protection against overpressure, e.g. pressure valve	no	Does not perform logic operations for the control of safety functions.
28	Equipment for stopping of movement, for example resettable check valve	no	Does not perform logic operations for the control of safety functions.
29	Contact expansion module; enhancement to safety switchgear (see No. 14); see No. 20 for time delay	no	Does not perform logic operations for the control of safety functions.

**Fig. 4** Components for safety functions

Literature:

- [1] Proposed definition of the BGIA currently up for discussion: “logic units to ensure safety functions” are devices, assemblies or components which are intended to be applied in safety-related parts of control systems to realise – solely or amongst other – safety functions and which generate output signal(s) based on an internal logic operation with the input signal(s).
- [2] Quoted from QZ – Year 54 (2009) 9, Carl Hanser Verlag, München; Tobias Henke: “Umfassende Qualitätssicherung mit der neuen Maschinenrichtlinie – Gestiegene Anforderungen”

- [3] The classification of a component as a “logic unit to ensure safety functions” constitutes an estimation on the part of the BGIA which has been agreed with further European test bodies. No responsibility is assumed for correctness.
- [4] Components are basically intended to be applied in safety functions if the following are stated: category, performance level (PL), probability of dangerous failure per hour (PFH) and/or Safety Integrity Level (SIL). The intended application of components cannot be clearly derived from a statement of  $MTTF/MTTF_d$  or  $B_{10}/B_{10d}$ .

## The “CE-attendant”

According to Machinery Directive 2006/42/EC,

*name and address of the person authorised to compile the technical documents*

must in future be provided both in the declaration of conformity for machinery and products equivalent to machinery and in the declaration of incorporation for partly complete machinery. This person must be resident in the Community (i.e. in the EU if the MRL text is followed exclusively). Refer here to “Explanations” in the MD Annex II. In the meantime it has since become clear that any person who is also resident in the EEA, e.g. in Switzerland, also satisfies this intention.

Against the backdrop of the intended greater market surveillance, the necessity to specify a person represents a new requirement of the MD 2006/42/EC. However, there is no further “job description” for this person either in the normative part or in the Annexes. Neither is the search for comments and interpretations particularly successful and there is currently a good deal of puzzlement, speculative in part, about this issue.

The term of “documentation officer” now appears to have become established. This term possibly misses the point and may go too far.

If one follows the little that one reads or hears, the general opinion is that still no legal second responsibility is created by specifying the person. The manufacturer making the respective declaration or his authorised representative is and remains responsible for conformity with the requirements of the Machinery Directive. However a personal union with a person who signs a declaration of MD-conformity can be realised..

The question should also be clarified as to whether the person must be a natural entity. The view was largely taken right from the beginning – also from very competent parties (see, for example, [www.maschinenrichtlinie.de](http://www.maschinenrichtlinie.de)) – and also coherently substantiated that a natural entity is meant. By contrast reference is only made in the Guide to the Machinery Directive 2006/42/EC (see loc. cit.) to “natural or legal person”.



There will now be agreement that the requirement does not mean that a personalised or organised officer responsible for CE or Machinery Directive is now necessary in the companies (or a kind of CE or Machinery Directive manager). Rather, the companies can continue to individually regulate the conformity procedure within the framework of their organisation according to their own ideas and necessities under consideration of the statutory requirements.

On the other hand, the “CE-attendant” or “documentation officer” – to keep with these terms – is also not the “senior archivist” of a company but rather a qualified contact partner for official inquiries etc. (see above “stricter market surveillance”). For this reason alone he should be well informed about the workflows, customs and responsibilities in the company and should also be integrated in these. It is contentious whether this also includes possibilities to influence content and control. By contrast, the possibility to influence completeness and plausibility of the technical documentation would make sense. The selection of the person can also be guided by the fact that a supervisory authority will always turn to this person if it wishes to find out about something (if doubt exists as to the conformity of the product).

It should be remembered in this context that only the documents mentioned in the Machinery Directive Annex VII are referred to (the so-called internal documentation) for which the person is assigned a role [1].

### **Supplementary information on Annex VII**

These documents are divided into the following depending on product

A: TECHNICAL FILE FOR MACHINERY  
B: RELEVANT DOCUMENTATION FOR PARTLY  
COMPLETED MACHINERY

Compared to the requirements of the MD 98/37/EC, a few differences are evident here in Part A which are commented on as follows in the KAN Report (see loc. cit.):

- *It must be remembered that the technical documentation is now to be compiled for all machinery using the same procedure (in the old directive 98/37/EC other procedures applied to Annex IV machinery with prototype testing). The first paragraph clearly shows the purpose of the technical documents.*
- *All documents on the risk assessment are now required. This is the most fundamental change with respect to the content of the technical documentation. (Directive 98/37/EC only requires the description of solutions which have been selected to prevent risks.) See Recital 23. The new EN ISO 14 121-1:2007 (revision of the earlier EN 1050:1996) and the Technical Report EN ISO 14 121-2:2007 will be important instruments for the conducting and documentation of risk assessment.*
- *The declaration of incorporation and assembly instructions are required for included partly completed machinery.*
- *The EC declaration of conformity of machinery or other products incorporated into the machinery is similarly required (“other products” are products that fall within the scope of directives requiring the EC declaration of conformity).*

- *The demand for a copy of the EC declaration of conformity is new.*
- *Relevant reports and results must now be included in the documentation.*

The requirements are essentially repeated in Part B (merely the cross-reference to the operating instructions is missing which is not required for partly completed machinery). A comparison with MRL 98/37/EC is not made because the subject of partly completed machinery has not hitherto been included. It is therefore merely stated as follows in the KAN comments (see loc. cit.):

*These documents (the list under Part B is meant here) are called “relevant technical documentation” to avoid confusion with the “technical file” for machinery. The documents are to be compiled by the manufacturer of a partly completed machine if one or several basic safety and health protection requirements apply or have been satisfied. The majority of requirements are similar to those for the technical documentation of partly completed machinery.*

Footnote:

- [1] The answer to the question frequently asked in this connection as to whether the documents need to be “delivered” with the machinery continues to be NO! An individual contractual agreement is required if the customer wants this. The law requires the documents to remain with the manufacturer and are intended only for inspection for authorised authorities.

## **Current and ongoing borderline questions of European and German machinery legislation [1]**

- **Modifications vs. significant modifications in machinery**
- **Assemblies of machinery**
- **Used machines**

For our readers outside Germany: the following refers to interpretations as represented in Germany. They are partly based on official interpretation papers which are also at the disposal of the EU Commission and have been acknowledged by it. However, there may well be other views in other EEA states because the issues discussed in the following also pertain to national law and also permit other interpretations.

### **Modifications vs. significant modifications in machinery**

This topic also cannot be found *expressis verbis* in the new Machinery Directive 2006/42/EC because the Directive continues to apply to machinery placed on the market or put into operation in the EU (or in the EEA) for the first time, i.e. practically to new machinery and – by way of exception – to used machinery (see also *loc. cit.*) if it originates from third countries (and is placed on the market or put into operation for the first time in the EU or in the EEA).

The fact that exceptions to this rule can exist, however, is now indicated in connection with the commentary on Article 15 of the Directive in the Guide to the Machinery Directive 2006/42/EC (see *loc. cit.*). To better understand the following quote (as shown in Figure 1) it should be said that the Directive 2009/104/EC referred to is not the Machinery Directive but the so-called Use of Work Equipment Directive [2] which is addressed to the employers as a social directive.

Exceptions of this type have, for example, long been represented in German law in transposition of the Machinery Directive at a national level under the umbrella of the Device and Product Safety Act (GPSG). The term of the “significant modification” exists here, i.e. in this case the machinery which is to be modified would have to be completely reclassified including its old components in accordance with the current Machinery Directive.

#### **Article 15**

##### **Installation and use of machinery**

This Directive shall not affect Member States' entitlement to lay down, in due observance of Community law, such requirements as they may deem necessary to ensure that persons, and in particular workers, are protected when using machinery, provided that this does not mean that such machinery is modified in a way not specified in this Directive.

#### **§ 140 National regulations on the health and safety of workers**

...

The provisions of Directive 2009/104/EC are applicable to machinery in service in workplaces. ...

...

This also applies whenever machinery is modified by the user during the course of its lifetime, unless the modifications are so substantial that the modified machinery must be considered as new machinery and be subject to a new conformity assessment according to the Machine Directive.

**Fig. 1** Quotes from Article 15 and Guide to MD 2006/42/EC

In this respect it will be advisable – also in the age of the new Machinery Directive – to apply an already known decision-making approach, as

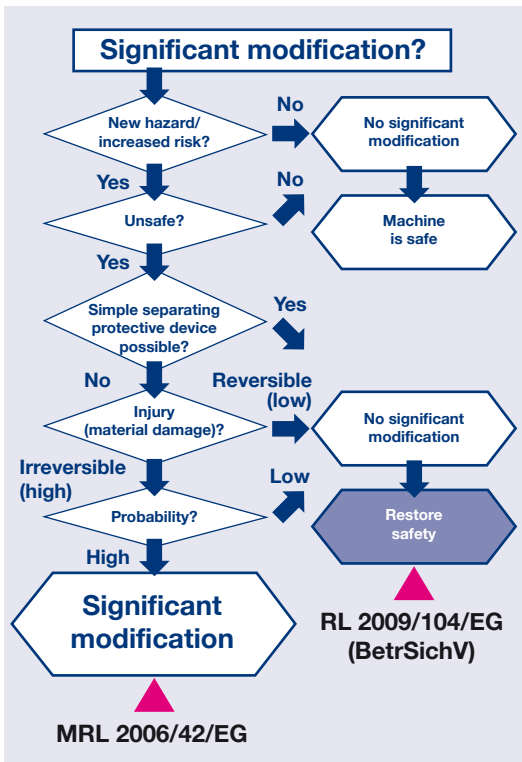


Fig. 2 Significant modification? Yes/No!

shown in the flow chart (based on an official government interpretation paper in this question [3], on which the Federal Government and German states already agreed in 2000).

One thing to note with respect to the interpretation paper and the above-mentioned flow chart is that the intention is usually not to reach the loop “Significant modification: Yes”. Consideration is given to the idea that some of the Machinery Directive requirements cannot be satisfied objectively when modifications are made to machinery. However, in no way does this mean that a disproportionate degree of reduced machinery safety would be tolerated. Rather, the German Ordinance on Industrial Health and Safety (BetrSichV) – the national implementation of the Use of Work Equipment Directive 2009/104/EC – must be applied. This means that the modifications themselves are to be realised in accordance with the state of the art, unless this is unreasonable for technical and economic reasons in exceptional cases. Only those machinery parts not affected by modifications need not be considered if they are least comply with the BetrSichV which applies under all circumstances.

Three cases can be assumed in the beside flow chart:

1. There is no new hazard and no increased risk so that the machine can continue to be viewed as safe.
2. A new hazard or increased risk does exist but the safety measures are adequate so that the machine can continue to be viewed as safe.
3. A new hazard or increased risk exists and the existing safety measures are not adequate.

In case 3 it must first be determined whether it is possible to return the machine to a safe condition using simple separating protective devices – i.e. the risk is not increased compared to the original safe state (but see also loc. cit. here).

Otherwise, 2 cases are possible based on a risk assessment:

1. The possible injury to humans is reversible or high material damage is not to be expected.
2. The possible injury to humans is irreversible or high material damage is to be expected.

In the first case the modification is not to be viewed as significant within the meaning of the GSG. In the second case the probability of this damage is to be examined, whereby two cases are possible:

1. The probability of the occurrence is not high.
2. The probability of the occurrence is high.

In the first case the modification is to be viewed as insignificant within the meaning of the GPSG. In the second case a significant modification in accordance with the current MD exists.

If the above procedure is followed, then the following aspects should be borne in mind:

- the analysis (in accordance with the flow chart), the content of which is equivalent to a risk assessment, should be made in a team at all events and must also be documented;
- modifications in the safety technology which exclusively serve the purpose of enhancing machine safety can never constitute a significant change. Only the opposite case, i.e. a reduction in safety technology (a “disarmament”) could be termed as a significant change within the meaning of the chart;
- experts are discussing controversially whether the “solution” through simple separating protective device cannot also be achieved by the installation of other protective devices,



**BG-PRÜFZERT-Information Sheet**

Berufsgenossenschaftliches Prüf- und Zertifizierungssystem

**Important Changes to Products**

In the European Union apply different criteria regarding used and new products placed on the market. However, there is agreement that products that have been subject to important changes must be treated as if they were new. Consequently, the relevant requirements in the Single Market directives must be observed when placing such products on the market, right down to the obligation to affix a CE mark to the product.

With regard to machinery within the meaning of the European Machinery Directive, a special additional point is that machinery built by an enterprise for its own use is also included. If such machinery has been subject to important changes, the requirements of the directive apply to it. In such cases, putting a machine into service is considered the same as placing it on the market.

But when is a change to a product an "important change"?

In 2000, the Germany ministry responsible for such issues and the federal states published a "Paper on the Interpretation of 'Important Changes to Machinery'", which also offers pointers on how to assess other products. The paper relates to the German Equipment Safety Act, which has since been superseded by the Equipment and Product Safety Act, but it remains useful nonetheless.

The content of the paper is shown below. It was originally published in "Bundesarbeitsblatt" 11/2000, page 35.

Paper by the Federal Ministry of Labour and the Federal States on the Interpretation of the Term "Substantial Modification of Machinery"

**Fig. 3** BG-Prüfzert information about "Important Changes to Products"

e.g. by the installation of interlocked or contactless protective devices.

This question can probably be answered in the affirmative if new sources of hazard can be controlled equally as well or better with the installation of other protective devices and the associated control-related interventions are superficial. However, a contactless protective device will only come into question if there is no danger of parts flying off and the safety distances are correct or exclusively an interlocking device with guard locking if hazardous after-travel is expected. This means that a correct risk assessment must, of course, be made if this option is to be used.



For our readers outside Germany: the following refers to interpretations as represented in Germany. They are partly based on official interpretation papers which are also at the disposal of the EU Commission and have been acknowledged by it. However, there may well be other views in other EEA states because the issues discussed in the following also pertain to national law and also permit other interpretations.



### Assemblies of machinery

The so-called assemblies of machinery (and of partly completed machinery) – for example, mechanical plant, interlinked machinery, integrated production systems and similar – continue to remain without alteration within the scope of the new Machinery Directive (see Annex I point 1.2.4.4) and therefore also the associated practical questions.

#### 1.2.4.4. Assembly of machinery

In the case of machinery or parts of machinery designed to work together, the machinery must be designed and constructed in such a way that the stop controls, including the emergency stop devices, can stop not only the machinery itself but also all related equipment, if its continued operation may be dangerous.

This subject in future as well must also be given special attention under the three aspects:

#### (1) Overall responsibility

Who bears the overall responsibility if an assembly of machinery does not come from a single source, whereby "not from a single source" can also mean that machinery (irrespective of whether complete or incomplete) of third manufacturers (including build for own use machinery) is provided/incorporated.

A general contractor (a system integrator) must be determined here (in advance would be best) who is responsible (beyond the conformity of the individual machines with the Machinery Directive) for the conformity of the assembly of machinery (i.e. the integration accomplishment) with the Machinery Directive.

If the question of overall responsibility is not regulated, the machine operator within the meaning

of the Machinery Directive will be the person responsible in cases of doubt.

## (2) **Mixtum compositum of different states of the art**

Following on from (1) a situation will frequently exist that if a machine is assembled anew, it will not consist exclusively of new machinery. Rather, the usual situation will probably be that older machines or parts of machines will be used.

The question then arising is how the incorporation of an earlier standard of (safety) technology is to be assessed with respect to the requirements of the Machinery Directive on assemblies of machines.

Similar to the question of when a significant modification to a machine exists and when not (see loc. cit.), the above question is also borderline.

A protection of vested rights firstly exists for **CE-compliant machinery with earlier years of construction**. This means that machinery that was safe on a date x within the meaning of the Machinery Directive requirements at that time remains “safe”.

But this situation also applies to traditional **old machinery**, i.e. to machinery before the Machinery Directive age. This means that old machines of this type can usually be incorporated in new machine assemblies as they are on the condition that they satisfy the requirements of the respective national implementation of the Use of Work Equipment Directive 2009/104/EC – in Germany of the BetrSichV, Annex 1 or the accident prevention regulations as of 31.12.1992.

At all events the **integration work** (the assembly) must be performed from the interface of the “old” machine (i.e. a) old machine in the traditional sense before the Machinery Directive age and b) CE machinery but constructed according to an earlier status of a Machinery Directive) making reference to the current Machinery Directive status.

This means that the general contractor (the system integrator), who is best determined in this case in advance, “certifies” the CE compliance of the integration work. It may be necessary to provide a supplementary page to the EC decla-

ration of conformity for old machinery with respect to those requirements of relevant single market directives which cannot be realised.

But here too there are exceptions from the rule (see MD Guide 2006/42/EC, §39): *If the replacement or the addition of new constituent units ... has .... a substantial impact to the operation or the safety of the assembly as a whole or involves substantial modifications of the assembly, it may be considered ... as ... a new assembly ... to which the Machinery Directive must be applied. ...* In cases of doubt the recommendation applies that national supervisory authorities or similar should be incorporated in the decision.

## (3) **Assembly of machinery: yes/no**

A decisive question which is evidently asked frequently in connection with assemblies of machinery is, however, when the putting-together of machines constitutes an assembly of machinery and when it doesn't.

An interpretation paper [4] (currently undergoing revision) has also existed on this question for some time. It concentrates on the so-called **linkage risks**.

Accordingly, an assembly of machinery within the meaning of the Machinery Directive is not said to exist if in an overall complex independently functioning machines (or independently functioning parts of machines) are linked in a functional and control manner, but these do not form a unit from a safety point of view in the above described sense. This will be the case, for example, if no or only small risks arise at the interfaces/transfer points between the individual machines due the interlinking (low level interlinked machinery). If, however, incomplete machinery is incorporated, this will usually be an assembly of machinery.

So-called **low-level interlinked machinery** can continue to be viewed independently from a safety point of view. In this case, the protective measures are aimed only at the individual machines. Otherwise, (in the case of risks caused by linking) the requirements apply as described under (1) and (2).

The following flow chart may be used for assessment purposes, whereby a spatial connection is assumed.



**1st step (does a functional link exist?):**

The functional link is characterised by the fact that machinery is functionally linked such that it forms a production unit to achieve a common objective. If there is no such link, this is not an assembly of machinery within the meaning of the Machinery Directive and there is no EC declaration of conformity for the entirety but only for individual machines.

**2nd step (does a control link exist?):**

If a functional link exists in the above described manner, it must be examined whether the machines are inter-linked by an overall control system and common command set-ups. Overall control guarantees the functioning of the machines as an entirety. The control system is therefore essential and facilitates the interaction of the individual machines and parts of machines. If there is no such control link, an assembly of machinery is not said to exist within the meaning of the Machinery Directive and no EC declaration of conformity is provided for the entire system but only for individual machines.

**3rd step (does a safety link exist?):**

If a risk arises in a machine which may lead to a risk to other machines in the plant due to the above described functional or control link, safety measures are required which are geared to the overall plant. In this case reference is made to a safety link. The EC declaration of conformity must be provided for the entire plant.

By contrast, if it is not possible for risks to be transferred from one of these machines to other machines or for new risks to arise to these other machines as a result of the interaction of individual machines, no safety link will be required. The machines interconnected in this way can be viewed as individual machines.

Fig. 4 Decision-making chart in the interpretation paper "Assemblies of machinery"

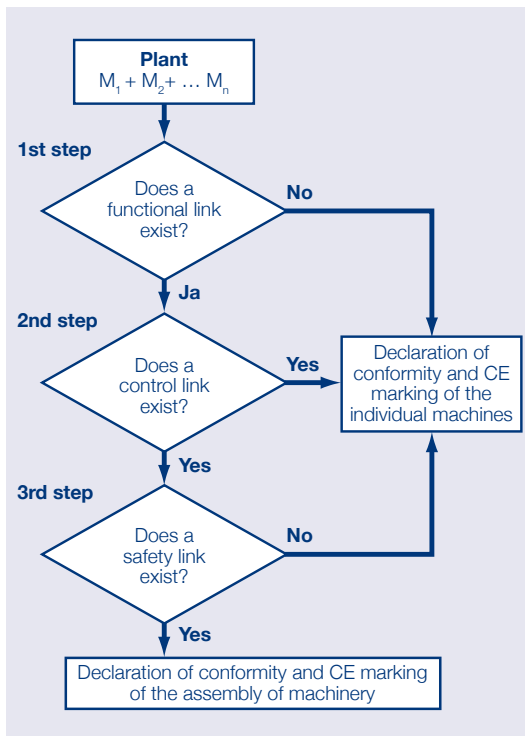


Fig. 5 Flow chart to assess link-related hazards – see also Fig. 4



Supplementary and further information on the subject of "assemblies of machinery" is also contained in the Guide to Machinery Directive 2006/42/EC, in particular the comments on point 1.2.4.4 of Annex I under § 38 and § 39 which we are unable to show here for reasons of space.

For our readers outside Germany: the following refers to interpretations as represented in Germany. They are partly based on official interpretation papers which are also at the disposal of the EU Commission and have been acknowledged by it. However, there may well be other views in other EEA states because the issues discussed in the following also pertain to national law and also permit other interpretations.

**Used machinery**

Used machinery which has already been placed on the market within the EU respectively EEA is also in future not subject to the requirements of the Machinery Directive. It is also not intended to make "used machinery" the subject of an independent domestic market directive.

The safety aspects of (EU) used machinery are regulated (indirectly) by the EC Use of Work Equipment Directive 2009/104/EC and its implementation (directly) into the respective national law of the Member States which may well go beyond the directive requirements of 2009/104/EC because it is a social directive.

In Germany used machines are addressed firstly (by name) in the GPSGV (Device and Product

Safety Act) which came into force on 01.05.2004. A reference is made again here to the German Ordinance on Industrial Health and Safety (BetrSichV) as national implementation of the Use of Work Equipment Directive, i.e. used machinery that complies with this status or the accident prevention regulations as of 31.12.1992 satisfy the pertinent requirements.

The following chart shows case examples of this:

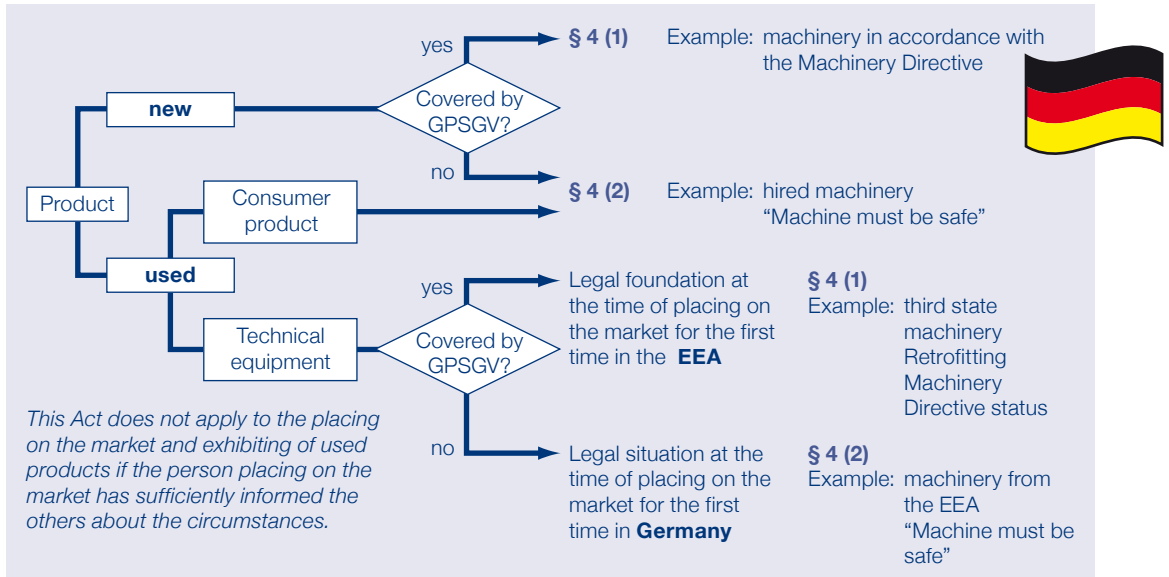


Fig. 6 Device and Product Safety Act, Section 4: Placing on the market and exhibiting

#### Used machinery. 1st case example

A used machine, year of construction before 1993, is resold in an unmodified form within the Federal Republic of Germany.

*Legal situation according to the GPSGV:*

According to § 4 (3) GPSGV, the date of placing on the market for the first time in Germany is decisive.

*Requirements placed on the nature of machinery:*

This machinery has the "grace of age". The concept of protection of vested rights is very frequently used for these machines because they satisfied the accident prevention regulations in terms of construction and equipment applicable at that time and – where necessary – were retrofitted by the operator to meet the requirements of the German Ordinance on Industrial Health and Safety (BetrSichV) Annex 1.

Statutory protective objective:

*Machine must be safe.*

*CE marking not applicable.*

#### Used machinery. 2nd case example

A used machine, year of construction before 1993, is sold without modification from an "old" EEA state in the Federal Republic of Germany.

*Legal situation in accordance with GPSGV:*

According to § 4 (3) GPSGV, the date of placing on the market for the first time in Germany is decisive.

*Requirements placed on the nature of machinery:*

The machine must comply at least with Annex I of the BetrSichV.

Statutory protective objective:

*Machine must be safe.*

*CE marking not applicable.*

### Used machinery. 3rd case example

A used machine with CE marking, year of construction after 1993, is sold without modification from an "old" EEA state to the Federal Republic of Germany.

*Legal situation according to GPSG:*

According to § 4 (3) GPSG, the date of placing on the market for the first time in Germany is decisive.

*Requirements placed on the nature of machinery:*

Since the machinery has already been placed on the market and put into operation in the EEA, it had to comply with the EC Machinery Directive 89/392/EEC (98/37/EC) or future 2006/42/EC. This should be the case in view of the CE marking.

### Used machinery. 4th case example

A used machine is sold without modification from a "new" EEA state (Estonia, Lithuania, Malta, Poland, Slovenia) to the Federal Republic of Germany after 01.05.2004.

*Legal situation according to GPSG:*

According to § 4 (3) GPSG, the date of placing on the market for the first time in Germany is decisive.

*Requirements placed on the nature of machinery:*

See case 2.

Statutory protective objective:

*Machine must be safe.*

*CE making not applicable.*

Exclusively **used machines** imported from **third party states** outside the EEA are to be viewed and treated as new machines under the Machinery Directive.

### Used machinery. 5th case example

A used machine is sold without modification from a non-EEA state (e.g. Japan, Canada, Turkey) to the Federal Republic of Germany. The year of construction is irrelevant in this case.

*Legal situation according to GPSG:*

According to § 4 (3) GPSG, the date of placing on the market for the first time in the European Economic Area is decisive.

*CE marking must be attached.*

*Requirements placed on the nature of machinery:*

The nature of machinery must comply with the basic safety and health requirements in accordance with Annex I of the EC Machinery Directive 2006/42/EC.

In the case of investments in any such **third country machinery** thought should be given beforehand to whether a requisite retrofit to the status required by the Machinery Directive is at all viable from a technical and cost point of view.

In every case the recommendations below should be heeded:

#### Before buying:

- ask about the safety status of the machine
- have the requisite retrofits performed by the dealer or existing operator, or
- written confirmation of the requirements placed on the nature of the machine for putting into operation

### Summary

It has not of course been possible to avoid simplifications and generalisations in view of the complexity of this subject. This will mean that details will still need to be examined to determine how a particular configuration is to be legally put into practice. It was the purpose of this summary to provide an approach to this subject. It may also be advisable to consult the respective regulatory authority (in Germany, for example, the employees of the employers' liability insurance association).

### Excursus: German Operational Safety Ordinance (BetrSichV)

The German Operational Safety Ordinance (BetrSichV) implements the Use of Work Equipment Directive 2009/104/EC in Germany and regulates the provision of work equipment during work and operation of plant requiring monitoring within the meaning of occupational health and safety.

The basic foundations of this concept are as follows:

- a uniform hazard assessment of the work equipment
- a safety-related assessment for the operation of plant requiring monitoring
- "state of the art" as uniform safety criterion set out in so-called "technical rules on operational safety" (TRBS)
- suitable protective measures and inspections
- minimum requirements for the characteristics of work equipment (in accordance with BetrSichV Annex I) unless regulated in the EU single market directives.



# Future changes in the Directives of the European Union (EU)



Only now, to be precise as from 29 December 2009, has the new version of the Machinery Directive MD 2006/42/EC come into force and there is already talk of imminent changes. These do not refer to the inclusion of pesticide spraying equipment in the scope of the Machinery Directive to become effective on 15 December 2011 through the supplementary directive 2009/127/EC, but rather to an adjustment of the MD 2006/42/EC (and a large number of other single market Directives) to the so-called

## New Legislative Framework (NLF),

sometimes also referred to as the “NEW New Approach” [1]. It is against this background that work is already in progress in Germany on an adjustment of the Device and Product Safety Act (GPSG) which is “responsible” for the majority of EU single market directives [2].

### What's it all about?

In the broadest sense the aim is to standardise the proof of conformity (the conformity assessment) for the different products for which single market directives exist in the EU (e.g. Machinery, Low Voltage, Pressure Equipment, ATEX or EMC Directive).

For example, it may be that different provisions exist in the Low Voltage Directive and in the Machinery Directive, e.g. who may issue a declaration of conformity or attach the CE label, although the circumstances for placing products on the market in the responsibility of the manufacturer are the same (module A of the so-called module paper 93/465/EEC with different test and certification procedures for products [3]).

The original intention was to make adjustments to the New Legislative Framework (NLF) in the “omnibus procedure” – as part of an amendment directive. In the meantime, according to a statement of the ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie e.V. → Germany’s Association of Electrical and Electronic Industry) *the Legal Services of the European Commission have thwarted these ideas of the reasonable General Directorate, however. ... The changes to the directives are viewed to be too serious to implement them in an amendment directive. In the so-called recast procedure every directive is now being given its own vehicle* (i.e. nothing more than that a revision takes place).

It remains to be seen what will now happen in individual cases as far as the Machinery Directive 2006/42/EC is concerned: when it becomes relevant and whether the changes are more or less only formal or the revision leads to substantial changes.

The latter question on substantial changes is to be understood particularly in view of the paragraph in the relevant document (decision 768/2008/EC) as follows:

*The main requirements* (meant are the basic health and safety requirements placed on a product) should be worded so precisely that they are legally binding. They should be formulated such that it may be assessed whether they have been observed, even if harmonised standards do not exist or the manufacturer has decided not to use a harmonised standard. Just how detailed these requirements must be will depend on the circumstances of the individual sectors.

Naturally this criterion is open to much discussion if Annex I of the Machinery Directive 2006/42/EC is considered.

### Official publication

The EU Commission who initiated the NLF explains its intentions as follows:



**The New Legislative Framework, the modernisation of the New Approach for marketing of products, was adopted in Council on 9 July 2008 and finally published in the Official Journal on 13 August 2008. This broad package of measures which has the objective of removing the remaining obstacles to free circulation of products represents a major boost for trade in goods between EU Member States.**

It will bring particular benefits for small and medium sized enterprises (SMEs), who will no longer be discouraged from doing business outside their domestic markets. Existing market surveillance systems for industrial products will be strengthened and aligned with import controls. These measures will reinforce the role and credibility of CE marking.

In addition, trade in goods which do not fall under EU-legislation will be improved. From now on a Member States that intends to refuse market access will have the duty to talk to the enterprise and to give detailed objective reasons for any possible refusal, making life for companies easier.

The package of measures will have an impact on a large number of industrial sectors, representing a market volume of around € 1,500 billion a year. ...

The objective of the package is to facilitate the functioning of the internal market for goods and to strengthen and modernise the **conditions for placing a wide range of industrial products** on the EU market. The package builds upon existing systems to introduce clear Community policies which will strengthen the application and enforcement of internal market legislation. It:

- Introduces better rules on **market surveillance** to protect both consumers and professionals from unsafe products, including imports from third countries. This particularly applies to procedures for products which can be a hazard for, health or the environment for instance, which in such a case will be withdrawn from the market;
- Enhances the confidence in and quality of conformity assessments of products through reinforced and clearer rules on the requirements for notification of **conformity assessment bodies** (testing, certification and inspection laboratories) including the increased use of **accreditation**; a reinforced system to ensure that these bodies provide the high quality services that manufacturers, consumers and public authorities need;
- Enhances the credibility and clarifies **the meaning of CE marking**. In addition the CE marking will be protected as a community collective trade mark, which will give authorities and competitors additional means to take legal action against manufacturers who abuse it;
- Establishes a common legal framework for industrial products in the form of a **toolbox of measures for use in future legislation**. This includes provisions to support market surveillance and application of CE marking, amongst other things and it sets out simple common definitions (of terms which are sometimes used differently) and procedures which will allow future sectoral legislation to become more consistent and easier to implement. The provisions are split for legal reasons, but must be considered in parallel, as they are fully complementary and together form the basis of consistent legal framework for the marketing of products. The provisions of the Decision will be fed into existing Directives as and when they are revised – in effect, it is a basis for future regulation.

The package also strengthens the internal market of a wide range of other products, which are not subject to EU harmonisation, such as various types of foodstuffs (for example bread and pasta), furniture, bicycles, ladders and precious metals, etc. Together they represent more than 15% of intra EU trade in goods. The new mutual recognition Regulation covers such products.

**Fig. 1** Statement on the NLF by the EU Commission

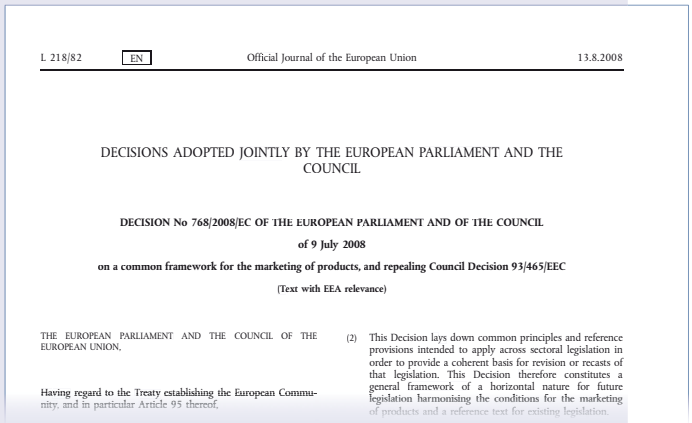
### **Initial guidance**

A few aspects of the NLF are explained in the following (see in particular “importer” and “dealer”)

which is based on a publication from the Koblenz Chamber of Industry and Commerce:

## Content of the "New Legislative Framework"

Decision 768/2008/EC now applies to future directives and to the revision of existing directives. It contains common principles and model provisions [4] for application in all sectoral legal acts (e.g. the Machinery Directive, Medical Devices Directive and others). Depending on the product the legislator can in future select the necessary procedures from the different modules which are then to be accepted in unaltered form where possible. This decision forms a general all-encompassing framework for legal provisions designed to harmonise the single market and also contains different clear definitions for certain basic terms. Up to now a large number of terms have been used in legislation on the free movement of goods some of which have not been defined or have been defined differently and this has not contributed to legal clarity.



### The future role of companies

Furthermore, general duties for economic players – these are the manufacturers, importers and dealers – have been described in the decision and procedures set out for CE labelling. **All** economic players in the supply and distribution chain **must** take the requisite measures to guarantee that only those products are placed on the market which comply with the applicable laws. It is expected both from the importers and from the dealers that they observe the applicable requirements with the necessary care if they place products on the market or offer them for sale.

A clear and proportionate distribution of duties is provided for in the decision which affects every individual player in accordance with his role in the supply and distribution process. Since certain tasks can only be assumed by the manufacturer, a clear distinction is made between **the manufacturer** and the players further down the distribution chain, such as the **importer** and the **dealer**.

Since the **manufacturer** knows all details of the design and production process he is the most suited to implement the entire conformity assessment procedure. *The conformity assessment will therefore remain the exclusive responsibility of the manufacturer in future.*

If the **importer** imports products to the EU from third countries, he must ensure that these products comply with the requirements applicable in the EU. The importer is responsible for ensuring that the products he places on the market satisfy the applicable requirements and do not represent a risk. *He must ensure that the conformity assessment procedure was conducted and that the product labelling as well as the documents created by the manufacturer are available to the regulatory authority for monitoring purposes. The importer must also state his name and contact address on the product.*

*The dealer must ensure that his handling of the product does not negatively influence the conformity of the product, i.e. he may make no changes to the product.*

An importer, dealer etc. placing a product on the market in his own name or with his own brand or changing a product such that this can influence its conformity with the applicable requirements, is viewed to be manufacturer ("**quasi manufacturer**") and must therefore also assume the obligations of the manufacturer. This interpretation applies even today.



Fig. 2 Statement on the NLF by the Koblenz Chamber of Industry and Commerce (continued overleaf)





### Notified bodies and market surveillance

The above decision, which must first be incorporated in future directives, stands alongside the **EC Regulation 765/2008 with provisions on accreditation and market surveillance which directly apply in the Member States from 01.11.2010**. Depending on risk, certain products must be examined by an independent conformity assessment office, the so-called “Notified Body”. It has become apparent, however, that the criteria contained in the individual directives which must be satisfied by the conformity assessment offices are not sufficient to guarantee a uniformly high quality level of the notified bodies throughout the EU. Therefore binding requirements on the conformity assessment offices were long overdue. This gap has now been filled. The Member States are responsible for a strong and efficient surveillance of the market in their sovereign territory. The market surveillance authority must be equipped with adequate powers and resources. For this reason the role of market surveillance has been strengthened by the new Regulation. Finally, this EC Regulation serves to protect the CE symbol from abuse.

**Fig. 2** Statement on the NLF by the Koblenz Chamber of Industry and Commerce (continued)

#### Footnotes:

- [1] The “New Approach” is a term generally used to denote that product Directives which have arisen on this basis are restricted to general “Basic Requirements”. The actual technical specification and interpretation of content is then performed as part of the European harmonised standard with the advantage that the user of the corresponding laws have a presumption of conformity (have done things correctly).
- [2] Single Market Directives: EC Directives which regulate the (minimum) requirements with respect to safety and health requirements of products and the procedure of proof of conformity.

- [3] See also (Blue) “Guide to implementation of directives based on the New Approach and the Global Approach”.

- [4] Model provisions refer to the uniform definition of general minimum requirements for all directives of this type (starting with definition of terms, through duties of the economic players [manufacturers, authorised representatives, dealers, etc.] to the assumption of conformity and similar).





## ***Comparison: with the non-European requirements placed on machinery safety [1]***



With the aim to remove obstacles to trade – a free circulation of goods on a high safety level – EU directives have created a unique kind of system in the European Economic Area (EEA) [2] that differs, sometimes significantly, from regulations in other countries in the world.

### **The duty of machine manufacturers**

The first difference comes from the fact that the legislator already places a duty on manufacturers of machinery in the EEA to observe specific fundamental safety requirements even at the design stage and during the construction of machinery, whereas in other regions of the world the risk is usually borne by the companies operating the machinery.

The background to placing obligations on machinery manufacturers was the realisation that the cost/performance ratio of the safety technology of a machine can be designed much more favourably during product development than when there is a need for subsequent adaptation and “retrofitting”.

In order to overcome this handicap, machinery purchasers from non-EEA states then in practice often completely or partially pass on their duties in advance to the suppliers selling the machinery within the framework of the purchase agreement.

The requirements to be observed are then subject to the respective national law of a state where the aspects to be considered and the depth of the regulations concerned naturally differ both formally and in terms of content. Added to this are differing sanctions in the event of failure to observe the requirements and for liability obligations in the case of accidents, as well as differences in the manner and intensity that such matters are followed up by public agencies and authorities.

Moreover, it may be necessary to obtain certain product certifications in order to deploy a specific product. Even if, according to the “rules of the game” of the World Trade Organisation, WTO product certifications must concern the products of all suppliers on the market irrespective of whether these are imported or are manufactured in the own country, an exporter may find it more difficult, complicated and finally expensive to obtain product certification, if only for communication reasons.

### **The respective national law applies outside Europe**

Where a duty is imposed on the exporting machinery manufacturer by customers or others, for example public or semi-public certification obligations, the manufacturer must devise ap-

appropriate certification procedures and compare the corresponding requirements with his own requirements, for example European regulations and standards.

As a rule these differ from each other so that it crucial to budget for the associated additional costs for development and approval. Furthermore, the product liability regulations in the individual countries must be clarified in order to be properly prepared for any claim. Ultimately this information is decisive for market success and for the “time to market”.

**New approach of the EU**

A second important difference compared to requirements elsewhere is the “New Approach” [3] system in the EEA with its presumption of conformity and, with certain exceptions (loc cit), the use of self declaration to confirm conformity (which the manufacturer is responsible for himself).

The safety-related EC directives set out below represent the requirements of the new approach:

- 2006/95/EC (Low Voltage Directive)
- 2004/108/EC (EMC Directive)
- 98/37/EC or its successor 2006/42/EC (Machinery Directive).

If the products and equipment covered by the New Approach comply with the basic require-

ments so that the corresponding conformity assessment procedure has been successfully completed, an EC declaration of conformity has to be issued and a CE mark has to be applied; these products and equipment may now participate in the free sale of goods in the EEA.

The situation in the global market sometimes looks very different. The CE mark is a legal requirement that applies exclusively in the EEA. Other market access requirements and legal systems apply in other economic areas. The term **Global Regulatory Product Compliance** is often used for this reason. This involves the complete satisfaction of all legally relevant statutory provisions for the respective product. “Compliance marks” play a role here.

These must be divided into

- Non-mandatory marks (e.g. the GS Mark, UL Mark) and
- Mandatory marks (e.g. CE, FCC).

The example provided in Figure 1 illustrates the requirements placed on product conformity.

However, it is more frequently the case that customers outside the EEA order machinery with CE conformity (possibly in combination with national features such as taking test marks into consideration). While a case such as this con-

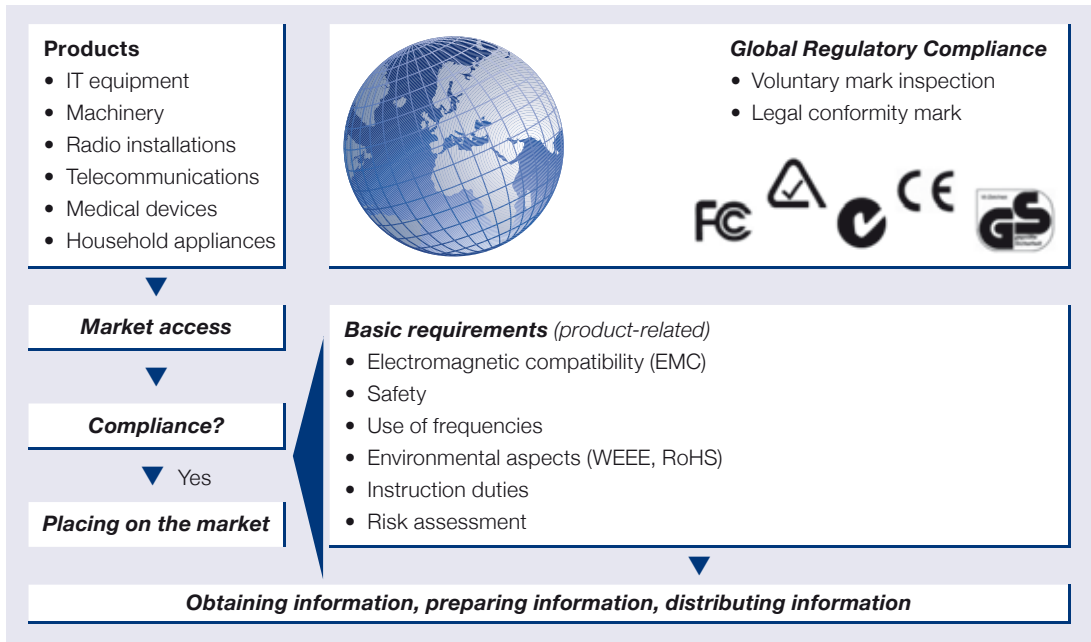


Fig. 1 Global Regulatory Compliance

### Excursus: The significance of standardisation in the EEA region

The principal requirements placed on product safety are specified in the annexes of the respective EU directives (see examples above) and they are so precisely formulated that they (may) create legally binding laws during transposition into the national law of the Member States. However, when it comes to the practical implementation of the respective requirements that can be defined as a description of the protective goals, one frequently would like support with more detailed specification and interpretation, as with a recipe or knitting pattern.

In EU directives, this support has been transferred to harmonised European standardisation and embedded via the establishment of the so-called presumption of conformity. According to the presumption of conformity, if harmonised standards are complied with it can be assumed that all basic safety requirements referring to the subject concerned have been satisfied. If no harmonised standards are applied, there is a reversal in the burden of proof for conformity to the directive, so that in this case it lies with the manufacturer. Therefore over the years, a collection of more than 500 standards, divided into A, B and C standards (as shown in Figure 3), has been created via the European standard organisations (CEN and CENELEC) just on the subject of “machinery safety”. This imposing set of standards has now almost completely replaced the national statutory provisions that were common up to 1993 which was when the first Machinery Directive came into force.

**Fig. 2** Significance of standardisation in the European Economic Area

cerns an individual contractual regulation, it can nonetheless make life easier for the machinery manufacturer.

#### Standards on the subject of “machinery safety” and their international significance

In this context it is remarkable that the vast majority of these harmonised standards are now international ISO and IEC standards. There is a similar trend for IECEx scheme standards in the area of “explosion protection”. In other words, where these standards have a recognised status in non-European countries, whether this is of a *de jure* or *de facto* nature, the trend at the inter-

### The structure of EN standards

The requirements of the Machinery Directive are specified in detail through the EN standards; these are divided into three hierarchically structured type classes.

**Type A standards** (basic standards), such as EN 12 100 “Safety of Machinery – basic concepts, general principles for design” and EN 14 121 -1 “Safety of Machinery – risk assessment” affect basic regulations for machinery safety.

**Type B standards** (group safety standards), for example ISO 13849-1 “Safety-related parts of control systems” deal with a safety aspect that can be applied to a wide range of machinery; these are then subdivided into standard classes B1 and B2.

**Type B1 standards** make regulations on safety aspects such as ergonomic, major safety principles and safety distances.

**Type B2 standards** describe features of protective devices that may be deployed in diverse types of machinery, for example EN 1088 “Interlocking devices with and without guard locking”.

**Type C standards** (engineering or product standards) refer to individual types of machinery or to application areas such as packaging, injection moulding/blow moulding machinery or machinery in bakeries.

**Fig. 3** Type A, B and C standards

national level is towards harmonising content in terms of the safety-related requirements placed on machinery.

Despite this, it is not automatically the case that the ISO and IEC standards will be accepted and implemented by all countries throughout the world. Decisions will be taken at a national level. Even if they are accepted, the various formalisms, types of conformity verification and national prefaces to be heeded may be regulated differently.

The following provides an example to illustrate how complex market access conditions outside the EU can be. It is comparatively easy for the large industrial nations such as the USA, Canada, Japan, India, China and Australia to obtain the relevant information via the internet, but the matter still has to be dealt with at all events. In detail:



### Safety requirements in the USA

The USA continues to be most sceptical about the trend towards an international aligning of requirements.

Large numbers of products fall under specific federal laws, the so-called Codes of Federal Regulations (CFR), and have to be approved before market launch. The respective federal authorities are, for example, the FDA (Food and Drug Administration, [www.fda.gov](http://www.fda.gov)) and the FCC (Federal Communications Commission, [www.fcc.gov](http://www.fcc.gov)). The most important provisions related to importing goods in terms of labelling and the forms to be submitted can be found on their websites.

A further authority is the OSHA (Occupational Safety and Health Administration, [www.osha.gov](http://www.osha.gov)), which is a federal authority assigned to the Department of Labor, DOL) and which issues binding joint legal rules for all federal states in the USA in the area of occupational health and safety (regulations for operators). These include the OSHA Standards with some regulations that are relevant to machinery:

- Occupational Safety and Health Standards, **29 CFR Part 1910** [4]
- Machinery and Machine Guarding, **29 CFR Part 1910 Subpart O**
- Electrical, **29 CFR Part 1910 Subpart O**.

By contrast with machinery safety requirements in Europe which can be found in a publication by the VDMA (the German Engineering Association),

*the USA has no federal US laws that are comparable to the machinery directive or other EC domestic market directives and which lay down the responsibility of a manufacturer or supplier. Rather, safety at work requirements are placed on employers that are intended to guarantee safe working equipment and occupational health and safety. In this area too the USA has no uniform law because federal states and County Authorities in the US can institute requirements that apply on a regional basis. And it is just such local provisions that, in individual cases, can cause substantial problems when placing machinery or systems on the market. For this reason it is worth obtaining information from the importer or US customer about applicable labour protection standards.*

While it can be said that there are certainly comparisons with ISO standards in terms of the requirements placed on functional machinery safety, e.g. concerning risk analysis and measures to reduce risk, the requirements for electrical safety (including fire hazards) differ, sometimes greatly.

The principle of single failure safety with fault detection also applies generally to functional safety (termed “control reliability” here); (see 29 CFR 1910.212 or, for example, ANSI B11 19-1990 sub-chapter 5.5): *“Control reliability” means the device, system or interface shall be designed, constructed and installed such that a single component failure within the device, interface or system shall not prevent stopping action from taking place but shall prevent suc-*

cessive machine cycle” (similar to the definition for Control Category 3 in accordance with EN 954-1:1996 or the Performance Level “d” in ISO EN 13849-1:2008 [2006] and SIL 2 in IEC EN 62061:2005).

Different requirements also apply to symbols and pictograms of indicative safety measures.

The basic rule is that OSHA requirements and OSHA references have precedence over national standards, e.g. the ANSI B11 series of safety standards for certain types of machinery (lathes, saws, pipe bending machines etc.).

By contrast the NFPA 79 standard is recommended for machinery that is not covered by specific OSHA standards; this standard is very similar to IEC EN 60204-1: “*NFPA 79 is a standard that would apply to machines not specifically covered by OSHA standards.*”

Other standards can be additionally applied as long as they do not contradict the OSHA (and other specific requirements). An OSHA comment on the application of European standards helps to illustrate this point: “*While compliance with European Community standards may produce the level of employee protection contemplated under the OSH Act, the only way for an employer in US to be assured that it is in compliance with the OSH Act is to provide machine guarding that conforms to the provisions of relevant OSHA standards.*”

The OSHA has put together a manual entitled “Concept and Techniques of Machine Safeguarding” to help machinery and plant engineering companies; this contains numerous tips on designing safe machinery.

In addition, all electrical installations in the USA must obtain a construction licence from locally competent authorities. Different agencies (termed AHJs or Authority Having Jurisdiction) are responsible in different federal states, such as the State Electrical Commission, the State Fire Marshal or the Department of Public Safety. Since these agencies do not inspect the equipment to be installed themselves, they rely on assessment by “third parties” such as UL. In this connection the OSHA is also responsible for the

accreditation and recognition of these National Recognized Testing Laboratories (NRTL).

In the fire protection area, the National Fire Protection Association (NFPA) which was founded back in 1896 can be mentioned. With its historical roots (keyword “fire hazard in wooden houses from electrical wiring and equipment”), the NFPA has drawn up the National Electrical Code (NEC) [5]. Reference is made here to the following sections of the NFPA 70:

**90.7 Examination of Equipment for Safety.** *For specific items of equipment and materials referred to in this Code, examinations for safety made under standard conditions provide a basis for approval where the record is made generally available through promulgation by organizations properly equipped and qualified for experimental testing, inspections of the run of goods at factories, and service value determination through field inspections. This avoids the necessity for repetition of examinations by different examiners, frequently with inadequate facilities for such work, and the confusion that would result from conflicting reports on the suitability of devices and materials examined for a given purpose.*

**110.2 Approval.** *The conductors and equipment required or permitted by this Code shall be acceptable only if approved.*

*FPN: See 90.7, Examination of Equipment for Safety, and 110.3, Examination, Identification, Installation, and Use of Equipment. See definitions of Approved, Identified, Labeled, and Listed.*

For these reasons an examination of electrical equipment by an NRTL is therefore essential in most cases if one does not wish to run the risk of the operating licence for machinery being turned down by an AHJ as part of a “red tag” procedure or the risk of becoming embroiled in a product liability case. What is more a customer, who as operator must satisfy the OSHA standards, will generally not buy such a “non-approved” machine, so that market access is impossible.

This brief presentation shows how important it is to have the relevant information about corresponding regulations in the USA even at the project definition phase.







### **Japan: JIS standards**

JIS standards (Japanese Industry Standards) have been present in Japan since 1999. These are structured in a similar way to the EN standards and have been implemented at a national level via the globally valid ISO and IEC standards. Examples of the first harmonised standards are ISO 12 100-1, ISO 12 100-2 and IEC 60204-1.

In addition a safety directive on the basis of ISO 12 100 came into force in June 2007, through which all EN standards as well as the division into A, B and C standards in effect became a Japanese standard. As such any machinery manufacturer complying with European standards can be relatively certain that he is also satisfying Japanese safety requirements. Furthermore, the international ISO and IEC standards are available as JIS standards in Japanese, while for some time Japanese standardisation committees have also been involved in developing ISO and IEC standards on the subject of “functional safety”.

However the application of standards is generally voluntary: with the exception of a few types of machinery such as presses, there is no authority that prescribes or monitors compliance and also no product liability as we know it that indirectly leads, via the liability question, to compliance with the standard (= state of the art). Despite this one can say that common standards on machinery safety are generally accepted.

Alongside this, a “Law on health, safety and hygiene at the workplace” has applied to machine operators in Japan since 1974; for a long time this constituted the basis for all safety provisions. In April 2010 this law was supplemented by Paragraph 28-2. This paragraph stipulates that the operator of machinery and installations must determine and document the respective sources of danger and hazardous substances. He must similarly document the safety measures that he takes. In concrete terms this means: the operator must deploy and provide evidence of a methodical risk assessment. This provides good legal protection for the operating companies, similar to that covered by the directives aimed at operating companies at EU level. Therefore the rule that applies here is once again that operators must basically meet their obligations.

The most important Japanese regulations pertaining to the manufacturer and operator level were introduced in 2006 and 2007. This means that European manufacturers were able to gain experience in the area of machinery safety and functional safety at a much earlier date. For this reason both the safety standard of European machinery and the products and systems of European manufacturers of safety components are valued by Japanese industry. The fact that the EU was committed at an early date to establishing common standards for machinery safety and also put this objective into practice is paying off here.



**CHINA: has adapted parts of the set of standards**

China has developed its own set of standards on machinery safety that is likewise partially based on national or European standards. The general requirements placed on electrical installations of industrial machinery that correspond to IEC 60204-1 are therefore specified in GB/T 55226.1. Other safety requirements are defined in the standards GB/T 15706.1 and GB/T 15706.2 which are modelled closely on the old European standards EN 292-1 and EN 292-2. There is also an equivalent of ISO 13849-1 – GB/T 16855 – indicating a similar trend towards internationalisation of standardisation. Without doubt this ben-

efits European machinery and plant engineering companies that export to China.

One must, however, qualify this on the component side by adding that trade obstacles exist from a European point of view in the form of national acceptances. An example is the “China Compulsory Certificate” (CCC), a mandatory certificate applying to diverse product groups and in particular to electrical and electronic products and to products in the automobile sector. CCC certification is especially important, however, when it is necessary to send components or spare parts to China.





### **Russian machinery directive**

On 27.12.2002 President Putin signed the Russian Federation law (No. 184-F3) on technical regulation (in brief: TechRegG) passed by the Russian Parliament on 15.12.2002. During the transition period of 7 years provided, the previous requirements for the mandatory certification and approval (GOS R-certification) of technical products and those requirements currently still valid are being newly regulated. The legally binding safety requirements for products will be specified in so-called “Technical Regulations” (TR) and must be passed as Federation law.

Pursuant to Article 9 TechRegG, 16 “Technical Regulations” were issued during 2010. The following regulations are of particular significance to industry:

- Machinery and installations
- Low voltage equipment
- Buildings and structures
- Elevators
- Power supply stations and grids
- Installations operating under high pressure
- Electromagnetic compatibility (EMC)
- Rail vehicles
- Medical devices
- Personal protective equipment (PPE)
- Equipment driven with gas-like fuel
- Equipment in a potential explosive environment

Some of these “Technical Regulations” have a similar structure to new approach European EC

directives, apart from the obligatory certification which is nevertheless required in Russia.

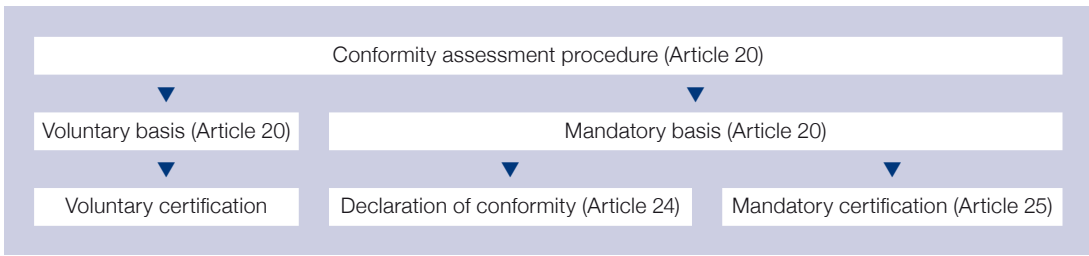
One highly significant regulation for those interested in exporting to Russia is the TR on the “Safety of machinery and installations” that was passed on 15 September 2009 and came into force on 1 October 2010. Unlike the “Fire protection” TR for example that came into force on 1 May 2009, this TR follows the European new approach.

### **The technical regulation on the safety of machinery and installations**

The Russian government regards this regulation to be one of the most important and paramount regulations to be enacted. Following a serious accident in the largest Russian hydro-electric power station, it decided to introduce more stringent regulations to monitor potentially hazardous manufacturing plant, power generating equipment, machinery and installations.

In a similar manner to the European Machinery Directive 2006/42/EC, the TR on machinery protection has an Annex 1 with general health and safety requirements, although unfortunately these have nowhere near the level of detail of those in the European Machinery Directive. Concrete technical requirements are described in the national GOST standards. While electro-technical IEC standards are increasingly being transferred to GOST standards, this is by no means the case in all areas and not as actually desired in the ISO area. The reason for this is





**Fig. 4** Conformity assessment

that Russian industry recognises no need to participate actively in standardisation work and is strongly “state oriented”. Consequently in individual cases it may be necessary to pay for expensive translations of GOST standards or to attempt to obtain such documents from the foreign standard service (Auslandsnormenservice – ANS) of the Beuth-Verlag ([www.beuth.de](http://www.beuth.de)). A tool for researching, monitoring and archiving complete texts is also available from the GLOBALNORM professional database ([www.globalnorm.de](http://www.globalnorm.de)).

The above legal provision for machinery is divided into the following sections:

1. General provisions
2. Safety requirements for machinery and installations during planning, production, transport and storage
3. Conformity assessment (as shown in Figure 4)
4. State supervision/checks
5. Final stipulations and transitional provisions.

The conformity assessment procedure on a mandatory (legally binding) basis offers two possibilities:

- the declaration of conformity and
- mandatory certification.

To prevent giving any wrong impression, it is important to state that the declaration of conformity cannot be compared to the self declaration procedure in Europe.

What is more, the declaration of conformity according to the Russian version is only valid for five years. In addition it must be registered at the “Federal Agency for Technical Regulation and Metrology” and therefore once again in effect corresponds to certification.

Nevertheless, it is helpful when accessing the Russian market if the person placing the product on the market can produce proof of conformity with the European Machinery Directive. However the certification authority (there are only two officially accredited certification authorities based in Germany, all others are agencies) will not recognise an EU declaration of conformity if no technical documentation with risk assessment, test reports, EMC verification etc. can be presented.





## Summary

To summarise, this overview illustrates the prevailing global trend towards harmonising standards. Apart from the ISO and IEC standards which by definition apply worldwide, individual countries also adopt directives and standards that have been tried and tested in other markets or use these as a basis. The European regulatory framework points the way here because it was created at a very early date and has been proven in practice. This benefits the export business of European machine and plant engineering manufacturers who can assume, with a few exceptions, that EU standards and directives will also be accepted beyond the direct jurisdiction of the EU as indicated above in the case of China and Japan, and also Brazil, certain Canadian provinces, Korea, India and Australia.

Of course several national regulations persist despite all efforts towards the internationalisation of rules and standards. Machine manufacturers or exporters who supply to non-EU countries are therefore well-advised to obtain information about the applicable requirements in each case.

## Footnotes:

- [1] This article is based on various publications in the MRL-News and in trade papers, including those written by Mr. **Michael Loerzer**, the Managing Partner of GLOBAL-NORM GmbH, Berlin ([www.globalnorm.de](http://www.globalnorm.de)), an enterprise that has specialised in researching international standards.
- [2] EEA (loc cit) = 27 EU Member States + Iceland + Liechtenstein + Norway + Switzerland (+ Turkey)
- [3] See the EU “Blue Guide” (Guide for implementing directives drawn up according to the new approach and global approach)
- [4] [www.osha.gov/pls/oshaweb/owastand.display\\_standard\\_group?p\\_toc\\_level=1&p\\_part\\_number=1910](http://www.osha.gov/pls/oshaweb/owastand.display_standard_group?p_toc_level=1&p_part_number=1910)

*Chapter 2:*

***New requirements placed on safety-related parts of control systems (replacement of EN 954-1 and standard successor EN ISO 13849-1:2006/2008)***



# EN ISO 13849-1: New category principle for machine safety

The “category principle” for safety-related control systems belongs in the past: the familiar control categories in EN 954-1:1996 have been replaced by performance levels from the standard EN ISO 13849-1:2008 (2006) and must be used by the end of 2011 at the latest to comply with the standardisation proposals to achieve safe safety-related parts of machine control systems. What changes result for design engineers and safety engineers?

Many design engineers and planners of machines and machinery will ask why we need a new standard in place of the control categories. Is the safety level too low so that it needs to be raised using new standards? This question can reassuringly be answered in the negative. The revision of EN 954-1 can be put down to other reasons.

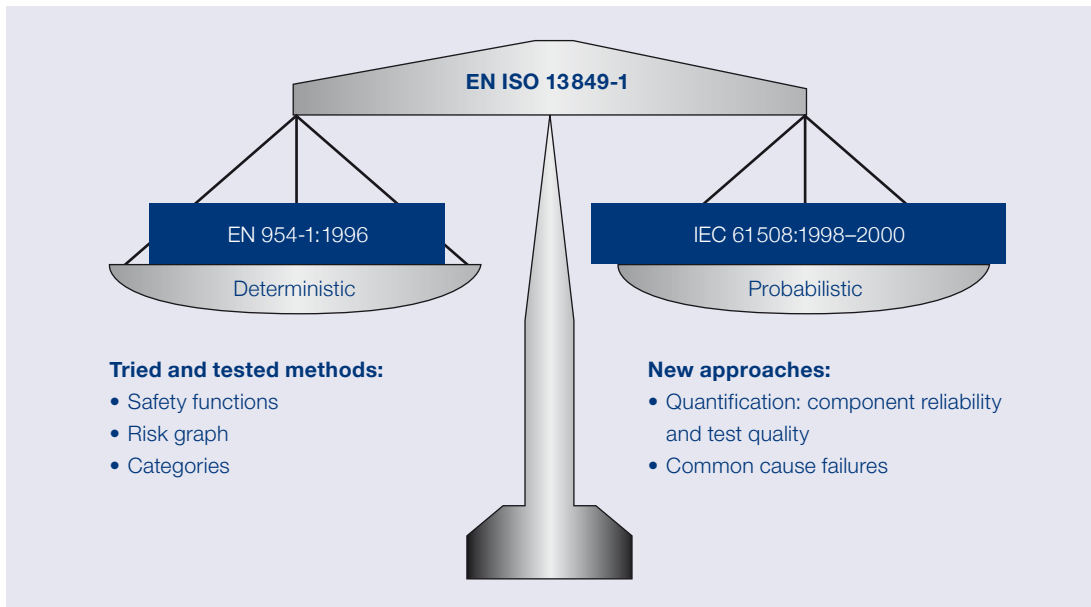
## Harmonisation of international standards

One rather formal aspect is the fact that there have long been aspirations to align standards at an international level in accordance with European harmonisation, i.e. in this case to IEC 61 508. In addition the EU standards committees

have agreed to continuously adjust standards in line with technical progress. This made sense for EN 954-1 because it had taken inadequate consideration of programmable electronic systems with safety function, for example. While IEC 62061:2005 (2008), a comparable “new” standard based on IEC 61 508 existed already, it concentrates completely on electrics and electronics. Therefore a “genuine” cross-technology replacement was required for EN 954-1 that is compatible with IEC 61 508.

What is more, EN 954-1 was repeatedly criticised. A central point of criticism was the fact that this standard pursues a deterministic approach. This means that the safety systems were regarded as “static” and constant. A probabilistic approach is more practice-oriented, and also takes into account the probability of failures of the individual components and therefore the overall system (as shown in Figure 1).

All of these points led to a decision by the standards committees to replace EN 954-1 with a new standard, the EN ISO 13849-1. Without any exaggeration, we can say that a number of



**Fig. 1** The new EN ISO 13849-1 also incorporates a probabilistic approach. A frequent criticism of EN 954-1, that of its purely deterministic approach, has therefore been addressed.

changes have taken place for the design engineers of machines and machinery.

**First step:**

**Establishing the hazard potential**

As before, when designing safety-related parts of control systems it is firstly necessary to establish the potential danger using a modified risk graph. Then come the changes: the risk analysis does not produce one of the familiar old control categories, but one of five “performance levels” (PL “a” to “e”) which reflect different amounts of residual risk (as shown in Figure 2). This residual risk is quantified as a PFH<sub>d</sub> value (Probability of dangerous Failure per Hour). Therefore probabilistics play a role here.

The performance level determined in this manner is also expressed as PL<sub>r</sub>, where “r” stands for “required”, i.e. this is the required performance level. The design engineer therefore now knows which PL should be achieved to put together a protective device (a safety-related part of a control system) that complies with the standard.

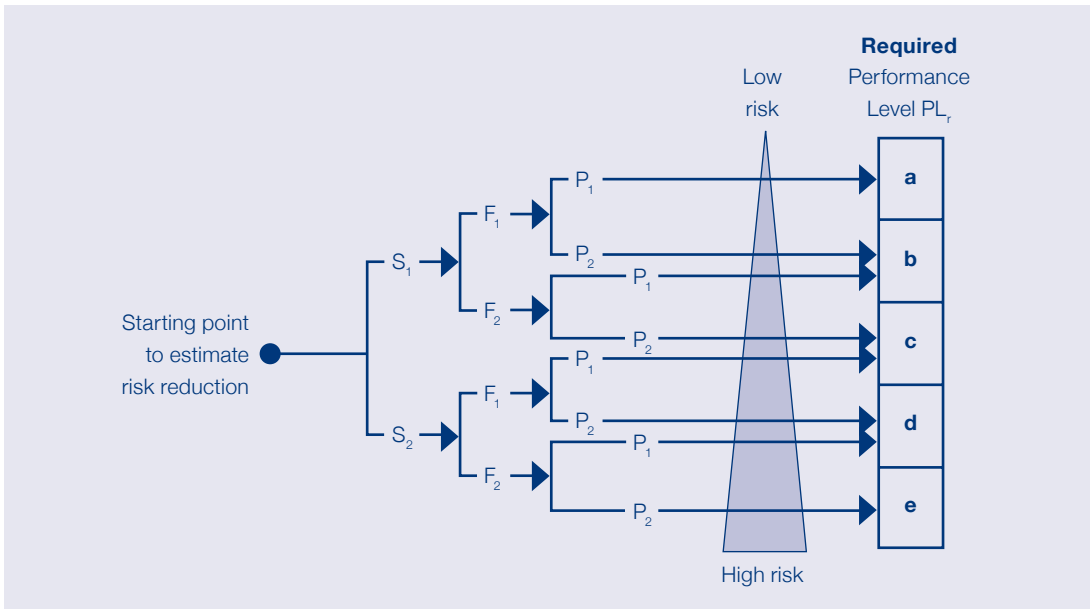
Another new element is the fact that PLs cover far more properties than the previous control categories. The values for MTTF<sub>d</sub> (mean time between safety-relevant faults or failures), diagnostic coverage (DC) and measures to prevent failures with common cause and effect (CCF for Common Cause Failure) are defined for each

separate PL. In this manner, probabilistic factors are incorporated in the estimation of the performance level.

Up to this point the design engineer only knows which performance level he should aspire to. How does he implement this knowledge in the practical design process? To answer this question one must consider the approach from a different angle. Manufacturers of safety switching devices and safety-oriented control systems have already prepared themselves for the new standard situation, taking IEC 61508 into consideration during design to achieve the so-called safety integrity level (SIL). These SILs provide the technical data using which the performance levels can be estimated. The compatibility of the new standard is moreover indicated by the fact that performance levels are each assigned to safety integrity levels. For example SIL 2 corresponds to PL “d”.

**Consideration of risk for the entire safety chain**

These values are specified in the product documents of the safety components so that the design engineer can select appropriate components. Because a safety chain always consists of several components (sensors, controller, actuator) he must combine values to produce an overall PL. This is the “actual” PL which must then be



**Fig. 2** Diagram showing modified risk graph. S = Severity of the injury; F = Frequency and/or duration of the exposure to danger; P = possibilities for preventing the danger

compared to the required  $PL_r$ . If the calculated PL is as great or greater than the  $PL_r$ , then the safety circuit has been constructed in compliance with the standard.

### Validation is included

Another new aspect is that of validation: EN ISO 13849-2 sets out a validation plan, and it is recommended that this is followed when estimating the performance level. This makes it easier to objectify the approach when selecting components and configuring the safety chain. The procedure must furthermore be documented, something also recommended in EN ISO 13849-2.

### Helpful: Designated Architectures

The so-called “Designated Architectures” to be applied in accordance with the new standard are also helpful when constructing the safety circuit. These concern pre-calculated structures of the safety-related parts of control systems that are already familiar from the application of EN 954-1. These pre-calculations do not, however, absolve the design engineer from the task of incorporating the specified parameter values for  $MTTF_d$ , DC and CCF into the calculation of the performance level.

### The standard is more complicated

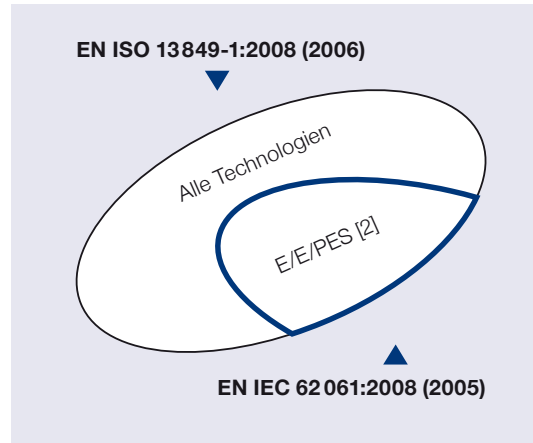
The consequence of this is that the design engineer in mechanical engineering needs to come to grips with this standard, and should take some time to do so, because EN 13849-1 is significantly more complex than EN 954-1. Discussions will certainly follow on whether, considering the high safety level found in machinery today, the trend of extending standards for machinery safety is a step in the right direction.

### Transitional problems cannot be ruled out

Moreover problems are to be expected when application of the new standard begins because, for example, some manufacturers of safety components have not yet calculated the necessary data required by their customers – the design engineers of machines and machinery. Additionally the more complex steps required when selecting the protective device that complies with the standard may present difficulties. But help is at hand: loc. cit.

### Excuse: EN IEC 62061:2008 (2005)

Although for practical reasons we recommend that our customers base their future design of



safety-related parts of control systems (SRP/CS) on standard EN ISO 13849-1, we would like to point out here that it is possible to use a different standard, namely EN IEC 62061:2008 (2005). This new standard, which has the title “Functional safety of safety-related electrical, electronic and programmable electronic systems (E/E/PES), also affects the area of “SRP/CS”; it has been introduced and can be viewed as an alternative to EN 954-1 and EN ISO 13849-1. EN IEC 62061 is derived directly from EN IEC 61508, and considers the control systems of the E/E/PES technologies (= SRECS [1]), and assesses them as safety integrity levels (SILs) or SILCLs (SIL claim limits). EN IEC 62061 has similarly been harmonised under the umbrella of the EC Machinery Directive since 2007 and can be applied as an alternative to EN ISO 13849-1.

Competency disputes that existed between the standards organisations ISO (CEN) and IEC (GENELEC) were responsible for the fact that there are now two standards for this area. As if the new approach combining deterministic and probabilistic analysis did not present enough of a challenge to users, this then adds to the confusion, at least at the beginning (*confusion, but on a higher level*).

The reason why we prefer EN ISO 13849-1 for our customers is because this standard also includes the technologies of “mechanics”, “hydraulics” and “pneumatics”, and also pays greater attention to the area of “electromechanics”. We also believe that EN ISO 13849-1 is easier to understand and use. Furthermore nothing is lost when the decision is made in favour of EN ISO 13849-1 because PL and SIL are essentially compatible with each other and the

idea behind them is also largely the same. Nevertheless there may be applications, e.g. very complex structures or in-house development of control systems, for which EN IEC 62061 is more suitable.

Footnotes:

- [1] **Safety-Related Electrical Control Systems (SRECS)**
- [2] **Electrical/Electric/Programmable Electronic Systems (E/E/PES)**



# New requirements placed on the design of safety-related parts of machine control systems

The new requirements placed by standard EN ISO 13849-1:2008 (2006) [1] on the design of safety-related parts of control systems [2] for products falling within the scope of the EC Machinery Directive add to the amount of “homework”. But the new standard also offers greater design scope. For example an arrangement that leads to a required control category 2 on the basis of EN 954-1:1996 will in future have five different design possibilities within performance level “c”. Even in the case of PL “d”, which until now has been comparable with control category 3, there are four possibilities.

The reason is that, in addition to the so-called Designated Architectures (i.e. the previous control categories which are also referred to as “Architecture”), the reliability of the hardware used (expressed as  $MTTF_d$  / Mean Time to dangerous Failure) as well as the efficacy of fault detection

measures (expressed as DC/Diagnostic Coverage) are also included as further relevant factors when estimating a performance level (in addition to an assessment of the so-called Common Cause Failure measures as from control category 2. Loc. cit.).

The new standard can be used here and now (it was incorporated in the list of standards under the umbrella of the MD in the 2<sup>nd</sup> quarter of 2007), although there is a transition period which, following a disputed extension, runs until December 2011 during which EN 954-1:1996 can still be used (as shown in Figure 1). EN ISO 13849-1 can be procured from the respective standard publishers (in Germany this is [www.beuth.de](http://www.beuth.de)).

## What is a performance level (PL)?

In simple terms, a PL is the safety-related overall quality (integrity) of a safety-related part of a

On publication of the Official Journal C 321/18 of the European Union dated 29.12.2009, the controversial discussion on extending the presumption of conformity of standard EN 954-1:1996 was resolved at the last minute. According to this, EN 954-1:1996 can basically still be used as harmonised standard with presumption of conformity until 31 December 2011 if the user has not yet converted to the requirements of the new standard. This means that up to this deadline, there is a choice of three standards when designing safety-related parts of machine control systems:

1. The “old” standard EN 954-1:1996;
2. The successor standard EN ISO 13849-1:2008 (2006);
3. Optionally (however only for electrical, electronic and programmable electronic systems) EN IEC 62061:2008 (2005) [a, b].

[a] “Functional safety of safety-related electrical, electronic and programmable electronic systems”

[b] The competency disputes mean that two standards are actually competing to succeed EN 954-1:1996. We recommend that manufactures of machinery falling within the scope of the MD use EN ISO 13849-1:2008 (2006) because this standard deals with all technologies (including electromechanics, mechanics, hydraulics and pneumatics) and, in our subjective opinion, is easier to use in the case of more complex structures. As such we concentrate on this standard in our presentation. However both standards are largely compatible with each other.

(ISO/IEC)	Reference and title of the harmonized standard and reference document	Date publication (0)	Reference of superseded standard	Date of cessation of application or conformity of superseded standard
CEN	EN ISO 13849-1:2008 + A2:2009 Safety-related parts of control systems – Part 1: General principles for design (ISO 13849-1:2008)	This is the first publication		
CEN	EN 954-1:1996 + A2:2009 Safety-related parts of control systems – Part 1: General principles for design (EN 954-1:1996)	This is the first publication		
CEN	EN ISO 13849-1:2008 + A1:2009 Safety-related parts of control systems – Part 1: General principles for design (ISO 13849-1:2008)	8.9.2009	EN 954-1:1996 + A1:2009	31.12.2011 (*)

\*) The date of cessation of presumption of conformity of the superseded standard (initially fixed as 31.12.2009) has been postponed for two years.

†) ISO: International Organization for Standardization  
 IEC: International Electrotechnical Commission  
 EN: European Norm  
 CEN: European Committee for Standardization  
 CEI: Comitato Elettrotecnico Italiano  
 DIN: Deutscher Normenausschuss  
 AFNOR: Association Française de Normalisation  
 BSI: British Standards Institution  
 AENOR: Asociación Española de Normalización  
 UNI: Ente Nazionale Italiano di Unificazione  
 CEN: European Committee for Standardization  
 CENELEC: European Committee for Electrotechnical Standardization  
 ETSI: European Telecommunications Standards Institute  
 EC: European Commission  
 EC: European Commission  
 EC: European Commission

Fig. 1 Extension of the presumption of conformity of EN 954-1:1996



Only from 2012 does EN 954-1:1996 then lose its special status, whereby market surveillance authorities doubting the conformity of a machine or other product within the scope of the MD must first assume that the statutory protective objectives of the EC Machinery Directive (as from 29.12.2009: 2006/42/EC) have been correctly interpreted and substantiated due to the application of a harmonised standard (a standard with presumption of conformity). This means that up to that time, if it came to the worst, the person responsible would have the legal advantage of a shift in the burden of responsibility (burden of proof) and only lose this on the above deadline.

However the extension of the presumption of conformity of EN 954-1:1996 has not been welcomed by all, as implied above. Rather the decision in Brussels has attracted hefty criticism from professional circles who assume, probably correctly, that this was backed by lobbying on the part of European mechanical engineering associations. Presumably arguments were centred on the expenditure required to switch standards in the light of the crisis in the sector at that time, as well as that some figures were still missing from suppliers and that some important questions regarding practical implementation had not yet been clarified. It is understandable that those who, despite this, “jumped through hoops” to complete the changeover in time, feel they have been duped.

The message from legal circles must also be taken into consideration in this context that, in cases of doubt the status issue of a standard (whether it is harmonised or not) can be ousted from primacy of the EC Machinery Directive together with the requirement to realise the respective “state of the art” (possibly also the “state of science and technology under product liability considerations). In this respect EN 954-1, a standard originating from 1996, certainly has weaknesses here and there that make it advisable to switch to the new requirements as quickly as possible.

**Fig. 1** Extension of the presumption of conformity of EN 954-1:1996 (continued)

control system (SRP/CS) taking into consideration the SRP/CS architecture (= deterministic approach) and the SRP/CS reliability (= probabilistic approach). The main aspects incorporated are safety-related reliability, resistance to failures and faults, fault tolerance, behaviour in the event of a fault, fault detection, prevention of fault accumulations and prevention of systematic faults.

The required PL of a safety function ( $PL_r$ , “a” ... “e”) results from the risk graph analysis of a safety function as shown in Figure 2 or from the respective C-standard.

From a mathematical probability point of view the average probability of a dangerous failure per hour  $PFH_d$  [3] is behind a performance level PL as shown in Figure 3.

To give you an idea,  $PFH_d$  values can also be “translated” as shown in Figure 4.

It will be clear by now at the latest that in future there is a common factor for PL (or EN ISO 13849-1) and safety integrity level SIL (or EN IEC 62061 and EN IEC 61508-1/-7) (loc. cit.),

namely the  $PFH_d$  value. This means a PL can be expressed as SIL and an SIL as PL (whereby the conversion from SIL to PL is only possible if the SRP/CS architecture corresponds to EN ISO 13849-1). Common assessment benchmark is the probability of a dangerous failure per hour ( $PFH_d$ ) as shown in Figure 5.

One could say that the parameters explained below in greater detail for determining the PL can be seen as nothing other than simplifying variables to circumvent the complex mathematics behind a  $PFH_d$  value.



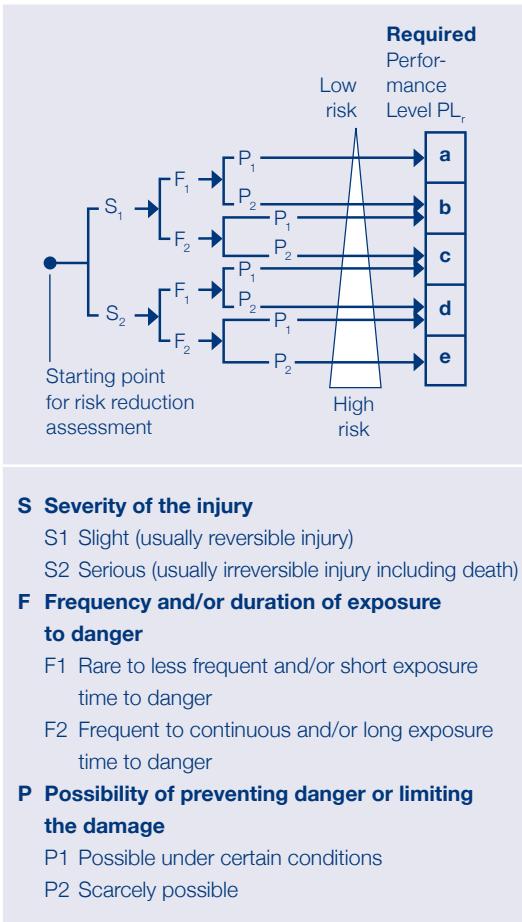


Fig. 2 Risk graph of EN ISO 13849-1:2008 (2006)

Performance Level (PL)	Average probability of a dangerous failure per hour(1/h)
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

NB: Other measures are necessary to achieve the PL in addition to the average probability of a dangerous failure per hour (loc. cit.).

Fig. 3 PL classification of a safety function dependent on the PFD<sub>d</sub> value (average probability of a dangerous failure per hour (1/h))

Performance Level (PL)	Max. tolerated failure level
a	1 dangerous failure per 10.000 hours
b	1 dangerous failure per 100.000 hours
c	1 dangerous failure per 333.000 hours
d	1 dangerous failure per 1.000.000 hours
e	1 dangerous failure per 10.000.000 hours

Fig. 4 Fig. 4 Attempt at a practical interpretation (however always related to a number of [collective] items of hardware [not to be understood as relating to an individual case])

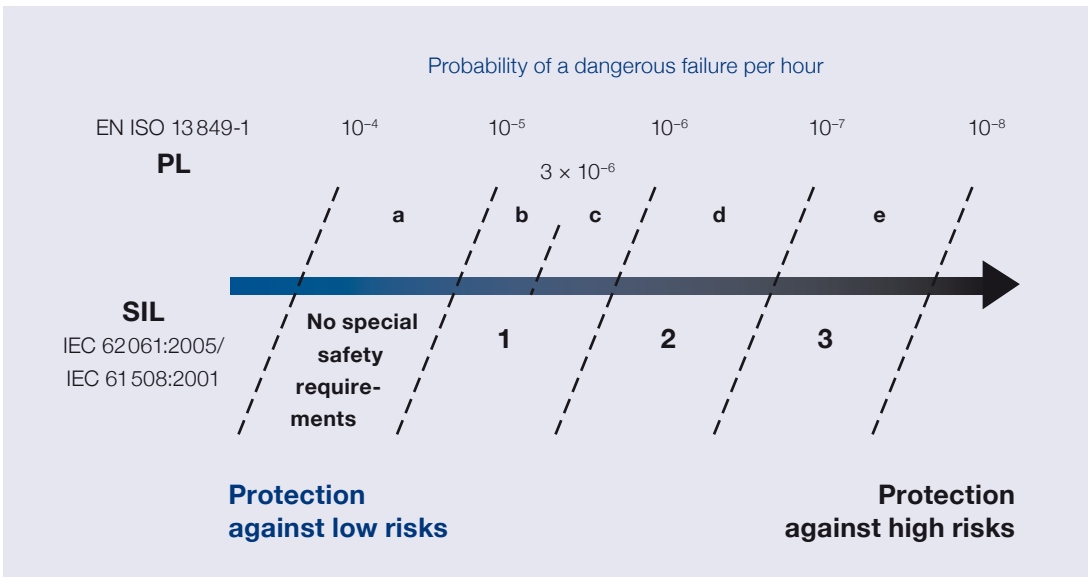


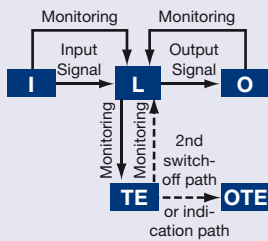
Fig. 5 PL ↔ SIL compatibility table

- The following are designated (1):
  - Control category B ... 4 (Designated Architectures): classification of safety-related parts of a control system in terms of its resistance to faults and subsequent behaviour in the event of a fault
- Fault exclusions in accordance with EN 13849-2 continue to be important or necessary

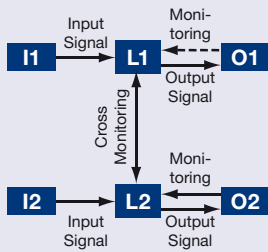
### Categories B and 1



### Category B



### Categories 3 and 4



- Caution: Changes in CC 2!

**Fig. 6** Diagram of the designated architectures (control categories)

Accordingly a PL comprises the following:

- **Architecture** (= CC/control category)  
Brief explanation: architecture of an SRP/CS (1-channel, 1-channel with testing, 2-channel with mutual testing, 2-channel with self diagnosis) for the chain [I] (Inputs) + [L] (Logic = signal processing) + [O] (Outputs), whereby EN ISO 13849-1 favours certain architectures, namely those of the familiar control categories, with the possibility of also being able to achieve fault exclusion in compliance with EN ISO 13849-2:2008 (2003) [4]. While other architectures are “permitted” under EN ISO 13849-1, the simplified calculation approach cannot be used for them as a matter of course so that recourse must be made to more precise

mathematics and therefore also to the effort this entails.

In addition to taking the architectures of an SRP/CS into consideration as discussed above, the requirements placed on a control category also include paying attention to the so-called (a) basic and (b) proven safety principles. Basic safety principles correspond to the state of the art and must fundamentally be taken into consideration (from control category B); in addition, as from control category 1 it is necessary to consider proven safety principles. Please do not confuse this with the requirement to use components that have been proven from a safety-related point of view (applies only to CC 1)! You can find the differences between the two in Annexes A to D of EN ISO 13849-2 (validation of SRP/CS).

- **Hardware reliability**

(=  $MTTF_d$  / Mean Time to dangerous Failure)  
Brief explanation: mean time, expressed in years (y) up to a dangerous (random) failure amount of an SRP/CS channel; the individual  $MTTF_d$  values of the hardware used per chan-

- The following are designated (2):
  - $MTTF_d^*$  per channel as total of the individual  $MTTF_{di}$ s of [I] + [L] + [O] and divided into the 3 groups “low”, “medium” and “high”

\* Mean Time to Dangerous Failure: mean value for the estimated operating time during which an individual channel of a system will have no dangerous failure.

- Expressed more simply: safety-related statistical hardware quality (derived from reliability)
- The so-called parts count method is used to calculate  $MTTF_d$  values in EN ISO 13849-1:2008 (2006)

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

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

**Fig. 7** Hardware reliability (keyword summary)

nel should be determined, possibly added (using the parts count method) and compared with the “low”, “medium” and “high” requirements in the standard.  $MTTF_d$  values are based on manufacturer information or information from pertinent reference works, e.g. SN 29500. But EN ISO 13849-1 also includes those data.

**CAUTION:**  $MTTF_d$  data only make a statistical statement on the survival probability of a large quantity of a product (statement that only 37% “survive” at this time). The reciprocal value  $1/MTTF_d$  is the failure probability per hour, that is also termed the  $\lambda$  or FIT value (for  $10^{-9}$  failures). The mathematical probability theory in the background is exponential distribution.

No direct  $MTTF_d$  values are available for hardware subject to wear due to its technology, such as is the case with electromechanics, hydraulics, mechanics or pneumatics [5]. A previous, so-called  $B_{10d}$  value approach is necessary here, i.e. the  $MTTF_d$  value is calculated using a  $B_{10d}$  value taking into consideration an estimated number of switching cycles and a statistical correction factor of 0.1 according to a formula (as shown in Figure 8):

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

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

$n_{op}$  = mean number of switching cycles per year  
 $d_{op}$  = average number of operating days per year  
 $h_{op}$  = average number of operating hours per day  
 $t_{cycle}$  = average requirement of the safety function in s (for example  $4 \times$  per hour =  $1 \times$  per 15 min. = 900 s)

**Fig. 8** Conversion of a  $B_{10d}$  value to an  $MTTF_d$  value

An additional step in connection with the use of technology subject to wear is the consideration of possible premature replacement of such hardware as preventive maintenance measure. We also term this a  $T_{10d}$  value method: If 10% of the  $MTTF_d$  value calculated according to the above formula is below 20 years

(y) (= the normative assumed mission time for a machine), the standard recommends replacement of the component after this time. Example: a device might have an  $MTTF_d$  value of 50 years on the basis of a  $B_{10d}$  value consideration. 10% ( $T_{10d}$ ) of 50 years would then be 5 years, i.e. the operating manual would point out that the device must be replaced every 5 years.

• **Diagnostic coverage**

(= DC/Diagnostic Coverage in %)

Brief explanation: probability-based extent of diagnostic efficacy (fault detection), which expresses the ratio between noticed dangerous failures and the total number of dangerous failures. However this ratio is also weighted using the  $MTTF_d$  value of the respective component. This means that it is not necessary to monitor components with a high  $MTTF_d$  to the same extent as those with low  $MTTF_d$ . 90% DC for example means that there is a 90%

- The following are designated (3):
  - $DC_{avg}$  of the complete SRP/CS (divided into 4 groups: “none”, “low”, “medium” and “high” = result of the efficacy of the individual DCs of [I], [L] and [O])
- Expressed more simply: efficacy/reliability of failure detecting measures expressed as a percentage ( $DC_{avg}$  calculation using formula).
- Assistance in EN ISO 13849-1:2008 (2006): look-up-tables
- Diagnostic coverage: fraction of the probability of dangerous failures  $\lambda_{dd}$  compared to the probability of all dangerous failures  $\lambda_d$ .

Qualification	Value ranges
Insufficient	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

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

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_d} \quad \begin{array}{l} \text{Probability of detected dangerous failures} \\ \text{Probability of total dangerous failures} \end{array}$$

**Fig. 9** Diagnostic coverage (keyword summary)



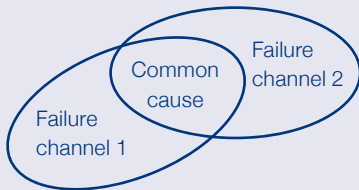
probability of dangerous faults being discovered (in good time) while 10 % will not be discovered (in good time) (in good time = discovery before so-called probability of a second fault occurring).

Evaluation suggestions for different measures for [I], [L] and [O] can be found in Annex E of EN ISO 13849-1; if necessary a specific formula can be used to calculate a mean  $DC_{avg}$  for a complete SRP/CS (“avg” stands for “average”).

- **Common Cause Failure Management (CCF)**  
Brief explanation: measures to prevent failures of both channels in an SRP/CS at the same



- The following are designated (4):
  - CCF measures (determining YES or NO, only as from control category 2): common cause failure: failures in diverse units due to a single event, and where these failures have no mutual impact
- Determination of measures in [I], [L] and [O] according to the look-up table (at least 65 of a possible 100 points must have been achieved)



No.	Measure to prevent CCF	Points
<b>1</b>	<b>Separation/disconnection</b>	
	Physical separation between the signal paths	15
<b>2</b>	<b>Diversity</b>	
	Different technologies/design or physical principles are used	20
<b>3</b>	<b>Design/application/experience</b>	
3.1	Protection from overvoltage, excess pressure, overcurrent etc.	15
3.2	Use of tried and tested components	5
<b>4</b>	<b>Evaluation/analysis</b>	

**Fig. 10** Common Cause Failure measures (keyword summary)

time resulting from a common cause, e.g. bridging of both channels by a foreign influence, overheating, by lightning (surge pulse) with redundant semiconductor outputs, contaminated oil in hydraulics or too much water in the air in the case of pneumatics. This means that a single cause removes the multichannel capability (typically the redundancy). The Annex to EN ISO 13849-1 contains a table with measures to prevent Common Cause Failures. Each measure has a point score. Measures should be realised that score  $\geq 65$  points out of a possible 100.

Added to these are measures to prevent systematic failures and faults in the SRP/CS.

- **Result**

One can either use a results graph/bar chart (as shown in Figure 11) to read off the PL achieved or, if more precise results are required, one can refer to Annex K of EN ISO 13849-1 (as shown in Figure 12) which produces a precise numerical assignment between  $PFH_d$  and PL parameters.

Example: if there is an SRP/CS with a architecture corresponding to control category 3 (redundancy with appropriate fault detection) and if quantification of the efficacy of fault detection measures achieves and corresponds to a diagnostic coverage DC of “medium”, the hardware reliability  $MTTF_d$  realised determines whether a PL of “e” ( $MTTF_d = \text{very high} = \geq 62$  y), “d” ( $MTTF_d = \text{high}$ ), “c” ( $MTTF_d = \text{medium}$ ) or “b” ( $MTTF_d = \text{low}$ ) has been attained. The CCF measures must fundamentally be satisfied.

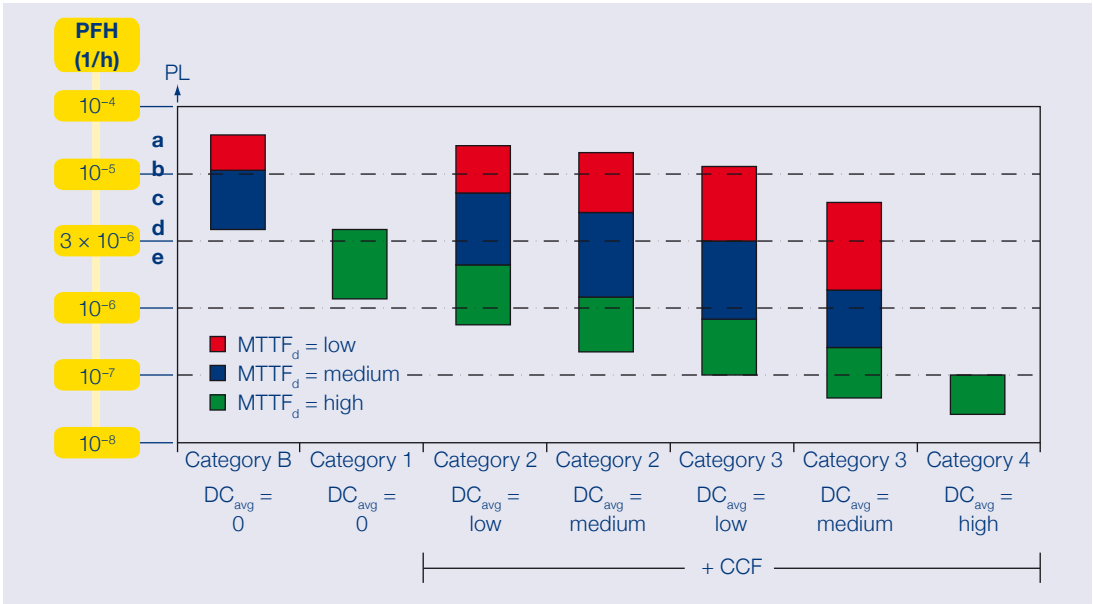
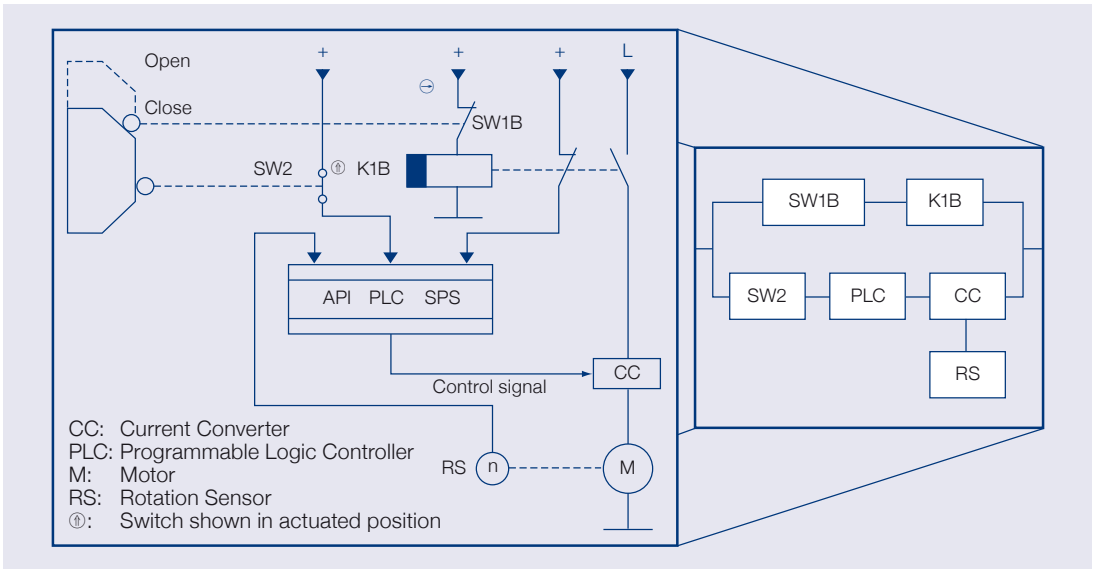


Fig. 11 Result graph/bar chart

Table K.1 – Numerical representation of Figure 5 (from EN ISO13849-1:2006 [D] – Annex K (informative))

MTTF <sub>d</sub> for each channel	Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
Years	DC <sub>avg</sub> = none		DC <sub>avg</sub> = none		DC <sub>avg</sub> = low		DC <sub>avg</sub> = medium		DC <sub>avg</sub> = low		DC <sub>avg</sub> = medium		DC <sub>avg</sub> = high	
3	3.80 × 10 <sup>-5</sup>	a			2.58 × 10 <sup>-5</sup>	a	1.99 × 10 <sup>-5</sup>	a	1.26 × 10 <sup>-5</sup>	a	6.09 × 10 <sup>-6</sup>	b		
3.3	3.46 × 10 <sup>-5</sup>	a			2.33 × 10 <sup>-5</sup>	a	1.79 × 10 <sup>-5</sup>	a	1.13 × 10 <sup>-5</sup>	a	5.41 × 10 <sup>-6</sup>	b		
3.6	3.17 × 10 <sup>-5</sup>	a			2.13 × 10 <sup>-5</sup>	a	1.62 × 10 <sup>-5</sup>	a	1.03 × 10 <sup>-5</sup>	a	4.86 × 10 <sup>-6</sup>	b		
3.9	2.93 × 10 <sup>-5</sup>	a			1.95 × 10 <sup>-5</sup>	a	1.48 × 10 <sup>-5</sup>	a	9.37 × 10 <sup>-6</sup>	b	4.40 × 10 <sup>-6</sup>	b		
4.3	2.65 × 10 <sup>-5</sup>	a			1.76 × 10 <sup>-5</sup>	a	1.33 × 10 <sup>-5</sup>	a	8.39 × 10 <sup>-6</sup>	b	3.89 × 10 <sup>-6</sup>	b		
4.7	2.43 × 10 <sup>-5</sup>	a			1.60 × 10 <sup>-5</sup>	a	1.20 × 10 <sup>-5</sup>	a	7.58 × 10 <sup>-6</sup>	b	3.48 × 10 <sup>-6</sup>	b		
5.1	2.24 × 10 <sup>-5</sup>	a			1.47 × 10 <sup>-5</sup>	a	1.10 × 10 <sup>-5</sup>	a	6.91 × 10 <sup>-6</sup>	b	3.15 × 10 <sup>-6</sup>	b		
5.6	2.04 × 10 <sup>-5</sup>	a			1.33 × 10 <sup>-5</sup>	a	9.87 × 10 <sup>-6</sup>	b	6.21 × 10 <sup>-6</sup>	b	2.80 × 10 <sup>-6</sup>	c		
6.2	1.84 × 10 <sup>-5</sup>	a			1.19 × 10 <sup>-5</sup>	a	8.80 × 10 <sup>-6</sup>	b	5.53 × 10 <sup>-6</sup>	b	2.47 × 10 <sup>-6</sup>	c		
6.8	1.68 × 10 <sup>-5</sup>	a			1.08 × 10 <sup>-5</sup>	a	7.93 × 10 <sup>-6</sup>	b	4.98 × 10 <sup>-6</sup>	b	2.20 × 10 <sup>-6</sup>	c		
7.5	1.52 × 10 <sup>-5</sup>	a			9.75 × 10 <sup>-6</sup>	b	7.10 × 10 <sup>-6</sup>	b	4.45 × 10 <sup>-6</sup>	b	1.95 × 10 <sup>-6</sup>	c		
8.2	1.39 × 10 <sup>-5</sup>	a			8.87 × 10 <sup>-6</sup>	b	6.43 × 10 <sup>-6</sup>	b	4.02 × 10 <sup>-6</sup>	b	1.74 × 10 <sup>-6</sup>	c		
9.1	1.25 × 10 <sup>-5</sup>	a			7.94 × 10 <sup>-6</sup>	b	5.71 × 10 <sup>-6</sup>	b	3.57 × 10 <sup>-6</sup>	b	1.53 × 10 <sup>-6</sup>	c		
10	1.14 × 10 <sup>-5</sup>	a			7.18 × 10 <sup>-6</sup>	b	5.14 × 10 <sup>-6</sup>	b	3.21 × 10 <sup>-6</sup>	b	1.36 × 10 <sup>-6</sup>	c		
11	1.04 × 10 <sup>-5</sup>	a			6.44 × 10 <sup>-6</sup>	b	4.53 × 10 <sup>-6</sup>	b	2.81 × 10 <sup>-6</sup>	c	1.18 × 10 <sup>-6</sup>	c		
12	9.51 × 10 <sup>-6</sup>	b			5.84 × 10 <sup>-6</sup>	b	4.04 × 10 <sup>-6</sup>	b	2.49 × 10 <sup>-6</sup>	c	1.04 × 10 <sup>-6</sup>	c		
13	8.78 × 10 <sup>-6</sup>	b			5.33 × 10 <sup>-6</sup>	b	3.64 × 10 <sup>-6</sup>	b	2.23 × 10 <sup>-6</sup>	c	9.21 × 10 <sup>-7</sup>	d		
15	7.61 × 10 <sup>-6</sup>	b			4.53 × 10 <sup>-6</sup>	b	3.01 × 10 <sup>-6</sup>	b	1.82 × 10 <sup>-6</sup>	c	7.44 × 10 <sup>-7</sup>	d		
16	7.13 × 10 <sup>-6</sup>	b			4.21 × 10 <sup>-6</sup>	b	2.77 × 10 <sup>-6</sup>	c	1.67 × 10 <sup>-6</sup>	c	6.78 × 10 <sup>-7</sup>	d		
18	6.34 × 10 <sup>-6</sup>	b			3.68 × 10 <sup>-6</sup>	b	2.37 × 10 <sup>-6</sup>	c	1.41 × 10 <sup>-6</sup>	c	5.67 × 10 <sup>-7</sup>	d		
20	5.71 × 10 <sup>-6</sup>	b			3.26 × 10 <sup>-6</sup>	b	2.06 × 10 <sup>-6</sup>	c	1.22 × 10 <sup>-6</sup>	c	4.85 × 10 <sup>-7</sup>	d		
22	5.19 × 10 <sup>-6</sup>	b			2.93 × 10 <sup>-6</sup>	c	1.82 × 10 <sup>-6</sup>	c	1.07 × 10 <sup>-6</sup>	c	4.21 × 10 <sup>-7</sup>	d		
24	4.76 × 10 <sup>-6</sup>	b			2.65 × 10 <sup>-6</sup>	c	1.62 × 10 <sup>-6</sup>	c	9.47 × 10 <sup>-7</sup>	d	3.70 × 10 <sup>-7</sup>	d		
27	4.23 × 10 <sup>-6</sup>	b			2.32 × 10 <sup>-6</sup>	c	1.39 × 10 <sup>-6</sup>	c	8.04 × 10 <sup>-7</sup>	d	3.10 × 10 <sup>-7</sup>	d		
30			3.80 × 10 <sup>-6</sup>	b	2.06 × 10 <sup>-6</sup>	c	1.21 × 10 <sup>-6</sup>	c	6.94 × 10 <sup>-7</sup>	d	2.65 × 10 <sup>-7</sup>	d	9.54 × 10 <sup>-8</sup>	e
33			3.46 × 10 <sup>-6</sup>	b	1.85 × 10 <sup>-6</sup>	c	1.08 × 10 <sup>-6</sup>	c	5.94 × 10 <sup>-7</sup>	d	2.30 × 10 <sup>-7</sup>	d	8.57 × 10 <sup>-8</sup>	e
36			3.17 × 10 <sup>-6</sup>	b	1.67 × 10 <sup>-6</sup>	c	9.39 × 10 <sup>-7</sup>	d	5.16 × 10 <sup>-7</sup>	d	2.01 × 10 <sup>-7</sup>	d	7.77 × 10 <sup>-8</sup>	e
39			2.93 × 10 <sup>-6</sup>	c	1.53 × 10 <sup>-6</sup>	c	8.40 × 10 <sup>-7</sup>	d	4.53 × 10 <sup>-7</sup>	d	1.78 × 10 <sup>-7</sup>	d	7.11 × 10 <sup>-8</sup>	e
43			2.65 × 10 <sup>-6</sup>	c	1.37 × 10 <sup>-6</sup>	c	7.34 × 10 <sup>-7</sup>	d	3.87 × 10 <sup>-7</sup>	d	1.54 × 10 <sup>-7</sup>	d	6.37 × 10 <sup>-8</sup>	e
47			2.43 × 10 <sup>-6</sup>	c	1.24 × 10 <sup>-6</sup>	c	6.49 × 10 <sup>-7</sup>	d	3.35 × 10 <sup>-7</sup>	d	1.34 × 10 <sup>-7</sup>	d	5.76 × 10 <sup>-8</sup>	e
51			2.24 × 10 <sup>-6</sup>	c	1.13 × 10 <sup>-6</sup>	c	5.80 × 10 <sup>-7</sup>	d	2.93 × 10 <sup>-7</sup>	d	1.19 × 10 <sup>-7</sup>	d	5.26 × 10 <sup>-8</sup>	e
56			2.04 × 10 <sup>-6</sup>	c	1.02 × 10 <sup>-6</sup>	c	5.10 × 10 <sup>-7</sup>	d	2.52 × 10 <sup>-7</sup>	d	1.02 × 10 <sup>-7</sup>	d	4.73 × 10 <sup>-8</sup>	e
62			1.84 × 10 <sup>-6</sup>	c	9.06 × 10 <sup>-7</sup>	d	4.43 × 10 <sup>-7</sup>	d	2.13 × 10 <sup>-7</sup>	d	8.84 × 10 <sup>-8</sup>	e	4.22 × 10 <sup>-8</sup>	e
68			1.68 × 10 <sup>-6</sup>	c	8.17 × 10 <sup>-7</sup>	d	3.90 × 10 <sup>-7</sup>	d	1.84 × 10 <sup>-7</sup>	d	7.68 × 10 <sup>-8</sup>	e	3.80 × 10 <sup>-8</sup>	e
75			1.52 × 10 <sup>-6</sup>	c	7.31 × 10 <sup>-7</sup>	d	3.40 × 10 <sup>-7</sup>	d	1.57 × 10 <sup>-7</sup>	d	6.62 × 10 <sup>-8</sup>	e	3.41 × 10 <sup>-8</sup>	e
82			1.39 × 10 <sup>-6</sup>	c	6.61 × 10 <sup>-7</sup>	d	3.01 × 10 <sup>-7</sup>	d	1.35 × 10 <sup>-7</sup>	d	5.79 × 10 <sup>-8</sup>	e	3.08 × 10 <sup>-8</sup>	e
91			1.25 × 10 <sup>-6</sup>	c	5.88 × 10 <sup>-7</sup>	d	2.61 × 10 <sup>-7</sup>	d	1.14 × 10 <sup>-7</sup>	d	4.94 × 10 <sup>-8</sup>	e	2.74 × 10 <sup>-8</sup>	e
100			1.14 × 10 <sup>-6</sup>	c	5.28 × 10 <sup>-7</sup>	d	2.29 × 10 <sup>-7</sup>	d	1.02 × 10 <sup>-7</sup>	d	4.29 × 10 <sup>-8</sup>	e	2.47 × 10 <sup>-8</sup>	e

Fig. 12 Numerical representation of Annex K of EN ISO 13849-1:2006



**Fig. 13** Possibility 1: entire consideration of a safety function → Block method → example in the standard

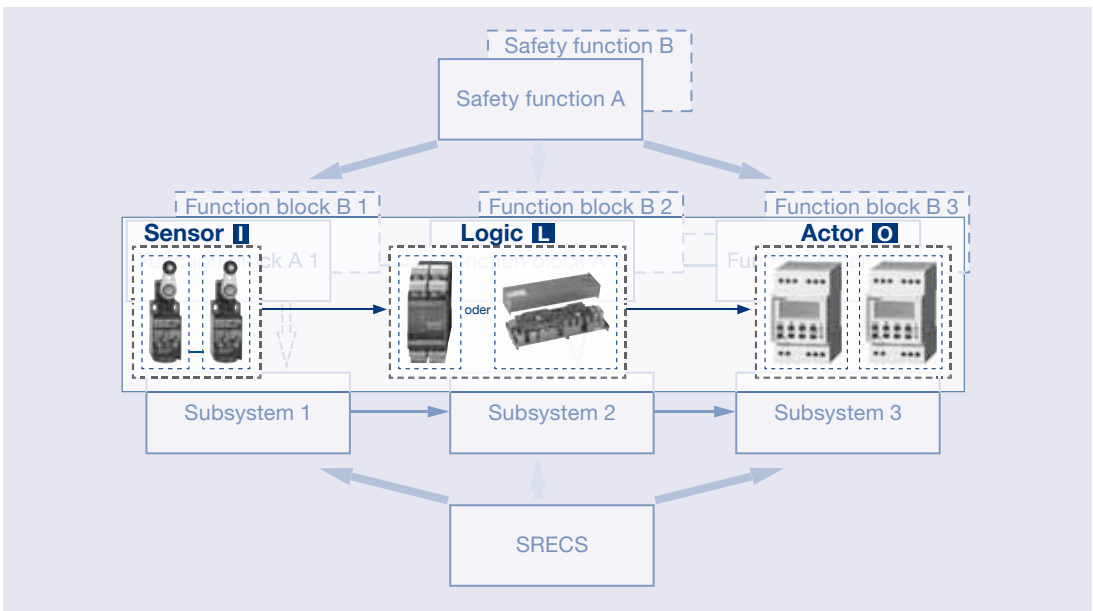
**PL assessment**

According to the standard, evaluation should preferably be made using manufacturer information.

**Possibility 1** (as shown in Figure 13) for a PL assessment based on the so-called block method in accordance with Annex B of EN ISO 13849-1; this is an analysis of the complete SRP/CS. The example in the standard found in Annex I of ISO 13849-1:2008 (2006) demonstrates an overall

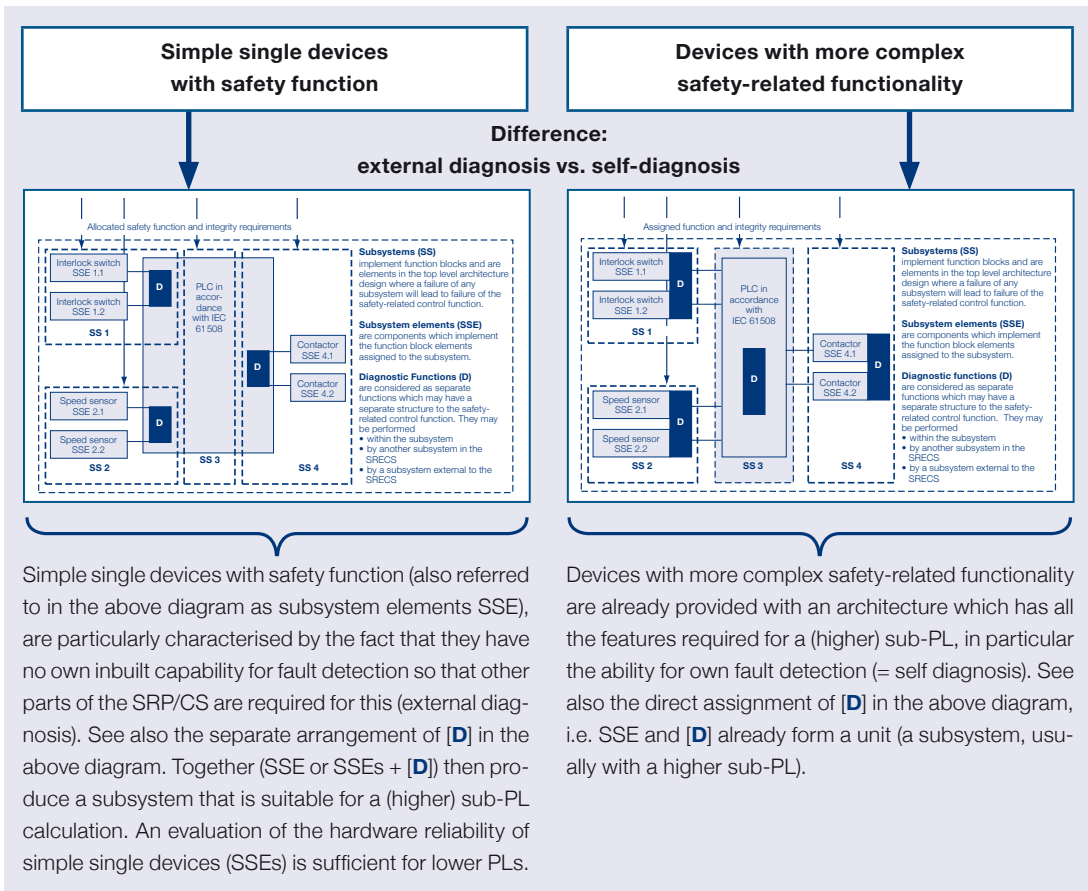
consideration using the block method. The use of the block method is recommended in particular for a complex interwoven SRP/CS and in special cases (as an alternative to the subsystem method).

**Possibility 2** (as shown in Figure 14) is the subsystem method designed as a simplification (also frequently termed the “Sub-PL consideration” or “Sub-PL method”), which may additionally refer to the so-called combination table (Table 11 of



**Fig. 14** Possibility 2: Classification of the safety function into [I], [L] and [O] (typical subsystems)





**Fig. 15** Difference between types of devices according to the aspect of PL calculation

EN ISO 13849-1). Also see Annex H of the standard.

The classification of the safety function into [I], [L] and [O]: sub-PLs (or Sub-SILs) are the basis of modularisation of an entire SRP/CS into sub-SRP/CSs (= part systems or subsystems), which are derived from function blocks (typically function blocks for the input, signal processing and output levels = [I] for input + [L] for logic + [O] for output) As already set out above, the classification permits a subsequent simplified calculation of the overall PLs.

The advantage of the subsystem method is on the one hand that devices and systems that already form a subsystem are available on the market and have been assessed with respect to the sub-PL (or sub-SIL) and corresponding  $PFH_d$  by the manufacturer so that in such cases there is no need to perform a calculation oneself; on the other hand, the calculation is considerably simpler if it does prove necessary to estimate a

Sub-PL oneself. Annex K of the standard can be referred to or used to derive “own”  $PFH_d$  values.

- On the basis of the Schmersal/Elan product range (as well as the product ranges of our competitors), we must then distinguish between two types of devices in connection with a Sub-PL or Sub-SIL approach, namely between the “simple single devices with safety function” group and the “devices with more complex safety-related functionality” group.
- The above mentioned distinction into two device groups does not signify any qualification, i.e. both device groups can perform their respective safety-related task in the SRP/CS equally well; merely the PL use is different.
- The fundamental difference between both groups is the different device architecture. Firstly there are architectures (as shown in Figure 15 on left) with (automatic) “external

diagnosis” and architectures (as shown in Figure 15 on right) with (automatic) “self-diagnosis”. Automatic here and in the two cases means “essentially performed by the system” or “independent of will”.

Additional remark on the sub-PL method: the advantage for many applications of working with sub-PLs (according to Possibility 2) is that a machinery manufacturer can assume a simplified procedure for determining the overall PL based on Table 11 of the standard – the so-called combination table. The total PL here is essentially determined by the lowest sub-PL.

### Summary (1)

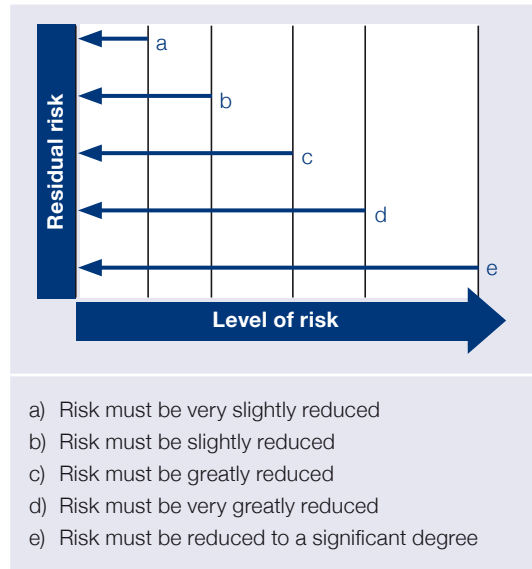
To summarise, a performance level as required in future by the new standard EN ISO 13849-1 when designing an SRP/CS is a consideration of several determining factors. It is now globally accepted as a means of establishing the safety and reliability of measuring and control systems that constitute the safety integrity of a system. Unlike common practices in mechanical engineering today, a performance level is a multidimensional approach. However, EN ISO 13849-1 uses a simplified method that considers four auxiliary variables in place of complex modelling.



Please bear in mind, however, that in addition fundamental requirements (basic requirements) apply to a performance level, irrespective of its level; these are measures to prevent and control systematic failures and faults, whereas a PL classification (PL “a” ... “e”) basically concerns the prevention and control of random failures and faults.

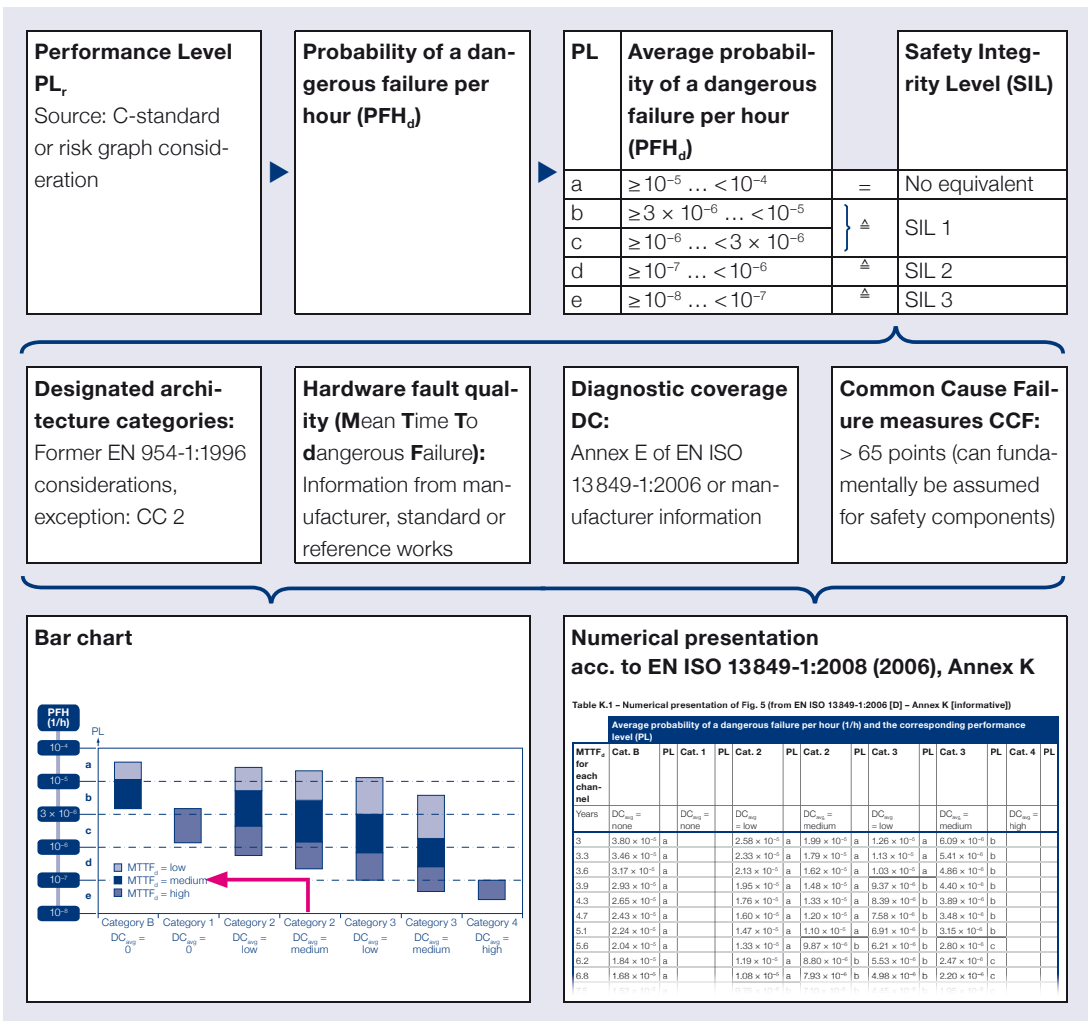
### Summary (2)

- The starting point for a PL consideration is the determination of various safety functions of a machine or machine control system.
- It follows the establishment of the required performance level  $PL_r$  for the safety function concerned. Which of the five possible performance levels (“a” ... “e”) should be selected results from the respective C standard (product standard) or using a risk graph evaluation.
- The performance level therefore reflects the required level of measures to minimise risk.



**Fig. 16** Expression of the necessary or realised risk reduction measures

- The efficacy of the (required) measures is expressed in the form of a  $PFH_d$  value (a value of the maximum residual average probability of a dangerous failure per hour tolerated = Average Probability of a dangerous Failure per Hour). The  $PFH_d$  value is also the reference point for the international safety integrity levels (SILs) as recognised in EN IEC 61 508:2000 and EN IEC 62 061:2005.
- According to EN ISO 13849-1, the estimation (calculation) of a performance level is now performed on the basis of four individual parameters (auxiliary variables):
  1. The architecture, essentially identical to the consideration of control categories and familiar from use of EN 954-1:1996 (ISO 13849-1:1999), has been adopted in EN ISO 13849-1;
  2. The evaluation of hardware reliability expressed as the Mean Time to dangerous Failure  $MTTF_d$  in years (a statistically based assumption on the period that the hardware will function correctly without random failures from a safety-related point of view);
  3. The evaluation (probability) of the efficacy of the fault detection measures in the SRP/CS or in the SRP/CS section concerned, expressed as diagnostic coverage DC) in %;



**Fig. 17** Diagrams summarising the assessment of a PL (continued overleaf)

4. The evaluation of measures to prevent so-called Common Cause or Common Mode Failures (CCF = Common Cause Failures = failures which could destroy the safety-related use of the multichannel capability of a system)
- The performance level PL achieved can then be determined using a bar chart or Annex K of EN ISO 13849-1 and compared and validated with the required PL<sub>r</sub> for the respective safety function.

Footnotes:

- [1] EN ISO 13849-1:2006 has now been replaced by EN ISO 13849-1:2008. The main difference merely refers to the reference to the new Machinery Directive 2006/42/EC in the new ZB Annex of the standard. We therefore refer to standard EN ISO 13849-1:2008 in the following.
- [2] Also referred to in the following as SRP/CS (Safety-Related Parts of Control Systems).
- [3] Probability of dangerous Failure per Hour

- [4] EN ISO 13849-2:2008 (2003) concerns the validation of safety-related parts of control systems (SRP/CS). While this standard – originally Section 2 of EN 954-1:1996, but already published at the ISO level – is being revised at the moment, the current 2003 basic version is also essential when using EN ISO 13849-1:2008. Its technology-related Annexes A to D are especially useful, and contain information on the following:
- basic and tried and tested safety principles;
  - safety-related, tried and tested components; and
  - fault exclusion possibilities and fault lists.
- [5] The exception is a rather conservative standard value of 150 y  $MTTF_d$  for mechanics and hydraulics stated by the standard in Annex C if no manufacturer data are available. Annex C also contains other standard values ( $B_{10d}$  values,  $MTTF_d$  values) that can be used if no manufacturer data exist.





### BGIA Report 2/2008

The 2/2008 report from the BGIA, the former German Institute for Occupational Health and Safety (Berufsgenossenschaftlichen Instituts für Arbeitsschutz), now called the Institute for Occupational Safety and Health (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, St. Augustin – IFA) due to the reorganisation of the German statutory accident insurance system (DGUV), deals with the new standard in an extremely detailed, sometimes scientific manner; it comprises 260 pages and is divided into eight parts:

- Introduction
- Generic standards concerning the functional safety of machinery control systems
- Report and standard overview
- Safety functions and their contribution to risk reduction
- Design of safe control systems
- Verification and validation
- Circuit examples for SRP/CS
- Bibliography.

It sets out the important content of the new standard. The report explains its application using numerous examples from the areas of electro-

mechanics, fluid power technology, electronics and programmable electronics, also including control systems that use a mix of technologies. It points out the connection between the standard and the basic safety requirements of the Machinery Directive and proposes possible procedures for calculating risk.

On the basis of this information the report permits selection of the required performance level  $PL_r$  for safety-related safety functions. The determination of the actual performance level  $PL$  is explained in detail. Detailed consideration is similarly given to the requirements for attaining the respective  $PL$  and to the corresponding categories, to component reliability, diagnostic coverage, software safety and measures to prevent systematic failures and common cause failures. Background information on control-related implementation in practice supplements the information provided.

Furthermore, 37 wiring examples show right down to the level of the component how the performance levels “a” to “e” with categories B to 4 can be implemented in respective technologies. They give details on the safety principles used and safety-related tried and tested components. Numerous references help to promote deeper understanding of these requirements.

The report demonstrates that the requirements in the standard can be implemented technically in practice and thereby contributes to uniform application and interpretation of the standard at a national and international level.

You can also request this document via your Schmersal/Elan contact partner or download it at [www.dguv.de/ifa/en/pub/rep/pdf/rep07/biar0208/rep22008e.pdf](http://www.dguv.de/ifa/en/pub/rep/pdf/rep07/biar0208/rep22008e.pdf).

### SISTEMA software tool

The SISTEMA software tool likewise published by the IFA (see above) stands for **Sicherheit von Steuerungen an Maschinen** (Safety of machinery control systems) has now become highly valued by those using the EN ISO 13849-1 standard who prefer a computer-assisted implementation instead of a traditional estimation of a performance level. SISTEMA is a free WINDOWS-based software tool prepared to provide support when assessing the safety of control systems within the framework of EN ISO 13849-1:2006.





The SISTEMA tool replicates the structure of safety-related parts of control systems (SRP/CS) on the basis of the so-called designated architectures and calculates reliability values at different detailed levels including the performance level (PL) achieved. The risk parameters to establish the required performance level (PL), the category, the measures to prevent common cause failures (CCF) in multichannel systems, the mean component quality ( $MTTF_d$ ) and the mean test quality ( $DC_{avg}$ ) of devices and blocks can be accounted for step by step. The impact of each parameter change on the overall system is displayed directly and can be printed out as a report.

You can download SISTEMA directly from IFA at <http://bgia-online.hvbg.de/DOWNLOAD/send-mail.aspx?lang=e>. Cross-references to manufacturer libraries and other useful information are also available on the SISTEMA website (<http://www.dguv.de/ifa/en/prasoftwa/sistema/bibliotheken/index.jsp>).

The Schmersal/Elan library for SISTEMA can be directly downloaded at: [www.schmersal.net](http://www.schmersal.net) → Download software → Schmersal library SISTEMA V1.1.x.



## PART 2: BORDERLINE ISSUES

Even if one spends considerable time getting to grips with the new EN ISO 13849-1 standard and makes use of the available help implementing it as provided in the abovementioned examples, uncertainties as well as borderline issues may well arise.

We address a few selected borderline issues of this nature below:



### Determination of a safety function

The definition of a safety function is given particular emphasis so that you can estimate a performance level (PL) correctly from a safety point of view and also so you do not present the situation in a worse light (*calculate to your disadvantage*) than is actually the case.

According to the definition, a safety function is the function of a machine control system where the failure of the function would directly increase the risk (risks) (see EN ISO 13849-1 Section 3.1.20).

This means that a machine generally has a number of safety functions, and complex circuitry may well comprise several safety functions or possibly be divided having regard to this. Figure 1 describes typical safety functions.

Based on the example of series connection of five guard doors, this can mean that there are five safety functions to be considered separately if, at a certain point in time X, only one of the five guard doors is ever opened by the operator. This perspective is even clearer in the case of emergency stop control devices with series connection because one can regularly assume here that in case of an emergency only one of several devices will ever be actuated.

This method can considerably simplify use of the new standard because it “shortens” the SRP/CS

Safety function	Example of possible application
Safety-related stop function, triggered by a protective device	Reaction to triggering of a protective device by STO, SS1 or SS2 (Table 5.2)
Manual reset function	Acknowledgement when leaving areas that are accessible from behind
Start/restart function	Only permissible for controlling guards in accordance with DIN EN ISO 12100-2
Local control function	Control of machinery movements from a place within the hazardous area
Muting function	Temporary disabling of protective devices, e.g. during transportation of materials
Set-up with automatic resetting (hold-to-run control)	Machinery movements controlled from a place within the hazardous area, e.g. when making adjustments
Enabling function	Machinery movement controlled from a place within the hazardous area, e.g. when adjusting equipment
Prevention of unexpected restarting	Manual intervention in the hazardous areas
Freeing and rescuing trapped persons	Moving rollers apart
Insulation and energy discharge function	Opening of a hydraulic valve to relieve pressure
Control functions and selection of operating mode	Activation of safety functions using the operating mode selector switch
Stop function in an emergency	Reaction to actuation of an emergency stop device by STO or SS1 (Table 5.2)

**Fig. 1** Examples of safety functions (see EN ISO 13849-1, Table 8). Please note that safety functions can also be sub-functions, e.g. the RESET signal in the case of hazardous machine areas accessible from behind or the actuation of Electromagnetically operated guard locking on an interlocking device etc.

chain [1] to be taken into consideration so that this leads to fewer blocks or subsystems. However this method is only permitted if it is based on thorough evaluation.

In each case it is necessary to consider the coincidence of man and control functionality (in the widest sense the interfaces between man and machinery). In principle a safety function is involved wherever greater risks to people (the operators) may arise as a result of failures, faults or malfunctions.

Examples of safety functions are moving rollers apart or protection from flying parts insofar as control functions are involved here.

Normally the individual protective device is always taken into account for a safety function in a functional series connection (keyword: coincidence man/machinery). Examples of exceptions

which prove the rule include double or telescopic doors or clamping mechanisms that jointly secure a part. Here it is necessary to add together the probabilities that the sensors (equipment) involved will fail.

Moreover all faults must be considered, e.g. also restricted fault detection or the risk of a fault being cleared in simple series connected electro-mechanical devices (loc. cit.).

To illustrate this, three examples are set out briefly below; these are also available in detail in the BGIA-Report 2/2008:

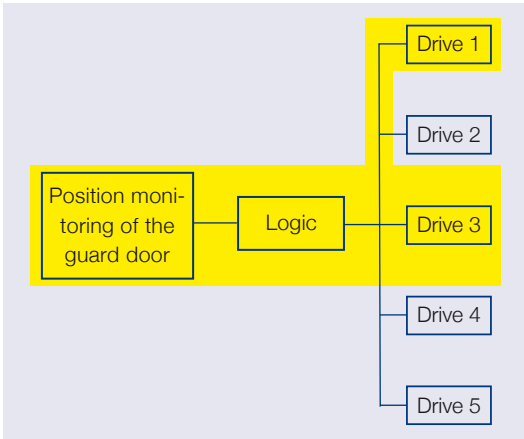
**Brief version taken from BGIA Report 2/08 – Example 1: Safety function: “Stopping when the safety guard is opened”**

- When the safety guard is opened a machine operator has access to a hazardous area in which five drives control movements of ma-



chine parts. Opening the safety guard causes all five drives to be brought to a stop as quickly as possible.

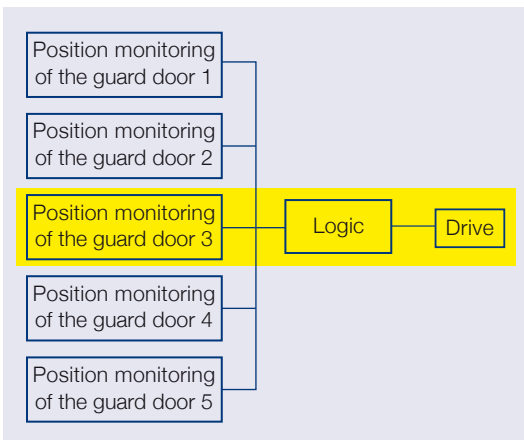
- The result may be a PL which is no longer adequate for the application, even though it may be that only drives 1 and 3 trigger movements hazardous to the operator, and the remaining drives are halted purely “functionally”. In this case, it is recommended that only the movements actually presenting a hazard be considered for the purposes of the safety function.



PS: Possible faults in the electrical system are assigned to the relevant blocks.

**Brief version taken from BGIA Report 2/08 – Example 2: Safety function: “Stopping when a safety guard is opened”**

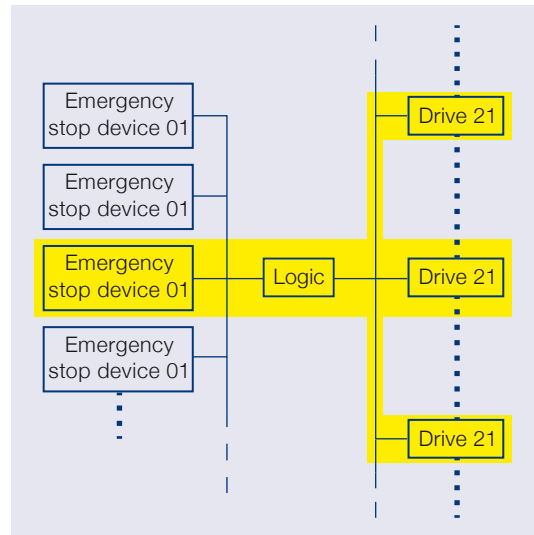
- A hazardous movement is safeguarded by a fence fitted with five safety guards. Opening any of the guards stops the movement. For determining the PL at a later stage, each guard can form part of a separate safety function SF1 to SF5 (see above).



PS: Possible faults in the electrical system are assigned to the relevant blocks.

**Brief version taken from BGIA Report 2/08 – Example 3: Safety function: “Emergency stop of an entire machine”**

- 20 emergency stop devices are installed on a larger machine; when actuated, they bring all 50 drives to a halt as quickly as possible. What components must be considered in this case for implementation of the safety function? It cannot be predicted which of the emergency stop devices will be actuated to trigger the safety function. Since the operator only ever actuates one emergency stop device, safety functions SF1 to SF20 are defined.



PS: Possible faults in the electrical system are assigned to the relevant blocks.

The respective position of an exposed person at the time of triggering of the emergency stop is unknown, but regardless of where this person is located, not all 50 drives represent a hazard. The worst case should therefore be considered representative for all conceivable situations. The worst case is determined by the worst PL, and is therefore dependent among other things on the number of drives in the safety chain which generate hazardous movements at the least favourable location and on the respective individual PL.

**Problem: overlapping hazards**

This refers to hazards “impacting” on an operator in a specific place (at a specific point) such as in



**Fig. 2** Front page of Information Sheet No. 47 from the Technical Committee of Metall-BG Nord Süd on the subject of “overlapping hazards”

a robotic system; the hazards may emanate from different machines (robots) or machine parts.

In other words (source: loc. cit. → information sheet): overlapping hazards are characterised by the simultaneous impact of several individual hazards on one or more people to be protected, on parts of their body or limbs, who are located in a place or who can access hazardous areas.

A single hazard is understood both as the movement of a single axis and, for example, as a hazard arising from the movement of an entire machine part. Therefore if the movement of a machine part results from the kinematic interaction of one or several axis and spindle drives (e.g. a milling tool



on the slide rest of a machining centre), then this can be viewed as an individual hazard.

In order to restrict the work involved in a calculation exercise of this nature as specified in EN ISO 13849-1 to a reasonable amount, the “Mechanical engineering, production systems, steel construction” Technical Committee of the metal employers’ liability insurance association in Mainz, the Metall-BG Nord Süd, has prepared an information sheet (047, Issue 05/2010) describing suitable procedures for such cases.

### Conclusions according to the information sheet

Depending on the individual risk assessment, it is permissible in practice to represent safety functions based on a consideration of their individual hazards, despite the fact that they are made up of overlapping hazards.



*If, however, several actuators contribute to reducing risk from the same individual hazard (for example contactors, valves, drive control systems), then all of these actuators must be viewed together in a safety function. Put another way, all actuators that can cause hazardous movements in one and the same machine part must be viewed together in one safety function.*

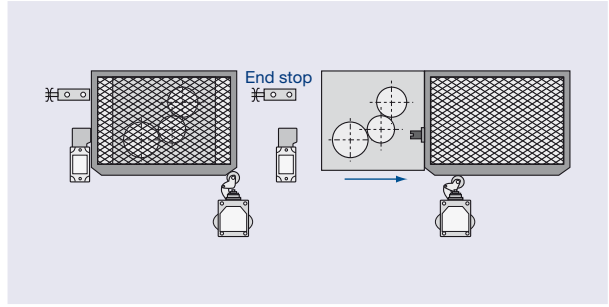
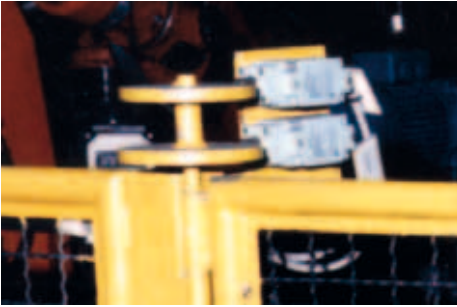
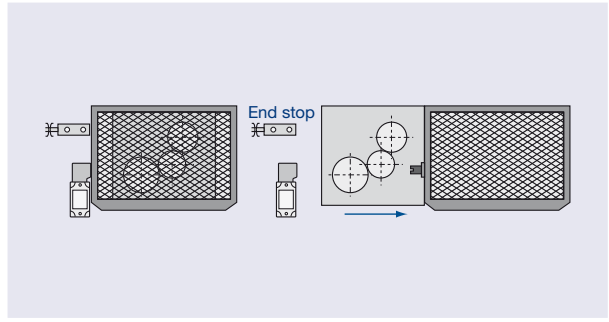
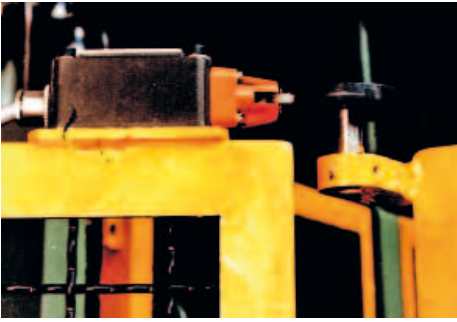
*If the individual risk assessment on the machine produces a differentiated hazard assessment with different PL<sub>r</sub> or SIL, the practice of representing safety functions on the basis of considering separate hazards is admissible.*

### Fault exclusions

This concerns the issue of whether single fault safety (where one fault must not lead to loss of the safety function) as applies to the basic requirement for control categories 3 and 4 always needs a physical redundancy (a double version) of the hardware involved in the function or whether, and under which conditions, certain fault scenarios may be excluded.

This therefore concerns the following matter, for example:

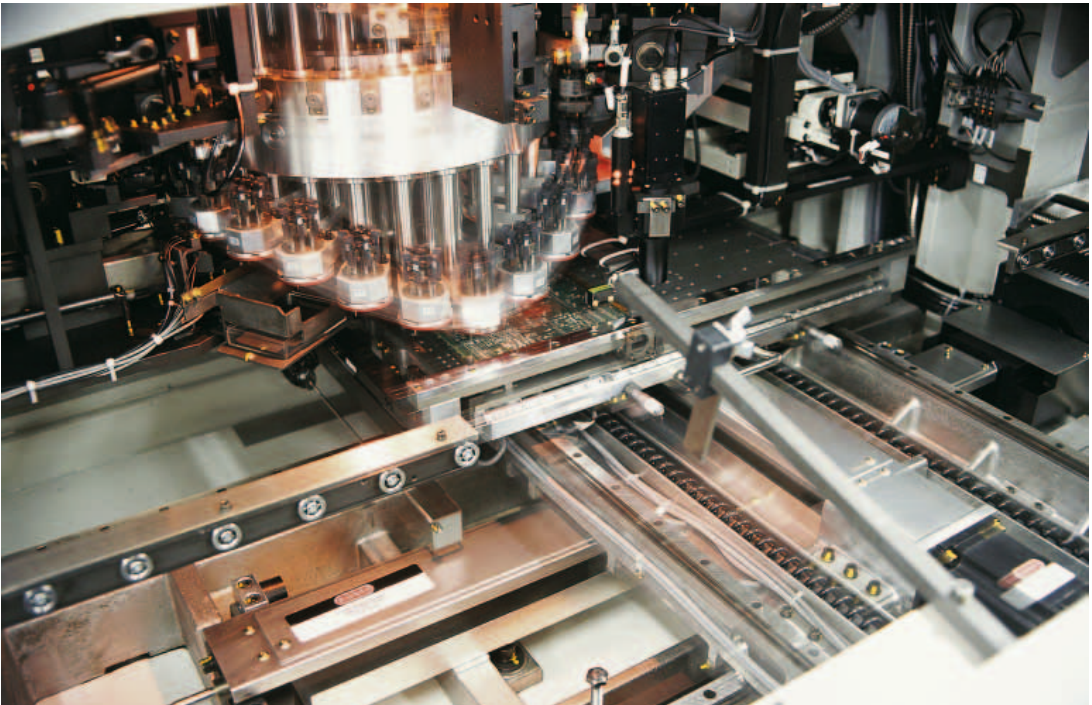
- Whether two-channel cable routing has to take place separately (i.e. not in a shared sheathed cable), or if not, under which circumstances;



**Fig. 3** Under which conditions is an electrical 2-channel capability implementation for interlocking devices satisfactory for control categories  $\geq$  CC 3 or performance level  $\geq$  PL “d”? What conditions are required for physical redundancy?

- Whether two devices are always required at the actuator level; or
- Whether interlocking devices with and without guard locking also only require an electrical 2-channel capability (instead of physically providing two switches for this).

As a matter of principle, the combination of an SRP/CS starts at the point where the safety-related signals are generated (including, for example, the actuator or the role of a position switch) and ends at the outputs of the power control elements (including main contacts of a contactor).



Section 7.3 of EN ISO 13849-1 deals with fault exclusions in the same way as in EN 954-1:1996, i.e. basically with cross-reference to EN ISO 13849-2:2008 (2003). One new aspect is the explicit requirement to document fault exclusions.

Annexes A to D of EN ISO 13849-2 are especially important to the subject of “fault exclusion” because they set out fault lists classified according to the different technologies, i.e. for mechanics, hydraulics, pneumatics and electrics, as well as lists of “permitted” fault exclusions (with the associated conditions for their application).

As such the question of fault exclusion enjoys a renaissance in EN ISO 13849-1 due to its special importance when evaluating the architecture of an SRP/CS (in the same way as it was previously for evaluating a control category).

The fact that there are now more enquiries on the subject of “fault exclusion” once again, in particular concerning electromechanical safety switches, may arise from the confusion caused by novel (electronic) interlocking devices and their promotion by some manufacturers. Whether intentional or not, the way these are advertised sometimes creates the impression that it is no longer permissible to deploy traditional solutions and use them where safety requirements are more stringent. This is not the case at all, and the previous consideration has actually not been changed.

As a rule, the question as to whether an electrical 2-channel capability (= the signal processing of two safety contacts) can be regarded as redundancy in terms of the requirements or whether a physical 2-channel capability is required to achieve this (a two switch solution) remains in the background.

Evaluating an electrical 2-channel capability as redundancy means being able to exclude faults during mechanical actuation (using the actuator, articulating mechanism etc.), i.e. it must be guaranteed that no damage or other adverse influences can impinge on the devices that will affect their ability to function correctly. Think of fractures resulting from material stress, random material faults such as cavities or blocking of the articulating mechanism caused by the penetration of foreign particles etc.

It is possible to exclude faults of this kind. Section 7.3 of EN ISO 13849-1 permits this (in the same way as EN 954-1:1996 did). The specific requirements of EN ISO 13849-2 then apply to the framework conditions for fault exclusion. When estimating a PL one should basically give great consideration to the “fault exclusion” parameters. The scope is set out in Section 7.3 of EN ISO 13849-1:2006, which states the following:

*“It is not always possible to evaluate SRP/CS(s) without assuming that certain faults can be excluded. For detailed information on fault exclusion, see ISO 13849-2.*

*Fault exclusion is a compromise between the technical safety requirements and theoretical possibility that a fault will occur.*

*Fault exclusion can be based on*

- *The technical improbability of occurrence of some faults;*
- *Generally accepted technical experience, independent of the considered application; and*
- *Technical requirements related to the application and specific hazard.*






*Detailed justification has to be documented for any faults that are excluded.”*

The above mentioned standard EN ISO 13849-2 is the original, conceived as Part 2 of EN 954, which was then realised at ISO level as the “validation of SRP/CS” section. Although a reworking is currently taking place, this standard also supplements EN ISO 13849-1 until further notice and its significance must not be underestimated. This not only applies to the area of “fault exclusion”. For example, Annexes A to D of EN ISO 13849-2 also contain the basic and tried and tested safety principles as well as lists of safety-related proven components to be taken into consideration for the architectures and different technologies that usually come into question for SRP/CS.

The Schmersal/Elan leaflet “Waiving of an additional monitoring switch for interlocking devices (physical redundancy vs. electrical redundancy for CC 3 or  $PL \geq “d”$ ; as shown in Figure 4) summarises the subject of “fault exclusion” for interlocking devices in conjunction with moving protective devices (this can be procured from your Schmersal/Elan contact partner).



# Waiving of an additional monitoring switch for interlocking devices (physical redundancy vs. electrical redundancy for CC ≥ 3 or PL ≥ “d”)

2 <sup>nd</sup> switch Yes/No?	Safety switches with separate actuators	Safety guard locks with separate actuators	Hinge switches	BNS magnetic switches	CSS-based electronic devices
	AZ range and similar Operating principle: electromechanical 	AZM range and similar Operating principle: electromechanical 	TESF range and similar. Operating principle: electro-mechanical 	BNS range Operating principle: contactless 	CSS, AZ/AZM 200, MZM range Operating principle: pulse-echo principle 
Max. CC/PL	Without 2 <sup>nd</sup> switch: max. CC 3, PL “d”	Without 2 <sup>nd</sup> switch: max. CC 3, PL “d”	Stand alone: max. CC 4, PL “e”	Stand alone: max. CC 4, PL “e”	Stand alone: max. CC 4, PL “e”
Relating only to SRP/CS <sup>1)</sup> -standardisation EN 13849-1/-2 (BUT: C-standard has priority!) In addition (also see reverse) please adhere to GEP <sup>2)</sup> ! Additional Schmersal/Elan recommendations if use is made of “fault exclusion”	Fault exclusion required (see reverse) In terms of their design features and their technical data, our devices correspond to the relevant requirements.		No 2 <sup>nd</sup> switch required	No 2 <sup>nd</sup> switch required – see also product standard IEC EN 60947-5-3: classification as PDF-M	No 2 <sup>nd</sup> switch required – see also product standard IEC EN 60947-5-3: classification as PDF-M
	<ul style="list-style-type: none"> <li>Hazard must be visible (no radiation etc.)</li> <li>Stress-free interaction between actuator and device</li> <li>Installation site free from risk and permeation of dirt/foreign particles etc.</li> <li>Form-fit working effect of the actuator (one piece of punched metal respectively in case of flexible actuators form-fit assembly of parts additionally)</li> <li>Actuator fixing into a stabil material</li> <li>Start-up test (recommendation)</li> </ul>	To be additionally heeded for devices with guard locking: <ul style="list-style-type: none"> <li>Devices with fail-locking mechanism</li> <li>Observance of the max. permissible extraction forces</li> </ul>			
Remarks	Particularly careful consideration recommended!				
Specific fault exclusion documentation required	Yes!	Yes!	No!	No!	No!
Requirements of other standards to be observed:					
<ul style="list-style-type: none"> <li>AMD 1<sup>3)</sup> to EN 1088:1996 (addition measures vs. manipulation)</li> <li>EN ISO 13849-1:2006</li> <li>EN 1088:2007</li> </ul>	<ul style="list-style-type: none"> <li>Yes (see suggestions overleaf) with the exception of “I” versions = individual coded versions (AZ “I” etc.)</li> <li>2-channelled signal processing</li> <li>No mechanical end-stop</li> </ul>	<ul style="list-style-type: none"> <li>Yes (see suggestions overleaf) with the exception of “I” versions = individual coded versions (AZ “I” etc.)</li> <li>2-channelled signal processing</li> <li>No mechanical end-stop</li> </ul>	<ul style="list-style-type: none"> <li>Non-detachable fixing</li> <li>2-channelled signal processing</li> <li>No mechanical end-stop</li> </ul>	<ul style="list-style-type: none"> <li>Yes (see suggestions overleaf)</li> <li>2-channelled signal processing</li> <li>No mechanical end-stop</li> </ul>	<ul style="list-style-type: none"> <li>Yes (see suggestions overleaf) except AZM 200 with B30-actuator</li> <li>2-channelled signal processing</li> <li>no mechanical end-stop with the exception of MZM 100</li> </ul>

<sup>1)</sup> SRP/CS: Safety-Related Parts of Control Systems; <sup>2)</sup> GEP: Good Engineering Practices; <sup>3)</sup> Integrated in EN 1088:2007

**GEP (Good Engineering Practices)**

- Observance of the basic and well-tried safety principles in accordance with Annexes A and D of EN ISO 13849-2:2003
- Observance of the technical data and installation information in accordance with the operating instructions of the devices
- Validation of the SRP/CS in accordance with EN ISO 13849-2:2003

**Additional precautions against manipulation (optional, but at least 1 of these)**

- Non-detachable actuator/possibly fixing for device (rivet, weld, tamperproof screws)
- Concealed device installation
- Pivot point installation
- Individually coded actuators
- Additional monitoring switch
- Control-related measures (start-up testing, plausibility tests etc.)

Basics/further information: AMD 1 of EN 1088:1996 (integrated in EN 1088:2007)

**Fault exclusion consideration**

- Basis: EN ISO 13849-1:2006 Section 7.3 in connection with EN ISO 13849-2:2003 Section 3.2
- Does not open with positive opening contacts (permissible fault exclusion in accordance with Table D.8 of EN ISO 13849-2:2003)
- Mechanical fault (permissible fault exclusion in accordance with Table A.4 of EN ISO 13849-2:2003)

Assumed fault	Fault exclusion
Wear/corrosion	Yes, if material, (over) dimensioning, manufacturing process, treatment process and suitable lubrication have been carefully selected in accordance with the established service life (see also Table A.2).
Do not tighten/loosen	Yes, if material, manufacturing process, locking devices and treatment process have been carefully selected in accordance with the established service life (see also Table A.2).
Breakage	Yes, if material, (over) dimensioning, manufacturing process, treatment process and suitable lubrication have been carefully selected in accordance with the established service life (see also Table A.2).
Deformation through excess strain	Yes, if material, (over) dimensioning, manufacturing process and treatment process have been carefully selected in accordance with the established service life (see also Table A.2).
Stiff/gets stuck	Yes, if material, (over) dimensioning, manufacturing process, treatment process and suitable lubrication have been carefully selected in accordance with the established service life (see also Table A.2).

• Revision von EN ISO 13849-2 (in preparation):  
fault exclusion mechanical fault no long permitted for PL “e”!



**Elan Schaltelemente GmbH & Co. KG**  
Im Ostpark 2, D-35435 Wetztenberg

Telephone: +49 (0)641 9848-0  
Facsimile: +49 (0)641 9848-420  
Email: info-elan@schmersal.com  
Internet: www.elan.de

**K.A. Schmersal GmbH**  
Industrielle Sicherheitssysteme  
Mödinghofe 30, D-42279 Wuppertal

Telephone: +49 (0)202 6474-0  
Facsimile: +49 (0)202 6474-100  
Email: info@schmersal.com  
Internet: www.schmersal.com

**Liability**  
The information and recommendations in this information sheet are provided according to the best of our knowledge and in good faith. However they do not absolve the user from his responsibility to conduct his own test and weigh up different aspects involved. With the exception of contrary and mandatory statutory provisions, we shall assume no liability for any errors and misunderstandings in this information sheet.

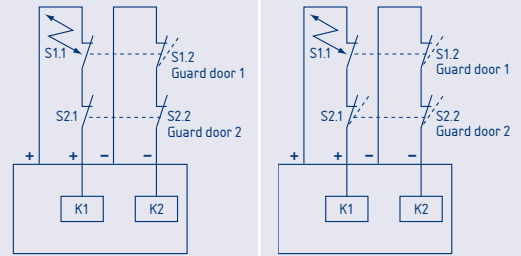
**Edited by**  
Friedrich Adams  
K.A. Schmersal Holding GmbH & Co. KG  
Head of Schmersal tec.nicum  
Telephone (mobile): +49 (0)178 6474-051  
Telephone (Wuppertal): +49 (0)202 6474-700  
Telephone (home office): +49 (0)6406 8362-37  
Facsimile (Wuppertal): +49 (0)202 6474-7007-19  
Facsimile (home office): +49 (0)6406 8362-38  
Email: fadams@schmersal.com

**Fig. 4** Front and reverse page of the Schmersal/Elan leaflet “Waiving of an additional monitoring switch for interlocking devices (physical redundancy vs. electrical redundancy for CC ≥ 3 or PL ≥ “d”)”

### Diagnostic coverage in series connections

This subject (DC in relation to series arranged electromechanical devices) is hotly disputed in professional circles. There is agreement that it will not be possible to discover all faults in such circuits and that it will be possible to “overwrite” some faults (see the example below), but not on

#### Starting point for the view



First fault:

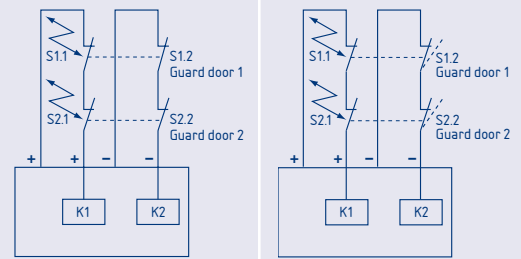
- Short-circuit via contact S.1 (guard door 1)
- Guard door 1 is opened
- Module switches off 1-channel
- Obstruction to operation (99% DC)

Clearing fault:

- Guard door 1 remains open
- Module switches off 2-channel
- Restart possible

PS: For applications where, for operational reasons, first faults are always overwritten such as double doors, we recommend additional fault discovering measures when safety magnetic switches are used (loc. cit.). This information can be ignored for electro-mechanical devices with positive break contacts.

#### Fault accumulation – variation 1



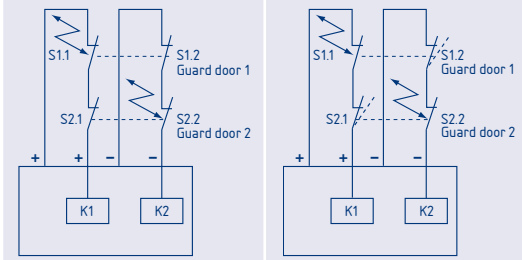
- Second fault in guard door 2
- Short circuit via S2.1

Analysis:

- (Any) guard door is opened
- Module switches off 1-channel
- Obstruction to operation (correct safety-related reaction, no re-engaging possible)

PS: A further guard door must be opened to overwrite the fault. A hazardous state requires a third fault (and possibly more if there are more guard doors)!

#### Fault accumulation – variation 2



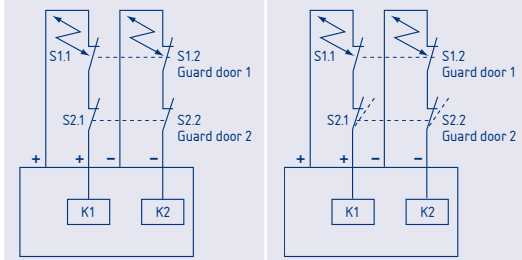
- Second fault in guard door 2
- Short circuit via S2.2

Analysis:

- (Any) guard door is opened
- Module switches off 1-channel
- Obstruction to operation (correct safety-related reaction, no re-engaging possible)

PS: Hazardous state when a third fault takes place (possibly more faults are required if there are more guard doors)!

#### Fault accumulation– variation 3



- Second fault in guard door 1
- Short circuit via S1.2

Analysis:

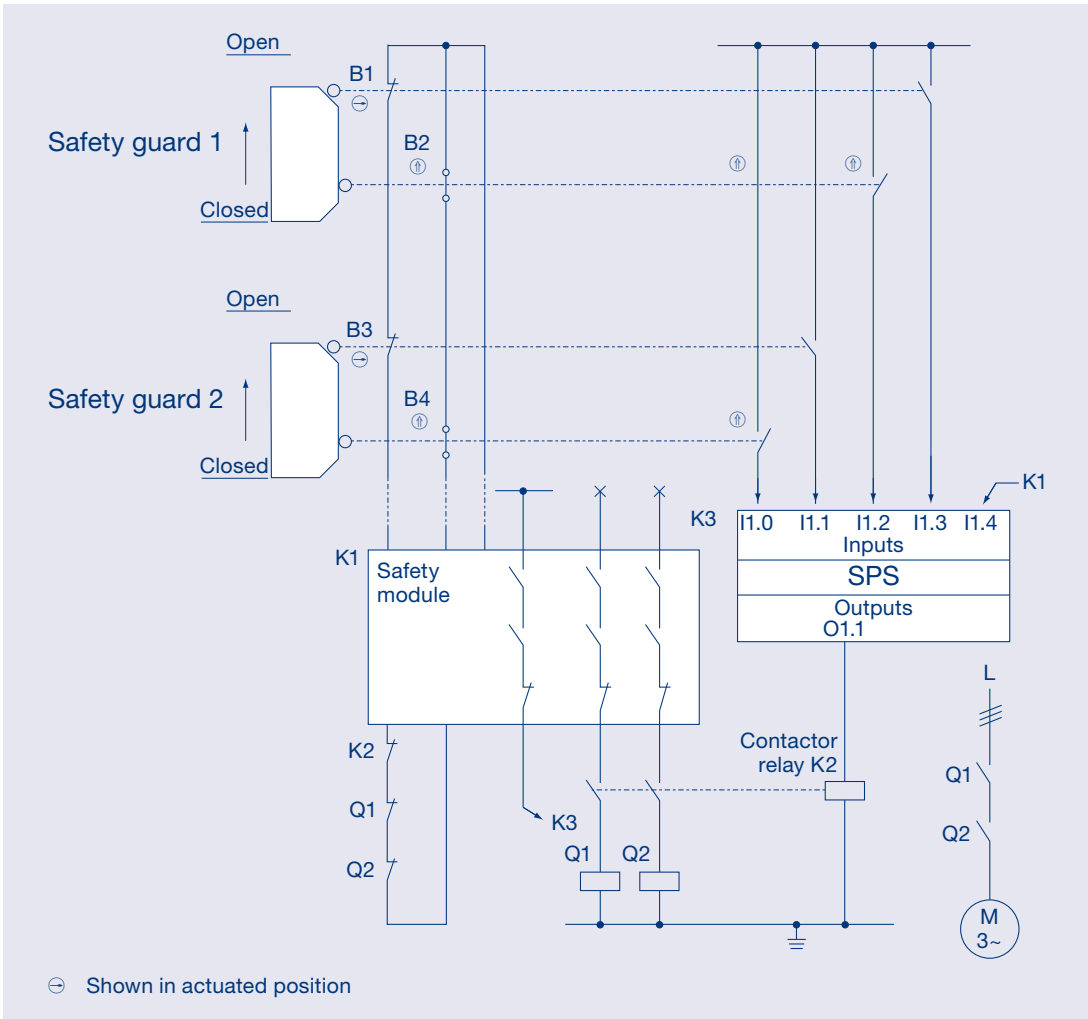
- Guard door 1 is opened
- Module does not switch off
- Hazardous state!
- Guard door 2 is opened
- Module switches off 2-channel
- Restart possible



the degree of fault detection remaining and possibly which conditions are attached.

We recommend only calculating a DC of 60% for electromechanical devices or similar with series connection if no additional measures are effective.

Further measures to increase the DC include reading in feedback contacts from the guard door switches in a PLC with subsequent plausibility assessment and the incorporation of this



**Fig. 5** Position monitoring of moveable guards for the prevention of hazardous movements – Category 4 – PL “e”: Safety function: Safety-related stop function, initiated by a protective device: opening of a moveable guard (safety guard) initiates the safety function STO (safe torque off). Source: BGIA-Report 2/2008 – Chapter “Circuit examples for SRP/CS – Figure 8.49)



**Fig. 6** 99% DC or PL “e” also with series connection thanks to the use of self-monitoring switching technology: contactless interlocking devices with and without guard locking – Schmersal CSS range

assessment in the restart circuit of the SRP/CS. How this can be achieved in principle is shown in the circuitry above (BGIA-Report 2/2008). A DC of 99% for B1 and B2 is assumed upon an additional plausibility monitoring of the break/make contact combinations in the PLC K3.

As an alternative other technologies can be used, e.g. the PES technology from the CSS range at Schmersal with contactless interlocking devices with and without guard locking.

A Schmersal/Elan leaflet dealing with this subject (“We shouldn’t throw the baby out with the bathwater!” – as shown in Figure 7) is also available from your Schmersal/Elan contact partner.



# We shouldn't throw the baby out with the bathwater!\*

\* Saying (already used by Luther and Thomas Murner)  
A figurative phrase to express the fact that – if we are over-eager – we are in danger of rejecting the good along with the bad!



## EN ISO 13849-1:2006: On the question of the degree of diagnostic coverage in the case of simple series connections (daisy-chain connections) of electromechanical safety sensors and safety switches



Concerns: Electromechanical safety switches and interlocks (with/without guard locking), safety magnet switches, e-stop control devices etc. arranged 2-channelled in a simple series connection (daisy-chain connection), i.e. simple single devices with safety function that are monitored for failures, faults and inconsistencies by safety relay modules, safety PLCs etc. ●

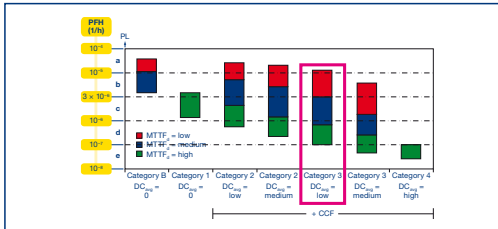
Please also note in the case of safety magnetic switches that their connection to an evaluator from a different brand takes place on own responsibility and that – as is always required for devices of this nature – a safe current and voltage limitation must be guaranteed that corresponds to the technical data of the devices

• When applying EN ISO 13849-1:2006 we recommend that our customers take a diagnostic coverage (DC) of 60% as a basis for switching systems of this nature insofar as the remaining requirements are satisfied for Control Category 3.

$$DC^{\ominus} = \frac{\sum \lambda_{dd}}{\sum \lambda_d} = 60\%$$

• The (rather conservative) approach of DC 60% makes it possible for simple series connections (a 2-channelled architecture that corresponds to Control Category 3 and where a prerequisite is a high hardware reliability MTTFF) to achieve a Performance Level (PL) "d".

• This recommendation simultaneously results in downwards compatibility to EN 954-1:1996 which has made it possible to classify tried and tested circuits like



these in Control Category 3. On the other hand a DC of 60% blocks an assessment of PL "e" due to a residual risk in which a hazardous failure accumulation cannot be completely excluded.

• Whereas single failure safety with appropriate failure detection (some but not all failures are detected) is required for CC3, CC4 requires that a failure may not lead to the loss of the safety function (1-failure safety as for CC3) and that (to a qualified extent) all failures must be detected in good time.

• Our recommendation of a restriction to PL "d" doesn't refer to the subsystem II (inputs) only, it refers to the entire PL as well (even if a PL "e" can be calculated).

It is undisputed that additional failure detection measures are necessary for simple series connections to be classified as a PL "e", for example:

- the incorporation of a PLC used in normal operating conditions (see BGIA switching example on the back);
- optionally deployment of our PROTECT-IE input extension modules with corresponding signal processing extender (see documentation);
- individual evaluation and dispensing with series connection.
- As an alternative the deployment of devices that operate electronically comes into question (e.g. devices from Schmersal's CSS range; see also ●).

• The information on the back demonstrates the considerations behind our decision in favour of the DC level of 60% that we propose and shows that even a failure accumulation in simple series connections, with one exception, does not lead to hazardous states if this is based on a balanced overall consideration that takes into account all potential failure possibilities and application conditions.

● The question does not affect series connections of electronic safety sensors with and without latching (CSS range) that have their own (implemented) capabilities for failure detection (always PL "e", DC 98%) as well as simple single devices (as mentioned above) if these are integrated into a safety bus system. E.g. with ASI-SaW these can generally similarly be calculated with 99% DC.

● DC = probability-based value of the efficacy of the diagnostic functions (failure detecting measures); DC expresses the relationship between detected dangerous failures and the total number of dangerous failures with respect to the total failure rate of a component (λ or 1/MTTF).

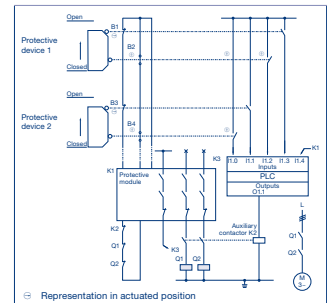
**Dear Reader!**  
Please note that the opinion which we have analysed carefully and put to paper here is not universally shared in the branch. We respect these doubts, without sharing them; our view is rather to refer the objections to the area of risk assessment. If after opening the protective safeguard an operator regularly (F2) has to handle stationary dangerous tools or machine parts, e.g. blades, squeezes, and a sudden machine restart (P2) can lead to serious injuries (S2), we recommend classifying the "unexpected restart inhibit" safety function as required Performance Level PL "e".

\* See risk graph in accordance with EN ISO 13849-1

### Consideration 1: Requirements for failure detection in accordance with EN ISO 13849-1:2006

Failure possibilities	Safe state/failure detection			Safe state/failure detection		
	1 <sup>st</sup> failure	DC in %	Remark	1 <sup>st</sup> failure	DC in %	Remark
• Earth fault	Yes!	99		Yes!	99	
• Cross-fault (by protected line installation or cross-fault recognition)	Yes!	99		Yes!	99	
• Short circuit via a safety contact	Yes!	≥ 49.5 ... 99	Diagnostic overwriting (masking) possible!	Yes!	99	
<b>ERGO:</b> Min. DC as average of all failure possibilities		>60	Also in worst-case!		99	
Failure accumulation	2 <sup>nd</sup> failure ff.	DC in %	Remark	2 <sup>nd</sup> failure ff.	DC in %	Remark
• Other short circuits	Qualified!	0 ... 99	Dep. on failure sequence	Yes!	99	Max. 3-failure consideration
• How is diagnostic coverage defined?	• The degree of diagnostic coverage describes the capability for fault detection and is given as a % (0% → no failure detection ... ≥99% → failures are detected in good time, accumulations of failures are taken into account).					
• Which failures are possible in the above case?	• Earth fault → is detected by the downstream logic → 99% • Cross fault → is detected by the downstream logic (or can be excluded with protected line installation) → 99% • Short-circuit via a safety contact (worst case): 49.5% for 2 devices in series, ≥66% as from 3 devices in series					

### BGIA switching example for PL "e" through additional integration of a PLC used in normal operating conditions for failure diagnosis in series connections



### Consideration 2: Switching examples related to short circuits on safety contacts

Starting point for the consideration	Failure accumulation – version 1	Failure accumulation – version 2	Failure accumulation – version 3
<b>First failure:</b> • Short circuit via contact S1.1 (safeguard 1) • Safeguard 1 is opened • Module switches off, single channelled • Operational hurdle → DC 99%	<b>Failure elimination (resetting of failure recognition):</b> • Safeguard 2 is opened • Module switches off, 2-channelled • Renewed start possible	• Second failure in safeguard 2 • Short circuit via S2.1 <b>Analysis:</b> • Safeguard (any) is opened • Module switches off, single channelled • Operational hurdle (correct safety-related reaction, no restart possible)	• Second failure on safeguard 2 • Short circuit via S2.2 <b>Analysis:</b> • Safeguard (any) is opened • Module switches off, single channelled • Operational hurdle (correct safety-related reaction, no restart possible)
PS: For applications where any first fault is always overwritten for operational reasons, e.g. for double doors or similar, we recommend additional fault detection measures where safety magnetic switches are deployed (see loc. cit.). This information can be ignored for electromechanical devices with positive break contacts.	PS: A further safeguard would have to be opened to overwrite the failure. A hazardous state requires a 3 <sup>rd</sup> (and in the case of more safeguards possibly further) failure!	PS: A hazardous state following the occurrence of a 3 <sup>rd</sup> failure (in the case of more safeguards possibly further required)!	• Second failure on safeguard 1 • Short circuit via S1.2 <b>Analysis:</b> • Safeguard 1 is opened • Module does not switch off • Hazardous state! • Safeguard 2 is opened • Module switches off, 2-channelled • Renewed start possible

Fig. 7 Front and reverse page of the Schmersal/Elan leaflet on the question of diagnostic coverage ...

**PART 3: ADDITIONAL NEW REQUIREMENTS OF EN ISO 13849-1**

In addition to performance level (PL), the future benchmark for the safety-related quality of a safety-related part of a control system (SRP/CS [2]) in terms of the required degree of risk reduction of a safety function, EN ISO 13849-1:2006 [3] contains a few further requirements or clarifies requirements that had already been addressed in EN 954-1:1996. Moreover, questions come up in this connection which, while not new, are afforded greater attention through application of EN ISO 13849-1.

**NEW: Requirements for application software**

There are new requirements in EN ISO 13 849-1 that must definitely be taken into consideration when using safety-related application software, so-called SRA/SW if, for example, safety PLCs or safety-related bus systems are deployed and if logical sequences for safety functions are programmed. Therefore not only developers of systematic software (SRE/SW for Safety-Related Embedded Software) have to satisfy (a great number) of requirements, but also the user (in other words the manufacturer of the machinery) who makes use of the programmable electronics.

The background to this is that the use of programmable control systems is associated with

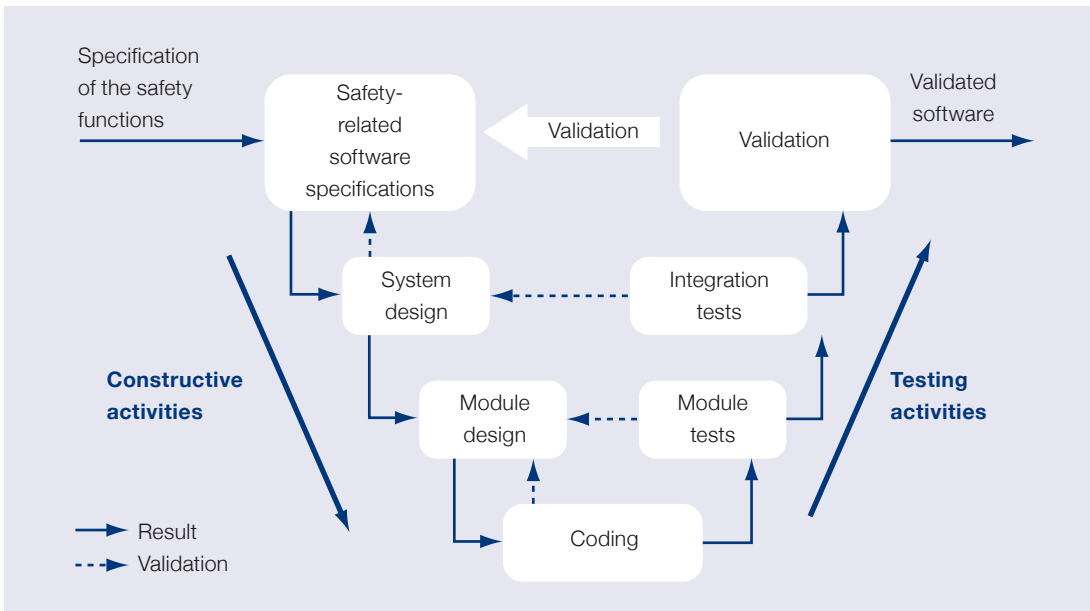
considerable degrees of freedom in a positive sense and a high degree of flexibility, but conversely and as a result of this, also opens up several “new” possibilities for doing something “wrong”. The SRA/SW requirements are designed to counter or prevent this.

On the one hand the user must be aware of a distinction in terms of the programming language of the application software (LVL vs. FVL [4]), and on the other hand between the different requirements (“rules of the game”) in terms of the performance levels to be attained. At all events a simplified V-model forms the basis of the SRA/SW application.

The relevant provisions in EN ISO 13849-1 can be found under Section 4.6 (specifically under 4.6.1 and 4.6.3 as well as under 4.6.4 with respect to parameterisation). Apart from this unfortunately little assistance is available concerning the interpretation and details of SRA/SW, at least to our knowledge. We refer again here to the BGIA Report (Chapter 6.3 et seq.) and to a VDMA brochure “Programmierbare Sicherheitstechnik” (order number vf 179100, VDMA-Verlag GmbH

**NEW: Annex G**

This annex concerns additional considerations connected to controlling and preventing sys-



**Fig. 8** Development model: simplified V-model; objective: software that is legible, comprehensible, can be tested and used

**Annex G**  
(informative)

**Systematic failure**

**G.1 General**

ISO 13849-2 gives a comprehensive list of measures against systematic failure which should be applied, such as basic and well-tried principles.

**G.2 Measures for the control of systematic failures**

The following measures should be applied:

- Use of deenergisation (see ISO 13849-2)

The safety-related parts of the control system (SRP/CS) should be designed so that with loss of its power supply a safe state of the machine can be achieved or maintained.

Measures for controlling the effects of voltage breakdown, voltage variations, over-voltage and undervoltage conditions should be predetermined.

SRP/CS behaviour in response to voltage breakdown, voltage variations, over-voltage and undervoltage conditions should be predetermined so that the

tematic failures in safety-related parts of control systems. One could say this is a supplement to EN ISO 13849-2 that affects the validation of SRP/CS and that specifies important measures to prevent risks of this nature, especially in its Annexes A to D.

With regard to the significance of preventing and controlling systematic failures, one must always bear in mind that this is the reason behind most machine accidents (estimates speak of 60%) and the realisation of corresponding counter-measures forms the basis for every performance level, starting from PL “a”.

### NEW! Trailing edge detection for manual reset function

In future a manual reset function (the “re-engaging”/acknowledgement of a protective device after triggering a stop command) must be designed such that it can *only take place by releasing the drive element (of a command device) in its actuated (on) position* (see EN ISO 13849-1 Section 5.2.2). This function is also commonly referred to as “signal processing of the trailing edge of a reset button” (or trailing edge detection).

The actual restart signal then takes place additionally and detached from acknowledgement by the normal machine control system.

The fact that acknowledgement may only take place from one position and that it is necessary to ensure that the hazardous area is always in sight so that the operator can ascertain that no colleague remains in this area should be patently obvious. Other measures may need to be taken

in this connection, for example double acknowledgement if there is poor visibility of the hazardous area.

The aim, therefore, is to prevent anybody being consciously or unsuspectingly in a shut-down hazardous area who will then be at risk when the machine suddenly starts up again.

Academics may argue about whether the requirement for trailing edge detection was already to be found with the same clarity in EN 954-1:1996. Whether or not this is the case, the requirement makes real sense; malfunctions in the acknowledgement button (whether these concern malfunctions resulting from manipulation or faulty NO contact) that might otherwise lead to the machine starting up unintentionally will be detected.

The manual reset function forms a safety function that must be considered separately, and for which a performance level must be established ( $PL_{r(\text{required})}$ ) and implemented accordingly ( $PL_{\text{actual}}$ )



**Fig. 9** Safety module SRB 100DR with double acknowledgement, for example, ensures additional safety in accessible hazardous areas. The module ensures that the machine control system can only be switched back on once the operator has left the hazardous area. This is because the operator must firstly actuate a reset or restart button located inside the system, followed by a second which is positioned outside the accessible hazardous area.

→ PL<sub>r</sub>). This means that signal processing via a customary PLC (max PL “b”) is generally not an option for acknowledgement functions; rather a specially strengthened control element (whether in the form of a safety relay module, a safety PLC or similar) will normally be required here.

A reset function must be provided if this is dictated by the risk assessment, i.e. as a rule in accessible hazardous areas such as accessible machinery rooms; it must/may (see EN ISO 13849-1 Section 5.2.2):

- be provided by a separate, manually operated device in the SRP/CS;
- only be reached if all safety functions and protective devices are functional;
- not initiate any movement or hazardous situation itself;
- enable the control system to accept a separate start command;



- may only take place by releasing the drive element in its actuated (on) position.

See pages 105 and 150 for more information on “RESET”.

Footnotes:

- [1] SRP/CS: **Safety Related Part(s) of (a) Control System(s)**
- [2] SRP/CS: **Safety-Related Parts of Control Systems**
- [3] EN ISO 13849-1:2006 has now been replaced by the release of EN ISO 13849-1:2008. The only difference concerns the reference to the new Machinery Directive 2006/42/EC in the new ZB Annex of the standard. We therefore refer to standard EN ISO 13849-1:2006 in the following.
- [4] LVL for **Limited Variability Language** (programming languages according to IEC 61131 are typical) vs. FVL for **Full Variability Languages** (e.g. Assembler, C or C++).



*Chapter 3:*

***Safety-related issues  
with cross-cutting significance***





# Risk assessment and the safe design of machinery\* [a]

\* Following introductory information, the following article is essentially based on a technical publication by Dr. Alfred Neudörfer, retired Academic Director at the Technical University of Darmstadt.

The design of safe and ergonomic machinery pursues three objectives:

- 1) to improve occupational health and safety;
- 2) to enhance efficiency; and thereby
- 3) to contribute to human productivity.

The prerequisites for achieving these objectives include risk assessment that is as complete and consistent as possible (where risk assessment is understood as an umbrella term for an iterative process of risk analysis, risk assessment and the establishment of corresponding risk reduc-

ing measures taking into account the limits of a machine = intended use that can be reasonably expected including foreseeable misconduct, spontaneous behaviour and reasonably foreseeable misuse).

While this basic aspect was somewhat pointed out indirectly in the previous 98/37/EC Machinery Directive under the heading “Hazard analysis”, this changed substantially in terms of clarification in the subsequent Directive 2006/42/EC. The subject of “risk assessment” is dealt with here much more comprehensively in Annex I Section 1.

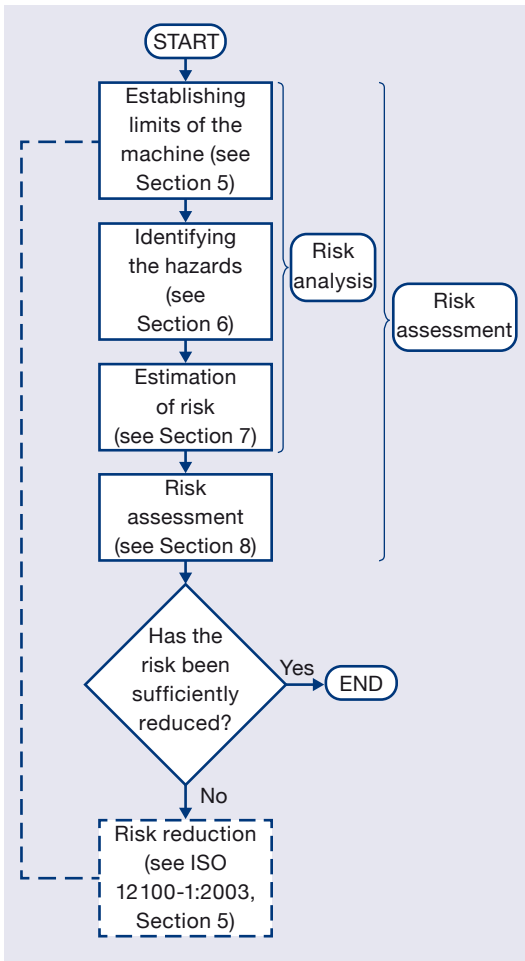


Fig. 1 Iterative process of risk reduction – excerpt from EN 12 100

**MD 2006/42/EC – Annex I –**  
**1. General principles**

The manufacturer of machinery or his authorised representative must ensure that a risk assessment is carried out in order to determine the health and safety requirements which apply to the machinery. The machinery must then be designed and constructed taking into account the results of the risk assessment.

By the iterative process of risk assessment and risk reduction referred to above, the manufacturer or his authorised representative shall:

- determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse thereof;
- identify the hazards that can be generated by the machinery and the associated hazardous situations;
- estimate the risks, taking into account the severity of the possible injury or damage to health and the probability of its occurrence;
- evaluate the risks, with a view to determining whether risk reduction is required, in accordance with the objective of this Directive ;
- eliminate the hazards or reduce the risks associated with these hazards by application of protective measures, in the order of priority established in section 1.1.2 b.

Fig. 2 Risk evaluation: a MUST to comply with the EC Machinery Directive!

The detailed approach to be taken (or which can be taken) with respect to these requirements is then explained in the relatively new standard ISO EN 14 121-1:2007 which replaces the previous “Risk assessment” standard EN 1050. A technical report ISO/TR 14 121-2 (Practical guidance and examples of methods) is also available for better understanding.

As well as the usual editorial revisions, the “new” standard has been adapted to ISO EN 12 100-1:2003 with respect to content, concept and the

scope of the conceptual stipulations has been widened. The usability of the standard has been improved by incorporating separate tables giving examples of hazards, hazardous situations and hazardous events in Annex A and through additional figurative presentation of typical examples of hazards. Bearing in mind the detailed and comprehensive informative technical report ISO/TR 14 121-2 with examples of methods, the former informative Annex B “Methods for examining hazards and estimating risk” has been deleted from the standard.

**EN ISO 14 121-1 – Annex A**

The most important changes in EN ISO 14 121-1 are probably those in Annex A (“Examples of hazards, hazardous situations and hazardous events”) that now has four subsections:

- A.1 General
- A.2 Examples of hazards
- A.3 Examples of hazardous situations
- A.4 Examples of hazardous events

The new structure of the hazard list in Table A.1 is of particular interest. “Hazards” are now split up into examples reflecting “potential consequences” and “origin”. This pragmatic approach shortens the list of hazards because redundancies are eliminated.

No.	Type or group	Examples of hazards		Subclause of ISO 12100-1:2003 or ISO 12100-2:2003	
		Origin <sup>a</sup>	Potential consequences <sup>b</sup>	ISO 12100-1	ISO 12100-2
1	Mechanical hazards	— Acceleration, deceleration (kinetic energy)	— Being run over	4.2.1	4.2.1
		— Angular parts	— Being thrown	4.2.2	4.2.2
		— Approach of a moving element to a fixed part	— Crushing	4.3 a)	4.3 a)
		— Cutting parts	— Cutting or severing	4.6	4.3 b)
		— Elastic elements	— Drawing-in or trapping	4.10	4.6
		— Falling objects	— Entanglement	5.1	5.1
		— Gravity (stored energy)	— Friction or abrasion	5.2	5.2
		— Height from the ground	— Impact	5.3	5.3
		— High pressure	— Injection	5.5.2	5.5.2
		— Machinery mobility	— Shearing	5.5.4	5.5.4
		— Moving elements	— Slipping, tripping and falling	5.5.5	5.5.5
		— Rotating elements	— Stabbing or puncture	5.5.6	5.5.6
		— Rough, slippery surface	— Suffocation	6.1	6.1
		— Sharp edges		6.3	6.3
				6.4	6.4
				6.5	6.5

**Fig. 3** New variation of determining hazards in accordance with EN ISO 14 121-1: Table A.1

It would appear to be important, however, that the examples of hazardous events contained in Table 4 are examined separately since Table A.1 no longer has any points dealing, for example, with hazards in conjunction with the failure of pneumatic or hydraulic equipment, electrical equipment, control system etc.

It is conspicuous when a comparison is made to the hazard list in EN 1050 that the special hazards regard-

regarding the specific classes of machinery in the Machinery Directive (MD Annex I, Sections 2-6) have been eliminated. Here too, this change has positive effects because redundancies can be avoided and the list of hazards is drastically reduced. Until now it has always been somewhat illogical as to why Point 7.1, for example, specifies examining hazards due to fire and explosion while hazards due to fire and explosion are dealt with again under Point 32 in the section covering specific considerations for machinery used in mining. Ultimately the entire process of identifying hazards is based on previously stipulated limits of the machinery (as shown in Figure 1), a process which, as is well-known, defines “intended use”. Ideally this intended use should therefore form the basis of the considerations in Point 7.1.

What pleases some experts results in scepticism in others because the new presentation of hazard lists means the direct connection to basic health and

Origin related to	Hazardous event	Subclause(s) of ISO 12100-2:2003 (useful references)
Shape and/or superficial finishing of accessible parts of the machine	— Contact with rough surfaces — Contact with sharp edges and corners, protruding parts	4.2.1
Moving parts of the machine	— Contact with moving parts — Contact with rotating open ends	4.2, 4.14, 4.15 5.1 to 5.3 5.5.2 to 5.5.4 6.3 to 6.5
Kinetic energy and/or potential energy (gravity) of the machine, parts of the machine, tools and materials used, processed, handled	— Falling or ejection of objects	4.3, 4.5 4.10 to 4.12 5.2.1, 5.2.2, 5.2.7 5.3 5.5.2, 5.5.4, 5.5.5 6.4, 6.5
Stability of the machine and/or parts of the machine	— Loss of stability	4.3 a) and b) 4.6 5.2.6, 5.2.7 6.3 to 6.5
Mechanical strength of parts of the machine, tools etc.	— Break-up during operation	4.3 a) and b) 4.11, 4.13 5.2, 5.2.7 5.3.1 to 5.3.3 5.5.2, 6.4, 6.5
Pneumatic, hydraulic equipment	— Displacement of moving elements — Projection of high pressure fluids — Uncontrolled movements	4.3 a) and b) 4.10, 4.13 5.2.7 5.3.1 to 5.3.3 5.5.4, 6.4, 6.5

**Fig. 4** Table A.4: Hazardous events

and safety requirements in accordance with Annex I of the Machinery Directive is no longer as transparent as it was previously. Added to this is the fact that cross-references to Annex I of the Machinery Directive (or Annex A of EN 292-2:1991/A1:1995 respectively) that were present in EN 1050 are literally missing now. The cross-references to EN ISO 12 100-2 which provide pragmatic solution approaches have also now been simply assigned to a complete hazard group (as shown in Figure 3), which at the very least will make it harder to find normative solution suggestions.

In practice this could mean that the process for achieving safety objectives is divided into two steps: firstly the hazards are determined according to the hazard lists, and then an examination takes place on the basis of the points in Annex I of the Machinery Directive to see whether all objectives of the Machinery Directive have actually been satisfied.

It is also essential to take note of Table A.3 “Examples of hazardous events”. Consideration of the different life cycles of the machinery is frequently “forgotten”,

especially in intuitive hazard analyses, and this would be compliant neither with EN ISO 14 121- 1 or EN ISO 12 100-1 (5.3) nor with the Machinery Directive! Annex A.3 in EN ISO 14 121-1 sets out details of the life cycles using typical “examples of tasks” that may occur when using the machinery or system, such as clamping/ securing the piece of work, settings, cleaning, disinfection, lubrication, troubleshooting, restarting after failure of the control equipment and protective devices ... .

Phases of machine life cycle	Examples of tasks
Transport	<ul style="list-style-type: none"> <li>--- Lifting</li> <li>--- Loading</li> <li>--- Packing</li> <li>--- Transportation</li> <li>--- Unloading</li> <li>--- Unpacking</li> </ul>
Assembly and installation	<ul style="list-style-type: none"> <li>--- Adjustments of the machine and its components</li> <li>--- Assembly of the machine</li> <li>--- Connecting to disposal system (e.g. exhaust system, waste water installation)</li> <li>--- Connecting to power supply (e.g. electric power supply, compressed air)</li> <li>--- Demonstration</li> <li>--- Feeding, filling, loading of ancillary fluids (e.g. lubricant, grease, glue)</li> <li>--- Fencing</li> <li>--- Fixing, anchoring</li> <li>--- Preparations for the installation (e.g. foundations, vibration isolators)</li> <li>--- Running the machine without load</li> <li>--- Testing</li> </ul>
Commissioning	

Fig. 5 Table A.3: Hazardous situations

If one follows the normative recommendations, the result should be a risk assessment that complies with the requirements specified in the introduction above.

Nevertheless, it is not sufficient to comply with regulations. Referring to answers by identifying them in the regulations does not go far enough. The real task of creative design engineers was, is and remains consideration of safety-compliant solutions and their realisation within the framework of normative stipulations.

**Terms**

The terms danger, hazard and risk are not always clearly differentiated or used correctly, either in everyday language or in some regulations and standards. From a physical perspective, danger constitutes an objectively existent energetic or material damage potential which exceeds the relevant limits of people and which may lead to health impairments or damage with different degrees of severity. While several limits are known for load and stress variables (MAC values and biological tolerance values for hazardous materials, retard limits for crash situations, limits for noise levels that are injurious to health etc.), only few re-

liable values have been published for mechanical strain on the body at or in dangerous positions.

Reference is made to hazards if there is a possibility that man and danger will meet spatially and temporally such that damage to health or health impairments may ensue so that the possibility of an undesirable event exists.

A special approach is required for the term ‘risk’. It stands for the impact on people or the environment that arises at differing frequencies as a result of hazards. The severity of the impact can differ. The degree of risk will be influenced by the possibility or impossibility of technical or organisational countermeasures (as shown in Figure 7).

The working area and above all the impact area of every work system in the respective life phases must be critically appraised using this terminological tool. It is helpful for design engineers if these considerations take place in the categories in which they are used to thinking: material, energy, information. These are variables that they must implement in the machinery to be designed so that it can satisfy the intended technological function.

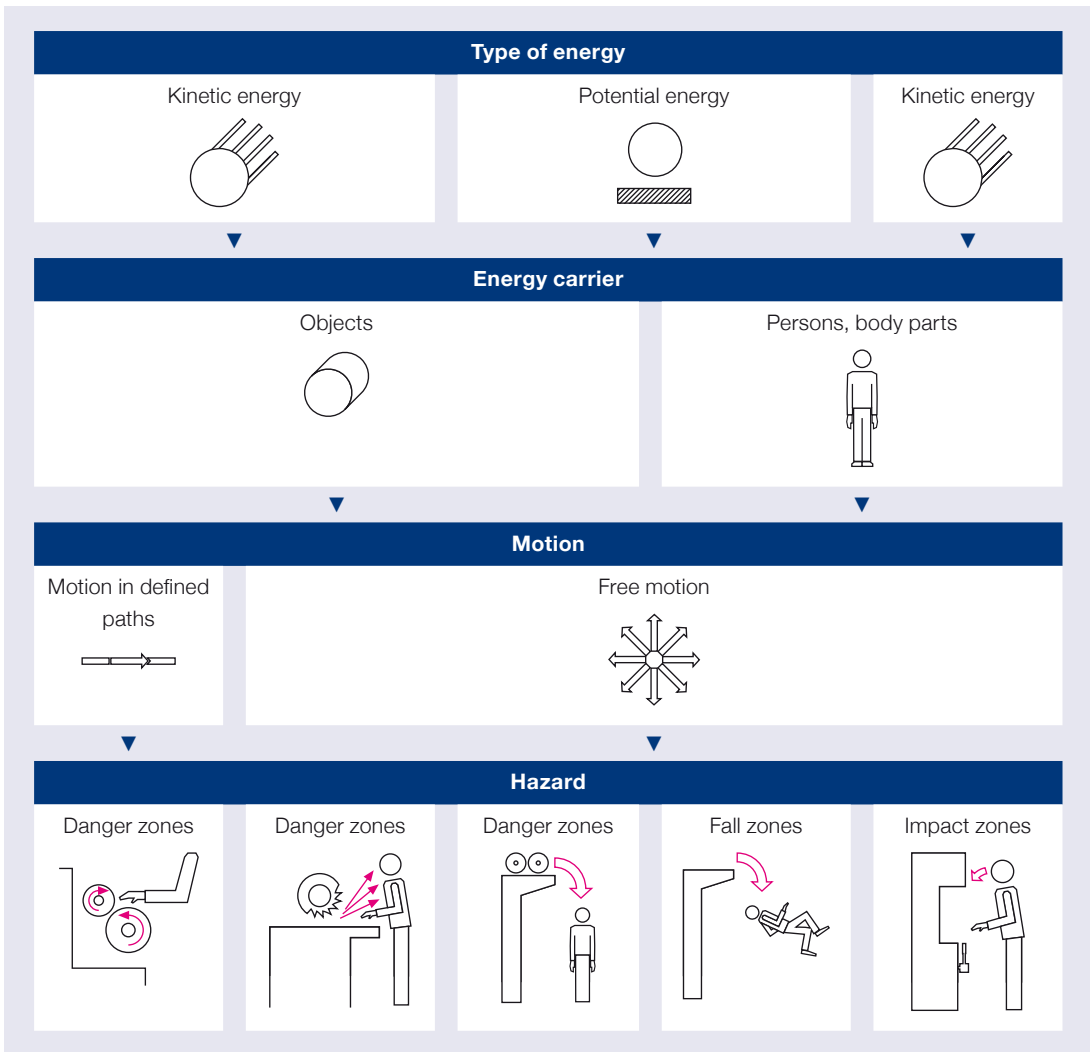


Fig. 6 Physical principles of hazardous situations



Fig. 7 Relationship between danger, hazard and risk

The actual manifestation of hazards within these categories can be diverse. Energetic impacts are of special significance to the area of accident prevention. How these can be further systematically arranged is demonstrated using the example of mechanical hazards. The basic differentiating feature concerns the type of mechanical energy (kinetic and potential energy) as well as the question of what the energy is connected to (objects or people) and which movements precede a possible accident (kinematic or free movements; Figure 6).

For each type of hazard it is necessary to be aware that dangers must be differentiated according to whether they are stochastic or deterministic, related to the frequency of their occurrence (as shown in Figure 8).

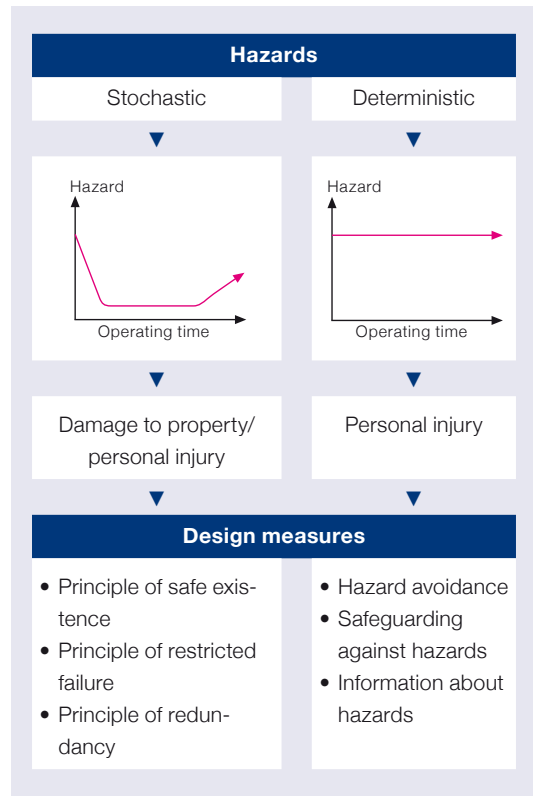
Stochastic dangers occur during the service life of the machine at a temporally-related frequency. The bathtub curve is a much described sequence. Typical cases are dangers caused by component failure which can occur relatively frequently at the start of a life phase (design and calculation errors come to light), then at a low level as a result of pure chance, increasing again in the final phase of the machinery due to aging, corrosion, wear etc. It is especially important to intercept component failure reliably in the case of safety-relevant parts of control systems. This can result in the loss of safety functions that in turn lead to risks occurring that go beyond an acceptable level of risk.

By contrast, deterministic dangers are latent throughout the entire life of the machinery at a constant frequency of 1. They are simply there, waiting for their opportunity. This means that every possible accident on them can also occur. Unlike stochastic dangers, deterministic dangers are usually clear and therefore directly recognisable, as is the case with an open chain drive.

### Determination of safety measures

What are the first hazards that design engineers need to address? This depends on the risk concerned: on the interaction between frequency of occurrence, level of hazard potential and any possibilities for avoidance.

The plan shown in Figure 9 is now generally used to make a preliminary selection, ensuring you re-



**Fig. 8** Measures to counter stochastic and deterministic hazards

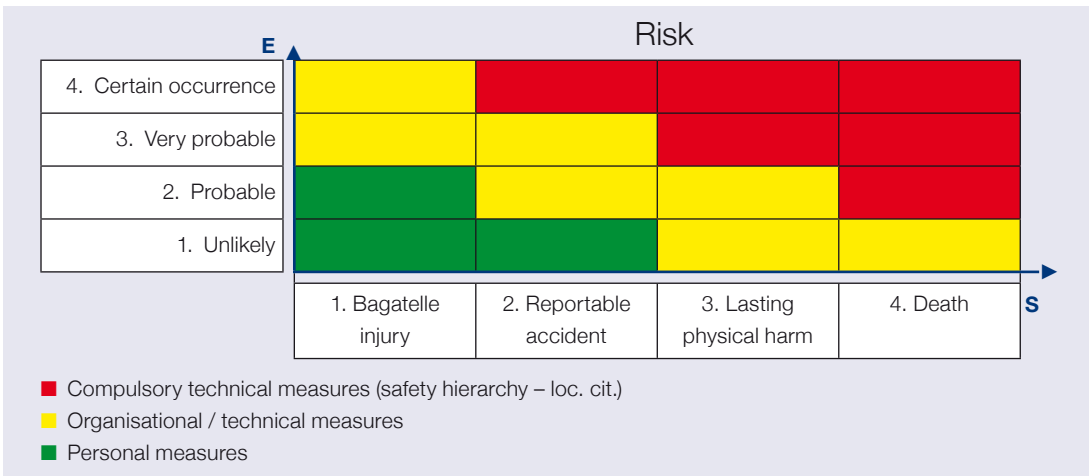
tain an overview in the face of the multitude of risks that can be determined when looking more closely at a machine (i.e. to avoid not being able to see the wood for the trees). The focus below is on the “red” columns.

The following must be taken into consideration when selecting design methods to eliminate hazards:

- Any risks present must basically be reduced using design measures to an extent that a tolerable risk from an individual and societal point of view is achieved.
- Since stochastic (random) and deterministic (systematic) dangers differ substantially from each other, it is only logical that the design measures directed at them must also differ (as shown in Figure 8).

Both types of hazard must be addressed from a design perspective if safe machines are to be built.

Design measures aimed at stochastic hazards pursue the objective of ensuring the function



**Fig. 9** Risk preselection

intended for the machine or components is reliably satisfied while at the same time constructing a certain resistance to interference. The most well-known principles are:

- Reliable existence
- Restricted failure
- Redundancy.

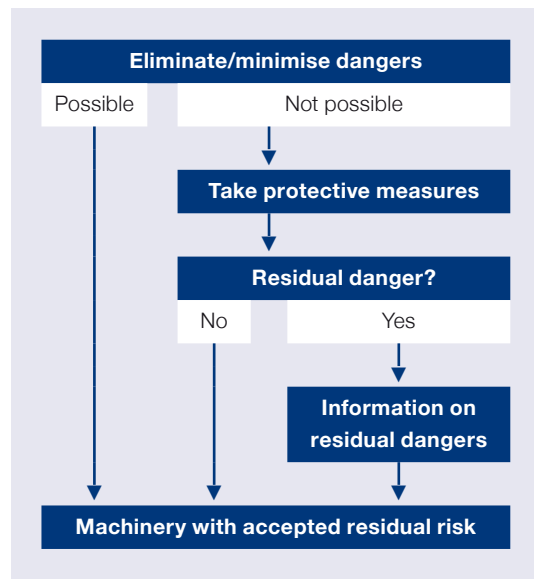
The assumption when implementing the principle of reliable existence is that all demands that can be experienced by a machine are known, that the calculation methods applied and resistance hypotheses are realistic and that no other influences will occur during the service life of the machine apart from those taken into consideration in the calculation.

The principle of restricted failure takes a completely different path. Faults are deliberately admitted here. However systems are designed such that the safety-related crash does not have bottomless consequences, but rather remains at an agreed level.

Redundant systems provide more components to satisfy the function than would actually be necessary in the hope that one of these systems completely satisfies the function of the other in the event of failure. The principle must be to achieve as much reliability with as little redundancy as possible. Namely the Achilles' heel of all redundant measures lies in the fact that there are situations where all redundant systems can fail simultaneously due to a common fault. It is not always possible to predict these situations.

The Machinery Directive [1] specifies the following three steps for design measures to prevent deterministic dangers being able to have an impact on people; these steps must be implemented in the following order:

1. Elimination or minimisation of dangers through design; integration of the safety concept in the development and construction of the machinery (direct safety technology).
2. Taking requisite protective measures to prevent dangers that cannot be eliminated (indirect safety technology).
3. Informing the user about residual dangers resulting from the incomplete efficacy of the protective measures taken; pointing out any



**Fig. 10** Strategy for safety technology

required special training and personal protective equipment (safety technology warnings).

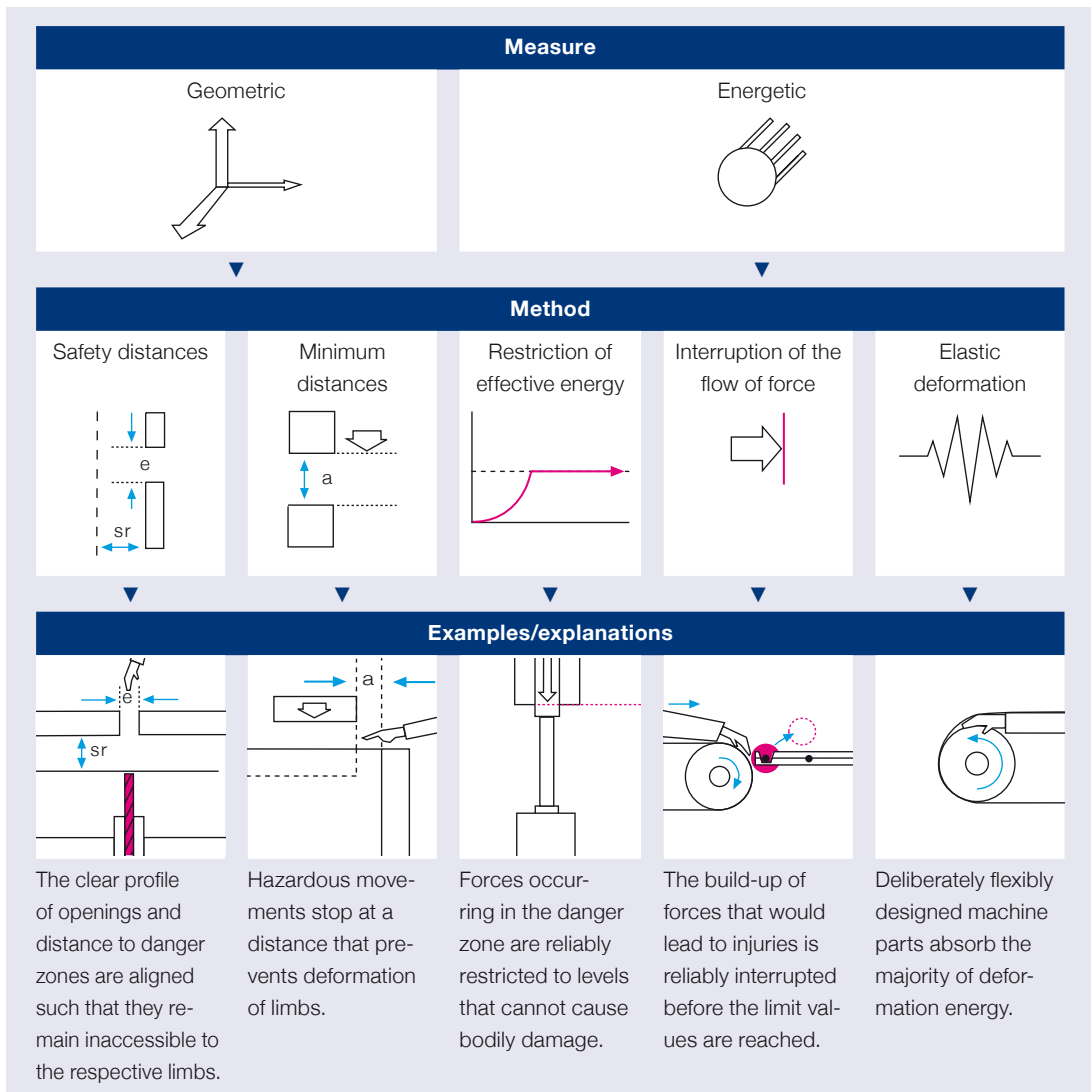
These steps have been generally introduced and accepted already at an earlier date under the headings of direct and indirect safety technology and safety technology warnings under the headings of “avoiding dangers, protecting against dangers and drawing attention to dangers” (as shown in Figure 10).

**Direct safety technology**

Direct safety technology methods are an attempt to design components, machines and processes in such a way that these result in no hazards or only slight hazards. However in the case of real

machines, the only ones where such dangers can be prevented are those that have no technological function. Technologically-related dangers, e.g. tool movements required for processing, must be approached using indirect safety technology methods.

The direct safety technology methods will be explained using the example of mechanical danger zones, i.e. machine parts or components moved by kinetic energy or drive energy that can cause injury to people. Mechanical danger zones can be avoided if the traumatic deformation of body parts that occurs in an accident is countered in advance using design measures. Geometric or energetic measures come into question here (as shown in Figure 11).



**Fig. 11** Methods for eliminating and minimising dangers



A deformation force and a deformation trajectory are required for deformation to take place. Both variables are determined by the geometric form of the danger zone and the energy converted in it. The design measures for these physical variables use direct safety technology.

Geometric design measures influence the spatial meeting of limbs and danger zones. They are directed towards the following:

- Maintaining minimum distances in danger zones;
- Complying with safety distances to danger zones;
- Influencing the effectiveness of danger zones through shaping of machine parts.

Minimum gaps between the moving machine parts prevent parts of the body getting caught. There is room for parts of the body to move safely between machine parts. This method is particularly effective in preventing areas between the end bearings of moving parts and the frame of the machine that cause crushing and shearing points between the end positions, but has little effect on areas where this is danger of being pulled in, cut or stabbed. The minimum gaps to be maintained are stipulated in DIN EN 349 [2].

Safety distances prevent accessibility to danger zones. Safety distances for upper limbs are stipulated in the standard DIN EN 294 (but see following note), while the standard DIN EN 811 (newly combined with 294 as DIN EN ISO 13857 now [3]) specifies the gaps for lower limbs. These levels must not only be taken into consideration for geometric measures in direct safety technology, but also when designing guards. If the levels cannot be realised for practicable reasons, compensatory measures must be applied or the non-compliance with the two above mentioned standards justified.

By varying the geometry and shape of machine parts that create danger zones it is in principle possible to avoid narrowing spaces or gaps. By contrast to the geometric methods, energetic methods permit interaction, but try to prevent injuries by influencing the energy that impacts on the body in the following ways:

- Restricting the effective energy
- Interrupting the flow of force to the danger zone
- Targeted deformation of machine parts.

The first method attempts to limit the energies and forces reaching the danger zone such that their impact on the part of the body remains below specific physiological levels. This method can only be used under certain conditions, because generally recognised limit values are only known for a few applications (e.g. closing edges on power-operated doors). What is more, the safe energy levels are so low that technological use is only possible in a few cases. The second method prevents the deforming effect of the danger zone on people by interrupting the force flow between the body and the danger zone where possible before the pain threshold has been reached. With the third method the rigidity of machine parts is reduced to the extent that, in the case of getting caught, the targeted deformation guides the damaging energy to parts of the machine that are insensitive to pain.

Although the application of direct safety technology is always cited in first place and represented as the ideal solution, it is only possible to use it to prevent danger zones that have no technological function. Otherwise this would question on the machine to be designed. In all other cases, i.e. for danger zones without technological function, an attempt should be made to apply the methods set out because these are reliably effective long-term without safety-related “extras”.

### **Indirect safety technology**

Indirect safety technology components, e.g. protective equipment, safeguard danger zones that cannot be avoided. Protective equipment is positioned between the user and the danger area or danger zone and interrupts the possibility for any spatial and/or temporal meeting between people and the danger zones or sources of danger. Guards or unguarded protective devices are used for this (as shown in Figure 12).

Guards are material barriers that prevent access or entry to the danger area. In addition they prevent people getting hit by objects that are ejected from the protected process area.

While unguarded protective devices do not necessarily prevent access/entry to the danger area, they make it safe by impacting on the process via the control system of the machine in such a way that non-hazardous machine or process states are established as soon as unguarded protective devices react or are triggered.

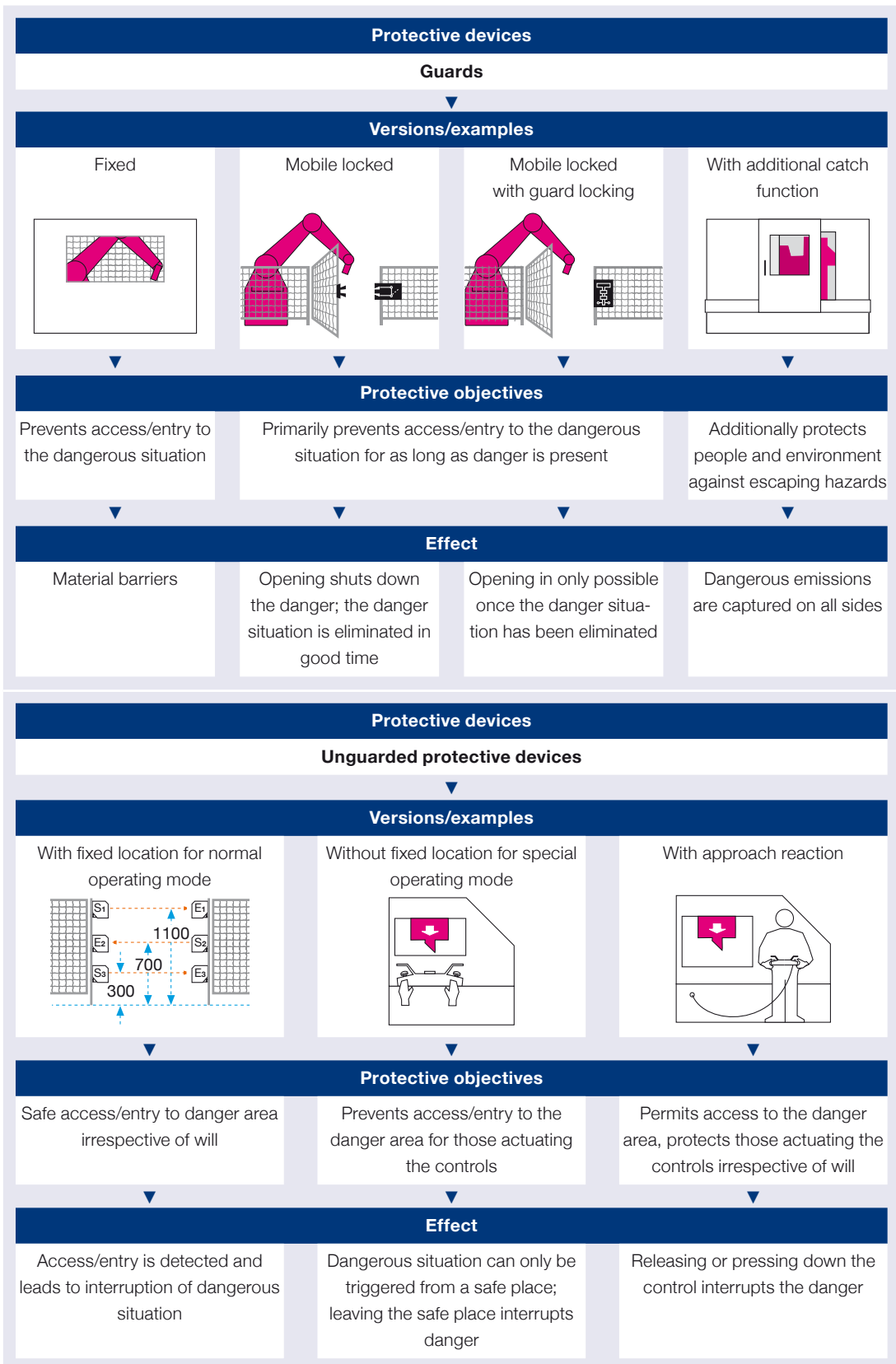


Fig. 12 Overview of protective devices

As additional components, protective devices do not achieve the safety level of direct safety measures. In order for them to have a reliable effect despite this they must be designed to withstand stresses and maintain their protective function, e.g. access safety, throughout the entire service life of the machine. Furthermore they must be integrated in the machinery concept and process flow such that they cause no malfunctions and are designed so as to be easy to use.

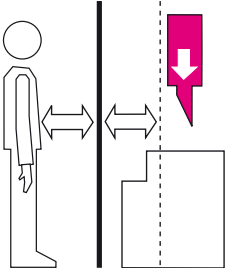
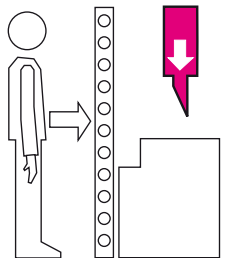
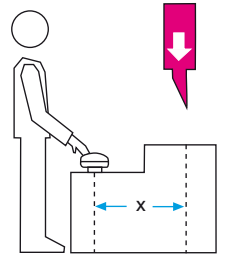
**Advantages and disadvantages of the respective protective devices**

The direct safety method provides safety without extras, but can only be deployed where danger zones have no technological function (operat-

ing function). Their characteristic low energy level also places narrow limits on applicability. The indirect safety technology has more flexible methods. Its assemblies (protective devices) offer greater possibilities for designing operating processes more safely. Protective devices have a long and successful history of development behind them. Nevertheless there is no universal protective device to reliably protect against all dangers at all times. Each type of protective device has certain advantages and disadvantages (as shown in Figure 13).

**Selection of protective devices**

There are many suppliers here and now offering an extremely wide range of the most diverse

Protective device	Advantages	Disadvantages
<p>Guard</p> 	<ul style="list-style-type: none"> <li>• Reliable material separation of man/danger and danger/man</li> <li>• Simple, reliable parts</li> <li>• Little technical/material expenditure</li> <li>• Modular system for fencing and retrofitting kits for machine tools as consumer items</li> </ul>	<ul style="list-style-type: none"> <li>• Difficult to use</li> <li>• Impair view</li> <li>• Safety to prevent circumvention and manipulation only possible with considerable effort</li> <li>• Costs increase with length in the case of fencing</li> </ul>
<p>With approach reaction</p> 	<ul style="list-style-type: none"> <li>• Clear view and access to process area during faults</li> <li>• Active protective devices that react in the event of acute hazards</li> <li>• Integration in contemporary control system and automation concepts is not a problem</li> <li>• Difficult to manipulate</li> </ul>	<ul style="list-style-type: none"> <li>• No protection from ejected parts</li> <li>• Relatively expensive to secure short distances</li> <li>• Prone to random fault triggering (risk increases with the length of the beam of light)</li> <li>• Reliable effect depends on the control system</li> </ul>
<p>With fixed location</p> 	<ul style="list-style-type: none"> <li>• Clear view of process area</li> <li>• Relatively manipulation proof</li> <li>• Mobile safety is created using a portable towing cable</li> </ul>	<ul style="list-style-type: none"> <li>• No protection from ejected parts</li> <li>• No protection for unattached persons</li> <li>• Several monotonous manual movements for cyclical actuation</li> <li>• Ergonomic design is not easy</li> <li>• Reliable effect depends on the control system</li> </ul>

**Fig. 13** Advantages and disadvantages of individual types of protective devices

types of protective devices (referred to as “safety components” in the Machinery Directive). The advantage of using them is that the user obtains a compact solution that is generally ready for connection, that has also frequently been certified by a test centre and which relieves them from having to get to grips with the requisite design properties and features themselves. Reference is made here, for example, to the Schmersal range that offers a package of devices and systems in a “one-stop shop” comprising almost everything used for protecting against dangerous machine movements.

Figure 14 contains an overview of these.

**Safety distances and access speeds**

Protective devices, e.g. protective devices with a fixed location (typically two-hand control devices) or protective devices with approach reaction (typically optoelectronic protective devices) do not directly physically separate people from danger, but rather has impact on the machinery via the control system in such a way that safe machinery or process states are set after they have reacted.

The important fact here is that these operating

Interlocking devices with and without guard locking						
						
Safety switches with separate actuator	Safety sensors with magnetic operating principle	Safety guard locking in plastic and metal versions	Wireless systems/key transfer systems	Position switch with safety function	Safety sensors with and without guard locking realised with an inductive working principle	Safety switches for rotating protective devices

Control devices with personal protection function				
				
Emergency stop control devices	Enabling switches	Pull wire emergency switches	Safety foot switches	Wireless control devices with personal protection function

Tactile protective devices/two-hand controls (operating devices with fixed location)				
				
Safety edges	Safety edges for corner areas	Safety bumper	Safety mats	Two-hand controls

Fig. 14 Overview of the protective devices in the Schmersal range (continued overleaf)

Optoelectronic protective devices					
					
Safety light grids/curtains AOPD types 2 and 4	..., optionally with muting, blanking and combination functions, with cyclic operation	..., optionally with protection type IP 69K, also in hygiene-compliant version	Through-beam safety light barriers AOPD types 2 and 4		
Safety-related control devices, safety control systems and bus systems					
					
Safety modules	AS interface safety at work monitor and sensor technology	Zero speed and movement detector	ESALAN-Compact safety control systems, safety PLCs from the PROTECT PSC and PROTECT-SELECT ranges (showing PROTECT-SELECT with optional safety-related wireless extension)		

Fig. 14 Overview of the protective devices in the Schmersal range (continued)

states exist before the endangered persons can reach the danger zones.

**Access speed [4]**

As soon as unguarded protective devices, such as two-hand control devices or light barriers, have been activated they trigger control-related sequences that terminate situations which threaten to be dangerous so quick that there is no danger to persons who consciously or unconsciously penetrate the protected area. Delaying and stopping the moving mass-afflicted machine parts of the drive chain and dangerous zones can only take place within specific time intervals due to the laws of inertia. In addition, every protective device and every control system has a characteristic final signal response delay. Adding both times together produces the total run-down time of the system (T), which in turn using the laws of motion produces a certain over-run traverse.

This specified time is the basis for determining the minimum distance between the protective device and the danger zone that the person covers with his or her body or limbs when moving at a certain speed. The minimum distance S is therefore calculated as follows:

$$S = K \times T + C \text{ (mm)}$$

where

- S is the minimum distance in millimetres, measured from the danger area to the detection point, to the detection line, to the detection level or to the protection field
- K is the average approach speed of the body or parts of the body in millimetres per second
- T is the run-down time of the total system in seconds
- C is the additional distance in millimetres based on the penetration of the danger area before triggering the protective device.

Which protective function (finger or hand detection, detection of persons in protected areas or where there is protected access) the protective device can perform will depend on the resolution (detection capacity) of the protective device. This also dictates which numerical values are to be used for the as yet undefined parameters K for access speed and C for additional distance to calculate the minimum distance.

If the minimum distance calculated is acceptable from ergonomic and economic point of views, it is then necessary to check whether the spatial arrangement of the protective device permits people to be able to remain undetected within the danger area. If this is the case, additional protective measures must be taken.

If the calculated minimum distance is unacceptable from economic and ergonomic points of view, an attempt must be made to shorten the run-down time of the machine or to deploy a protective device with shorter signal processing.

### **Combination of different methods and protective devices**

Basic types of protective device can be combined with each other on actual machines to produce bespoke safety systems. These facilitate characteristic operating conditions and processes with accepted and acceptable residual risks to be performed for the machine as demonstrated using the example of a cutting machine.

Cutting machines are used to cut stacks of paper or similar material. This machinery has substantial potential to injure the operator due to the tools (moving saddle, press beam and extremely sharp blade) and the mode of operation (periodic intervention in the operating area of the tools). Despite this, hardly any serious accidents occur on this machinery thanks to coordinated protective and safety measures.

Cutting machines comprise of a stand and a bench across which a cross-head is spanned. Press beam and blade move out from the bridge of the cross-head. The operator places the cut material on the bench. The saddle accurately slides the stack mechanically under the blade level. In the process crushing and shearing points are created on the reverse of the cross-head between the saddle and press beam during the forwards movement as well as shearing points

between the saddle and bench cut-out during the reverse movement. Both danger zones are safeguarded with a cover that is effective on all sides.

The cutting cycle is triggered using a two-hand control device and maintained by the permanent actuation of the control button, see DIN EN 574. The press beam lowers and presses the stack of paper together forcefully (crushing point) so that the blade following quickly behind (cutting point) is able to perform the cut cleanly and accurately. The blade is then first to return to the cross-head, followed by the press beam. The crushing point between press beam and stack and the cutting point on the blade are protected for the person cutting the paper by the fixed location effect of the two-hand control and the approach function of the light curtain. The light curtain furthermore prevents serious accidents that would necessarily result from other people encroaching in the movement level of the sharp blade.

### **Restriction of availability and high servicing costs where measures are too elaborate**

The design safety measures deployed must work together and must not contradict each other. Machinery operators and machinery users must view them to be necessary and acceptable. Too much safety can jeopardise the attainment of protective objectives in the same way as too little can. The principle must be to approach complex hazards with simple safety measures.

After all, safety technology will only be accepted if the user finds it transparent, practicable and of use. Aside from a lack of acceptance by operators of the additional costs involved, an excess supply of safety does not necessarily boost the availability and manageability of a machine or promote operations. Elaborate safety technology is necessarily accompanied by a need for more servicing. The servicing required for perfect functioning of the safety systems can itself become a source of special events that have a negative impact on safety at work. Faults in maintenance and servicing may lead to early failures, random failures and late failures.

The reason for early failures may be unnecessary routine maintenance, excessively invasive measures or lack of technical knowledge and craftsmanship of staff (damage caused by repair work).



Random failures with serious effects on safety at work are frequently caused by servicing faults such as leaving tools in the machine or by forgotten mechanical or electrical bridges.

Characteristic late failures are isolated servicing and maintenance measures carried out without proper coordination.

### **Danger of circumvention in the case of measures that lack practical relevance**

Protective devices are function machine components. If not all dangers have been prevented by design measures, machines only become usable within the meaning of the EC Machinery Directive once they contain these devices. Statutory stipulations should serve as orientation during design and the functional integration of protective devices and other protective measures in the machinery concept. In this context it is of far greater importance, however, to take a precise and detailed analysis of operational requirements as the starting point. Requirements for protective devices can be derived from this and documented in the specifications as fixed demands. There is little benefit to safety at work if a machine formally satisfies all statutory requirements, but the protective measures limit the performance of the machine or the operator. Safety measures of this nature will not gain acceptance and almost force the machine user to breach safety regulations.

Once each safety measure has been taken, an honest risk analysis must also consider the possibility for manipulation. In doing so, the technical intelligence and creativity of the operators must not be underestimated. Above all, one must be guided by the thought that manipulation does not take place willingly, but rather that it is an indication that the protective measure has not been ideally integrated into the operating concept of the machine.

It is rare for a situation to be improved by intensifying the protective measure. If, for example, the interlock of a protective device has been replaced by guard locking but the concept whereby the machine cannot be moved further along after opening remains unchanged, the conflict is merely intensified. It is better to ensure in advance using graduated measures that the requisite activities can be performed with open protective device at an acceptable level of risk.

Practical experience has demonstrated that the risk of misuse with guards is always increased in the following situations:

- Protective devices need to be removed or opened too frequently and too laboriously because the machine or process is prone to faults;
- The protective device vibrates and rattles;
- The protective device is difficult to manage;
- Little craftsmanship and intellectual effort are required to circumvent the protective devices;
- The required view of operations is not possible;
- The interlock response causes follow-up malfunctions; or
- It is not possible to carry out necessary work in special operating mode when guards are open;
- If, in the case of guard locking, there is a long waiting period when opening protective devices.

Moreover, unguarded protective devices are especially at risk if

- They are an obstruction for the user;
- They are positioned in the working and traffic areas in such a way that they are triggered unintentionally too often, thereby causing interference to processes.

The practical demands passed on to design engineers should not be regarded as complicating the design task. Rather these are important sources of information for practical, safety-compliant machines. Market observation of products must include systematic collection and evaluation of information (customer and repair service, spare part consumption, complaints, damage and accidents) and produce feedback for development and design departments.

### **Safety technology warnings**

If residual risks remain for users of machinery which can neither be completely prevented by direct safety technology measures during design nor mitigated using modules and functional parts from indirect safety technology, the prerequisites and conduct under which safe work is possible must be pointed out using safety technology warnings.

Manufacturers must ensure that the users of machinery are able to detect threatening dangers in good time. They must indicate dangers



so these produce effective behaviour and those at risk are obliged to behave in a safe way. However this situation can only become established if those concerned are also aware of what to do when a warning has been indicated and are also in a position to do it. Safety technology warnings must always be combined with operational training and operating instructions. Manufacturers must point out the obligations of operators to prepare operating instructions and carry out training in the documentation accompanying the machinery.

Safety technology warnings are the weakest link in the safety chain because they are geared towards actions that depend on the more or less defined degree of safety consciousness of the machine user. For this reason, safety technology warnings must never be used as sole measure. They must fall back on artificial sources of information whose message can be picked up and understood by those at risk using their senses (principally using their sight, hearing and sense of touch).

The informative signs can be of a static or dynamic nature. Sources of information are static if the information is present at all times as is the case with safety signs. Operating manuals, pictograms and warning signs are also important carriers of static safety messages. By contrast, dynamic sources of information only signal danger when this is acute. Visual and acoustic warning devices, active machine diagrams and leading protective devices are typical dynamic sources of information in safety technology warnings.

References (standards):

- [1] **EN ISO 12100-1:**  
Safety of Machinery – Basic concepts, general principles for design – Part 1: basic terminology, methodology
  
- EN ISO 12100-2:**  
Safety of Machinery – Basic concepts, general principles for design – Part 2: Technical principles
  
- [2] **EN 349:**  
Safety of Machinery – minimum gaps to prevent crushing of parts of the human body
  
- [3] **EN ISO 13857:**  
Safety of Machinery – Safety distances to prevent hazard zones being reached by upper and lower limbs
  
- [4] **EN ISO 13855:**  
Safety of Machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body

Further references:

- [a] You can find a detailed description in the book publication (as shown in Figure on right) *Neudörfer: „Konstruieren sicherheitsgerichteter Produkte (Methoden und systematische Lösungssammlungen zur EG-Maschinenrichtlinie“*. A new edition is currently in the process of fundamental revision and will be published shortly.
- [b] **Montenegro, S.:**  
Sichere Steuerungen, München; Wien: Hanser-Verlag 1999
- [c] **Neudörfer, A.:**  
Konstruieren sicherheitsgerechter Produkte, Methoden und systematische Lösungssammlungen, Berlin, Heidelberg, New York: Springer, 1997
- [d] **Reudenbach, R.:**  
Sichere Maschinen in Europa, Bochum: Verlag Technik & Information, 1997
- [e] **IVSS (Hrsg.):**  
Vermeidung von mechanischen Gefährdungen, Mannheim, 1994
- [f] **IVSS (Hrsg.):**  
Schutzeinrichtungen an Maschinen, Mannheim, 1999
- [g] **Defren/Wickert:**  
Sicherheit für den Maschinen- und Anlagenbau, publisher K.A. Schmersal GmbH, Wuppertal



New edition in progress

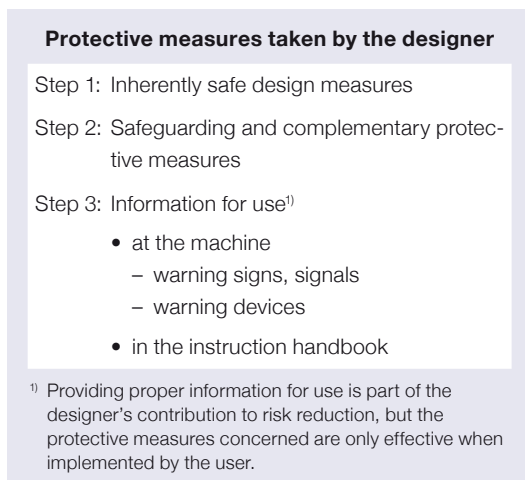
# Protective devices for machines

The designer dealing with machine risk minimisation will very quickly come across clause 5 of EN ISO 12 100-1 [1], “Strategy for risk reduction“. It is indicated in this clause that the designer must take measures to eliminate any risks determined.

Clause 5.4 of this standard describes the procedure (in three steps) to be adopted in the following order:

- Inherently safe design measures (direct safety technology)
- Safeguarding and complementary protective measures (indirect safety technology)
- Information for use on the residual risk (instructing safety technology).

Figure 1 of EN 12 100-1 shows the procedure very clearly (as shown in Figure 1).



**Fig. 1** Excerpt (copied) from Figure 1 of EN ISO 12 100-1

This procedure is described in detail elsewhere in this book.

In many cases the safety-related design of a machine cannot be realised exclusively using inherently safe design measures. Usually step two “Safeguarding and complementary protective measures” will and must be considered for design purposes.

Assemblies of indirect safety technology, such as protective devices, secure hazardous areas which cannot be avoided. Protective devices are

arranged between the user and the hazardous area or the source of the hazard. They interrupt the possibility of persons coming into contact with hazardous areas or sources of hazard in terms of space and time. Guards or safety devices are used for this purpose.

## Selection of protective devices

There are a large number of technical measures enabling the designer to find a solution which is suitable for his application. In view of the great variety of protective devices offered on the market, an overview of possible solutions is provided in the following.

The designer is well advised to give great consideration to the selection of the protective device and its incorporation in the machine and in process sequences. The selection he makes determines not only the safety level and rules out any safety gaps which may exist in the inherently safe design. The selection of protective device to be used also determines the productivity of the machine, the acceptance of the protective devices and ultimately also the resistance to manipulation (defeating) which should always be considered as a factor not to be underestimated.

An overview of the different types of protective devices is provided in the following. Special remarks on the selection of interlocking devices with guards are also contained in the EU standard EN 1088 [2].

## Guards

These are very simple protective devices and form a material barrier between persons and hazardous area.

Fixed guards may be located directly in front of the hazardous areas (cladding) or more sparsely around several hazardous areas (fencing). Fixed guards must be attached permanently with the basic structure of the machine using fixed connecting elements (e.g. with rivets) or connecting methods (e.g. welding) or such as to be dismantled with non-permanent connecting elements (e.g. with screws).

They consist of simple components with a reliable effect. Designed in a safe and ergonomic

manner, the material barriers permanently prevent persons coming into contact with hazardous areas and prevent sources of hazards reaching persons.

However, guards may also have disadvantages. Large guards are frequently difficult to handle, for example. The controlled suspension of the protective effect of guards always requires additional mechanical and technical work. In the case of fences the costs grow proportionate to the secured length. Security from manipulation (defeating) and circumvention can only be achieved with control technology. The basic possibility of simple manipulation (defeating) must always be taken into consideration, however.

Guards include the following:

- Cladding
- Covers
- Fencing
- Shielding
- Enclosures

#### Fencing/enclosures

prevent access to hazardous areas. Reaching over or below them may not lead to hazardous situations. Cladding prevents access from all sides. Covers only protect from specific or unspecific directions. For all passive guards which have openings it is important that they do not allow persons to come into contact with hazardous areas.

If guards have openings because they are executed as protective grids, for example, or have chute-like openings for the feed of materials into the process area, people should not be able to reach through these to reach the hazard zones. In view of statistically verified anthropometric sizes and their distribution in the population, the standard EN 13857 [3] sets out geometrical correlations between reach and width of opening and distances to hazard zones which reliably prevent persons coming into contact with them.

When reaching over the top edge of a fence the height of the edge, the floor distance from the hazard zone and the horizontal distance between the fence and the hazard zone must be coordinated. These safety distances are composed from experimentally determined ranges and safety mark-ups.

When determining safety distances for persons

reaching through openings, it is assumed that the clear profile and its dimensions determine the reach. The greater the opening the further a person will be able to reach through and the larger the distance to the hazard zone must be. The smaller the opening, the closer the fence can be moved to the hazard area. In order to consider the different human dimensions, the safety distance is determined by the reach of the tallest persons coming into question, and the clear width of the openings determined by the arm thickness of people with the smallest limbs.

Experience has shown that virtually every protective device must be dismantled and assembled again once during the life of a machine. This is why preference is to be given to non-permanent connecting elements which must be designed such that dismantling for maintenance work and re-installation is only possible with tools. According to the Machinery Directive, the fixing elements of the protective devices must be executed such that they may not be lost. This will also permit re-installation after dismantling. Without fixing elements, fixed protective devices may not remain in the protective position.

To enable the technicians to conduct maintenance work safely, i.e. without any surprise restart of drives, the machine must be switched off and secured against unauthorised restart, e.g. by blocking the energy supply by locking the main switch. After the work has been performed the protective devices must be fixed correctly again.



**Fig. 2** Example of a supply disconnecting device (e-off)

## Safety devices

With safety devices the spatial separation effect can be temporarily suspended. The suspension of the protective effect, e.g. by opening, must be possible without tools. The control system must recognise the opened status, however, in order to eliminate the hazard in opened states, e.g. the hazardous movement must be interrupted in good time. The positions of the guards to be monitored may be executed as sliding or pivot doors or as removable protective device.

Removable protective devices should only be provided for occasional intervention. Not only the fixing elements but all machine parts which permit the mobility and fixing of the parts to be opened must be able to withstand the actual operating and ambient conditions during the lifetime of the machine.

If moving, interlocked protective devices are opened for operational purposes, control measures must ensure that hazardous situations are brought to an end in the protected area before hazard zones can be reached. For this purpose, the after-travel time of the hazardous movements and the distance of the protective device must be attuned to the approach speed. The opening and switch-off mode must also be harmonised with the existing risk.

### Interlocking without latching (guard locking)

Before the start of the hazardous situation, the protective device must automatically take effect (the guard is closed), while the hazardous situation is present. The opening of the protective device must lead to a safe status in the protected hazard zone.

Controller and drive and the spatial position of the protective device must be attuned to each other such that, for example, the after-travel of the hazardous movement has ended in the time necessary for opening the protective device under consideration of the speed or approach speed in accordance with EN ISO 13855 [3] and the safety distances set out in EN ISO 13857 [4].

A further and just as important protective objective – in addition to shutting down the hazardous movement by opening the guard – must be the avoidance of unexpected start-up of the machine with open guard.

Predominantly mechanically actuated or electro-sensitive position switches are used as signal sensors which transform the opening of a protective device into an electric signal.

### Interlocking with latching (guard locking)

Moving protective devices can first be opened once the hazardous situation has come to an end. Guard locking requires that the standstill has been reliably initiated by the controller and that the possibility to open is released by a triggered interlocking element, e.g. mechanically.

Guard locking is always necessary if after opening the protective device tools would aftertravel due to high mass inertia. Examples are shredders, centrifuges and separators.

Guard locking is also increasingly used in machines with lower damage potential to increase availability.

Protective devices are not to be opened during operation so that the production process is not interrupted or to deliberately stop the machine. In the case of the two interlocking measures the reliable functioning must be correctly checked on a regular basis.

These protective devices are developed, checked and produced in accordance with the pertinent product standards. Many series are certified by notified bodies. Schmersal and Elan offer a large number of this switchgear, attuned to many applications, in their product portfolio.



**Fig. 3** Interlocking devices with and without latching (guard locking)

### **Non-material barriers, sensor mats etc. (protective devices with approximation function)**

They do not physically separate but monitor a geometrical safety field (line, level, room). They have the task of recognising the penetration (person, body part) in the safety field and then interrupting the hazardous situation in good time or not permitting it to come about in the first place. Depending on signal formation which is necessary for this, a distinction is made between contact trips and electro-sensitive trips.

### **Tactile safety devices**

These devices which react to deformations through body contact primarily cover pressure-sensitive mats, pressure-sensitive floors, pressure-sensitive edges and pressure-sensitive bars.

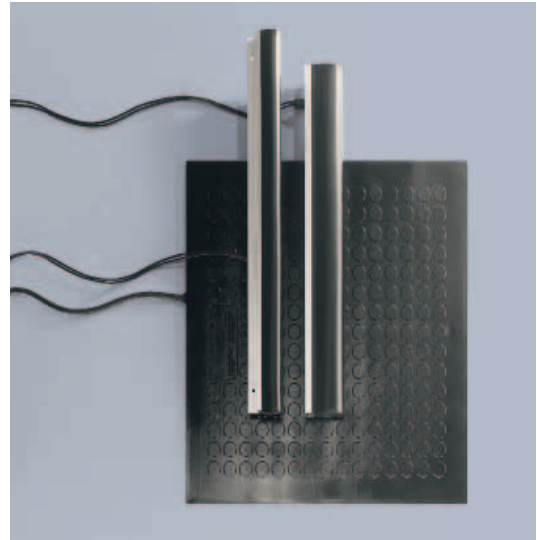
Their purpose is to stop machines or moving machine elements or to bring them to a different safe operating status if people or body parts approach the hazard area.

Pressure-sensitive mats, pressure-sensitive floors, pressure-sensitive edges and pressure-sensitive bars consist of transducer, signal transmission and signal processing. The system components may be executed as individual components or unified in the transducer.

**Pressure-sensitive mats** are distinguished from **pressure-sensitive floors**, in the same way as pressure-sensitive edges and pressure-sensitive bars, by the effective contact surface of the transducer. While in the case of pressure-sensitive mats or floors, the effective contact surface is locally deformed, the effective contact surface in pressure-sensitive edges and pressure-sensitive bars moves in its entirety.

Pressure-sensitive mats and floors are usually used to secure accessible hazard zones. If a person treads or stands on one, this is recognised and the stop command for the hazardous movement given by the output switching device.

**Pressure-sensitive edges and bars** are used to secure linear hazard zones (e.g. crushing, shearing and intake points). If a part of the body comes near the hazard zone this similarly leads to the hazardous movement being brought to a standstill.



**Fig. 4** Tactile protective devices

The market currently offers different versions of these systems which may be subdivided into

- optical
- pneumatic
- electric

depending on principle of operation.

Pressure-sensitive mats are relatively rare in practice because optical systems are more economical in many cases. However, they are increasingly used in areas in which protection from back access is required and other systems are not used.

By contrast, pressure-sensitive edges are frequently used to secure closing edges of power-actuated guards or power-actuated doors and gates.

The requirements placed on tactile safety devices are described in the general principles for the design and testing of pressure-sensitive mats and pressure-sensitive floors, pressure-sensitive edges and pressure-sensitive bars in the standards EN 1760-1 and EN 1760-2 [5].

### **Electro-sensitive protective equipment (ESPE)**

Electro-sensitive protective equipment generates a signal through change of disturbance in an energy field which is processed by a downstream controller to end the threat of a hazardous movement. No physical contact is necessary to trigger the signal. In electro-sensitive



protective equipment the following principles of action are used for signal generation:

- optical principle of action
- ultrasonic principle
- systems reacting to thermal radiation.

Depending on type, this protective equipment can monitor linear protective fields, areas and rooms.

### Optoelectronic protective devices

are active optoelectronic protective devices (AOPDs). They only lead to safe states if a hazard becomes acute (access or entrance to the protected area). The triggering of the safety function is not linked with direct body contact. Optoelectronic protective devices can be integrated without problem in contemporary control or automation concepts.

The following systems have proven their worth for the electro-sensitive monitoring of protective areas:

#### Unidirectional light barriers

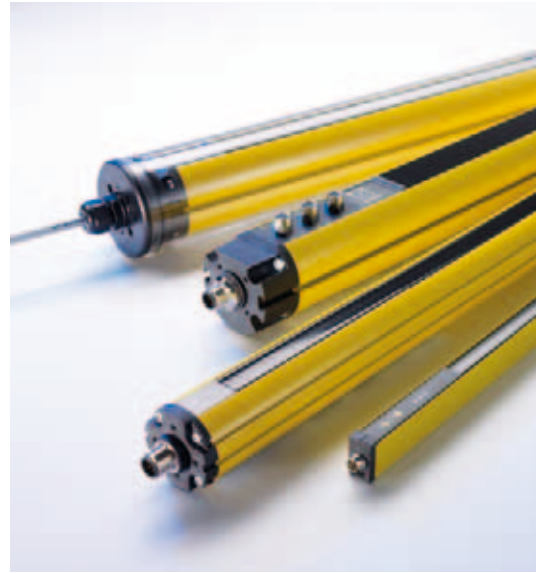
consist of transmitter and receiver which are located in separate housings. The light beams in the infrared range from the transmitter to the receiver and runs through the line only once. The light beam can be redirected via mirrors. The penetration of objects along the light beam interrupts it and a switch signal is generated.

#### Light grids

The protective field is created by a few unidirectional light barriers lined up at regular intervals. The arrangement of 2, 3 or 4 individual beams can be used to recognise the penetration of an entire body into the hazard zone. But they are not suitable for recognising body parts (e.g. hand or fingers). If the risk assessment performed in accordance with EN ISO 13855 [3] shows that several individual beams are suitable, these must be arranged at a minimum distance calculated in an equation to the hazard zone. The safety distance to the hazard zone must be dimensioned such that under consideration of the approach speed of body parts and the response time of the light barriers, hazardous movements are interrupted in good time before the hazard zones can be reached.

#### Light curtains

are created either through a large but finite number of individual light barriers in line or by a mov-



**Fig. 5** Safety light curtains and grids are available in many versions

ing fanned light beam which moves completely through the monitored level periodically. The distance of the individual sensors is decisive for the detection capacity of the protective device which in its turn determines the minimum distance to be observed to the hazard zone and the area of use (finger and hand protection or securing of area).

Light curtains are available in all possible protective field heights and different versions:

- Range  $\leq 0.3$  m to  $> 6$  m
- PL “e” or PL “d” in accordance with EN ISO 13849-1
- SIL 2 or SIL 3 in accordance with IEC 61508
- Resolutions  $< 14$  mm to  $> 70$  mm
- Safe semi-conductor outputs or relay outputs
- Master-slave operation (cascading)
- Muting
- Chopping operation
- Class of protection up to IP 69K.

**Muting.** Electro-sensitive opto-electronic protective devices monitor lines or levels so as to recognise an inadmissible approach if they are interrupted by body movement and initiate control measures which lead to safe states. Usually hazardous movements are concerned which are often technological or functional related movements.

Not only the persons to be protected trigger these signals but also work pieces. So as not to



unnecessarily interrupt the processes, the efficacy of the AOPD must be deliberately interrupted in certain situations. The process-related time-restricted bridging (suspension) of a protective device is described as muting. For example, the light barrier must be bridged in automatic palleting system when the pallet passes the entry or exit area. Immediately after the pallet has passed through, the muting state must be cancelled and the protective device is re-activated. The muting system must therefore be able to distinguish between pallet and persons.

Muting therefore deactivates the effect of the protective device in specific time-restricted operating phase and then automatically restores the protective effect at the end of the bridging. Both electro-mechanical and opto-electronic sensors are used as signal transmitters.

The automatic temporary bridging and above all its cancellation must be controlled solely by the machine, i.e. must be independent of the will of the machine worker. Two safety-related aspects are of special significance here:

- Attempts of persons to enter the protected room during the use phase must be reliably recognised and prevented. Muting signals occurring in an invalid combination may not permit bridging and must ensure that the protective function remains intact. The access may also be prevented by the geometrical shape of the transport device or human detectors are deployed.
- The control system must guarantee that the protective effect is reliably restored. The safety category of this control part must be the same as that of the protective device.

Literature (standards):

- [1] **EN ISO 12100-1:**  
Safety of machinery – Basic concepts, general principles, Part 1: Basic terminology, methodology
  - [2] **EN 1088:**  
Safety of machinery – Interlocking devices associated with guards – Principles for design and selection
  - [3] **EN ISO 13857:**  
Safety of machinery – Safety distances to prevent hazard zones being reached by upper and lower limbs
  - [4] **EN ISO 13855:**  
Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body (ISO 13855:2010)
  - (5) **DIN EN 1760-1:**  
Safety of machinery – Pressure-sensitive protective devices – Part 1: General principles for the design and testing of pressure-sensitive mats and pressure-sensitive floors
- DIN EN 1760-2:**  
Safety of machinery – Pressure-sensitive protective devices – Part 2: General principles for the design and testing of pressure-sensitive edges and pressure-sensitive bars

Other literature:

**Neudörfer, A.:**

Konstruieren sicherheitsgerechter Produkte, Methoden und systematische Lösungssammlungen, Berlin, Heidelberg, New York: Springer, 1997

**Defren/Wickert:**

Sicherheit für den Maschinen und Anlagenbau, publisher K.A. Schmersal GmbH, Wuppertal

**BGI 575 – BG-Information:**

Auswahl und Anbringung elektromechanischer Positionsschalter für Sicherheitsfunktionen

**BGI 670 – BG-Information:**

Auswahl und Anbringung von Näherungsschaltern für Sicherheitsfunktionen

# Manipulation (defeating) of Protective Devices

The manipulation of protective devices is not a small matter but rather the cause of many accidents and near-accidents in the operation of machines. It is not without reason that this subject has now been given greater attention in the respective standard. Firstly, there is amendment AMD 1 on the subject of “design for the minimisation of defeat possibilities” to EN 1088 which has since been incorporated in the current edition of the standard (currently EN 1088:2008 “Interlocking devices in connection with separating protective devices – guidelines for design and selection”) and is also given attention accordingly in the follow-up standard EN ISO 14 119 (draft).

By defeating an interlocking device, which is colloquially also referred to as “manipulation” and which involves a conscious, inappropriate intervention in the safety technology, the machine control system is “tricked” into believing that a protective device is fully effective, in other words that it is correctly closed and locked. In actual fact, however, work can be processed or observed with the guards open while in full automatic operating mode. There is neither protection against the risk of hazardous machine movements or parts flying off, nor against the risk of a machine starting up unexpectedly. An act bordering on the criminal is when machines with a manipulated protective device are then passed on (left) to somebody else who knows nothing about it (and who trusts that the protective device is effective when in reality it no longer exists).

But even the specific threat of punishment, as now exists in Switzerland, has done little or nothing at all to change the bad practice of manipulated production devices. There too in over one third of all protection plants, systems exist whose protective devices have been rendered ineffective despite the fact that the Swiss Penal Code (StGB) threatens imprisonment of up to 3 years or a fine if employers do not satisfy their obligation to ensure that protective measures and protective devices are not impaired in terms of tolerated by the employer. It is not necessary for an accident to have taken place.

Even if this subject is primarily one that concerns machine operators, we return to it once again



**Fig. 1** Examples for manipulations

in view of the justified assumption that around 25 % of all industrial accidents with machines in Germany can be traced back to manipulated (defeated) protective devices. Focus is placed once again on this topic because machine designers will also have an obligation if the EN 1088 standard is amended (less so the manufacturers of safety components because a number of specific requirements already applied to them with respect to their product design, whether on the basis of product standards or the test principals of German Employers Liability Insurance Associations).

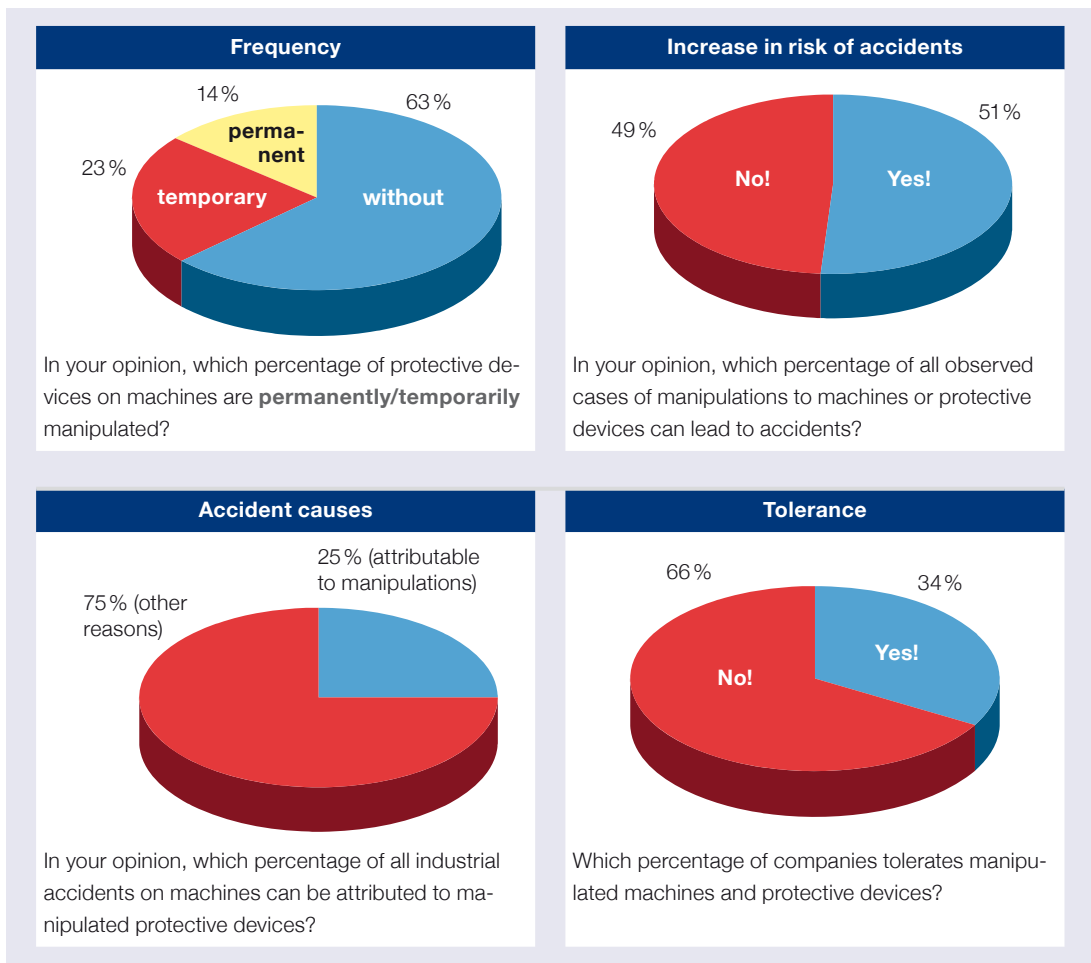
It is true that the amendment of the standard only concerns interlocking devices, while the above mentioned figure of 25 % and the entire subject refers to all kinds of protective devices such as

optoelectronic equipment, enabling switches etc. Reference is made here to the empirical study conducted by Employers Liability Insurance Associations [1] and to a similar study in Switzerland that was conducted by the Swiss National Accident Insurance Association (SUVA) [2].

With respect to Germany, a translation to German Employers Liability Insurance Association study results means that each year around 15–20 deaths and approximately 20,000 more or less serious accidents are caused by manipulated (defeated) protective devices. This is to be seen against the background that around 37 % of all

protective devices are manipulated (14% permanently and 23 % temporarily) and (sic!) manipulated protective devices are tolerated in 34 % of all companies. A number of companies are even said to exist where even expect employees to manipulate protective devices. The figures cited above were obtained from companies that primarily operate in the metal industry; however, there is general agreement that in terms of magnitude they can be applied to other areas of the manufacturing industry.

The main empirical results of the study are summarized in the charts below:



**Fig. 2** The “most important results of an empirical study conducted by the Employers Liability Insurance Association on the manipulation of protective devices

**What’s new?**

The subject matter of the amendment in EN 1088 is that in future, from a selection of suggestions on possible additional measures against the manipulation of interlocking devices, at least one

measure must be realised to satisfy the assumption of conformity set out in EN 1088 (measures of different kinds are excepted which provide a comparable degree of safety). The suggestions of additional measures refer to the different



**Fig. 3** In the case of safety switches – also referred to as class 2 switches – the switching element and actuator are not connected structurally to each other but are functionally joined or separated during switching. The actuator is separated from the basic unit when the protective device is open. Here, NC contacts in the safety switch are positively opened and NO contacts are closed.

types of interlocking devices and are differentiated accordingly. EN ISO 14 119 (draft) updates this approach.

The following measures are referred to for interlocking devices with separate actuators (see Fig. 3) as are to be very frequently found in the securing of moving protective devices:

### 1. Permanent actuator fixing

Using either non-reuseable screws or welding, riveting etc. it is possible to easily and effectively realize the fixing of separate actuators which is practically impossible to reverse. The fixing

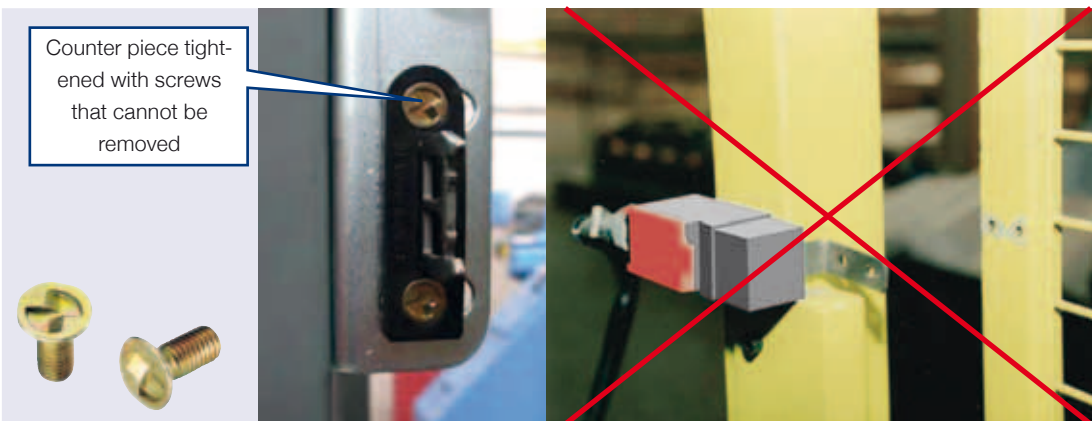
of actuators which cannot be reversed at least prevents actuators being simply unscrewed and inserted into the devices. The fact that the fixing of actuators which is practically impossible to reverse may cause problems for service technicians and fitters performing repair work should rather be viewed as a helpful counter-argument in this context and underestimates the creativity and abilities of these employees.

Where it is sometimes necessary to make final adjustments to the protective device at the installation site, we also know that it is also easier said than done to attach fixing screws on separate actuators such that they may not be removed.

In a case such as this, this must then be the last step taken and one that may be effectively delegated where necessary; alternatively, other measures should be taken. However, it is doubtful that securing screw heads with varnish is sufficient. Welding, riveting or glueing using a special glue would then be more suitable.

Non-removable screws do not necessarily need to be procured separately since these are available as standard accessories in the Schmersal/Elan product range, for example. They either form part of the scope of delivery or can be ordered separately.

However, since this measure only has a limited effect (what about “straying” actuators?), we recommend that this measure is not used exclusively to satisfy the AMD 1, but that in addition another of the measures available for selection should be realised.



**Fig. 4** Example of permanent actuator fixing (right: unscrewed actuator)

## 2. Individually coded actuators

Even if considering how spare parts logistics should be organized requires additional thought here, individually coded actuators represent an extremely effective means of preventing the manipulation of locking devices. In a similar way to a key and lock, an actuator only fits and functions in one device out of many thousands of permutations, i.e. a straying actuator also does not make sense in terms of manipulation.

By contrast with standard actuators, an individually coded actuator is practically unique. While standard actuators are also coded, this is uniform and is intended to distinguish them from simple tools such as screwdrivers, simple pieces of wire, etc.

This means that it is all the more important for the individually coded actuator measure to have actuator fastenings that can not be released.

A little self-praise can be excused here: these device versions have been available in the Schmersal/Elan program range for many years (pre-dating the current discussion on manipulation).



**Fig. 5** Electro mechanical safety switch with individual actuator coding

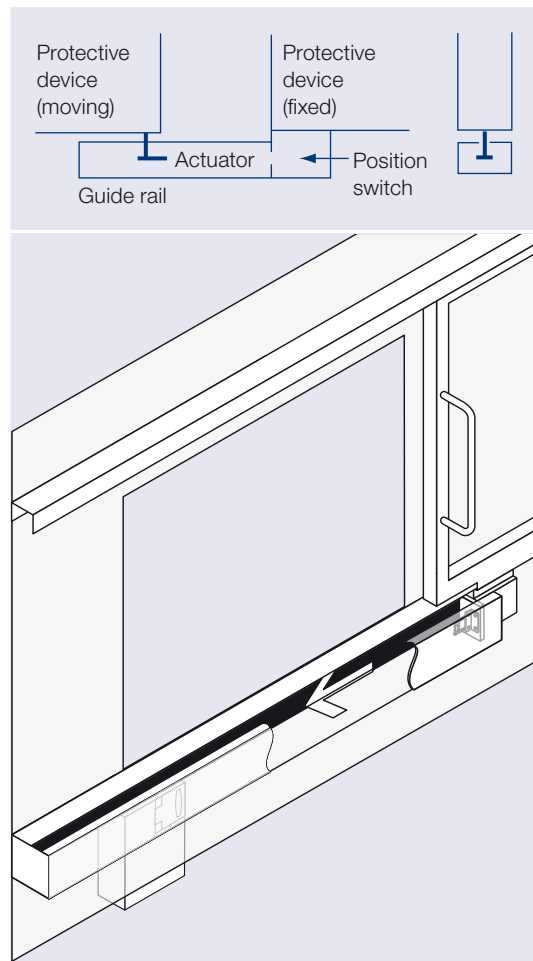
## 3. Concealed device installation

The concealed installation of devices is based on the idea of installing interlocking devices in a machine design in such a way that there is no free access to the insertion opening of the devices. This means that even somebody with a

straying actuator will be unable to place this in the insertion opening without difficulty.

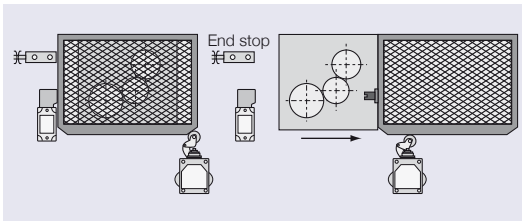
This measure is particularly suitable for sliding doors; these can be easily provided with a cover behind which the interlocking device is situated. Depending on design, concealed installation in the interior of a machine also comes into question.

Whether there is sufficient space to make access impossible (interlocking device is appropriately far away or is high enough away from the direct access area of the operator) must be checked in individual cases. At all events this must not produce any additional sources of accidents that arise by being able to simply climb onto the machine. In this connection, a further consideration should be a combination with other measures, e.g. with start-up tests or plausibility checks by the machine control system (see loc. cit).



**Fig. 6** Example of implementation of concealed device installation





**Fig. 7** Position monitoring of a protective device by two switches

#### 4. Additional monitoring switch

The installation of a second switch also provides a good means of preventing manipulation, especially if switching signals are additionally monitored for plausibility, e.g. that they close within a certain timeframe or in a particular order. This means that anyone defeating a device needs to overcome two obstacles that must be effectively “outsmarted”. However, it cannot be denied that this measure also has cost implications and should only be a last result when you solely prevent manipulation or make it more difficult.

A slightly different situation arises if a performance level “e” or a safety integrity level 3 must be achieved for a safety function due to the need to maximize the risk reduction. For reason of the requisite safety related architecture alone, a second switch is necessary here if electromechanical technology is deployed. Under certain circumstances the question of a second switch can also arise for PL “d” or SIL 2. In this case other considerations also come into play.

#### 5. Testing of other device designs

The market now offers a number of new possibilities for the safety-related monitoring of moving guards and guard locking them where necessary, e.g. special hinge monitoring switches (TVS 410 range) or non-contact interlocking devices with double position monitoring (AZ/AZM 200 range) from the Schmersal/Elan product range. Other benefits are also possible in conjunction with the use of these devices; these benefits may be of a logistical nature, related to visualization and diagnostic possibilities or availability in the case of unfavourable application conditions.

In the case of hinge monitoring switches (see Fig. 8), the monitoring is integrated in the hinge of an assembly so that it cannot be manipulated, while the double monitoring of AZ/AZM 200 range firstly detects the inserted actuator (with an elec-



**Fig. 8** Hinge safety switch TVS 410 range

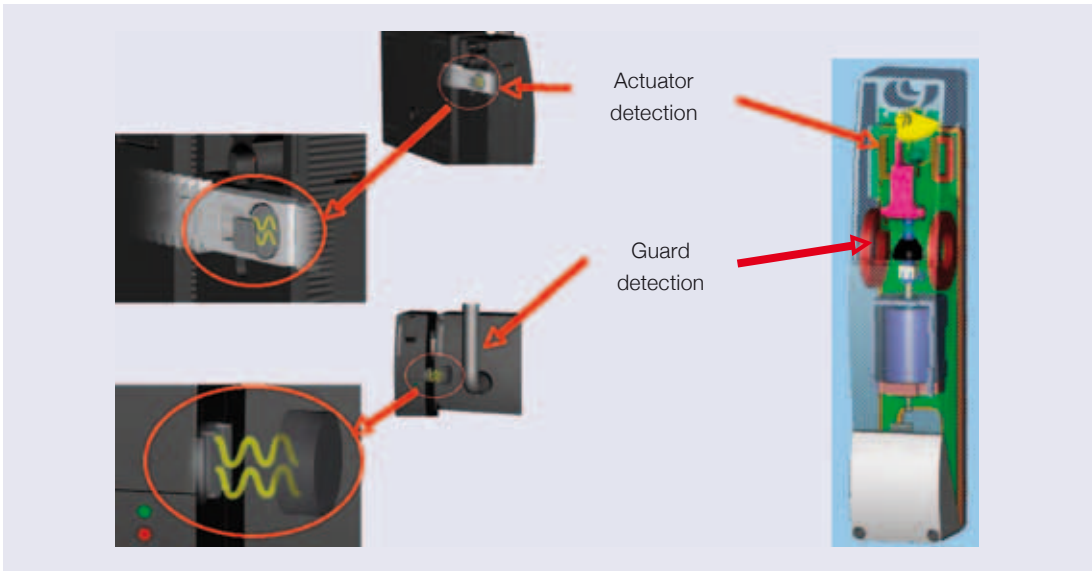
tronic counter part for the evaluation electronics located in the device) and secondly the closed position of the guard that is monitored via a second non-contact sensor in the device. The machine is only able to start up if there is an AND operation from both signals (see Fig. 9).

In both of these cases – both for the hinge monitoring switches from the TVS range and for the type AZM 200 non-contact devices (with guard locking) and AZ 200 (without guard locking) – the complete protective device would have to be dismantled in order to cancel their protective effect. Here too the devices must be fixed such that they cannot be removed.

#### 6. Control-related measures

Manipulation can be very effectively countered using control-related measures, even if it is only detected when it has already occurred. This can take a place in the form of a start-up test at the beginning of a shift, for example (correct signal changing by an interlocking device is monitored by opening and closing the protective device) or continuous plausibility checks, e.g. by checking the number of signal changes to be expected under normal operating conditions or by blocking certain operations that can only be executed when the protective device is in an open position if the corresponding signal status is not present. These measures do not need to be carried out via a safety control system such a safety PLC. The operative control system is sufficient in that case.

Of course, if manipulation is actually detected using the control-related measures it would not be enough to have a simple acknowledgement signal. Rather, it would have to be a reason for the person responsible to look into the cause and to put it nicely, to take the employees re-



**Fig. 9** Non-contact interlocking devices with double sensors, additionally with emergency unblocking

sponsible to task. This is a question of “safety culture” of the respective company.

**Measures with other types of interlocking devices**

Other types of interlocking devices are also addressed in EN 1088 in addition to devices with separate actuators. Examples of these are interlocking devices with cam-operated position switches or commercially available proximity switches, but also include key transfer systems etc. Added to these, even though they are considered under the product requirements in EN IEC 60947-5-3, are so called PDFs = Proximity Devices with defined behaviour under Fault conditions. Safety solenoid switches or safety sensors (for example devices from the Schmersal CSS family) should be included here in particular.

To some extent it is possible to apply the above measures to these types of interlocking devices, while in other cases alternative or additional measures come into question. At all events the requirement to use additional measures to minimize the possibilities for circumvention also apply to all other types of interlocking devices, and therefore also to these (see EN 1088 for details).

One should also not be misled when the descriptions provided by the manufacturer state that some PDF devices (typically PDF-M device models) are constructed redundantly and are a substitute for two switches, concluding from this

from the outset that any further considerations on the subject of “manipulation” are superfluous. This is not the case or at least requires checking depending on the type and design of device. For example, the CSS 34 from Schmersal are PDF-Ms in the same way as the Electromagnetically operated guard locking AZM 200 or the safety switches AZ 200. In the case of the devices AZM 200 and AZ 200, additional measures may actually be dispensed with due to the double monitoring of actuator and guard, but by contrast not in the case of CSS 34 (at least the counter piece must be fastened so that it cannot be removed here).

Since the counter piece in PDFs is “superior” compared to the mechanical actuators of safety switches (more valuable in terms of procurement costs and superior in terms of the precision and technical skill required to copy it), ensuring that the counter part cannot be released can be re-



**Fig. 10** RFID-based safety sensor with individually coded counter piece (RSS 36)



alised as a sole measure. However, this too will depend on the case in hand and on the “stress and strain”. If necessary in the Schmersal range there are RFID-based sensors with unique counter parts available as well as options of paired individually coded devices of Schmersal’s CSS-“family”.

### **But you don’t need to be a fortune teller!**

We can assume that taking the new requirements into consideration will help to avert or prevent the manipulation of interlocking devices. BUT: you do not need to be a fortune teller to say that, despite this, protective devices will continue to be manipulated in the future using different methods and tricks.

It therefore makes sense to ask the following question: Why does manipulation of protective devices/interlocking devices occur in the first place?

Without claiming to be a psychologist, on the one hand this surely comes down to human curiosity and/or the human play instinct; both can induce manipulation. On the other hand, protective devices can be obstructive, getting in the way of workflows, complicating target achievement of performance-related pay etc. The last aspects may be all the more significant where safety technology on machines is only carelessly “bolted on” retrospectively and is not an integral component of the whole process of machine design or as our colleague Frank Schmidt likes to put it: *The best kind of protective device is the one you do not notice.*

A contributory factor in this entire situation is certainly also that the operators are unaware of risks associated with the manipulation of protective devices because everything runs to plan, the machine and its sequences are known (familiar) etc. In other words: taking one’s own abilities into account, the user imagines a sense of subjective safety and reliability regarding the machine, i.e. no thought is given to protection in the albeit unlikely probability of a fault or disturbance, nor to the possibility of his own imprudent or stress-related behaviour.

As far as these aspects are concerned, machine operators in their function as employers with corresponding statutory obligations are particularly required (and obliged) to act to prevent the

manipulation of protective devices and to inform, instruct and raise the awareness of employees accordingly, and ultimately also to supervise them and also where necessary to back-up any wrong doing with sanctions. It is also important, however, for operators to set a good example.

In this context, employer obligations in particular have only recently been highlighted once again in an expert forum from the BGN (the German Employers Liability Insurance Association for the Food Industry and Catering) entitled “Findings and approaches to prevent the manipulation of protective devices”.

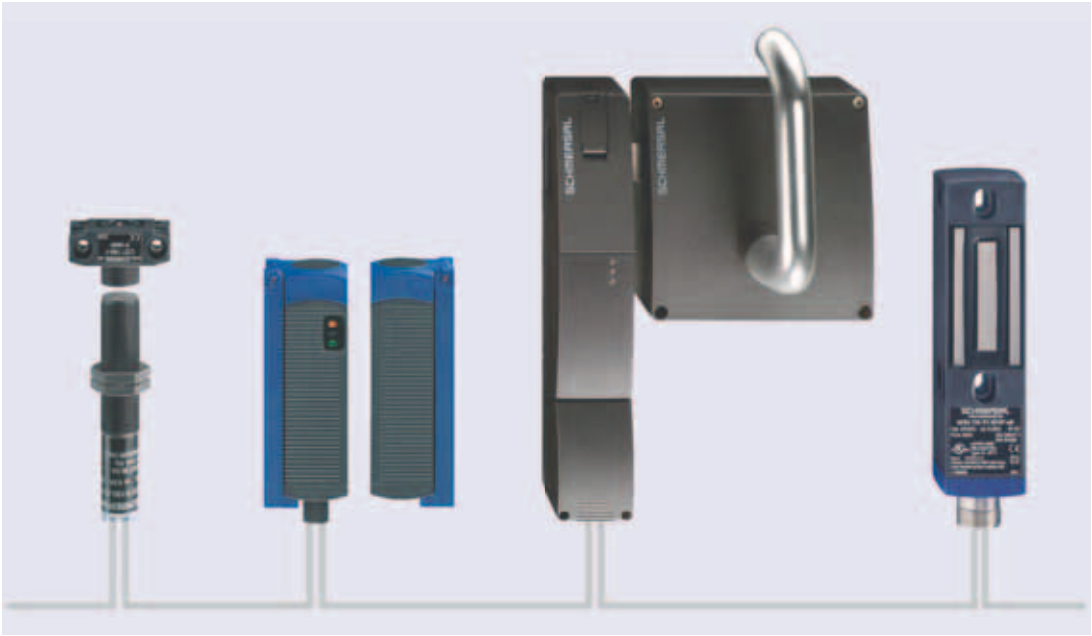
One option may also involve making technical changes (or having these made). At this point it is important not to forget to take into account the fact that interlocking devices themselves can cause disruptions, particularly where tolerances or offset arise during interaction between moving and fixed parts of a protective device, i.e. the separate actuator no longer finds its way out of its opening when closing the guard and must be “helped” for example. It is then frequently just a question of time before manipulation takes place.

Precisely with respect to this question non-contact interlocking devices can make full use of their advantages since in addition to the advantage of non-contact operation, they also have substantially greater production tolerances. One example of this is once again the CSS family from Schmersal which has devices with and without guard locking.

### **Can misuse be reasonably foreseen?**

There is usually no justification in the argument sometimes used that it is possible to reasonably predict the manipulation of protective devices. This attempts to pass responsibility back to machine designers, although the primary obligation lies with the machine operator in his role as employer.

It worth reading an interview with Prof. Dr. Thomas Klindt [3], the well-known expert on technical law, published in the trade journal “Die BG” (01.09 edition) in this respect. The emphasis of this interview is placed on questions of occupational health and safety organisation in companies but also lays down the law to employees who manipulate protective devices. We quote a



**Fig. 11** Non-contact interlocking devices with and without guard locking from the Schmersal CSS family: in addition to functional benefits, including those arising from greater tolerances for the interaction between the fixed part and the moving part of a moving protective device as well as improved visualisation and diagnostic possibilities, the new technology also offers safety-related advantages. An example here is series connection with unrestricted fault connection (PL “e”, SIL 3, SC 4). Moreover, the Electromagnetically operated guard locking have two other special features: under the heading of manipulation protection, model AZM 200 has double guard monitoring; model MZM 100 (right) functions without the insertion of an actuator using electromagnetic force for guard locking and is intended for special tasks.

few interesting excerpts from Prof. Dr. Klindt’s responses:

- *In particular the extremely vague and tirelessly used accusation of so-called “foreseeable misuse” is an attempt to shift the conduct of employees, however perverse and careless this may be and despite the risk it subjects them to, onto the manufacturer.*
- *It is not stated anywhere that it is not sufficient to clearly warn of the undesirable, hazardous wrongdoing in manuals, operating instructions and in pictograms. What is the manufacturer to do if the employee ignores his warnings?*
- *Every employee who uses technical equipment incorrectly, despite corresponding instruction in accordance with Section 12 (1) of the Occupational Health and Safety Act, is infringing provisions of the Act himself.*

### Borderline cases

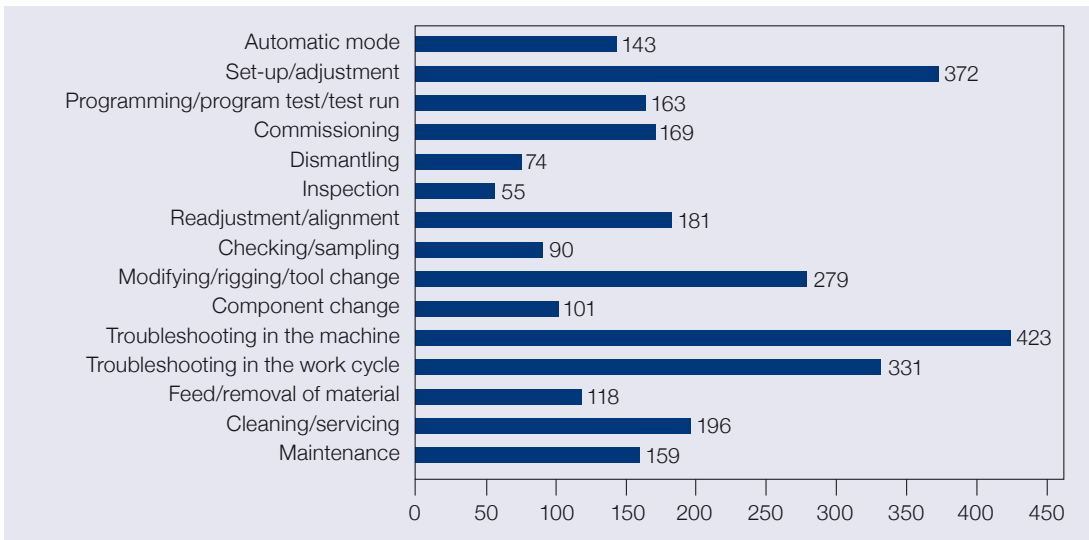
But we need to be careful here: This is no carte

blanche for ignoring design possibilities and ultimately courts will decide in individual cases. The fact that borderline cases exist, i.e. that it is possible to discuss reasonably foreseeable misuse under certain circumstances, cannot be completely denied and this impression is certainly not intended in the above interview.

A particular point addressed here is where correct machine operation is not possible or is substantially complicated so that this leads to a high (urgent) motivation to defeat.

For example, operators frequently complain that with “their machines” the visibility to the process is too restricted or that there are insufficient special operating modes. The following question was therefore posed in the above mentioned BG study: *Please specify three operating modes where manipulation preferably takes place!* The responses are evaluated below in Figure 12.

From the responses it can be seen that it is precisely the necessary operations outside of auto-



**Fig. 12** Subjectively perceived “necessity” of manipulating protective devices according to operating modes (n = specifications as part of an empirical study; multiple answers possible)

matic operating mode that incite operators objectively or subjectively to manipulate protective devices in order to perform their work.

Intelligent designs as well as the possibilities offered by modern control technology can help to prevent or reduce such incentives to manipulate devices.

Extracts of solutions specified by the Swiss National Accident Insurance Organization (SUVA) are set out in Figure 13 as examples of intelligent design (for adjustment and alignment work on running machines).

The other possibility is to provide more special operating modes, right through to the exceptional process monitoring operating mode, which have now finally become legalised by the new Machinery Directive. As a general rule, the MD 2006/42/EC will in future permit greater leeway for special operating modes because the previous rigid AND operation for the four input conditions will be relaxed when there are compelling operational needs for this and as long as personal safety is not compromised as a result (as shown in Figure 15).

**The most effective measure:  
Avoid manipulation incentives!**

However, the Employers Liability Insurance Associations have not stopped at the empirical study on the subject of “Manipulation of pro-




TECTIVE DEVICES” first used for stocktaking and already mentioned several times above. There are now further thoughts on the subject which in particular involve reducing manipulation incentives. These have since been incorporated in an evaluation scheme by the German Statutory Accident Insurance (BGIA) Institute for Occupational Health and Safety (BGUV). A few aspects from extracts from this document are set out below (download at [www.dguv.de/ifa/en/pr/manipulation/index.jsp](http://www.dguv.de/ifa/en/pr/manipulation/index.jsp)).

The document once again clarifies the correlations:

1. *Protective devices that do not hinder work cycles are generally not manipulated because no advantages would result.*
2. *Protective devices that hinder work cycles provoke circumvention of these protective devices.*
3. *The probability of unsuitable protective devices being circumvented is directly proportional to the benefits.*
4. *The advantages of manipulated protective devices depend on the actions to be performed on the machine.*
5. *Manipulation will not necessarily be reversed. Manipulation carried out for rare interventions can therefore lead to a constant pre-circumvented protective device in the worst case scenario.*
6. *If certain activities have not been taken into consideration during the design of a machine,*

**Problem/Danger**

It must be possible to perform adjustment or alignment work on running machines and at full production speed with protective hoods closed (exception: jog operation at reduced speed). This is guaranteed using adjusting elements, for example, that can be operated from the outside or through electronic fine adjustment. In the absence of such design measures, there is a risk that monitoring of the protective hood will be reduced and there will be access of the hazardous area while the machine is running.

		Solutions
	<p><i>Fig 1: Tunnel permits safe access to adjustment elements.</i></p>	<p><b>Variation 1:</b> The adjustment elements can be reached through the closed protective hood via a tunnel (as shown in Figure 1). The tunnel is designed so as to prevent access to the hazardous area.</p>
	<p><i>Fig 2: Control panel for electronic fine adjustment.</i></p>	<p><b>Variation 2:</b> The setting is implemented electronically using a control panel (as shown in Figure 2) with servo motors. This design permits diverse settings to be stored. This makes it easier to change formats.</p>
	<p><i>Fig 3: Adjustment elements arranged outside the protective hood.</i></p>	<p><b>Variation 3:</b> Fine adjustment using adjustment elements that are arranged outside of the protective hood (as shown in Figure 3).</p>

**Fig. 13** SUVA suggestions (examples) to reduce the motivation to manipulate protective devices.

**MD 2006/42/EG, Annex I/main amendment**

- Legalisation of the “process monitoring” mode
- Special operation of machines with bridged protective devices
- Previously: Greatly restricted!
- Relaxing of the AND operation
  - Blocking automatic mode
  - Movements only using enabling switch/joke key
  - Reduced speed/power (as non-critical as possible) – no command chains
  - Only absolutely necessary actuators remain active
- ... in the case of compelling operational reasons (doc! Individual agreement with customer is necessary -\* substitute measures)
- Under no circumstances: standard or similar to standard operating mode (C-norm and other possibilities must be exhausted)



**Fig. 14** Example of the special robot operating mode T1 or T2



Fig. 15 Helpful BG-informations

e.g. setting up, then the manipulation of protective devices will be unavoidable as the machine could otherwise not be used.

- The CE label does not necessarily mean that the machine is not/need not be manipulated.

Against this background the aim is to produce an evaluation scheme (with 0, + and ++, as shown in Figure 15), showing whether and how high the manipulation incentive is during work (operations) that have been shown by the BG study to

Fig. 16 Assessment scheme on manipulation incentive

be particularly susceptible to manipulation. This can distinguish between operating modes so that it takes a systematic look at the question: "What advantages does the manipulation of the (a) protective device have for work on the machine?"

The assessment of entries will be made individually for each activity. The term manipulation incentive (MI) is introduced to depict the incentive to circumvent protective devices, and is divided into three levels. This approach – in principle the motivation to manipulate and make it the subject matter of a risk assessment – will be incorporated in successor standard EN ISO 14 119 (draft) of EN 1088:2008.

The following manipulation incentive (MI) results can occur here:

MI =	if ...
no	no "+" or "++" entries are present for an activity
present	at least one "+" or "++" entry is present for an activity
high	the activity is implemented in a prohibited operating mode or the activity is not possible without circumventing the protective device.

Fig. 17 Assessment possibilities (example) for manipulation incentives

- An **MI = low** describes a machine where the protective device clearly does not impair the work cycle so that there would be no advantage to circumvention. There is no need to act. If manipulation takes place in spite of this, then the causes are not to be found in defective machine design.
- MI = present** indicates that the protective device hinders the work cycle and that circumvention would be associated with advantages. Whether manipulation would actually take place or not cannot be determined using this evaluation scheme alone. Further interdependencies must be taken into consideration such as the stress of individual persons and the corporate culture. How great is the inhibition threshold when it comes to manipulation? Is manipulation tolerated/encouraged in the company or is action taken to restrict





Fig. 18 SUVA checklist, Switzerland

it? Therefore, the only exception here can be that activities have been identified where there is a manipulation incentive and where further clarification is required.

- **MI = high** identifies a machine that cannot be operated at all without manipulation. Improvements are necessary and this machine is not safe!

**SUVA checklist**

SUVA takes a slightly more pragmatic approach by creating a checklist (see Fig 18, download at <https://www.epp1.suva.ch/webshop/4C/4CA2E45B5F1C0388E10080000A63035B.pdf>) that should be taken into consideration by purchasers and technicians when procuring machines that the machine manufacturer can in turn also use to check whether he has satisfied his obligations (see extracts from questionnaire, Fig 19).

**What the machine designer should do**

If you have been reading attentively up to now you have already done something, namely familiarize yourself with the problem, some of the new requirements and other considerations. It would furthermore appear to be worth recommending that the subject of the “manipulation of protective devices” or “manipulation incentives” be

incorporated into the risk assessment of a machine.

In any case this will probably be a future *expressis verbis* obligation. It is worth considering the findings from the production observation duty and feedback from sales and service departments and – last but not least – making use of the opportunities provided by the new safety components available. Explicit mention is made here again of the innovative contactless interlocking devices with and without guard locking, of which the Schmersal CSS family is a good

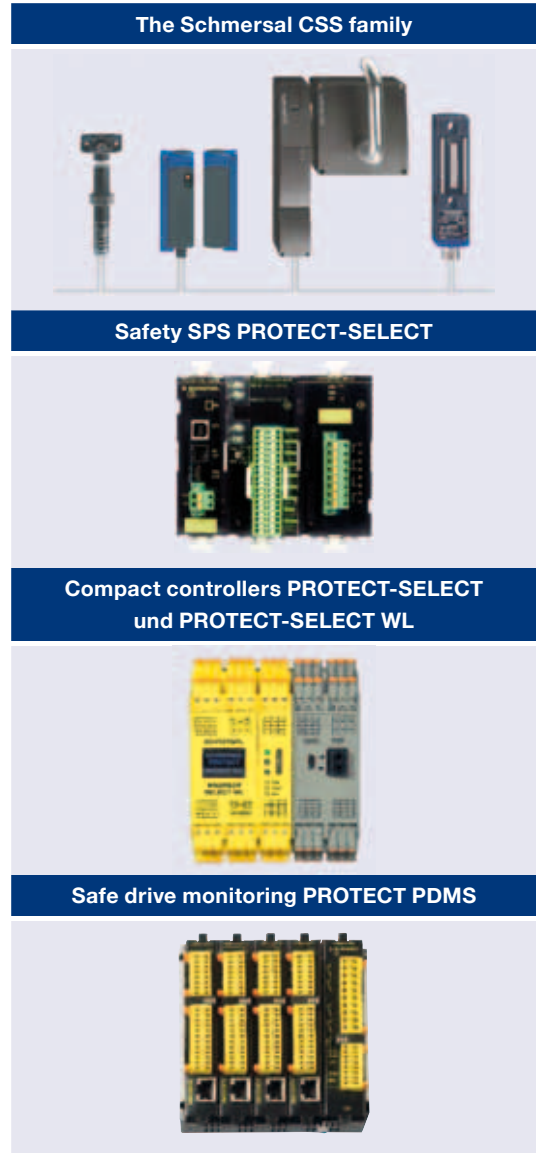


Fig. 20 New solution approaches for interlocking devices and controllers which contribute to preventing manipulation incentives.

## Questionnaire (excerpt)

Normal operating mode	Special operation mode, maintenance
<p>Are protective devices designed and attached so that it is not possible to access the hazardous area of the machine while the machine is running? <input type="checkbox"/> yes <input type="checkbox"/> partially <input type="checkbox"/> no</p> <ul style="list-style-type: none"> <li>– No gaps in hood, also in the case of interfaces</li> <li>– Tunnel entry and exit at material transfer points</li> <li>– Safety light barriers</li> </ul> <p>Sicherheitsabstände gemäß EN 294 beachten.</p>	<p>Can the machine be set up safely? <input type="checkbox"/> yes <input type="checkbox"/> partially <input type="checkbox"/> no</p> <p>The following apply if the machine must be operated with open protective hood when setting up:</p> <ul style="list-style-type: none"> <li>– Block the automatic control and</li> <li>– Reduce speed/power and</li> <li>– Use the enabling key or jog mode or electronic handwheel</li> </ul>
<p>Is visibility to the work process guaranteed if necessary also when the protective hoods are closed? <input type="checkbox"/> yes <input type="checkbox"/> partially <input type="checkbox"/> no</p> <p>Possible solutions: Add extra window or grids, install camera or mirror, replace “misted” windows, bulls eye.</p>	<p>Is fine adjustment possible while the process is running if necessary? <input type="checkbox"/> yes <input type="checkbox"/> no</p> <p>The following apply if the machine needs to be aligned at production speed:</p> <ul style="list-style-type: none"> <li>– Adjustment elements can be operated from outside or</li> <li>– Electronic fine adjustment or</li> <li>– Access tunnel to the adjustment element or</li> <li>– Probe for setting to zero (for CNC machines)</li> </ul>
<p>Has it been guaranteed that it is never necessary to manually intervene in the ongoing production process? <input type="checkbox"/> ja <input type="checkbox"/> teilweise <input type="checkbox"/> nein</p> <p>Possible solutions: Ensure adjustment elements can be operated from the outside, gripping aid for removing the product, handling device, central lubrication from outside, provide a break point, parts removal</p>	<p>Can cleaning work be carried out when the machine has been stopped? <input type="checkbox"/> yes <input type="checkbox"/> partially <input type="checkbox"/> no</p> <p>Protective measures must be provided if this is not the case (see first question)</p>
<p>Has it been guaranteed that protective devices are not easy to manipulate? <input type="checkbox"/> yes <input type="checkbox"/> partially <input type="checkbox"/> no</p>	<p>Are protective measures regularly checked for correct function and is maintenance conducted in accordance with the manufacturers specifications? <input type="checkbox"/> yes <input type="checkbox"/> partially <input type="checkbox"/> no</p>
<p>Are problems that lead to disruptions to productions reported, recorded in a list and eliminated within a useful deadline? <input type="checkbox"/> yes <input type="checkbox"/> partially <input type="checkbox"/> no</p> <p>Protective devices are often manipulated because the production cycle is not ideal or the same fault occurs again and again (program fault, incorrectly set or badly serviced tools etc.)</p>	
<p>Is the manufacturer of the machine or plant consulted when solving problems? <input type="checkbox"/> yes <input type="checkbox"/> no</p>	

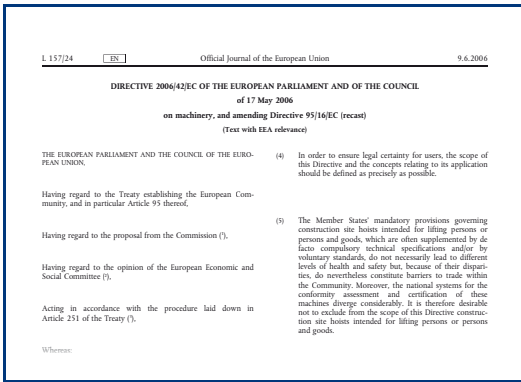
**An additional measure is required where one of these questions has been answered with “no” or “partially”**

**Fig. 19** SUVA checklist to determine manipulation incentives

example, but also of mobile enabling switches and jog keys that operate without cables across a safety-related radio link and/or the possibilities offered by safety control systems, optionally including speed and movement monitoring.

The new considerations also come at the right time for the amended statutory and normative framework conditions. While we do not wish to get caught up in the proposition that, according to the theory of the lesser of two evils, there





**Fig. 21** EC Machinery Directive (excerpt) with a clear pleading to consider all operating stage of a machine in the safety concept to prevent manipulation incentives.

could be a design possibility involving arbitrary optimization between the safety level and manipulation incentive, a little optimisation is surely justified, for example taking into consideration the operation qualification, alternative safety measures and the kind of work (no routine etc.).

There is no other motivation behind the corresponding amendments to the EC Machinery Directive (keyword: greater leeway for special operating modes), and also in the prevention policy of the Employers Liability Insurance Associations.

**Summary**

This article has set out the most important aspects that must be heeded in future both directly and indirectly in connection with the subject of “manipulation of interlocking devices”. It certainly concerns a multidimensional problem for there is no easy solution; however, it is one that challenges all involved, both manufacturers of safety components and machines as well as machine operators.

**Footnotes:**

[1] Report „Manipulationen von Schutzeinrichtungen“, Download unter: [www.dguv.de/ifa/de/pub/rep/pdf/rep05/manipulation\\_schutzeinrichtungen/ReportGesamt.pdf](http://www.dguv.de/ifa/de/pub/rep/pdf/rep05/manipulation_schutzeinrichtungen/ReportGesamt.pdf)

[2] [www.suva.ch/home/suvapro/branchenfachthemen/schutzeinrichtungen.htm](http://www.suva.ch/home/suvapro/branchenfachthemen/schutzeinrichtungen.htm)

[3] **Prof. Dr. Thomas Klindt:**  
Partner of the international Society NÖRR STIEFELHÖFER LUTZ and responsible there for occupational health and safety law, CE guidelines and compliance management among other things, also honorary professor for product and technical law at the University of Kassel

# Risk: Unexpected start-up

Yesterday at a recycling plant in Einbeck:

## Fatal industrial accident

(Ms). A 43 year old worker at a recycling plant in Einbeck, Lower Saxony, was killed yesterday (Saturday). According to the police, the man had been cleaning a shredder when when a 51 year

old plant operator started up the machine in the usual way, unaware that maintenance work was being carried out. The fitter was then caught up in a worm thread, sustaining fatal injuries.

One may not wish to imagine the details of the event that took place in this accident which was recently reported in a Sunday paper. However, again and again we hear of this kind of accident and others like it that take place due to unexpected or unseen starting-up of difficult-to-see machines and plants (even if thank God, these do not always end in death, even less severe accidents affect the course of human lives).

Without knowing the precise situation and the associated circumstances of this individual case, we will refrain from making any assumptions here about probable causes and what could have been done to prevent the accident.

Nevertheless we would like to take this opportunity to investigate a few aspects that must be heeded in connection with this and which illustrate the possibilities that safety components offer today for minimizing risks of this nature.

Firstly: The re-engaging of a machine, a mechanical plant or a production system is always a safety function if risks of unexpected starting-up (restarting) exist by virtue of hazardous movements in accessible machine areas or it is possible to move behind protective devices. This problem can be worked through while conducting the risk assessment that every machine manufacturer or system integrator is legally obliged to carry out and to document.

### EN 1037: Prevention of unexpected start-up (current version: 2008)

EN 1037:2008 defines unexpected (unintention-



Fig. 1 Reference source of the standard: Beuth Verlag GmbH, Berlin; [www.beuth.de](http://www.beuth.de)

a) start-up (which includes the term “restart”) as any start-up that is caused by the following:

- A start command generated by a failure in or caused by external influence to the control system;
- A start command generated by an operating error on a start actuator component or to a different part of the machine, such as a sensor or power control elements;
- Return of the energy supply after interruption;
- External/internal influences (gravity, wind, auto- ignition of combustion engines etc.) on parts of the machine.

NB: Automatic start-up of a machine in normal operation is not unintentional but can be regarded as unexpected from the point of view of the operator. In this case accidents are prevented using protective measures (see EN ISO 12 100-2 (section 4).

The standard EN 1037 provides an overview of a

Contents	Page
Foreword .....	3
Introduction .....	4
1 Scope .....	4
2 Normative references .....	4
3 Definitions .....	5
4 General .....	6
4.1 Isolation and energy dissipation .....	6
4.2 Other means to prevent unexpected [unintended] start-up .....	6
5 Devices for isolation and energy dissipation .....	6
5.1 Devices for isolation from power supplies .....	6
5.2 Locking [securing] devices .....	7
5.3 Devices for stored energy dissipation or restraint [containment] .....	7
5.4 Verification .....	8
6 Measures - other than isolation and energy dissipation - intended to prevent unexpected start-up .....	9
6.1 Design strategy .....	9
6.2 Measures intended to prevent accidental generation of start commands .....	9
6.3 Measures intended to prevent accidental start commands resulting in an unexpected start-up .....	10
6.4 Automatic monitoring of the category 2 stopped condition .....	13
Annex A (informative) Examples of tasks which can require the presence of persons in danger zones .....	14
Annex B (informative) Signalling, warning .....	15
Annex ZA (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 98/37/EC .....	16
Annex ZB (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 2006/42/EC .....	17
Bibliography .....	18

**Fig. 2** Download from [www.beuth.de](http://www.beuth.de) → entry field “EN 1037” → PDF table of contents (free of charge)

number of aspects and requirements that must be heeded and stipulates design safety measures that are aimed at preventing unexpected start-up in order to facilitate safe contact for people in hazardous areas. It concerns unexpected start-up resulting from all types of energy, i.e. to the energy supply (e.g. electric, hydraulic, pneumatic) to easily overlooked stored energy (e.g. from gravity, springs under tension) or to other external influences (e.g. from wind). Figure 2 provides a detailed overview of the standard.

Some solutions to the problems on this subject offered by the Schmersal range are set out below by way of example.

### Executing of the stop command

The assumption in the following executions is always firstly that a stop command is safely generated by the triggering of a protective device in the [I]nput, [L]ogic and [O]ut-put chain with the necessary performance level and is implemented in the form of stop category 0, 1 or 2.

Please do not confuse the above mentioned

“category” term with control category or similar. What is meant here is rather the distinction in Section 9.2.2 of EN 60 204-1:2007 [1], according to which a stop command can be implemented

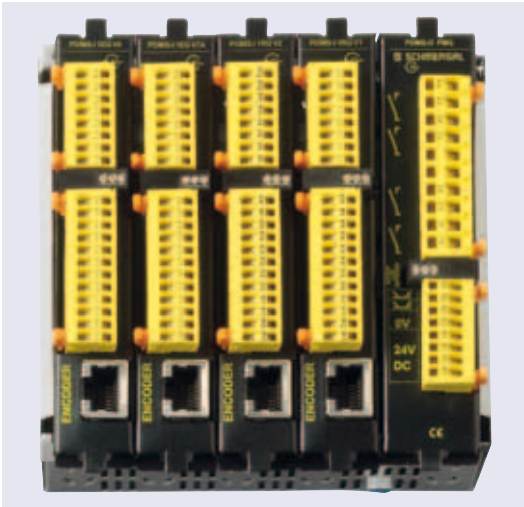
- as uncontrolled shut-down (by immediate interruption to the power supply → Stop 0) or
- as controlled shut-down (by time delayed interruption to the power supply → Stop 1)

according to the best possible hazard minimization. A safety related shut-down monitoring is additionally necessary (also see EN 1037:2008 Section 6.4 in this respect), if a stop command is to be executed as stop category 2, i.e. likewise with a controlled shut-down where the energy supply also remains when the machine has been shut down.

All protective devices and safety-related control devices in the Schmersal range have been designed precisely to offer numerous possibilities for the realization of safety-related stop commands. For example, reference is made to the shut-down monitoring devices specifically intended for stop category 2 from the FWS range (as shown in Figure 3) or, for more complex operations, the safety control systems of the PDMS range (as shown in Figure 4).



**Fig. 3** The shut-down monitors from the FWS range serve to safely record the machine’s shut-down. Depending on the external circuit in conjunction with a safety monitoring module from the AES or SRB range, it is possible to safeguard a protective device up to PL “d”.



**Fig. 4** The Protect Drive Monitoring System (PDMS) serves to expand the PROTECT PSC safety control system designed for universal use. With its modular construction, the PDMS represents a solution for safe shut-down and speed monitoring, e.g. of spindle or axle drives up to PL “e”.

**Measure: Permanently present stop command**

The permanently present stop command plays an important role, especially if somebody has to work for a prolonged period in a hazardous area that is difficult to see. “Permanently” in this connection will primarily mean the main separation device (colloquially also still frequently referred to as “main switch”) (see EN 60204-1 Section 5.3). However, should this not be possible for

reasons of the work cycle, permanently is re-interpreted for the following statements so is to be able to address other possibilities provided by today’s safety components.

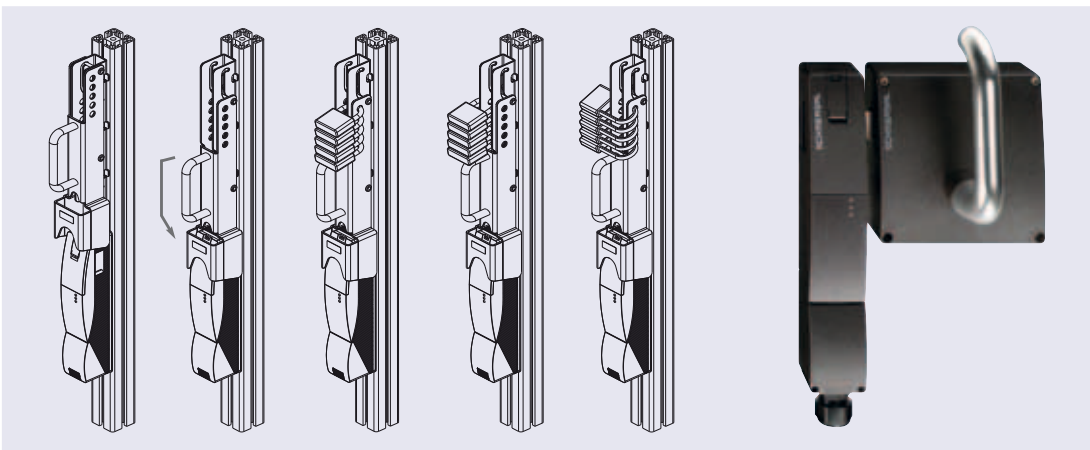
“Permanently” is interpreted here in an exemplary manner, i.e. that the starting-up of the machine cannot be set in motion or initiated by any third party. The difficulty in seeing a hazardous area for a third party can occur quickly if one considers linked individual machines, integrated production systems and machine installations.

A simple but therefore more effective means of achieving this aim is offered by moving protective devices (guards, protective grilles etc.) – so-called lock-out tags in the terminology used by the Schmersal group (as shown in Figure 5). These accessories make it possible to secure interlocking devices (safety switches with and without guard locking) in an open state using padlocks so that renewed actuation of the devices is prevented, i.e. the renewed closing of the moving protective device and renewed starting-up of a machine by a third party is effectively prevented both by mechanical and control-related means.

An execution example for model AZM 200 electronic safety interlocks with lock-out tag SZ 200 is shown in Figure 5.

**Key transfer systems**

Key transfer systems offer intelligent possibilities to protect against unexpected (unintentional)



**Fig. 5** A lock-out tag (the example depicted here is an SZ 200 as Electromagnetically operated guard locking and safety sensors from the AZ/AZM 200 range) prevents actuation of an interlocking device by enabling the operating staff to protect themselves by guard locking individually coded commercially available padlocks.

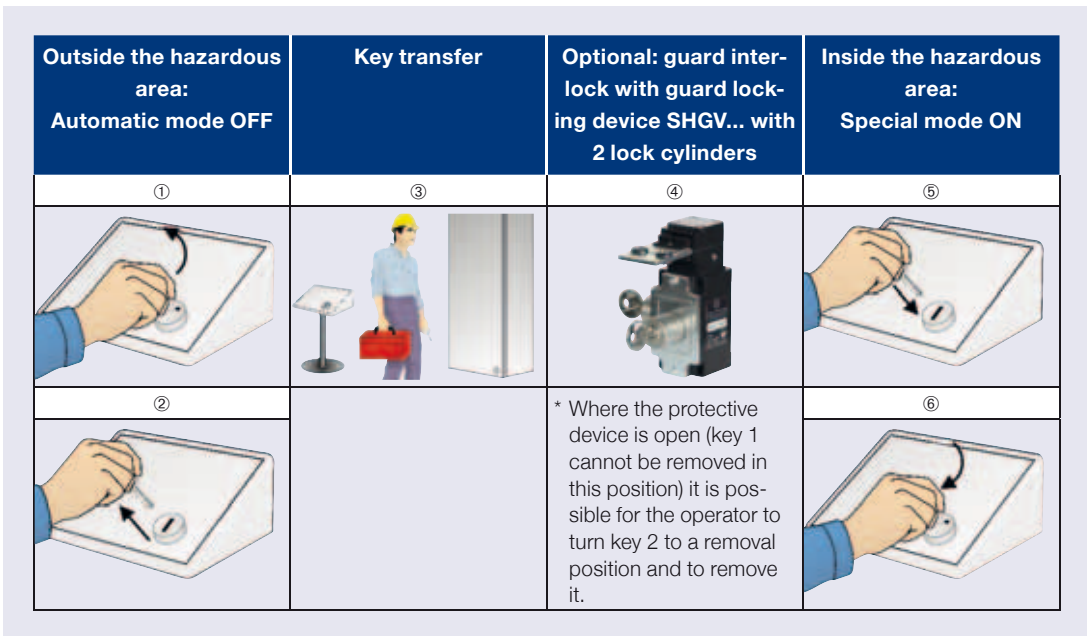


Fig. 6 Key transfer system

starting-up where special operation modes also need to be performed by operators in the inside of a hazardous area that is difficult to see.

Actuation of a key-operated selector switch firstly ensures that the automatic operating mode is safely interrupted, i.e. the switch is moved from the I to the O position and a contact with positive break opens. Using the key that can only be removed in this position, the operator is then able to actuate a second key-operated selector switch in the inside of the machine (O position → I position) that enables the special mode, whereby in this position the key cannot now be removed. Due to an individually coded closing nobody, apart from the operator himself, can reverse the setting on the outer control panel. The stop command for the automatic operating mode is permanently and safely present.

Diverse embodiments for using the philosophy behind a key transfer system are conceivable. It would, for example, be possible to place an interlock in the intermediate cycle, likewise equipped with a key transfer station, i.e. the key from the external key-operated selector switch would firstly be used to unblock the protective device, whereupon a second key could be removed which could then be used to enable the special operating mode in the inside of the ma-

chine (refer to Fig 6 to get a clearer understanding of this). The restarting of the machine takes place in reverse order.

Other possibilities for using the key transfer system idea to protect against unexpected start-up are provided by the key distribution stations (SVM range) and interlocking devices (SVE range).

**Reset using double acknowledgement**

These types of additional measures will not be necessary in all cases and – if we consider opto-electronics for example – the protected devices do not always involve moving guards that must be safeguarded using interlocking devices.

For other applications in hazardous areas that are difficult to see, the use of the double acknowledgement procedure comes into question, for example that is illustrated using the PROTECT SRB 100DR safety relay module (as shown in Figure 7).

The function of the module ensures that it is only possible to restart the machine control system

- once the reset or restart button 1 has first been actuated by the operator and after he has left the hazardous area and if necessary has closed and locked a guard again;

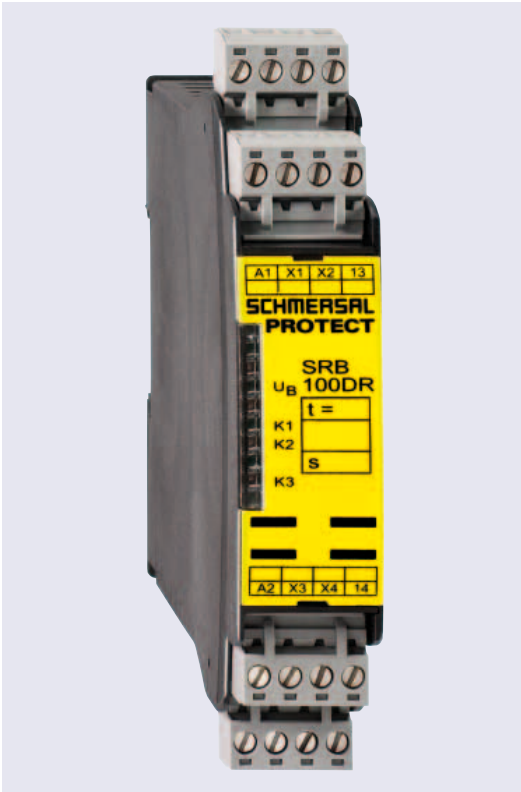


Fig. 7 PROTECT SRB 100DR safety relay module

- once a reset or restart switch 2 that is situated outside the hazardous area has been actuated. For executing this “double” acknowledgement an adjustable timeframe of between 3 and 30 seconds is provided (set via a DIP switch) within which actuation must take place (exclusively in the order button 1 → button 2). The timeframe can be oriented towards operational processes.

If the operator fails to actuate button 1 or to actuate button 2 within the timeframe, no enabling takes place and the double acknowledgement procedure must be repeated. Further signal processing of the reset signal then takes place via the commercially available safety relay modules such as those from the PROTECT-SRB range, i.e. in the case of the SRB 100DR module this is an upstream device that is implemented with performance level “e”.

### Fundamentally in future: Signal processing of the trailing edge with reset buttons

Irrespective of whether a reset signal (synonym for restart or acknowledgement signal) is implemented singly or doubly after leaving an accessible hazardous area or one that can be accessed from behind, whether with a key selector switch or using a commercially available push button etc., the requirements for detection of the trailing edge will in future apply to signal processing. This means that the acknowledgement may only take place by releasing the actuator element from its (actuated) “on” position. This requirement will in future arise from Section 5.2.2 of EN ISO 13 849-1:2008 (2006), irrespective of the type of protective device which is acknowledged.

This requirement for dynamic signal processing of the reset signal related to the trailing edge means that any failures and faults in the control device will be detected that would otherwise have constituted a potential risk for an unexpected restart.

The following also apply to the reset function:

- that it must be provided by a separate, manually operated device in the safety related part of the machine control system; and
- that the device may only be reached if all safety functions and protective devices are fully functional;
- that it must not itself initiate any movement or hazardous situation and that the reset function is an intended action that permits the control system to accept a separate start command.

The performance level must not reduce the safety of the corresponding safety function here.

Further requirements on the subject of “acknowledgement” are also contained in EN ISO 12 100-2:2008 (2003) section 4.

Footnote:

- [1] Electrical equipment of machines; standard may be procured from: Beuth Verlag GmbH, Berlin; [www.beuth.de](http://www.beuth.de)





# New standard EN ISO 11 161: Safety of integrated manufacturing systems

Although the standard was only finally published as a harmonised standard in January 2008, we have been involved with the subject since 2003 in the form of seminar events.

Here we were able to present Mr. Christoph Preuße as guest speaker to the large number of participants; Mr. Preuße is a recognised expert on the subject of EN ISO 11 161. He is Technical Supervisor (TAP) and member of the “Mechanical Engineering, Manufacturing Systems and Steel Manufacture (MFS)” technical committee at the employer’s liability insurance association Metall-BG Nord-Süd (BGMET) in Mainz and has been working for the standardisation committee of EN ISO 11 161 for several years.

An excerpt from our summary at that time is set out below.

## EN ISO 11 161: A special machinery standard

This standard is no classic product standard that focuses on a specific type of machinery, as a C standard on “machine tools” would, for example. Rather EN ISO 11 161 is a cross-cutting (lateral cut) standard which may be applied for example both to the manufacture of foodstuffs and to the area of metal processing. Although this was not the original intention of the standard setters it will also therefore be afforded the status of a B1 standard within the context of European terminology, despite the fact that according to the standard there is no such thing as an “integrated manufacturing system” as type of machinery. A need arose for a more abstract and application-neutral formulation to take different dimensions and degrees of complexity as well as the interaction of different technologies into consideration.

The new EN ISO 11 161 standard was only finally prepared by the international standards committee in September 2003; it bridges a gap in the set of European standards that has been present for many years since the first standardisation project on the subject of “integrated manufacturing systems” (prEN 1921) fell through.

It was possible to manage in the meantime using VDI 2854 as well as other standards and sets of

DIN EN ISO 11161:2010-10 (E)	
Safety of machinery - Integrated manufacturing systems - Basic requirements (ISO 11161:2007 + Amd 1:2010) (includes Amendment A1:2010)	
Contents	Page
Introduction .....	5
1 Scope .....	7
2 Normative references .....	7
3 Terms and definitions .....	8
4 Strategy for risk assessment and risk reduction .....	12
4.1 General .....	12
4.2 Specification of the limits of the IMS .....	12
4.3 Determination of the task .....	12
4.4 Identifying hazardous situations .....	14
4.5 Risk estimation and risk evaluation .....	14
4.6 Risk reduction .....	14
5 Risk assessment .....	16
5.1 Specifications of the IMS .....	16
5.2 Identification of hazards and hazardous situations .....	16
5.3 Risk estimation .....	19
5.4 Risk evaluation .....	20
6 Risk reduction .....	20
6.1 Protective measures .....	20
6.2 Validation of the protective measures .....	20
7 Task zone(s) .....	20
7.1 General .....	20
7.2 Determination .....	21
7.3 Design .....	21
7.4 Functional analysis .....	22
8 Safeguarding and span of control .....	22
8.1 Safeguarding of task zones .....	22
8.2 Span of control .....	23
8.3 Electrical equipment requirements .....	23
8.4 Modes .....	23
8.5 Safeguards .....	24
8.6 Protective measures when safeguards are suspended .....	24
8.7 Muting and blanking .....	26
8.8 Control .....	26
8.9 Reset of perimeter safeguarding devices .....	27
8.10 Start/stop .....	27
8.11 Emergency stop .....	28
8.12 Measures for the escape and rescue of trapped persons .....	28
9 Information for use .....	28
9.1 General .....	28
9.2 Marking .....	28
10 Validation of the design .....	29

10.1 Validation that the design meets the requirements .....	29
10.2 Validation of the protective measures .....	29
Annex A (informative) Examples of integrated manufacturing systems (IMS) .....	30
Annex B (informative) Flow of information between the integrator, user and suppliers .....	33
Annex C (informative) Span of control examples within an IMS .....	34
Annex D (informative) Temporary observation of the automatic process .....	38
Bibliography .....	42
Annex ZA (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 98/37/EC .....	43
Annex ZB (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 2006/42/EC .....	44
Figure 1 – Configuration of the limits of the IMS .....	6
Figure 2 – Specification of the limits of the IMS .....	13
Figure 3 – Determination of tasks (requirements, location, access) .....	13
Figure 4 – Identification of hazards/hazard zones and associated hazardous situations .....	14
Figure 5 – Determination of the task zone(s) .....	15
Figure 6 – Determination of the safeguarding including the span of control .....	16
Figure A.1 – Examples of machines and parts of machines of IMSs .....	30
Figure A.2 – Examples of IMSs .....	32
Figure C.1 – IMS composed of five machines and the machine-handling system .....	34
Figure C.2 – IMS as in Figure C.1, but divided into two zones .....	35
Figure C.3 – IMS as in Figure C.2, but zone C is equipped with presence-sensing .....	36
Figure C.4 – IMS as in Figure C.2, but access 8 allows entry between zones A and B” .....	37
Figure D.1 – Safeguarding during process observation .....	39
Tables Table B.1 – Information flow between the integrator, user and suppliers .....	33
- 2 -	

Fig. 1 Table of contents of DIN EN ISO 11161:2010-10 (E)

rules and regulations; VDI 2854 is a German set of rules that is also included in the so-called helpful list. This list is published by the Federal Government to inform interested parties about which standards and sets of rules and regulations it believes to be expedient and helpful for correct implementation of the protective objectives of the EC Machinery Directive if there is not yet any European standardisation for the area concerned. However the structure and content of EN ISO 11 161 look completely different to VDI 2854.

It is more a kind of management system and less a set of rules and regulations with details on the subject of “required properties” or “construction and equipment”.

In addition to the fact that it closes a gap in the set of standards that objectively exists, a further advantage of the new standard is that it has been created from the outset at international level and for this reason alone can expect greater acceptance outside Europe.

**Terms and fields of application**

In order to define a clear and autonomous profile (and not come into conflict with related standards that already exist), an Integrated Manufacturing System (IMS) will firstly be understood as

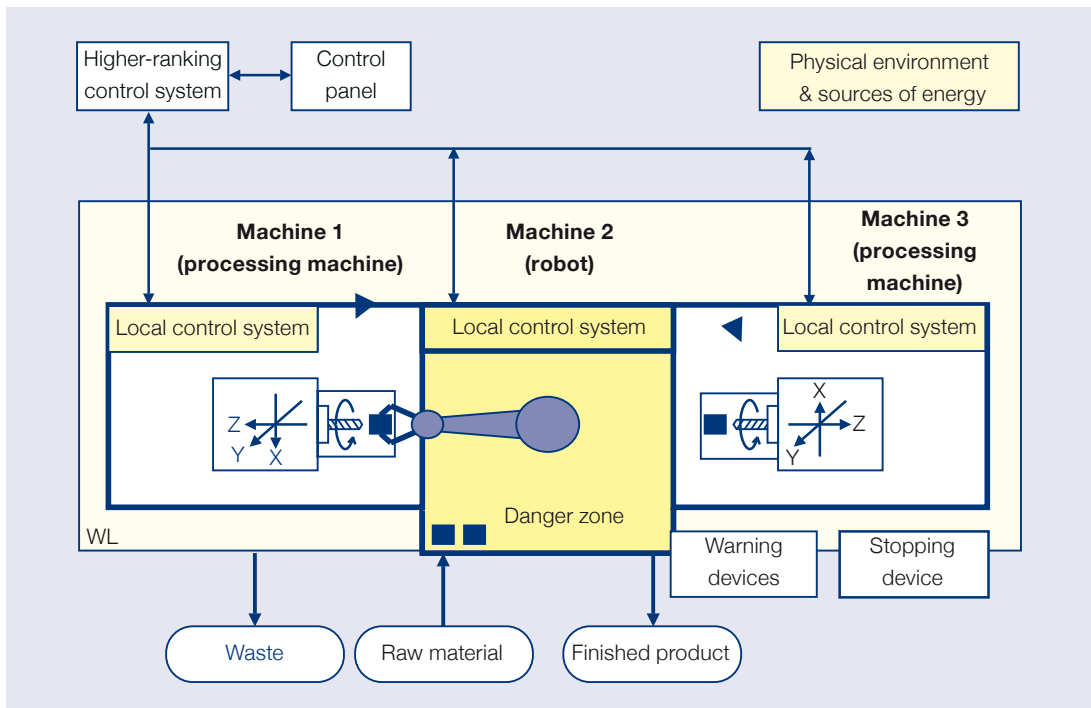
a group of co-ordinated industrial machines (two or more connected and controlled machines) working collectively, that are linked in order to manufacture, treat or process different pieces of work (products) in them.

The special feature is that the IMS has a higher-ranking control system (or a higher-ranking control system intelligence exists in one of the decentralised control systems) in addition to decentralised control systems in the various individual machines and individual units of the system. This enables it to also be partially operated. This feature distinguishes an IMS within the meaning of EN ISO 11 161, in this case from a transfer machine or a robotic system, for example.

The objective of EN ISO 11 161 is to formulate safety requirements in the context of this specification, based on the guidelines in EN ISO 12 100-1/-2 and EN ISO 14 121-1/(-2), that are directed at protection for the person operating such an IMS.

**System integrator**

The so-called system integrator (an “institution” which in future will also exist in the robot standard ISO 10218-1) is a special creation in EN ISO 11 161).

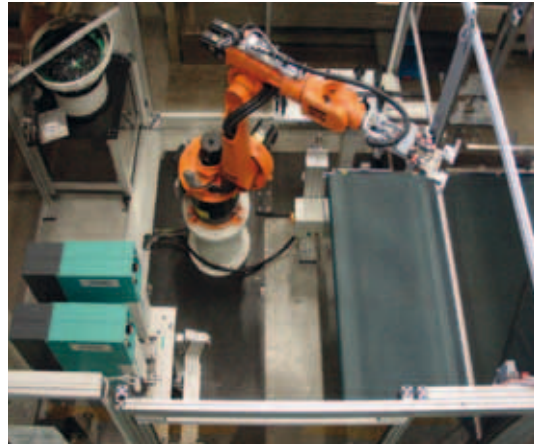


**Fig. 2** Schematic diagram of an IMS

This concerns a natural or legal person who develops or composes integrated manufacturing systems (or who has them developed or composed); this includes all control parts (in particular those that are relevant to safety). The system integrator is therefore the person responsible for bringing an IMS onto the market within the meaning of the EC Machinery Directive, and who must consequently carry out the conformity assessment and sign the CE declaration of conformity.

Which of the co-operating persons involved is ultimately the system integrator can differ. It may be the subsequent operator of the IMS himself, a selected supplier who is additionally responsible for safety-related system integration, or a third person on whom this responsibility has been specially conferred.

At all events, special demands are placed on the system integrator. On the one hand the task requires knowhow and special knowledge, together with the ability to communicate (and to resolve conflicts) between the different “parties” (the supplier and the operator). Last but not least, it is therefore also essential to have corresponding authority with respect to design. For example the system integrator must be able



**Fig. 3** Reis robot deployed in an integrated manufacturing system

to specify the responsibilities in the project and have knowledge about the components that are provided or supplied by third parties and/or the operator.

The checklist published in the informative Annex B of EN ISO 11 161 is a helpful tool for the system integrator; it contains a list of objectives to bear in mind, the requisite communication flows and the various aspects to be considered in the process (as shown in Figure 4).

Safety Integration related tasks	Information flow	Item	Sub-item
IMS functionality	U > I > S	IMS performance	Availability Maintainability ...
Tasks & interventions description	S > I > U	Invention conditions	Intervention location Operating modes Working, troubleshooting modes and maintenance Frequency Duration Necessary means Power On/Off (parts of) IMS Personnel/operator qualification
Hazard situations identification	S > I I > S	Linked risks to IMS configuration	–
Risk assessment & evaluation	S > I & I > S I > U	Risks linked to IMS configuration	Residual risk

S = Supplier; I = Integrator; U = User

**Fig. 4** Annex B: Checklist (extract)

## Content of EN ISO 11 161

In addition to the three standard opening chapters and final chapter contained in every standard on the subject of “machinery safety”, ISO 11161 is currently divided into the following specific sections:

- Safety implementation strategy
- System specification
  - System concept
  - Movements in an emergency
- Risk analysis
- Risk reduction
  - General
  - Zone concept
- Requirements placed on the design of the system
  - Design at system level
  - Zone concept
  - Protective devices in zones
  - Span of control of the control system
  - Electrical installation requirements
  - Modes
  - Protective devices
  - Local control systems
  - Suspension of individual protective devices
  - Start/restarting
  - Emergency stop
  - Operating manual.

### The zone concept

While the zone concept is not unknown in practice it acquires special significance in EN ISO 11 161.

Zones should be seen as spatial areas within an integrated manufacturing system that operating personnel may or must enter depending on certain operating modes while the rest of the IMS continues to operate. This means the aim is attaining (increased) availability of integrated manufacturing systems without neglecting personal protection in the process; keeping both of these aspects in mind, this is achieved by ensuring that

shutting down (or transferring to a special mode) is kept to a minimum.

In other words, the IMS continues to work in other areas of the production process while tasks such as troubleshooting, alignment, observation and/or maintenance are performed in a certain zone within the primary protective devices. If such differentiation is not possible or makes no sense, then this is not an IMS in terms of ISO 11161.

Zones are defined on the basis of system limits (designated purpose of the IMS, IMS function, foreseeable use, foreseeable misuse)

- Tasks for tasks of this kind and
- Determining the respective associated hazards;
- Specifying customised protective measures
- and designing the control systems accordingly

### Determining the protective strategy

The main content of the protective strategy is to identify appropriately varied safety-related operating modes (of which there may be a great number) to be performed for the respective task within the primary protective devices (i.e. generally inside the perimeter guarding).

The identification of operating modes will depend both on the overall system and on the defined zones, but also on individual components within a zone. For simplification it is possible to combine zones if this is acceptable from a safety and functional point of view.

It is established using the operating mode which parts of the system (delineated by additional protective devices inside the system) can continue to work in automatic mode and which part (which zone) gets special treatment with regard to safety depending on the task carried out by the person who has to be located here.

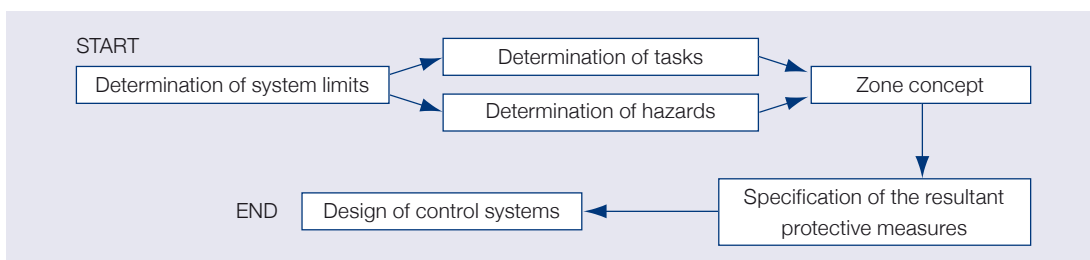


Fig. 5 Zone concept: workflow

This special safety-related treatment (protective strategy) can, for example, consist of safe stopping of the zone affected if it is necessary to rectify a fault, of a permissible manual mode in this area or operation there at reduced speed with enabling switch for setup work (or where there is no safe limited reduced speed).

Where necessary adjacent sections (zones) may also be subject to special safety-related consideration, e.g. it may be necessary to “run” at reduced speed here too.

Re “process observation” mode: see loc. cit.

It is clear from these general conditions that special safety-related significance is attached to the precise description of layout and access possibilities (man/machine interfaces) within the zone concept. Firstly there is a need for precise knowledge of the critical safety parts of the system, and secondly special attention must be paid to the thoroughfares for the operator and/or the servicing and maintenance personnel.

### Safe stand

It is essential to ensure that every activity in the system, insofar as it is necessary, is performed from a safe stand and that all system functions include the foreseeable statuses of the system (also faults).

If no satisfactory solution is arrived at in terms of the protective strategy, it may be necessary to check the system design once more, for ex-

ample to see whether it is possible to satisfy safety requirements by changing the specification or the limits of the system, whether changes or modifications to the equipment deployed are possible etc. Last, but not least special attention must also be paid to the control system concept in this connection.

All control-related measures must firstly be commensurate with ISO 13849-1 (EN 954-1) and/or IEC 62061 (IEC 61508). The above mentioned higher-ranking control system must recognise the status of each “local” control system and may only have targeted influence on the local control system. Resetting after triggering protective devices should always be a conscious manual procedure and take place from outside the protected area. Added to this is a special emergency stop strategy (see loc. cit.).

### Emergency stop concepts

The subject of “actions in an emergency” (emergency stop, as shown in Figure 6) is also of great significance in the case of integrated manufacturing systems.

Which devices should have a higher-ranking effect, and which devices only partial impact? Should this distinction also be reflected in the design of the devices? If so, should this be in the form of a different colour, shape or labelling?

The EN ISO 11 161 standards committee decided in favour of the classic route when it came to these questions.

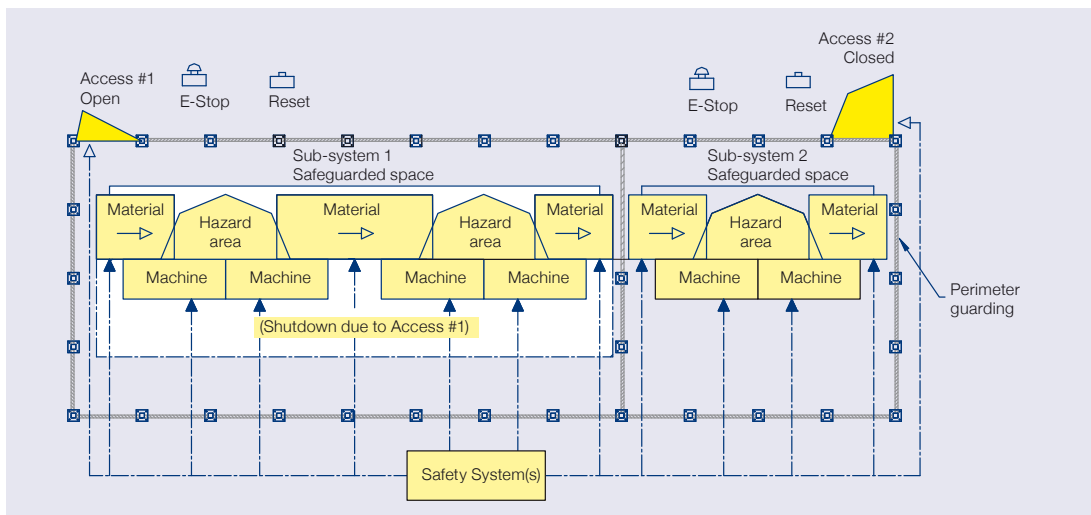


Fig. 6 Annex D: Example for the design of a control device

This takes account of the “actual” (traditional) *raison d'être* of emergency stop devices (putting machine protection to one side for a moment), which is namely that somebody will still be able to react and help if an unforeseeable residual risk for someone else leads (produces) a risk to the health or life of that person.

This perspective is expressly underlined by the idea of an additional precautionary measure which, when used correctly, will only be required extremely rarely in view of the level of safety technology present today in machinery or a machine system. As such emergency stop devices are not designed to be used as operational stop signals or for any other considerations motivated by convenience.

On the one hand this requires the design engineer to take operating requirements into consideration using other measures (other control devices), while on the other hand it is a question of “educating” the machine operator’s staff.

The new terms are taken from EN 60204-1 (1998-11). Consequently a distinction is made between the following:

- **Stopping in an emergency:**  
An action in an emergency that is designed to stop a process or a movement arbitrarily that was or could become hazardous.
- **Actuation in an emergency:**  
An action in an emergency that is designed to start a process or a movement in order to eliminate, prevent or limit a hazardous situation.
- **Disconnection in an emergency:**  
An action in an emergency that is designed to disconnect the power supply to a complete installation or to part of it if there is a risk of electric shock or other risk originating from the electrical system.

Disconnection in an emergency should be provided (Section 9.2.5.4.3) of EN 60204-1 where

- protection is provided by means of gaps or obstacles to prevent direct contact (e.g. with conductor lines, slip rings, switchgear in electrical service rooms);
- there is a possibility of other hazards or damage from electric power.

- **Switching on in an emergency:**  
An action (which differs from actuation) in an emergency that is designed to supply power to part of a system in an emergency situation.

#### **Possible access for everyone from the outside**

In other words, an emergency stop control device that is attached to the primary protective device and is accessible from the outside must have an overall effect, whereby the overall effect may be limited to the visible (audible) area.

In the case illustrated in Figure 6 it is assumed that in case of emergency it is not acceptable in the interests of personal protection to rely on specific employee knowledge or on subsequent reflection of which of the several devices installed on perimeter guarding (which may be distributed in different locations) should be actuated to produce a safety-related stop signal at the “right” place. Doubts about the efficacy of an emergency stop devices for an insider or outsider will not be tolerated, and there is conscious acceptance of the consequences in terms of the availability of a machine (new setup before re-starting, repairs possibly also necessary).

#### **Access inside**

The situation is different where emergency stop control devices are inside the integrated manufacturing system, irrespective of whether these are installed permanently on the individual machines or are in mobile handsets. Here the device is solely intended to protect the person who is authorised to be inside the system. As such only partial effect of a safety-related stop signal is acceptable (albeit tailored to the operator concerned). Here it is not assumed that a third person can actuate the device in an emergency, but that this can only be performed by the operator.

#### **Design**

No differences are planned in the design of emergency stop control devices, i.e. whether the device is accessible from outside or only from inside, the shape of the operating element in both cases is mushroom or palm-shaped, its colour is in “red” and it is highlighted underneath in “yellow”. It is assumed as a matter of course that the devices will also correspond to EN ISO 13850 and IEC 60947-5-5.



With regard to mobile (pluggable) handsets this furthermore means that the operator has an obligation to lock devices away (to remove them effectively) if they are not connected to the control system. Alternatively other measures have to be taken into consideration to avoid confusion if an e-stop device is connected (or not).

### Requirements concerning operating manuals

Although it is actually obvious, the draft of the EN ISO 11 161 explicitly stipulates that the operating manual of an integrated manufacturing system must firstly contain an overview of how the IMS is constructed (zone concept etc.), how it interacts etc. and, if one wishes in Part 2, then contains operating instructions for individual components. The basis for content and implementation of the operating manual can be found in ISO 12 100-2:2003 Chapter 6 (former EN 292-2).

### New “process observation mode”

The draft of ISO 11161 was one of the first standards on the subject of “Machinery safety” to deal explicitly with the (new) process observation mode which it permits solely in relation to observation (“just looking”). In the case of inte-



**Fig. 7** Observation of processes, e.g. for overlay welding during reprocessing of the extruder screws.

grated manufacturing systems it is not permitted to intervene in the process to optimise it. Interventions must be carried out from a safe place (unlike the “process observation” mode currently being discussed for machine tools where this separation between observation and intervention in the IMS is not possible for reasons of space alone; in other respects the requirement is the same or similar).

While subject to compliance with strict conditions, it is understandable that agreement on this operating mode has involved disputes when one considers that the process observation mode “permits” a process in an integrated manufacturing system to run at a “speed required for the process” under the direct observation of an operator, and where this “speed required for the process” can extend to automatic speed.

In this case the acceptability of what is undoubtedly a slightly increased residual risk for the observer is justified by an assumption, which is borne out in practice sometimes in conjunction with “very nasty” accidents, which it is highly probable that protective devices on the IMS will otherwise be defeated. For the observer and uninvolved third parties this (foreseeable) manipulation would then mean a more hazardous unrestricted automatic operating mode. One could say that the “process observation” mode is acceptable as it is the lesser of two evils.

### Strict requirements

Firstly: the process observation mode is an operating mode for exceptional cases, and only for when its use is vital from a production point of view to observe processes at high speed “face to face” and where other technical options such as windows, mirrors, cameras etc. do not come into question as alternatives. Its appraisal must also take the enabling mode and other “less critical” operating modes into consideration, for example.

Furthermore, the admissibility of a process observation mode must always be weighed up individually, where the machine supplier (or system integrator) must convince himself of its necessity and the IMS operator undertakes to only instruct trained personnel who are familiar with the dangers (possibly authorised by name) with carrying out this operating mode (including an obligation to train new personnel accordingly). Therefore



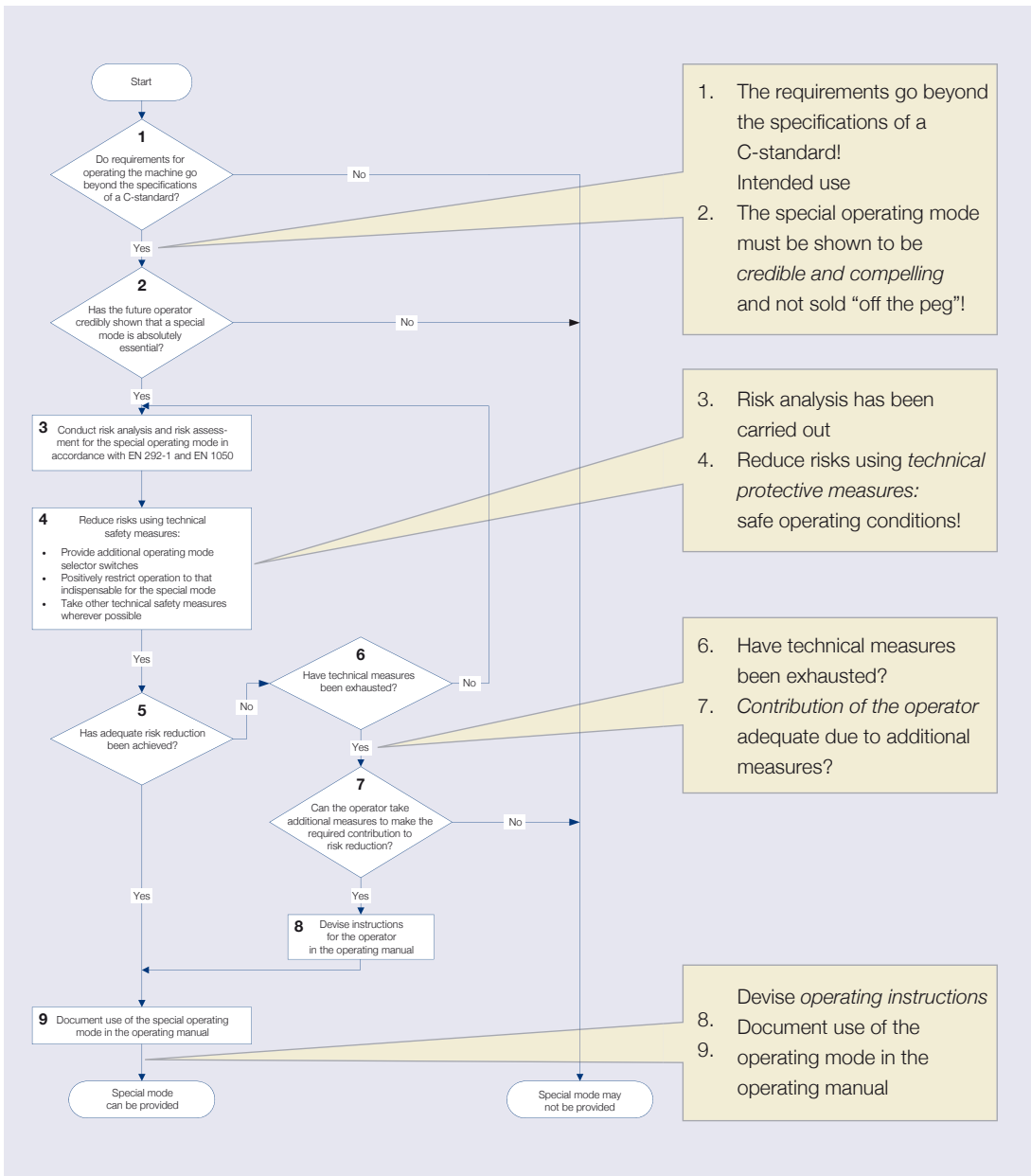


Fig. 8 Solution aid: flowchart showing the special “process observation” mode

critical co-operation with the operator is an absolute must for the new operating mode to be applied responsibly.

In addition to a design that is as inherently safe as possible, other entry prerequisites for the process observation mode are that all sources of danger that are not absolutely necessary in accordance with regulations are shut down safely and that running movements are monitored using safe technology. Therefore everything must be realised in terms of safety technology that is

facilitated by the current state of the art, such as control systems with safely monitored speeds, paths or positions.

If one wishes to comply with the rules governing the process observation mode, it is worth considering the solution approach set out in the flowchart in Figure 8.

See page 55 for information on the subject of integrating new and used machinery in an integrated manufacturing system.

*Chapter 4:*

***Technological development of safety components –  
illustrated using  
the example of the Schmersal range***



# **Technological development of safety components**

## *– illustrated using the example of the Schmersal range*

While this article is no foray into the history of safety at work\*, we could not resist the temptation to start with the following excursus, despite the fact that it is admittedly not entirely apt at this juncture and is also somewhat macabre. It concerns the example of an “occupational health and safety-related” measure for the sugarcane harvest in the West Indies around 1840. We quote from a contemporary description:

*... When it is ripe, the cane propagated from cuttings is cut and then crushed and squeezed between rollers in sugar mills. However this work is both arduous and dangerous at the same time. Since the sugarcane cannot be stored and goes bad after just 24 hours, the Negros frequently have to stand day and night in front of the rollers in the sugarcane harvesting period, holding the sugarcane. They often become sleepy and, without noticing, place a finger between the rollers; these then draw in the finger, followed by the hand which is then completely crushed. For this reason there is al-*



*ways somebody ready with a sharp axe to cut off the finger or hand if it has become caught, preventing the whole body from being drawn into the machinery.*

The keywords “risk assessment” and “risk reduction” come to mind here!

\* If you are interested in the history of safety at work in Germany however, we have included some information on this starting on page 177.

### **Preamble**

That is as far as our foray into history goes at this point.

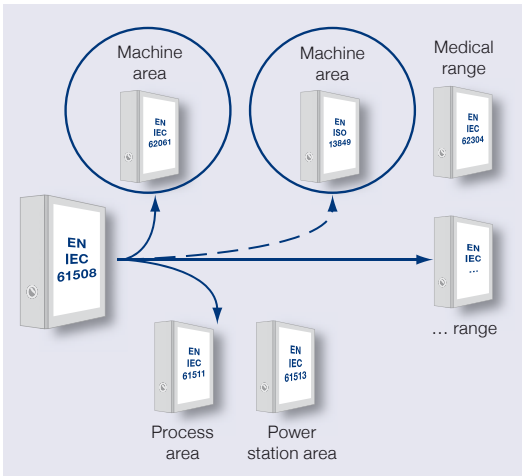
We would actually like to start this chapter with a more recent historical cross-reference which still seemed inconceivable at the start of the 1990s; this concerns the deployment of a broad range of microprocessor-based technology for safety functions, representing the establishment of a substantial paradigm shift. This also took place within a relatively short space of time, after all the 1990s are not that long ago. Programmable electronic systems with safety function (PES) are now part of the state of the art; they have made a significant contribution to improving both the safety and the functional cost/performance ratio of safety components [1] and to making them more attractive.

The original scepticism directed at this technology was basically explained by an inability to calculate the safety of thousands of software-

controlled transistor functions on these chips. Deterministic approaches used in traditional technologies could no longer be applied here. Added to this were reservations with respect to transparency, fault possibilities, possibilities for testing and regarding manipulation.

Rail signal technology and in particular the international standard IEC 61508 [2] initially played a pioneering role in making programmable electronics “acceptable” for safety-related tasks. To some extent it was inspired by the German preliminary standard V VDE 0801.

Special requirements on the design of such systems, on redundancies, highly dynamic cross-wise test routines – also in conjunction with dissimilar approaches and “rules of the game” for writing and testing software – on this basis have ensured a high degree of safety and reliability. In the area of machine safety at least the trust in the new opportunities presented by PES technology has not disappointed to date.



**Fig. 1** “Sponsors” of EN IEC 61508 functions

In the meantime IEC 61508 (which, while not harmonised, has also got the status of a European EN standard since 2001) has even supported several specific industry standards derived from it. Examples for mechanical engineering are the standards ISO 13849-1 and EN IEC 62061, the standard EN IEC 61511 and others for chemicals and process technology. As a rule the developers of complex electronics go directly to the IEC EN 61508 while users refer to the more simplified specific standard for the industry.

The Schmersal Group has been supplying new solutions on the basis of programmable micro-processor-based electronics with safety function (PES) for several years. In the case of several new developments we can claim to have been the first or at least among the first on the market.

The following PESs from the Schmersal range will be discussed:

- Optoelectronic protective devices (see page 164)
- Safety control systems for digital functionalities (see page 167)
- AS-i Safety at Work (see page 168)
- Control systems for safety-related speed and movement monitoring (see page 170)
- Wireless with safety function (see page 173)
- Electronic safety sensors/interlocks (see page 174).

### Optoelectronic protective devices

Safety-related light barriers, light grids and light curtains can be numbered among the programmable electronic equipment used for many years. Their use in practice as electro-sensitive protective equipment is indispensable. While the initial aim was to come to grips with reliability and availability, additional functions in the form of special operating modes (such as blanking, floating blanking, EDM, muting, cyclic operation or restart inhibit) were later in the foreground as well new solution approaches (of which scanners can be cited as an example). The companies Sick and Leuze largely played the pioneering role here. The development of a number of application-related variations appeared parallel to this. Today people are excited to see which new possibilities will open up, for example the use of safe camera technology.

With the acquisition in the Autumn of 2008 of the companies Safety Control GmbH and Safety Protect GmbH with registered office in Mühlendorf am Inn, the Schmersal Group substantially expanded its optoelectronic protective device (AOPD [3]) product range. The devices offered can optionally be Type 2 devices for applications up to a performance level “d” (equivalent



**Fig. 2** Safety Control GmbH – a company that has been part of the Schmersal Group since 2008 – is a young and innovative team that has been specialising in the development, production and sale of optoelectronic protective devices since 1994. The product range comprises all kinds of commercially available devices to safeguard danger zones on machinery, access protection at danger zones and protection of areas. In addition customers are given comprehensive advice (starting from the design phase of a danger zone analysis through to implementation of the most efficient solution).

### Blanking

In blanking mode, objects located permanently in the protective field of the light curtain are blanked out. In the case of fixed blanking the objects remain at a fixed spot in the light curtain. If the objects move within the area of the protective field from time to time, this is referred to as floating blanking.

### EDM (External Device Monitoring)

Term from EN 61 496-3: a means by which the electro-sensitive protective equipment (ESPE) monitors the status of control elements arranged outside the ESPE (monitoring function of downstream devices).

### Muting

In muting mode, the protective function of the ESPE is temporary and automatically suspended. This function is used wherever material is delivered to or transported from a danger area via a transport system. The safeguarding function is achieved using 2 or 4 muting sensors which can distinguish between people and objects. The muting condition is (optionally) displayed using a muting signal lamp.

### Cyclic operation

In the case of cyclic operation, there is manual intervention in danger zones in the mechanical work cycle. Protective measures here must achieve a high safety level in monitoring the protective device and in signal processing. If these conditions have been satisfied the start command can be given in this operating mode to return the guard correctly to the protective position.

### Restart inhibit

A device preventing the automatic restart of the machine, when the protection field is interrupted during a dangerous machine cycle or when the operating mode of the machine is set or changed.

**Fig. 2** Operating modes of AOPDs (examples)

to  $\leq$  SIL 2) or Type 4 devices for applications up to a performance level “e” (equivalent to  $\leq$  SIL 3). In addition to safety light grids and safety light curtains with protection field resolutions, widths and heights to satisfy all usual commercial tasks, the new product range also contains a number of special features that will be introduced below by way of example.

### Applications of AOPDs at freezing temperatures

Applications of this nature represent a particular challenge for all devices, and therefore also for safety light grids and safety light curtains. Due to the changing temperatures around freezing, humidity condenses regularly to condensation which can temporarily freeze or ice over, for example during the day/night cycle.

Diffusion or capillary action, additionally promoted by the mechanical stress resulting from temporary freezing, play their part in devices whose protection class only features standard measures even if the criterion for water leak tightness is also satisfied for more heavy duty

requirements. To put it plainly, moisture can permeate seals to get inside devices. In the case of optoelectronic protective devices, this fault means short circuiting or other device malfunctions for example.

While the phenomenon of condensation formation is also present in other alternating climates



**Fig. 3** SLC 425 (connection for muting sensors)

where condensate is present, these are different because they lack the problem of freezing temperatures. Almost all machines in or bordering outdoor areas such as wood processing or construction machines, agricultural machinery as well as vehicle-mounted mechanical structures etc. are affected by such problems caused by climatic conditions.

In order to exclude risks of this kind, the AOPD range from Safety Control GmbH has specific versions available that are equipped with special “breathable” membranes. Pressure equalisation prevents moisture being able to permeate the devices. The protection class of the devices, even if they are little affected by the special problems discussed here, corresponds to IP 69K (see loc. cit.).

In other words the fault potentials that could arise when deploying around the freezing point do not affect correct availability of these safety light grids and safety light curtains (ranges SLC/SLG 220 and 420). This avoids the machinery stopping, or more probably the bridging of manipulated protective devices, combined with a hazardous state for the operating staff on the one hand and with considerable liability risks for the responsible operator on the other.

One could argue that formation of condensation might also affect the availability of device optics and as such is only a partial solution whose effect is too limited. It is true that this objection cannot be completely dismissed in extreme cases, however it comes down ultimately and decisively to the power reserves of the devices. Therefore (where the mounting distances between the transmitter and receiver have been adapted) the optoelectronic protective devices from Safety Control would be able to withstand a reduction of up to half the radiation intensity.

The temperature range in which the safety light grids and safety light curtains referred to can be deployed is from  $-10 \dots +55 \text{ }^\circ\text{C}$  as standard. Special low temperature versions are also available on request.

#### **Safety light grids and safety light curtains with protection class IP 69K**

The series of AOPDs with protection class IP 69K represents a further feature of the Safety Control range.

IP 69K means that the devices, which are mounted on a turntable moving at a speed of 5 revolutions per minute, are exposed to extremely critical water jets which must not lead to any detrimental effects. The test conditions here simulate high pressure cleaners as used in the food processing industry and other similar industries. During testing, each specimen is sprayed with water every 30 seconds at angles of  $0^\circ$ ,  $30^\circ$ ,  $60^\circ$  and  $90^\circ$ . The stream comes from a fan nozzle at a distance of between 100 and 150 mm, and the water jet has a temperature of  $80 \text{ }^\circ\text{C} (\pm 5^\circ)$ , a flow rate of 14 to 16 l/min and pressure of 8 to 10 kPa. While the conditions may appear to be extreme, they are oriented to those witnessed in industry in such applications.

If one disregards other hygiene considerations in highly critical applications for one moment (refer to the next paragraph in this respect), the suitability of the devices when exposed to a high pressure cleaner – expressed in the protection class IP 69K – is an important prerequisite for applications in the food and beverages industry, as well as in pharmaceuticals, cleanroom technology, petrochemicals, waste treatment, recycling reusable materials etc. It is also very common to work with high pressure cleaners in these industries.

#### **IP 69K + hygiene-compliant versions**

Depending on the criticality of the material or feedstock to be processed and of the installation site of the devices, compliance with protection class IP 69K does not automatically equate, however, to all requirements relating to hygiene-compliant design having been satisfied, and in particular those which apply to manufacturing and processing machines used in the food and feedstuff industries.

There are further aspects to be considered in accordance with EN 1672-2 [4]; examples, which do not claim to be complete, include moulding and assembly with respect to cleaning ability, avoiding gaps where deposits of bacteria colonies or similar could form, and last, but not least, the material stability. While protective devices, and therefore also safety light grids and safety light barriers, are only deployed in immediate food areas in the rarest of cases, the risk of cross-contamination must nevertheless be taken into consideration also where installation is outside these “high risk zones”.





**Fig. 4** SLC 420, Schutzart IP 69K

This issue is especially critical in the case of manufacturing and processing raw products such as raw meat, fish and poultry and for eggs, milk etc.

Consideration is also given to increased hygiene suitability in the new range by additionally covering the versions with protection class IP 69K (range SLC/SLG 220 and 420) with a transparent protective membrane suitable for use in food-stuffs; this guarantees easy cleaning and avoids any impediments to hygiene caused by corners or edges.

#### **AOPD special modes**

Naturally the new range also includes safety light grids and safety light curtains that are able to realise muting, blanking and cyclic operation.

A feature of muting operation is that the protection field can be divided up, i.e. part of the protection field reacts to muting or to the muting sensors while another part, for example above or below a taught area, does not. This function enhances protection against manipulation, and

makes it harder or impossible to ride on pallets etc.

#### **Summary**

This section has presented a selection of features from the Schmersal Group's new AOPD range. We would be happy to test the potential for realising specific design features and product properties that go beyond those in the normal standard. Please contact us in this respect.

#### **Safety control systems, safety bus systems etc.**

The objective

- on the one hand of saving and simplifying wiring;
- of replacing hardwired programming and being able to reproduce logic or even change it simply;
- on the other hand of being able to control machinery more efficiently in terms of safety-related logic nesting depth;
- and, last but not least, of reducing downtimes through more user-friendly and informative visualisation and diagnostics functions

means that systems such as these are similarly part of the state of the art today when it comes to more complex tasks.

For example, products offered on the market include mini safety controllers which, depending on application, can replace 5 to 10 traditional safety relay modules, compact safety controllers for a medium number of I/O functions and safety PLCs which, depending on the configuration level, can serve hundreds of I/O functions, something that can frequently involve working on a mix of safety-related and operational tasks. Depending on design and manufacturer, all equipment can either be parameterised or is freely programmable. Added to this there is often the option of decentralised request in the field via safety-related bus systems.

With PROTECT-SELECT (or the PROTECT-SELECT WL with a safe radio connection), the Schmersal Group offers users a range that has similar performance to a safety mini controller but which is as easy to use as a safety relay module.

Examples of programmable controllers in the Schmersal range (from "small" and "medium" through to "large") are the safety controllers in



**Fig. 5** With the newly developed PROTECT-SELECT range, the Schmersal Group presents a compact safety controller that can be configured without knowledge of programming and without manufacturer-specific parameterisation.

the ESALAN and PROTECT series. However the safety bus system AS-i Safety at Work will be examined more closely at this point; several contributions to this area can be found in the Schmersal range which arguably represents the broadest and deepest range of such products on the market.

The reason why special emphasis is given to AS-i Safety at Work is because, as a system specifically designed for the lowest level, it avoids the “field bus” dispute (*which is the right one?*) by being compatible with all leading factory automation systems on the market, whether these are PROFIBUS/PROFINET, DEVICENET or CC LINK. The special suitability of AS-i Safety at Work arises simply from the fact that safety-related signals are generally simple digital functionalities that do not need the overheads asso-



**Fig. 6** Examples of components for the safety bus system AS-Interface Safety at Work

ciated with more complex systems. AS-i Safety at Work is now an international market leader in the lowest field bus level area.

### Simple, safe and well tried and tested

AS-Interface Safety at Work (SaW) is the first safety bus system based on the open standard of AS-International. Safety components such as EMERGENCY STOP, safety switches, guard locking or safety light curtains are simply interconnected via the AS interface cable. Only a safety monitor is required to evaluate the safety signals.

### AS-Interface standard in accordance with EN 50295

The AS-Interface network remains unchanged, also when the AS-Interface SaW has been integrated. The familiar components consisting of the standard AS-Interface master, the mains adapter and the AS-Interface 2-wire cable can still be used. These form the basis for integrating the transmission of safety-relevant data. It is therefore very easy to retrofit an existing system with AS-i SaW safety components.

### The safety core

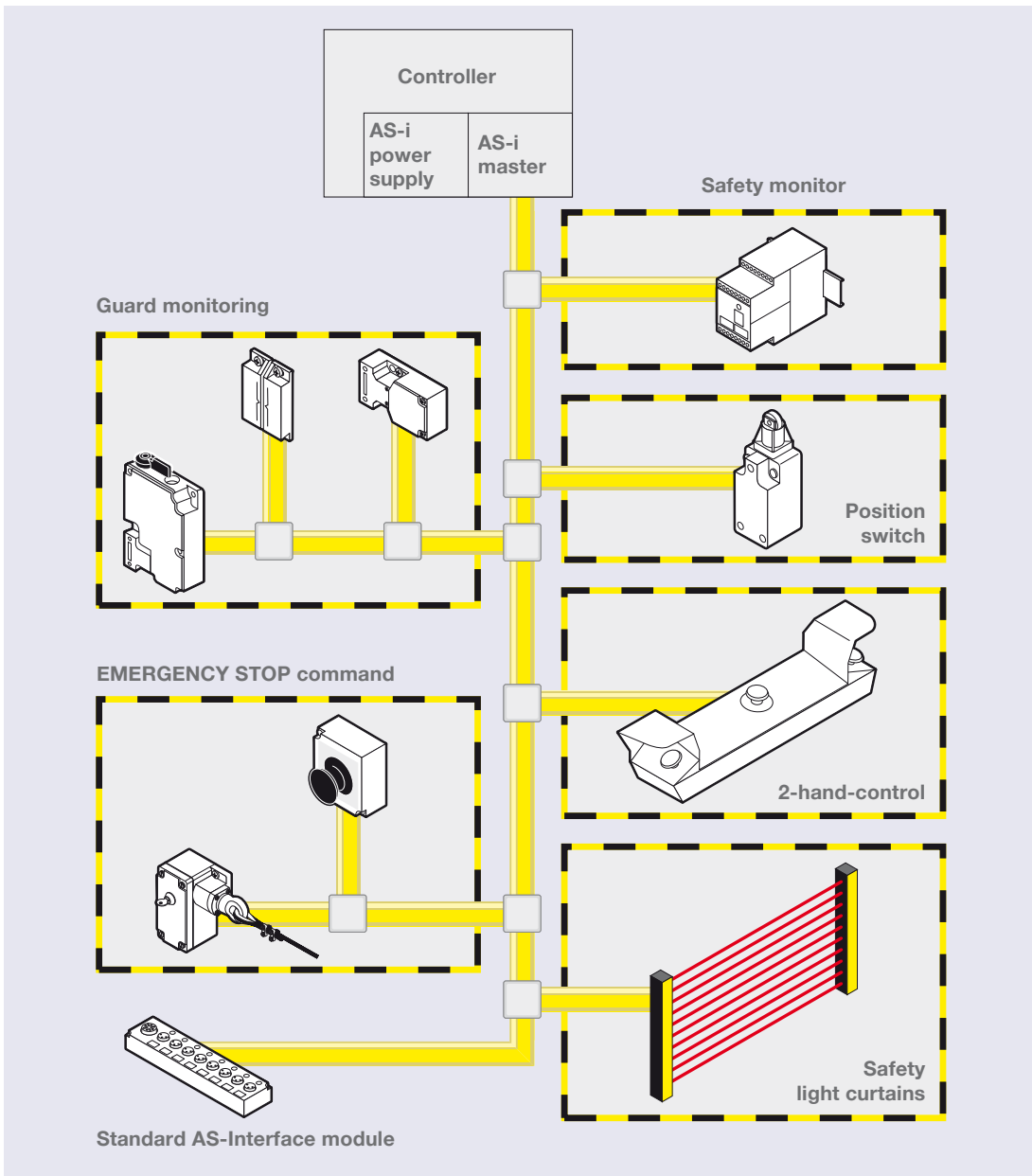
The safety monitor monitors the information on all safety components transmitted via the AS-Interface network and switches the system to a safe state if a safety circuit is activated or in the event of a fault in one of the safety components. In order to do this it is equipped with one or two redundant enabling circuits for applications up to performance level “e” in accordance with EN ISO 13849-1. The configuration of the individual safety functions takes place using drag & drop software. The configuration is finally transferred to the safety monitor and protected by password.

### Safe transmission mechanism

The transmission mechanism for safety relevant applications is based on the unchanged AS-Interface standard protocol. A defined telegram is sent with each master call through interaction between the safety monitor and safety components. The monitor analyses this information and opens the enabling paths if there is deviation from target values. The maximum response time for a safe shutdown is 40 ms.

### Cost reduction with AS-Interface Safety at Work

Who doesn’t need to reduce costs and work expenditure? During installation, commissioning



**Fig. 7** AS-i Safety at Work system design (example)

or later in the event of servicing, AS-Interface SaW supports the user with integrated system diagnosis. This provides the user with detailed information about the cause and location of a fault and enables rapid exchange of the safety components in the event of a defect, thereby minimising downtimes.

*Greater flexibility with AS-Interface Safety at Work*  
With its diverse range of safety components, Schmersal offers the greatest degree of flexibility when realising individual safety solutions.

A comprehensive set of safety components is available for the user to choose from in line with the application. Because AS-Interface SaW is an open system, the user is also able to incorporate safety components and control devices from other specialist suppliers.

*Fast installation and commissioning*

No further settings are required on the safety components, elaborate wiring between the safety components and switch cabinet is reduced and assembly times are shorter. Even the power

supply for the safe sensor technology is provided using AS-Interface 2-wire cable.

*AS-Interface SaW system features*

- Up to 31 safety and standard slaves on one AS-Interface-System
- No safety PLC necessary
- Group formation of safe signals and distribution across several safety monitors
- Safety enabling circuits are shut down after max. 40 ms
- Integration of the safety signals in the system diagnostics
- Safety integrity:
  - ≤ PL “e”/category 4 in acc. with EN ISO 13849-1

- ≤ SIL 3 in acc. with IEC 61508
- TÜV-certified

**Other control-related developments**

While the control of I/O functions was at the fore in the above information, two further trends can be observed for the application of programmable electronic technology with safety function.

The first is the incorporation of movement and speed signals in safety-related control systems (see Fig. 8 for functions), and the second is the substitution of wiring by wireless systems.

A corresponding solution is also offered in the Schmersal range in the form of the PDMS (Pro-

Additional safety-related functions of electrical power drive systems			
Abbreviation	English designation	German designation	Function
STO	Safe Torque OFF	Sicher abgeschaltetes Moment	Motor receives no power to generate a rotating movement; stop category 0 in accordance with DIN EN 60204-1.
SS1	Safe Stop 1	Sicherer Stopp 1	Motor is delayed: monitoring of brake ramp and STO after shutdown or STO after expiry of a delay period; stop category 1 in accordance with DIN EN 60204-1.
SS2	Safe Stop 2	Sicherer Stopp 2	Motor is delayed: monitoring of brake ramp and SOS after shutdown or SOS after expiry of a delay period; stop category 2 in accordance DIN EN 60204-1.
SOS	Safe Operating Stop	Sicherer Betriebshalt	Motor is stationary and resists external forces.
SLA	Safely-Limited Acceleration	Sicher begrenzte Beschleunigung	This prevents an acceleration being exceeded.
SLS	Safely-Limited Speed	Sicher begrenzte Geschwindigkeit	This prevents a speed limit being exceeded.
SLT	Safely-Limited Torque	Sicher begrenztes Moment	This prevents a torque/force limit being exceeded.
SLP	Safely-Limited Position	Sicher begrenzte Position	This prevents a position limit being exceeded.
SLI	Safely-Limited Increment	Sicher begrenztes Schrittmaß	The motor is moved at a specific pace and then stops.
SDI	Safe Direction	Sichere Bewegungsrichtung	This prevents movement of the motor in an unintended direction.
SMT	Safe Motor Temperature	Sichere Motortemperatur	This prevents the motor temperature limit being exceeded.
SBC	Safe Brake Control	Sichere Bremsen-ansteuerung	Safe control of an external brake.

**Fig. 8** Additional safety-related functions of electrical power drive systems (continued overleaf)

Additional safety-related functions of electrical power drive systems (continued)			
Abbreviation	Designation	Abbreviation	Function
SCA	Safe Cam	Sicherer Nocken	A safe output signal is generated while the position of the motor is in a specified area.
SSM	Safe Speed Monitor	Sichere Geschwindigkeitsüberwachung	A safe output signal is generated while the motor speed is below a specified level.
SAR	Safe Acceleration Range	Sicherer Beschleunigungsbereich	The acceleration of the motor is kept within specified limits.

**Fig. 8** Additional safety-related functions of electrical power drive systems (continued)

tect Drive Monitoring System) (as shown in Figure 9); this is especially suitable for retrofit automation. By contrast, for typical OEM use reference is made to the products supplied by drive manufacturers which, not least prompted by the EN IEC 61 800- 5-2 standard [4], now offer almost all solutions in this area.

However, standard solutions are not suitable everywhere, and also not for robotics for example. With the ESALAN SafetyController (as shown in Figure 10), several robots have a standard of safety that is unique in the world and have therefore set new safety benchmarks in the robotics area.

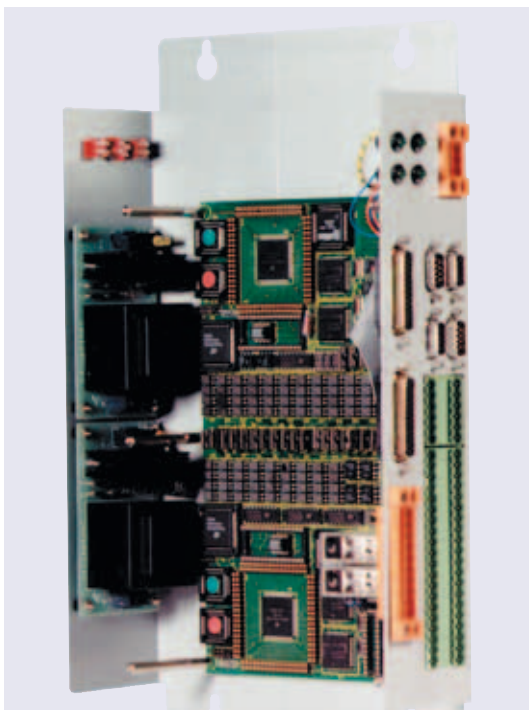


**Fig. 9** The “Protect Drive Monitoring System” PDMS, a solution with modular structure for safe shut-down and speed monitoring, e.g. of spindle or final drives up to PL “e”, serves as an extension to the universally applicable PROTECT PSC safety controller.

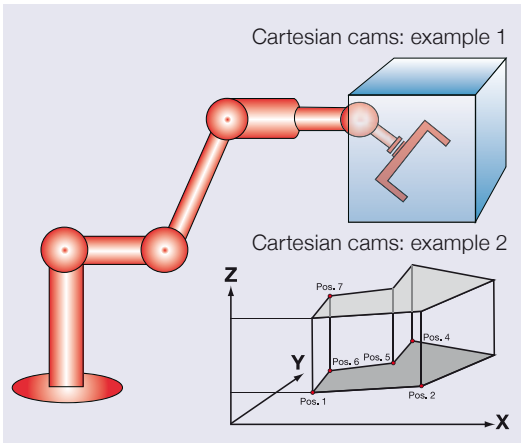
**The ESALAN SafetyController**

The ESALAN SafetyController is basically integrated in the structure of a robot control system at a higher-ranking level by the individual manufacturer and mainly performs merely monitoring functions. An internal control command is only generated in the event of a fault, i.e. only then is the main contactor of the system switched off safely.

The operational part of the machine controller usually works autonomously, with all control functions (torque, speed, position etc.) between the controller and drive motor being maintained, also if a guard door has been opened, for example.



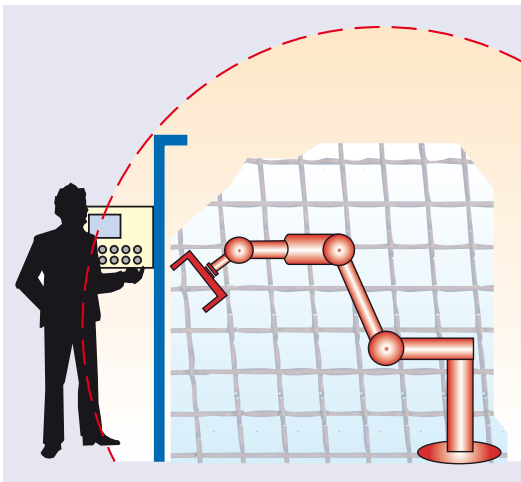
**Fig. 10** ESALAN SafetyController



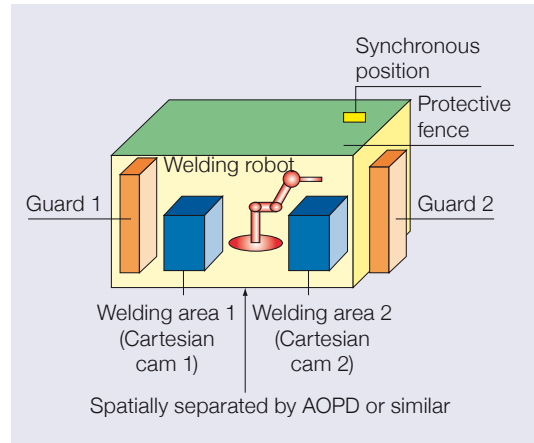
**Fig. 11** Cartesian cams

In addition to safety-related digital functions as also realised in safety control systems, the ESALAN SafetyController also monitors the speed of each individual machine or peripheral axis, typically according to the operating mode, for example the “safely reduced speed” mode.

The exceeding of a safe speed, the crossing of a position limit or leaving a safe position are detected and lead to immediate safe shutdown of the machine. The limits, which are activated subsequently using safe inputs in line with the respective operating mode, are preset by the factory and when commissioning the system.



**Fig. 12** The ESALAN SafetyController uses safe technology to monitor both specific axes and cartesian speed limits, thereby enabling new machine functions in robotics and in other multi-axis machinery, for example adjusting virtual protective fences.



**Fig. 13** In this example of a standard welding cell, the movements of the robot in welding areas 1 and 2 are monitored by the cartesian cams 1 and 2. The guard contacts are connected to the Cartesian cams of the robot. If the robot leaves the cam area, a shutdown is executed. For example guard 2 can be opened for reloading welding area 2 while the robot can continue to work in welding area 1 (and vice versa).

### Cartesian cams

In addition to specific axis monitoring, the ESALAN SafetyController also monitors the cartesian speed of robot axes and of the robotic tools, i.e. the movement in the space.

It is also possible to form so-called cartesian cams with safety function, i.e. virtual work areas within which the robot or robotic tool may or may not move depending on definition.

The speed is simultaneously monitored in the direction of the restriction at all times, i.e. the speed may only be as great as that which permits braking without leaving the permitted area of movement. For this, the specific axis values in the ESALAN SafetyController are subjected to a forwards transformation in order to determine the position of individual points in the movement sequence of the robot in the global coordinate system. Since the Cartesian cams are also defined in the global coordinate system of the robot, it is possible with the help of a special algorithm to establish whether the cam has been damaged.

### Virtual protective fences

The functions of the Cartesian cams furthermore make it possible to build protective fences that



are smaller and lighter and to make better use of them because the cams inside the work area form a kind of upstream virtual protective fence. The ESALAN SafetyController monitors movements and switches the machine to a safe state when there is infringement of the virtual working space due to a fault in the operational robot control system or due to another cause. As such the only purpose of the actual protective fence is to prevent people penetrating the working area of the robot (but not vice versa).

**Keyword: wireless**

Wiring, whether this is traditional or series wiring, is not ideal for all applications. Sometimes there is a call for wireless solutions, especially in ramified machinery systems and in particular for special operating modes with mobile control devices, e.g. for process observation or troubleshooting, or during retrofit automation. In such cases it is worth considering deploying the ESALAN Wireless System.

This technological standard achieves the greatest transmission reliability through a combination of different design and HF-related properties and features even where there are unfavourable industrial conditions with numerous emissions, HF

sources and several other wireless devices, as is frequently the case. With this system it is possible to achieve solutions up to Control Category 4 in accordance with EN 954-1 or SIL Level 3 in accordance with EN ISO 61508 and performance level “e” in accordance with EN ISO 13849-1.

The MHHW test centre in BG-Prüfzert (the test and certification bodies of the German employer’s liability insurance association) tested the system concept early on during the development process and granted concept approval. The BG type test was successfully completed in June 2006. The wireless system itself satisfies the requirements of the competent EU European regulatory authorities and may be placed on the market without licence and registration in all EU Member States. Current further development on the basis of the 2.4 GHz band even permits global licence-free use.

This means there are no restrictions at all for mechanical engineers, also where the greatest requirements exist with respect to the safety level. Practical trials of ESALAN Wireless have shown that the system really does guarantee reliable signal transmission even under very unfavourable conditions.



**Fig. 14** With the addition of a “wireless module”, the compact safety controller PROTECT-SELECT in the PROTECT-SELECT WL version allows the user to integrate a mobile handheld control device wirelessly into the safety concept of the control system.



### Electronic safety sensors and guard locking

These devices serve as interlocks within the meaning of EN 1088:1996 (in future EN ISO 14119) for position monitoring and possibly guard locking of movable guards.

Compared to traditional safety switches with and without guard locking, electronic safety sensors and guard locking have fundamental advantages due to their non-contact method of operation and, thanks to the use of programmable electronics (PES), advantages due to substantially greater safety-related and functional “intelligence”. The main advantage of this method of operation is the determination of the guard position without contact. Using this, the devices operate without any wear and tear and are comparatively resistant with respect to a misalignment of sensor and actuator.

As an alternative to the RFID-based device developments that are now frequently available on the market, the Schmersal Group has supported use of a special technology for electronic interlocking devices in addition to the RFID series. This is the so-called pulse-echo method.

With this method the sensor transmits electromagnetic impulses. When the actuator approaches the sensor, the actuator oscillates at a predefined resonance frequency due to the induced energy. In turn these oscillations are read in by the sensor. The sensor then evaluates both its distance to the actuator and the actuator code. The actuator identified by the sensor is interpreted as closed guard and the safety outputs are activated.

The electronic monitoring of moving guards, which includes actuation in non-contact safety

interlocks, makes it possible for the respective actuator to be detected without contact and free of wear. The patented pulse-echo method deployed for this permits large tolerances both in the switching distance and in the lateral offset when approaching the coded actuator. Despite this, the switching points and hysteresis are repeatable and constant. The performance of the safety sensors and interlocks is confirmed by application of the following test standards:

- Defined behaviour in the event of a fault in accordance with EN 60947-5-3, classification of self-monitoring PDF-M
- Requirements placed on safety-related parts up to PL “e” / Cat. 4 in acc. with EN ISO 13849-1
- Requirements of IEC 61508 / use up to SIL 3 applications.

The requirements of IEC 61508 moreover are a guarantee of high interference immunity for the user. The standard additionally permits a signal to be emitted for certain faults before the system is shut down. This enables the system to first be moved to its basic position in a fault-tolerant manner before a shutdown.

The microprocessor technology used facilitates intelligent diagnosis and simple and rapid fault identification, e.g. in the case of a cross-short or wiring fault. The safety channels of the electronic sensors and electronic interlocks can be switched to a chain of up to 31 devices in series one behind the other, depending on the types of device used. An internal function test ensures there is no loss of PL “e”/Cat. 4 in accordance with EN ISO 13849-1 for this series wired chain. Similarly, sub-SIL 3 or Sub-PL “e” in accordance with IEC 61508 (EN IEC 62061) or EN ISO 13849-1 are regularly attained here due to the self-monitoring switching technology and resultant favourable PFH<sub>d</sub> values. The chains can also have a structure containing a mix of the safety sensors and interlocks described here.

### NEW: Electromagnetically operated guard locking

Electromagnetically operated guard locking represent a new generation of interlocks where the actuator is simultaneously the anchor for the magnet which is attracted at a monitored force. They are used to monitor guards or covers.

The product is characterised by the fact that

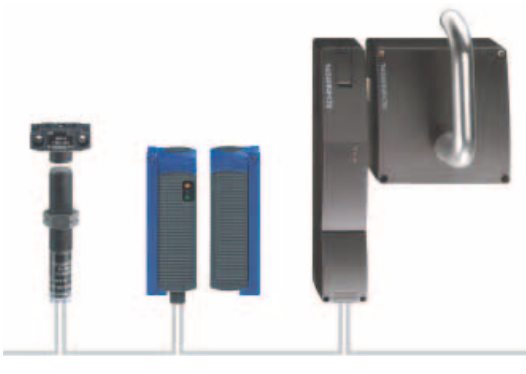
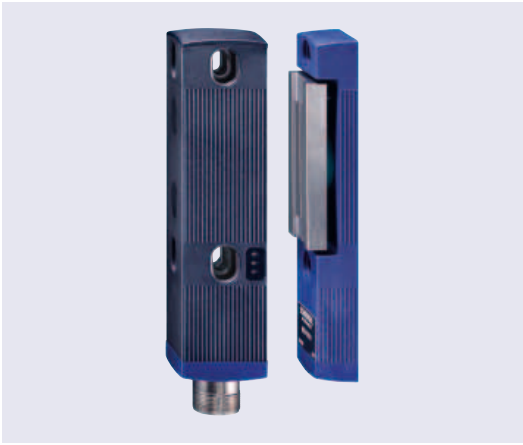


Fig. 15 Safety sensors and guard locking



**Fig. 16** MZM 100 Electromagnetically operated guard locking

potential holding force between the anchor and cross-head is monitored by measuring magnetic parameters and that the anchor is detected using the CSS principle. This effect of this non-contact principle is that both units can be generously adjusted to each other. The actuator unit (anchor) and the interlock unit (magnet) together form a closed system.

#### **Interlock unit**

The interlock unit is attached to the guard, while the actuator unit is directly attached to the moving part of the door. The anchor plate must rest on the pole shoes of the electrically charged magnets to block the actuator unit.

Continuous monitoring of the magnetic parameters guarantees a safe holding force. Unlocking is achieved by switching the magnetic power off. The interlock unit contains a redundantly constructed two-channel processor system that similarly monitors the two enabling paths to measure the holding force and record the actuator in the actuator unit.

These outputs are suitable for controlling two contactors or a relay safety combination, or to be evaluated by a safety controller.

The use of the pulse-echo method precludes circumvention of defeating the interlocking devices.

This then has provided an overview of the innovative contributions to PES in the Schmersal range.

Please see page 177 if you are interested in the excursus on the history of safety at work in Germany alluded to at the beginning of this chapter.

#### **Footnotes:**

- [1] The term “safety components” is used here in a comprehensive sense as referred to in the MD (as a generic term for all kinds of safety switches and sensors, guards, safety relay modules and safety-related control systems as well as control devices with personal protective function).
- [2] **IEC 61508:**  
Functional safety of electrical/electronic/programmable electronic safety-related systems.
- [3] **AOPD:**  
**Active Optoelectronic Protective Device** (formerly ESPE → **Electro-Sensitive Protective Equipment**)
- [4] **EN 1672-2:2009:**  
Food processing machinery – basic concepts – Part 2: hygiene requirements



## Excursus into the history of safety at work in Germany

Bismarck's social legislation is an important milestone here.

The regulation of the area of "safety at work" within the framework of a fundamental reform law was instigated in 1884 by the then Reich Chancellor Otto von Bismarck (1815–1895) under the reign of Kaiser Wilhelm I (1797–1888). This took place with the enactment of the first law on accident insurance in the world, one of three laws that later were to become known as Bismarck's social legislation [1].



**Fig. 17** Reich Chancellor Otto von Bismarck at the proclamation of King Wilhelm I of Prussia to German Kaiser in Versailles

The subject of "safety at work" was not completely unknown before this time, neither is it the case that legislative implementation of the subject was "discovered" in the German Reich at the time of Bismarck.

What one can say is that Germany, a latecomer to the modernisation process that had been on-

[1] To be precise, the Accident Insurance Act was passed by the Reichstag on 27 June 1884 and came into force as a Reich law on 6 July 1884. With a lead time of over a year, it became effective on 1 October 1885.

going since the start of the 19th Century, was the first state to develop a wide-ranging social security system organised under public law, whereas other states such as England, the pioneer of industrialisation, only followed this development with comparable measures at a later date, partially prompted by the German example.

Until that time social policy not only in Germany left responsibility for safety at work, which was in any case only fragmented, partially to commercial and partially to civil law.

This, for example, is the statement in the German Industrial Code of 1869:

*Every commercial entrepreneur is obliged at his own cost to provide and maintain all devices necessary considering the special nature of the business and business premises to best safeguard workers against risks to their life and health.*

However when something "happened", the principle applied was fault-based liability where the injured worker had to prove negligence on the part of the entrepreneur or his authorised representative in order to obtain damage compensation by means of legal action. For practical reasons this route was usually not feasible and also financially difficult.

### Historical development of safety at work

As discussed above, however, the inclusion of safety at work as an area of social policy was in no way a realisation made in the 1870s or 1880s or even a realisation made by Bismarck.

Hippocrates probably addressed the possible negative consequences of work for the first time in the period before Christ. He pointed out damage to posture in tailors, lead and mercury poisoning in miners and inflammation of the eyes in blacksmiths.

In Roman times too in the era after Christ, air pollution was forbidden. A further major change took place in the 14th Century.

Until that time the journeyman assisted the mas-

ter with his work; he was fed, the work was bearable and the pay was not bad. The number of journeymen and withdrawal of the master from actual craft activities produced a more top down system that pays piece rate wages and had poorer working conditions.

In 1303 the “Bremer Recht” law obliges the master to keep and care for journeymen in sickness and in health, and in 1329 the girdle makers (brass locksmiths) from Breslau strike for better working conditions in the first known strike in Germany.

In 1430 the linen weaver ordinance limits working time and bans night work. In 1469 miners strike for more pay and shorter working hours in Altenberg in the Erzgebirge and in Basel in 1471 printer labourers do the same due to bad working conditions. A decision is taken by the Strasbourg carpenters’ guild in 1478 that the master must nurse journeymen who have had an accident at work back to health and must continue to employ them. In 1496 Henry VII limits working hours to 12 hours in the summer. It is only permitted to work from 5 am to nightfall in the winter.

In 1554 the working conditions and self-help measures of miners among other things are regulated by the new mining ordinance in Electoral Saxony. In 1567, in addition to his famous paper on poisons and their general definition, Theophrastus von Hohenheim, also known as Para-

celsus, describes the occupational diseases of metal workers, goldsmiths and others.

The precursors of trades unions are created in the form of education societies in 1833, and working conditions and protective measures are numbered among the subjects they deal with.

The Prussian Industrial Code is introduced in 1845, is subsequently amended several times and adapted to the respective political situation. Despite work safety regulations for children, which arose not least as a result of pressure from the military who were worried about the health of their recruits, children still represent almost 40 % of the total workforce in 1850.

However without adequate checks, the 1853 and 1855 Prussian factory laws aimed at child protection also remained relatively ineffective for example, even if they prescribed the first factory inspectors.

Since state supervision also had trouble keeping up with technical development in other respects, very soon after the constitution of the VDI in 1856 free inspectors for regular monitoring of plant were proposed and approved, not only because of the serious danger to the public, but also because the financial losses due to technical disruptions were no longer acceptable to the entrepreneur from a business point of view. The Prussian general mining law, which also contains safety at work regulations, is enacted in 1865.

The aforementioned Industrial Code of the Reich containing comprehensive obligations for employers to protect the life and health of employed workers then comes into effect in 1869.

The factory inspection (occupational safety and health inspectorate) that has existed since 1853 only becomes obligatory in 1878 (i.e. 25 years late). Its most important task is also to monitor compliance with safety at work law, including the bans or limits on employing children, young people, women and women who have recently given birth.

#### **Employer’s liability insurance associations since 1885**

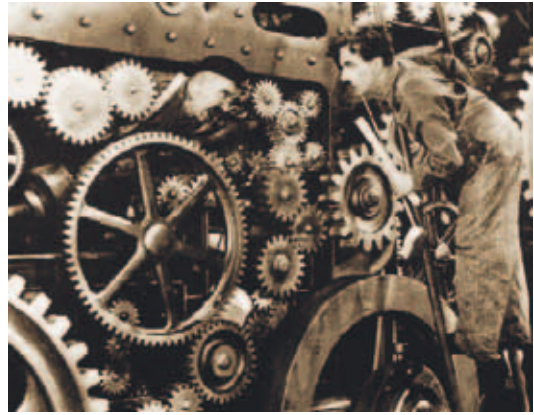
Bismarck’s accident insurance in 1884 led to the replacement of earlier safety at work regulations and in particular the fault-based liability which



**Fig. 18** Shoemaker in the Middle Ages



ultimately resulted from the Reich liability law of 1871 and which was generally felt to be unsatisfactory. This was not least because the risk of accidents had increased greatly due to the growth in industrial work and the escalating deployment of machinery. In place of previous regulations was a self-organised and decentralised insurance [2] called a “Berufsgenossenschaft” (plural: Berufsgenossenschaften) or employer’s liability insurance association based on compulsory company membership; this assumed joint liability in the case of accidents.



In addition to the obligation of the employer to pay a contribution of 2 to 3% of the gross wages into the insurance for damage payments, the law also gave the Berufsgenossenschaft the power to make accident prevention regulations that they were allowed to monitor themselves using technical supervisors.

The so-called combining of these tasks (damage compensation + accident prevention + supervision) created the basis for professional occupational health and safety.

#### **Market for technical safety at work**

A market was opened up by the second and third combined task elements in this accident insurance. Therefore in addition to the Berufsgenossenschaft assuming the task of damage compensation (the 1st element), the task of accident prevention was also transferred to them along with the authorisation to pass accident prevention regulations (the 2nd element) and to monitor company compliance with these themselves (the 3rd element). The creation of this market was demand led, subsequently followed on the supply side with corresponding ranges of protective equipment and protective devices etc. (very similar to the push triggered by the EC Machinery Directive when it came into force in 1993, for example).

To this extent one can rightly say that the nucleus of Germany’s position in the area of industrial

[2] Based on the legal form of a co-operative, a society without closed membership numbers whose purpose is to promote purchasing or the economy by means of a common business. Today insurance companies are no longer permitted to use the legal form of a co-operative.

health and safety today lies in the Accident Insurance Act.

#### **First accident prevention regulations and technical supervisory service**

Authorising Berufsgenossenschaften to pass accident prevention regulations had special significance simply by virtue of the fact that passing them meant that, within the framework of the Accident Insurance Act, binding law had been transferred from the state legislature to the Berufsgenossenschaften. Despite this (or for that very reason) when accident insurance began, accident prevention regulations still had to be approved by the Reich Insurance Office before they could come into effect.

Added to this, as the other side of the “accident prevention” coin so to speak, it was the case from the beginning with respect to the activities of Berufsgenossenschaften that their “authorised agents” (of whom there were already 93 in 1889, whereby some worked for more than one Berufsgenossenschaft at the same time) really did check that the accident prevention regulations passed were correctly complied with.

While they had been given a legal mandate to oversee the enacted accident prevention provisions themselves, one might have expected their handling to be “generous” if there had been any general, extensive justification in the criticism about company-oriented partiality in the Berufsgenossenschaften. However it would appear that this was not the case.

#### **Advances in technical safety at work**

At any rate, technical safety at work must have made great progress in the years following the enactment of the Accident Insurance Act.

Das Reichs-Versicherungsamt hat in seiner Plenarsitzung vom 25. September 1886 den nachstehenden, in der Genossenschaftsversammlung vom 23. Juni 1886 beschlossenen Unfallverhütungsvorschriften der Berufsgenossenschaft der Feinmechanik die Genehmigung erteilt.  
Berlin, den 25. September 1886.

Das Reichs-Versicherungsamt.  
Höbiker.

### Unfallverhütungsvorschriften der Berufsgenossenschaft der Feinmechanik.

#### 1. Allgemeine Einrichtung der Betriebe.

##### Baulichkeiten und innere Einrichtungen.

1. Alle Fabrik- und Arbeitsräume sollen möglichst hell, geräumig und gut gereinigt sein.
2. Alle Treppen in Fabrikgebäuden oder auf Arbeitsplätzen müssen stets in gutem Zustande erhalten werden und sind, soweit sie nicht von beiden Seiten von festen Wänden eingeschlossen sind, mindestens an einer Seite mit festem Geländer zu versehen.

The first “General Accident Prevention Exhibition” took place in Berlin in 1889; it came about through an initiative by a few brewery owners started in the summer of 1887, and was initially planned only as a trade exhibition for this particular accident-prone industry. However the organisers were able to gain the support of the Berufsgenossenschaften for a wide-ranging exhibition.

Kaiser Wilhelm II who had been on the throne since June 1888 was enthusiastic about the exhibition. In September 1888 he assumed the protectorate for it (one would say “patronage” today) and finally opened it at the end of April 1889. He then visited the exhibition himself several times.



1 million people visited the exhibition in five and a half months, 300,000 of whom were workers. By this time at the latest, safety at work had become a subject for public debate, and accident prevention no longer appeared to be an act imposed by the authorities but rather a charitable initiative on the part of entrepreneurs.

There was also international propaganda about accident insurance. For example an exhibition was set up on “industrial insurance in the German Reich” as part of the 1904 world exposition in St. Louis that was later loaned to Harvard University as a permanent exhibition; among other

things, it contained almost 1,000 photographs illustrating the latest accident prevention equipment in Germany.

#### The early Berufsgenossenschaften: an employer organisation

Delegates for insured persons in the executive boards of local, company (factory) and guild health insurance funds as well as in the miners’ health insurance scheme elected a workers’ representative for the Berufsgenossenschaften. However these did not participate in the self-management of the Berufsgenossenschaft or in damage compensation issues in the first instance.

They just elected two committee members to the arbitration tribunals who, together with the employer representatives who had likewise been elected, made decisions under the chairmanship of a public functionary on objections to pension awards by injured parties; they also had to be consulted for the appraisal of accident prevention regulations.

Moreover insured persons were involved in the examination of accidents via an authorised representative and, like entrepreneurs, made up two non-permanent members of the Reich Insurance Office which, among other things, supervised the Berufsgenossenschaften and took decisions in the last instance when there were appeals against the legal decisions of the arbitration tribunals.

It was only with the law on self-management in social security dated 22 February 1951 following the establishment of the Federal Republic of Germany that a change was seen towards “equal-



ity” in the self-management of Berufsgenossenschaften that we know today. Prior to this, in the course of the Basic Law (Grundgesetz) coming into effect in 1949, they had already been given the status of a public corporation.

In the abovementioned law on the self-management of social security, the guiding principle with respect to the Berufsgenossenschaften that had prevailed since 1934 under the Third Reich was abolished again in favour of a decision to reintroduce self-management. However from now on (and by contrast with the Accident Insurance Act of 1884) the self-management bodies have equal representation.



The Berufsgenossenschaft landscape is currently undergoing a period of change again. The background to this is the law modernising the statutory accident insurance UVMB. The objective of the reform is to adapt organisation of accident insurance to the changed conditions in industry, to better distribute the common management of contaminated sites and to modernise administrative structures as a whole. Among others, the new umbrella association

DGUV, which has resulted from a merger of the Berufsgenossenschaften and other statutory accident insurance funds, is in favour of this. What is more the number of specialist Berufsgenossenschaften is to reduce from 23 to 9 and that of accident insurance funds from 23 to 17, mainly due to mergers.

#### **Accident prevention also the focal emphasis of Berufsgenossenschaft activities today**

The Berufsgenossenschaften continued or resumed the policy of prioritising accident prevention after the 2nd World War and after the establishment of the Federal Republic, especially since the area of accident prevention was still the one which enabled Berufsgenossenschaften to take its own creative actions with the fewest restrictions.

As such a number of investments and initiatives were made with the objective of “accident prevention”. By contrast, the use of compulsion and the imposition of penalties are limited to only dire emergencies.

In fact, post-war Berufsgenossenschaften placed great value on being constructively involved in events and on passing regulations re-



**Fig. 19** Setting up work on an eccentric press: in the 1950s a focus of accidents continued to be the numerous serious accidents on presses. The precision engineering and electrotechnical Berufsgenossenschaft BG FE tried to inject fresh impetus into this area with the help of its own design office for press protection. Metal employer’s liability insurance associations joined in with this initiative.

lated to practice that take into consideration the respective state of the art of technical development.

By doing so, German industry furthermore opened up a “playground” for new, innovative solutions to safety at work.

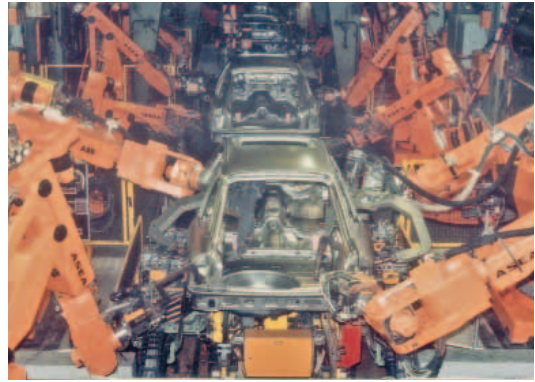
**Accident development**

Prioritising the task of accident prevention really did appear to be a matter of urgency.

While the numbers of proven industrial accidents were low in the early years of 1885/1886, this was probably because it was not possible to be certain with these figures whether all accidents had been reported and/or statistically recorded (keyword: teething troubles) On the other hand if one follows the development of accident figures up to the start of the 1950s (!) one can speak of a continuous increasing trend despite prioritising accident prevention.

However numbers fell steeply after this period.

Accordingly, the number of reportable industrial accidents in 2001 for every 1,000 insured persons in all Berufsgenossenschaften was 34.51 compared to 37.10 in 2000. This was the lowest post-war level (comparison: the figure for 1953



**Fig. 20** There is also a need to continuously face up to new safety-related challenges to achieve effective accident prevention. The example shown here is robot deployment and automated manufacturing systems.

was 186.32, falling to just 90.96 in 1984). At 24.3 per 1,000 full workers, the accident risk today is far lower (something that also applies to fatal accidents at work, of which there were 456 in 2009).

If we draw conclusions from these and other statistical records, we can see that the main focus of attention of the Berufsgenossenschaften has now shifted to the areas of “accidents on the way to work” and “occupational diseases”, while the

	2006	2007	2008	2009
<b>Accidents at work and on the way to work</b>				
Reportable industrial accidents	948,546	959,714	971,620	886,122
– for every 1,000 full workers	26.95	26.81	26.80	24.30
Reportable accidents on the way to work	191,186	167,067	176,608	178,590
– for every 1,000 insurance relationships	4.78	4.05	4.23	4.24
<b>Sum of reportable accidents</b>	<b>1,139,732</b>	<b>1,126,781</b>	<b>1,148,228</b>	<b>1,064,712</b>
Fatal industrial accidents	711	619	572	456
Fatal accidents on the way to work	535	503	458	362
<b>Sum of fatal accidents</b>	<b>1,246</b>	<b>1,122</b>	<b>1,030</b>	<b>818</b>
New pensions for industrial accidents	18,539	17,171	16,823	16,590
– for every 1,000 full workers	0.530	0.480	0.464	0.455
New pensions for accidents on the way to work	7,142	6,170	5,629	5,944
– for every 1,000 insurance relationships	0.178	0.150	0.135	0.141
<b>Sum of new accident pensions</b>	<b>25,781</b>	<b>23,341</b>	<b>22,452</b>	<b>22,534</b>

**Fig. 21** Industrial accidents at work and on the way to work (source: DGUV)

“classic” industrial accident has been pushed down the list of priorities.

### The first accident prevention regulations

If the first accident prevention regulations were of an appellatory nature, they soon became more concrete and detailed and were furnished with penalties.

An example of this is one of the first accident prevention regulations dated 21.12.1887 from the Rhenish-Westphalian Iron and Steelmaking Employer’s Liability Insurance Association (Rheinisch-Westfälischen Hütten- und Walzwerks-berufsgenossenschaft) (as shown in Figure 22):

This already contains concrete regulations for general accident prevention because it contains provisions that are separated into obligations for the entrepreneur of the business and those for workers; examples are (as obligation for the entrepreneur) how flooring, lighting, railings, stairs and steps must be provided, how to deal with those who are drunk and sick, how to prevent bad air and furnace gases and that ongoing work, including repairs, in areas with a risk of gas explosions, can only be carried out taking specific safety regulations into account.



It likewise contains obligations for workers, for example, and this is a subject that persists to this day, that it is strictly forbidden to remove or fail to use protective equipment.

In addition there were special regulations for steam boiler operation, motor equipment, drive lines, engines, gears and work machines.

In the event of infringement there was a threat of penalties for both the employer, for example classification in a higher risk tariff or the doubling of contributions, and for the employee, e.g. a fine if they were not actually dismissed from their job.

But awards in the form of bonuses (of up to 100 marks) can also be paid by the executive board of a Berufsgenossenschaft if workers or third parties have averted accidents or have contributed to rescuing casualties.

Objectives are formulated in Chapter V “Vor-

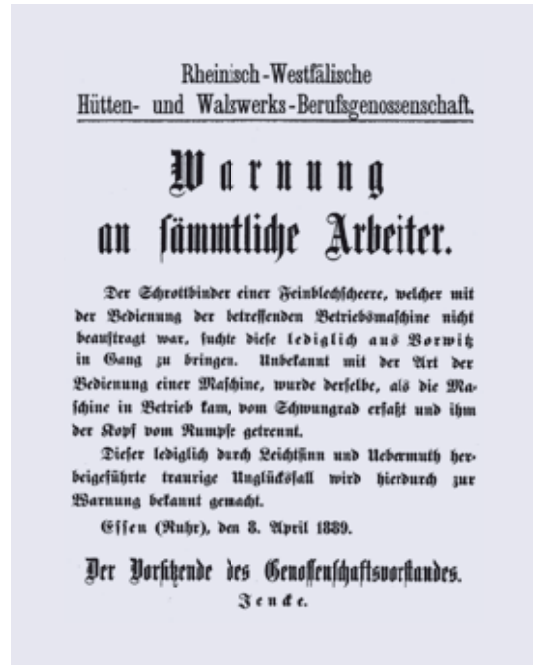


Fig. 22 Example of a historical accident prevention regulation (extract/example 1)

schriften für Arbeitsmaschinen” (regulations for work machines) of the abovementioned accident prevention regulation that appear very familiar today as source of danger and which are therefore quoted here for information purposes (as shown in Figure 23).

### Safety at work from the end of the 19th Century to the present day

It would go beyond the limits of this book if we were to set out the many steps taken in the development of accident insurance as a detailed historical report, especially those in the first half of the 20th Century.

Things continued after the social legislation and Bismarck’s dismissal under Kaiser Wilhelm II; despite everything Bismarck’s social policy did not go far enough for Wilhelm, otherwise the following quote would not exist:

*Almost all revolutions can be attributed to the fact that there was a failure to make reforms at the right time.*

Five weeks later he announces his February decrees, designed among other things to promote better safety at work legislation as an additional counteraction to the workers’ movement.

**Disengaging mechanism.** Every work machine must have a disengaging system that makes it possible to shut it down independently of the drive line at any time. The disengaging mechanism must be designed to protect against every self-engagement where possible; it must also be easily accessible from the position of the worker.

**Cogs.** For all work machines that are operated with a belt with a width of more than 40 millimetres or equivalent mechanism, the cogs positioned in the area of the worker must be covered up on the intake sides and where they run closely past fixed parts. This regulation does not apply to slow-running change gears or to gear wheels if these are not in a particularly dangerous position.

**Flywheels.** For flywheels on work machines whose lowest point is less than 1.5 metres about the floor, and to the extent that operation so permits, either protective grilles should be attached or the arms of the same should be clad from the outside with a solid metal sheet or similar.

**High speed edge tools.** Work machines with high speed edge tools must where possible be set up and operated in such a way that people working on them do not come into contact with them and are not hit by flying splinters.

**Drop hammers.** Drop hammers driven by drive lines must be equipped with a simple, safe operated, mounted mechanism to hold the hammer tups up high.

**Fig. 23** Example of a historical accident prevention regulation (extract/example 2)

In his global newsletter one year later, Pope Leo VIII announces that it is a “crime” to deny workers the wages they have earned and that it is in the interest of the state to enhance the position of the working population so that workers did not remain in need.

The Industrial Code is amended that same year (1891). Among other things this newly regulates protection of young people, women and women who have recently given birth, the ban on Sunday work and child labour as well as health protection and accident prevention. In addition trade supervision officers are given greater authority, including police powers. This amendment is viewed as the first real turning point in the power of control held by employers.

There is a further amendment to the Accident Insurance Act in 1900. The Reich Insurance Ordinance comes into being in 1911, and extends safety at work to include work performed in the home. The roots of the liaison officer (safety officer as from 1963), who was to be the first point of contact at operational level for questions relating to occupational health and safety, also lie here.

In 1917 the major employer associations and

trades unions come to an agreement on the eight hour working day starting from 1918 and on decentralised collective agreements on working conditions at the level of trade associations.

For the first time in 1919 a right of co-determination is introduced in the Reich Constitution under Friedrich Ebert; among other things, Article 165 provides for equal participation of workers and salaried staff in working conditions. The duty to maintain health and the ability to work was also anchored in Article 161.

The International Labour Organisation (ILO) is founded the same year within the League of Nations; its purpose is to promote working conditions, safety at work and other basic social conditions throughout the world.

The first Occupational Disease Ordinance covering eleven industrial occupational diseases comes into force in 1925. Now compensation applies not only to sudden accidents but also to the defined industry-related illnesses. In this way, after lengthy resistance by employer associations, the state relieved itself at the cost of the corresponding Berufsgenossenschaft. However this was also designed to encourage companies to take precautions themselves in order to keep



their contributions low. The journey to work is also incorporated as an insured risk under the accident insurance.

A more comprehensive safety at work act considered by the Reichstag falls through in 1928. In 1936/37 (during the “Third Reich”) every third schoolchild is working again; youths are permitted to work up to 10 hours a day, and night work is possible for them again. The eight hour working day is raised to ten hours. Working conditions worsen, also for youths in the Reichsarbeitsdienst (Reich labour service), and the number of accidents increases by 30 % (fatal accidents) and 46% from 1934. We will not examine the other reprehensible acts connected with the subject during this period in further detail here.

We must now jump a few decades to get to another major milestone which is of decisive significance to the subject of “occupational health and safety” in Germany.

#### **Safety of Machinery Act as from 1968**

This further important milestone designed to permanently reinforce the efforts of Berufsgenossenschaften regarding accident prevention comes at the end of the 60s with the passing of the so-called Maschinenschutzgesetz (Safety of Machinery Act) , or to put it precisely, the Gesetz über technische Arbeitsmittel or GSG (Law on Technical Working Equipment – Equipment Safety Law) dated 24 June 1968.

With the GSG, for the first time the legislator obliges manufacturers and importers explicitly to only supply machinery (and household appliances and toys) that comply with special safety regulations.

With respect to machinery it is stipulated that these special safety regulations are the accident prevention regulations of the Berufsgenossenschaften. The GSG therefore conferred a completely new quality on the accident prevention regulations.

Until then observance of accident prevention regulations had been a duty of the operator or entrepreneur. From now on the provisions concerned statutory manufacturer obligations, not on the legal basis of social security law but on the legal basis of general civil law or the law of obligations.

The fact that the product safety provisions (in this case “machinery”) in the GSG were inspired by accident prevention regulations can be understood as an explicit recognition of the previous actions of the Berufsgenossenschaften.

At all events, the consequence of this change to the legal situation on the composition of future accident prevention regulations was that in future there was a new section on “Regulations pertaining to construction and equipment”.

Further special significance for safety at work can be attributed to the GSG because it created a basis, and in particular the economic basis, for “putting hands in pockets” and investing the money in the design and development of new safety components and systems as well as boosting the safety of existing devices and systems. The prospect of a “return on investment” was guaranteed by the fact that the legal requirement for safety technology meant that standardised series deployment of such solutions could be expected.

#### **The end of our story: the EC Machinery Directive**

The EC Machinery Directive (MD) that came into force on 1 January 1993 represented a break, reversing much of what we have reported, or – expressed neutrally – placing it on a new footing. The objective of the Directive was the free movement of goods within EU Europe for machinery and safety components on the basis of equal “rules”, and without trade barriers from individual states; this also included different safety regulations.

The consequence of this was that, through the coming into force of the MD, Berufsgenossenschaften were no longer responsible for dealing with the area of “construction and equipment of machinery” within the framework of accident prevention. As a result most accident prevention regulations had to be rewritten as they were only permitted to contain obligations for the operator.

Applicable in their place was Annex 1 of the MD, i.e. the so-called “Basic safety and health requirements for the design and construction of machinery and safety components” as well as the harmonised European standard (EN standardisation) with the interpretation of the protective objectives specified in it.

The Berufsgenossenschaften therefore quickly recognised that co-operation in the corresponding standards committees would from now on be their main “territory” for continued active participation in the shaping of industrial protection and machine safety.

**Directive of the European Parliament and of the Council**  
for harmonisation of the legal and administrative regulations of Member States with respect to Machinery



# *Index*





# Index

Page numbers may also stand for “f” (page and following page) and for “ff” (page and following pages)

1-channel, 2-channel etc.	84, 99	Authorised representative (for declaration of conformity/incorporation)	31
2 monitoring switches vs. 1 monitoring switch	99	Authorised representative for compiling technical documents/documentation	31, 51
2006/42/EC	21	Authorities	29
2006/95/EC	32	Average probability of a dangerous failure/hour	82
2009/104/EC	53, 54, 56, 58	AZ/AZM 200	140, 174
2-switch design	137		
95/16/EC	25		
98/37/EC	21		
		<b>B</b>	
<b>A</b>		B <sub>10d</sub> value assessment	85
A/B/C standards	67	Bar chart in accordance with EN ISO 13849-1:2008 (2006)”	87
Access speeds and safety distances	121	Basic (MD) requirements for health protection and safety	35, 39
Accessible danger areas	151	Basic safety and health requirements	35
Accident insurance (historical)	177	Betriebssicherheits-Verordnung (BetrSichV) (German Ordinance on Industrial Health and Safety)	54, 56, 58, 59
Accident prevention regulations (historical)	179	Berufsgenossenschaften (Employer liability insurance associations) (historical)	179
Accidents (today and historically) in figures	182	BG information on implementation of EN ISO 13849-1:2008 (2006)	93
Acknowledgement function	106, 150	BGIA report 2/2008: Information on implementation of EN ISO 13849-1.2008 (2006)	94
Acknowledgement function (acknowledgement signal)	150	Bismarck, Otto, Graf von	177
Acknowledgement, double ...	150	Blanking	164
Active Optoelectronic Protective Devices (AOPDs)	131, 164	Block diagram (functional vs. safety-related)	97
Actuation in an emergency	158	Block method	88
Actuator fixing, undetachable	135	Borderline issues in the application of MD 2006/42/EC	53
Additional monitoring switch	137	Brazil: requirements placed on machine safety	74
Amendments to MD Annex I	37	Brochure on implementing EN ISO 13849-1:2008 (2006)	93
Annex G of EN ISO 13849-1:2008 (2006)	105	Bumper	130
Annex I requirements (MD 2006/42/EC)	35	Bus systems, safety-related	167
Annex IV procedure (MD 2006/42/EC)	33		
Annex K of EN ISO 13849-1:2008 (2006)	86	<b>C</b>	
Annex VII Documentation (MD 2006/42/EC)	27, 51	Cams, Cartesian (safety-related rooms)	172
Annex X (QM/QA/QAS procedures/ MD 2006/42/EC)	35, 45	Canada: requirements placed on machine safety	74
AOPD application at freezing point	165	Cartesian cams (safety-related rooms)	172
AOPDs (Active Optoelectronic Protective Devices)	131, 164	Categories	79, 81, 83
AOPDs (optoelectronics) – operating modes	164	CC (control categories)	79, 81, 83
AOPDs for hygiene-critical applications	166	CCF (Common Cause/ Common Mode failures)	86
AOPDs with protection class IP 69K	166	CE marking	33, 62
Approach switch with safety function	174	CE, Person responsible for the ...	31, 51
ArbSchG (Employment Protection Act)	15		
Architecture	79, 81, 83		
AS-interface Safety at Work	168		
Assembly instructions	28		
Australia: requirements placed on machinery safety	74		

Changes to machinery	53	Design measures to prevent manipulation	
Changes to machinery (vs. significant ...)	53	of protective devices	141
Changes to the application field/scope (MD 2006/42/EC)	23	Designated architectures	79, 81, 83
Channel function	84, 99	Determination of safety functions	95
Checklist as indicator of manipulation incentive	143, 144	Deterministic failures, faults and malfunctions	111
Checklist(s) for checking work equipment	60	Deutsche Gesetzliche Unfallversicherung – DGUV (German statutory accident insurance)	181
China: requirements placed on machine safety	71	Diagnostic Coverage	85
Circuit (function vs. safety-related)	97	– ... and series connections	101
Circumventing protective devices (also see “manipulation”)	124, 133	DIN V VDE 0801	163
Classification of a safety function	89	Direct safety technology	113, 127
Common Cause Failures	86	Directive 2009/104/EC	53, 55, 58
Common Mode Failures	86	Directives of the European Union (EU)	15
Compact controllers, safety-related ...	167	Document officer	31, 51
Compact safety controllers	167	Documentation (technical .../ MD Annex VII)	28, 52
Compatibility PL ↔ SIL	83	Documents (technical documentation)	28, 52
Complete machinery	23, 55, 154	Double acknowledgement	150
Complex devices and PL estimation/ calculation	89	Double detection of guard position	136
Components for safety functions	48	<b>E</b>	
Comprehensive QA in accordance with MD Annex X	34, 35, 45	E/E/PES (Electrical, electronic and programmable electronic systems with safety function)	163
Concealed installation of safety switches (etc.)	136	EC declaration of conformity (MD 2006/42/EC)	23
Conciliation committee	18	EC Machinery Directive 2006/42/EC	21
Conformity assessment procedure – partly complete machinery	26	Edge detection on RESET	105, 150
Construction site lifts	25	EDM function	165
Control categories	79, 81, 83	EEA/EEA Member States	22
Control systems, safety-related	167	Electrical and electronic products (2006/95/EC)	25
Control systems, safety-related parts of ...	77, 81, 93	Electrical power drive systems, additional safety-related functions	170
Control-related measures to prevent manipulation of protective devices	138, 141	Electronic interlocking devices with/ without guard locking	140, 174
Council of the European Union	18	Electro-sensitive protective equipment	130, 164
CSS family	140, 174	– (application of ...) at freezing temperatures	165
Cyclic operation	165	– for hygiene-critical applications	166
<b>D</b>		– with protection class IP 69K	166
Daisy chaining machinery	154	Emergency stop	158
Danger areas, accessible ...	148	Emergency stop concepts (IMS/ integrated manufacturing systems)	157
Danger, hazard, risk (terms)	111	Empirical study results on manipulation of protective devices	134
DC/DC <sub>avg</sub> (diagnostic coverage/diagnostic coverage average)	85	Employee obligations (keyword: manipulation of protective devices)	141
– ... and series connections	101	Employer liability insurance association information on implementing EN ISO 13849-1:2008 (2006)	93
Declaration of conformity (MD 2006/42/EC)	23		
Declaration of incorporation (MD 2006/42/EC)	29		
Delimitation of MD vs. other EU directives	25, 32		
Design measures (risk reduction)	112		

Employer liability insurance associations (Berufsgenossenschaften) (historical)	178	Fault overwriting/deletion (Masking in the case of simple series connections)	100, 101
Employment Protection Act (ArbSchG)	15	Faults (dangerous)	83
EN 294	118	Faults (failures and malfunctions)	91
EN 811	118	Faults with common cause (and effect)	86
EN 1037	147	Field of application for MD 2006/42/EC (product-related)	22
EN 1088	134	Fixtures (fixing elements), undetachable	127, 135
EN 954-1	77, 81	Floating blanking	165
EN 13855 (EN 999)	129, 131	Functional vs. safety-related circuit	97
EN 13857	118, 128, 129	Further information on MD 2006/42/EC	41
EN IEC 60204-1	158	Future amendments in EU directives	61
EN IEC 60947-5-3	174		
EN IEC 61496	165	<b>G</b>	
EN IEC 61508	77, 81, 163	General entrepreneur	55
EN IEC 61800-5-2	171	German Device and Product Safety Act (GPSG)	15
EN IEC 62061	79, 81	German Equipment Safety Act (GSG)	185
EN ISO 11161	153	German statutory accident insurance (Deutsche Gesetzliche Unfallversicherung – DGUV)	181
EN ISO 12100-1/-2	111, 127	Global Regulatory Compliance	66
EN ISO 13849-1	77, 81	Globalnorm GmbH, Berlin	65
EN ISO 13849-2	84, 100	GPSG – Geräte- und Produktsicherheitsgesetz (German Equipment and Product Safety Act)	15
EN ISO 14119 (draft)	135	GSG – Gerätesicherheitsgesetz (German Equipment Safety Act)	185
EN ISO 14121-1/-2	35, 52, 67, 112	Guard locking (safety switch with ...)	175
EN ISO 9001	30, 47, 48	(MZM 100)	175
EN standards	15, 67	Guard locking, solenoid ... (MZM 100)	175
Ergonomic (requirements)	36	Guard monitoring (and fault exclusions)	98
ESALAN Compact	122	Guard monitoring (with/without guard locking)	129
ESALAN SafetyController	171	Guards	127
ESPE (electro-sensitive protective equipment)	130, 164	Guide to MD 2006/42/EC	41
– application in freezing temperatures	165	Guidelines to MD 2006/42/EC	41
– for hygiene-critical applications	166		
– with protection class IP 69K	166	<b>H</b>	
EU directives	15	Hardware quality reliability	
EU institutions	18	– safety-related ..., $B_{10d}$	85
EU Member States	22	– safety-related ..., $MTTF_d$	84
European Commission	18	Harmonised standards	15
European Economic Area (EEA)	22	Hazards, overlapping	97
European legislation	17	Hierarchy of safety technology	11, 127
European Parliament	18	Hinge monitoring switches	137
Examples of typical safety functions	95	History of safety at work in Germany	177
Exceptions to the application field/scope (MD 2006/42/EC)	24	Hüning, Alois	21, 53
Explanations	23, 29		
Extension of the presumption of conformity in EN 951-1:1996	81	<b>I</b>	
<b>F</b>		IEC 60204-1	158
Failure (dangerous)	82, 83	IEC 61508	77, 81, 163
Failure, degree of	82, 83	IEC 62061	79, 81
Failures (faults and malfunctions)	91, 111		
Failures, systematic vs. random	105		
Fault detection	85		
Fault exclusions	98		

IFA (BGIA) Report 2/2008 for implementation of EN ISO 13849-1:2008 (2006)	93	Lock-out tags	149
IMS system integrator	154	Loerzer, Michael	65
IMS zone concept	154	Logic units with safety function	46, 48
IMS/integrated manufacturing systems – terms and application field	154	Low Voltage Directive 2006/95/EC (delimitation)	25
Inactivation of protective devices (also see “manipulation”)	124, 133	<b>M</b>	
India – requirements placed on machine safety	74	Machine systems	23, 55, 154
Indirect safety technology	118, 125	Machinery Directive 2006/42/EC	21
Individual coding		Machinery Directive vs. other EU directives	32
– safety switch with ...	136	Machinery for research purposes and laboratory applications	25
– safety sensors with ...	137	Machinery not ready for use	15, 67
Information (further information) on implementing EN ISO 13849-1:2008 (2006)	93	Machinery Protection Act	179, 181
Inherent safety technology	127	Machinery term (definition of machinery)	23
Institutions (legislative) of the EU	18	Machinery, daisy chained ...	23, 55, 154
Integrated manufacturing systems, safety-related requirements placed on ... (see also IMS)	153	Machinery, partly completed, not usable etc.	26
Interfaces (machine term)	23, 25	Malfunction (dangerous)	83
Interlocking devices (with/without guard locking)	129	Malfunctions (failures and faults)	90
Domestic market directives	15	Manipulation incentives (MPAs): determining/preventing	143
Interpretation paper IIIb6-39607-3 dated 10.03.2006	56	Manipulation of protective devices	124, 133
Interpretation paper IIIc 3-39607-3 dated 07.09.2000	54	– empirical study results	134
ISO 11 161	153	– suggestions and considerations from the Berufsgenossenschaften in the DGUV	141
ISO 12 100-1/-2	111, 127	– suggestions and considerations of the SUVA, the Swiss Accident Insurance Institution	144
ISO 14 119 (draft)	135	Manufacturer’s declaration (MD 98/37/EC)	23
ISO 14 121-1/-2	35, 52, 67, 112	Market for technical safety at work	179
ISO 9001 ff.	30, 47, 48	Market supervision/monitoring	32
<b>J</b>		Marking, CE	33
Japan: requirements placed on machine safety	70	MD vs. other EU directives	25, 32
<b>K</b>		Mean Time to dangerous Failure	84
KAN report on MD 2006/42/EC	41	Measures (control-related) to prevent manipulation of protective devices	138, 143
Key transfer systems	150	Measures (design) to prevent manipulation (SUVA examples)	145
Klindt, Thomas, Prof. Dr.	139	Measures to prevent manipulation	135
Korea: requirements placed on machine safety	74	Measures to prevent unexpected start-up (restarting) of machinery	147
<b>L</b>		Member States of the EU/EEA	22
Legal bases	15	Methods for estimating the PL	88
Lift Directive 95/16/EC (delimitation)	25	Microprocessor-based safety technology	163
Light barriers, light grids, light curtains (safety-related ...)	131	Mini controllers, safety-related	167
Linking machinery	57	Minimising incentives (keyword: manipulation of protective devices)	141
		Minor amendments in MD Annex I	39
		Misuse, reasonable, foreseeable ...	35, 138
		Molitor report	21
		Monitoring switch, additional or second ...	137
		Monitoring switches	128
		Moving guards	129

MPA (determining/preventing manipulation incentive)	143	PL estimation/calculation	
MTTF <sub>d</sub>	84	– and (simple) single devices	87, 89
Muting	131, 165	– and (more complex) devices	87, 89
MZM 100	140, 175	Plant (machinery ...)	23, 55, 154
<b>N</b>		PL <sub>r</sub> (Performance Level <sub>required</sub> )	77, 83
Neudörfer, Alfred, Dr.	111	PL <sub>r</sub> (required)	77, 83
New approach procedure	15, 66	Presumption of conformity	81
New Legislative Framework	61	Preußé, Christoph	153
NLF	23	Preventing unexpected start-up (restarting of machinery)"	147
Non-contact interlocking devices with/without guard locking	138, 174	Preventive maintenance (replacement)	85
Non-European requirements (overview)	65	Probability of a dangerous Failure per Hour (PFH <sub>d</sub> )	82
<b>O</b>		Process observation	36, 141
Operating instructions (operating manual)	37	– IMS/integrated manufacturing systems	159
– IMS/Integrated manufacturing systems	159	Production check	30
Operating manual (operating instructions)	37	Products equivalent to machinery	24
Operating mode selection		Programmable electronic systems with safety function (PES)	163
– new possibilities arising from MD 2006/42/EC	36, 142	PROTECT SRB 100DR	151
Operating modes		Protection in event of failure/fault	82
– IMS/Integrated manufacturing systems	156, 158	Protection of vested rights	53, 56, 58
– of AOPDs (optoelectronics)	165	Protective devices that are accessible from behind	151
– process observation	36, 141	Protective devices	
Operator obligations (keyword: manipulation of protective devices)	140	– selection, advantages/disadvantages	120, 127
Optoelectronics with protection class IP 69K	166	– ... on machinery	120, 124
Optoelectronic protective devices	131, 164	– ..., electro-sensitive protective equipment	130, 164
Optoelectronics (AOPDs) ↔		– moving guards	129
operating modes	165	– ..., accessible from behind	151
Optoelectronics for hygiene-critical applications	166	– ... in the Schmersal/Elan product range	121
Optoelectronics, application at freezing point	165	– ... with approach function	130
Overlapping hazards	97	– ... with fixed location (two-handed)	129
<b>P</b>		– ..., optoelectronic	164
P(erformance) L(evel) calculation	87	– ..., tactile	130
P(erformance) L(evel) estimation	87	– guards	127
Paradigm shift (SRP/CS)	77	Protective fences, virtual (safety-related)	172
Part machines	25	Protective strategy (IMS/integrated manufacturing systems)	156
Partly completed machinery	25	PROTECT-SELECT	168
PDMS (Protect Drive Monitoring System)	171	PROTECT-SELECT WL (wireless)	173
Performance level	77, 81	Pulse-echo procedure, sensors with ...	174
– required .../... <sub>required</sub>	83	<b>Q</b>	
PES (programmable electronic systems with safety function)	163	QM/QA/QAS (quality management, quality assurance, quality assurance system) procedure in accordance with Annex X (MD 2006/42/EC)	34, 35, 45
PFH <sub>d</sub> (Probability of a dangerous Failure per Hour)	82	<b>R</b>	
PL (Performance Level)	78, 81	Radio link (safety-related)	173
		Random failures , faults and malfunctions	111

Random failures vs. systematic failures	105	Safety distances and access speeds	121
Reasonably foreseeable misuse	138	Safety function(s), determination of ...	95
Redundancy	98, 112	Safety function, allocation of a .../ structuring of a ...	88
– ... vs. fault exclusions	100	Safety functions, typical examples	96
Requirements (safety-related) for integrated manufacturing systems ... (see also IMS)	153	Safety Integrity Level	79, 81, 83
Requirements (safety-related) for the “Process observation” operating mode	159	Safety light barriers, light grids, light curtains	131, 165
Requirements for software	105	Safety mats, switch plates, edges, switch rods	131
Requirements of MD 2006/42/EC	21	Safety of machine controls (SISTEMA)	94
Requirements placed on machine safety in China	71	Safety PLCs	167
Requirements placed on machine safety in Japan	70	Safety sensors	138, 174
Requirements placed on machine safety in other industrial countries (Australia, Brazil, Canada, Korea, India)	74	– ... with individual coding	137
Requirements placed on machine safety in Russia	72	– ... with/without guard locking	138, 174
Requirements placed on machine safety in the USA	68	Safety sensors, RFID-based ... (RSS 36)	174
Requirements placed on partly-completed machinery	26	Safety switches	128
Requirements, basic MD requirements for health and safety protection	35, 39	– ... with individual coding	136
RESET and edge detection	106, 150	– ..., concealed installation	136
RESET as safety function	150	– ..., additional or second	128
Reset function (reset signal)	150	Safety switches/sensors with/without guard locking	129
Responsibilities	31	Safety technology (strategy, hierarchy)	113, 127
Restart inhibit	165	Safety technology warnings	177
Restarting	105	Safety technology, microprocessor-based	163
– ... (restart signal)	150	Safety-related bus systems	167
RFID-based sensors (RSS 36)	138, 173	Safety-related controllers	167
Risk (consideration, assessment, level, reduction of)	35, 77, 83, 90, 111	Safety-related mini controllers	167
Risk analysis	35, 111	Safety-Related Parts of Control Systems (SRP/CS)	77, 81, 93
Risk graph	77, 83	Safety-related parts of control systems (SRP/CS)	77, 81
Risk graph analysis	77, 83	Safety-related shut-down and movement monitoring	148, 170
Risk pre-selection	116	Safety-related vs. functional circuit	97
Risk, danger, hazard (terms)	111	Schmersal/Elan information on implementation of EN ISO 13849-1:2008 (2006)	93
Robotics, safety-related	171	Schmersal/Elan product range (protective devices)	121, 122
RSS 36	138, 173	Scope (product-related)	22
Russia: requirements placed on machine safety	72	Second monitoring switch	137
Russian machinery directive	72	Selection of protective devices	120, 127
		Sensors, RFID-based ... (RSS 36)	138
		Series connections and diagnostic coverage	102
		SHGV	150
<b>S</b>		Shut-down and movement monitoring, safety-related	170
Safe position (IMS/integrated manufacturing systems)	157	Shut-down in an emergency	158
Safety at work in the Middle Ages	178	Shut-down monitoring, safe ...	148
Safety components	30, 46, 48	Significant changes to machinery	53
Safety Control GmbH, Mühldorf	164	SIL (Safety Integrity Level)	81, 83
SafetyController (ESALAN...)	171	SIL/SILCL (SIL Claim Limit)	79



Simple single devices and PL assessment/calculation	89	Systematic failures, faults and malfunctions	91, 111
Single-channelled, two-channelled etc.	84, 100		
SISTEMA software assistant	94	<b>T</b>	
SLC/SLG (AOPD/BWS ranges)	165	T <sub>10d</sub> value assessment	85
Social legislation (historical)	177	Tactile protective devices	130
Social protection/occupational health and safety directives	16	Tamperproof screws	135
Software-assisted PL estimations	94	TCP monitoring (safety-related)	171
Electromagnetically operated guard locking (MZM 100)	175	Technical documents (documentation)	28, 52
Spatial scope (MD 2006/42/EC)	22	Terms for danger, hazard, risk	111
Special modes	36	Trailing edge (edge detection) on reset	138, 151
– ..., new possibilities due to MD 2006/42/EC	142	Transitional period	81
Sporadic failures, faults and malfunctions	91, 111	Transposition into national law	15
SRA/SW (safety requirements of application software)	105	Transposition of EN ISO 13849-1:2008 (2006)	93
SRE/SW (safety requirements of embedded software)	105	– step by step ...	90
SRECS	79	Two monitoring switches vs. one monitoring switch	99
SRP/CS (Safety-related parts of control systems)	77, 81, 93	Type A/B/C standards	67
Standards	15, 67	<b>U</b>	
Standards (with presumption of conformity)	15	Undetachable actuator fastening	135
State of the art	82	Undetachable fixtures (elements)	39, 127
Step-by-step implementation of EN ISO 13849-1:2008 (2006)	90	Unexpected start-up (restarting) of machinery	147
Stochastic failures, faults and malfunctions	111	USA: requirements placed on machine safety	68
Stop commands (stop 0, 1 and 2)	147	Use of Work Equipment/Work Equipment Safety Directive 2009/104/EC	53, 55, 57
Strategy of safety technology	113, 127	Used machinery	57
Structuring a safety function	89	<b>V</b>	
Sub-system method	88	Virtual protective fences (safety-related)	172
Switching off in an emergency	158	<b>W</b>	
Switching on in an emergency	158	Warning safety technology	124, 127
Synchronous position (safety-related)	172	Wireless (safety-related)	173
Synopsis of MD 2006/42/EC vs. 98/37/EC	41	<b>Z</b>	
System integrator	55	Zone concept for IMS/integrated manufacturing systems	156
– ..., IMS/integrated manufacturing systems	154		
Systematic failures vs. random failures	105		











This book compiles various Schmersal/Elan publications on the subject of “functional machine safety” together which concern areas that have been the subject matter of recent changes and amendments. In particular we have referred to articles in our company newspaper “MRL News”, which we have expanded and updated accordingly. The book also contains guidelines and background information and furthermore addresses borderline issues of machinery law.

Focal subjects here are as follows:

- The EC Machinery Directive 2006/42/EC which came into effect in 2009;
- The EN ISO 13849-1 standard which places new requirements on the design of safety-related parts of control systems; as well as
- Risk assessments, technological development etc.

We hope it makes enjoyable reading.



**Sicherheit im System: Schutz für Mensch und Maschine.**

