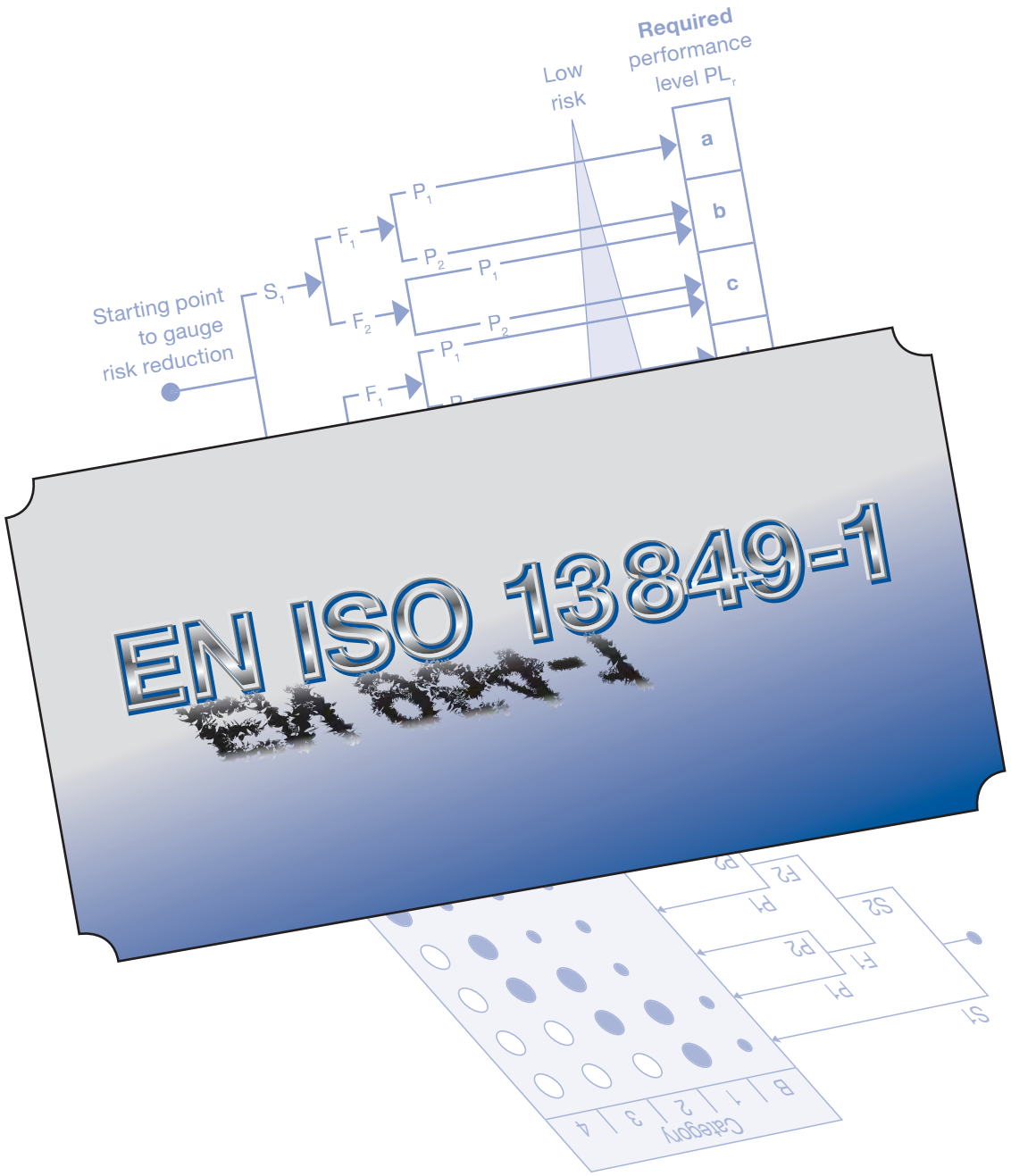
A New Approach to Machine Safety:

EN ISO 13849-1:2006 – Safety-related Parts of Control Systems



SCHMERSAL

Elan

Update

Wuppertal/Wettenberg in May 2007

Dear SCHMERSAL Customer,
Dear Elan Customer,

After having had some more internal trouble the revision of the present standard ISO 13849-1:1999 (EN 954-1:1996) has passed in autumn of 2006 and the new EN ISO 13849-1:2006: “Safety-related Parts of Control Systems” (as its successor) has become into force.

To say it in other words: The paradigm shift in the philosophy of safety-related parts of machine control systems takes place to supplement probabilistic considerations to the previous proven in use deterministic considerations.

Therefore the time table of coming into force on page 46 of our brochure “A new Approach of Machine Safety: prEN ISO 13849-1” (with an editorial deadline of March 2006) needs an update.

According the latest decision-making process the now concluded standard has a transition period until November 2009 (which means the new provisions can be already applied from now on, but there is not yet a must to do so). But in November 2009 at the latest conflicting standards (in practical terms: ISO 13849-1:1996 respectively EN 954-1:1996) have to be recalled. Than the “old” standard finally will be replaced by EN ISO 13849-1:2006.

In all other respects our brochure on backgrounds, application and practical implementation of the new standard are still up-to-date and (besides some smaller printing mistakes) correct.

Yours sincerely,

Friedrich Adams
K.A. Schmersal Holding GmbH & Co. KG

When do I have to apply the new EN ISO 13849-1:2006? Is there any transition period?

Wuppertal/Wettenberg in March 2006

Dear SCHMERSAL Customer,
Dear Elan Customer,

In this brochure we extensively highlight the core speech at the Elan lecture event 2005, which dealt with the discontinuation of the EN 954-1 standard and the new regulations in the revised standard EN ISO 13849-1. With the initiative to release this brochure, the SCHMERSAL Group intents to emphasise their advanced competence on safety of machinery. For us as a supplier of safety switchgear and safety systems designed to protect people, machines and equipment we also wish to provide our customers with additional information on boundaries and background knowledge in order to become their partner of preference when it comes to the implementation of safety components for machines and machine controls.

Below is a summary of the relevant speech by Mr. Thomas Bömer (engineer) and Mr. Karl-Heinz Büllesbach (engineer), both employees of the Berufsgenossenschaftliches Institut für Arbeitsschutz BGIA (the employer's liability insurance association institute for health and safety – BGIA) in St. Augustin, whose work at the "electronics" unit within the machine protection & control systems engineering department there is closely related to our theme. The figures in the following contribution are based on the PPT presentation of the two gentlemen; thus the copyright for the figures belongs to them.

The Berufsgenossenschaftliches Institut für Arbeitsschutz BGIA in particular, as well as various engineering-oriented employer's liability insurance associations have been especially committed to the design of the revised standard EN ISO 13849-1. In the foreground are the clientele of small and medium sized engineering and control systems companies who are to be given a guide on the future execution of safety-related control system parts which is as simple but also as substantial as possible.

If the enactment of EN ISO 13849-1:2006 is nevertheless currently highly contentious, this is connected with a particular constellation within the standards scene, in which the sector specific IEC EN 62061 standard (derived from IEC EN 61508) is also competing to replace EN 954-1, even if only in the area of electrical, electronic and programmable electronic systems with safety functions.

Irrespective of this, the product range from the companies in the SCHMERSAL Group already takes account of and can now support both future standards with the relevant specifications. If you have any questions pertinent to this subject therefore, please discuss them with us.

In the interests of clarity we have divided the theme of "EN ISO 13849-1:2006: A New Approach to Machine Safety" into separate sections which are themselves subdivided – subject to how "deeply" you wish to probe while reading.

We ask for your understanding with respect of abbreviations in the text in advance (which are unfortunately unavoidable). The glossary, however, tries to maintain readability (please refer to the fold out page).

Although we have attempted to make the summary clear and comprehensible, this may only have succeeded in part due to the complexity of the subject. Unanswered questions are also bound to occur at different points.

Nevertheless, we hope you find this reading interesting and look forward to working with you in the future.

Yours sincerely,

Heinz Schmersal
Managing Director
K.A. Schmersal Holding GmbH & Co. KG

Friedrich Adams
K.A. Schmersal Holding GmbH & Co. KG

Contents

!

Publisher
Elan Schaltelemente GmbH & Co. KG
Im Ostpark 2
35435 Wettenberg
Telephone +49 (0)641 9848-0
Fax +49 (0)641 9848-420
E-Mail: info@elan.schmersal.de
Internet: www.elan.de

Editor
Friedrich Adams
c/o SCHMERSAL Holding GmbH & Co. KG
Möddinghofe 30
42279 Wuppertal
E-Mail: fadams@schmersal.de

Overall production
Werbe-Grafik Heinz Flick, 35075 Gladenbach/
Druckteam Peter Bork, 35435 Wettenberg

Introduction

When EN 954-1[1] is replaced in a few years – something we now take for granted – this will also represent a kind of paradigm shift. In future, the importance of the deterministic approach to executing safety-related control system parts will decline and probability approaches will emerge.

Two standards are competing to be the successor to EN 954-1: the first is EN ISO 13849-1:2006[2], which has been specifically designed to follow on from EN 954-1. The second standard competing to succeed EN 954-1 is IEC EN 62061[3], a sector-specific derivative of IEC EN 61508[4].

The theory of probability with regard to the execution of safety-related parts of machine controls will also hold in the future with either standard (at least with regard to the generic term for reliability engineering), irrespective of the decision taken. In contrast, the approach in EN 954-1 is based essentially on an examination of structures.

Although we will concentrate on EN ISO 13849-1:2006 in the following article, based on the contents of the Elan lecture event 2005, probabilistics in the form of the mathematical calculus of probability theory and modelling play a much greater role in IEC EN 61508 and IEC EN 62061. In contrast, the standard-setter of EN ISO 13849-1:2006 has strived to achieve a delicate balancing act between deterministic and probabilistic thinking, breaking down the new aspects into a requisite and practicable size for the “average user” (refer to Figure 1).

1) EN 954-1: 1997-03: Safety of safety-related parts of control systems – Part 1: general design guidelines (corresponds also to ISO 13849-1: 1999-11)

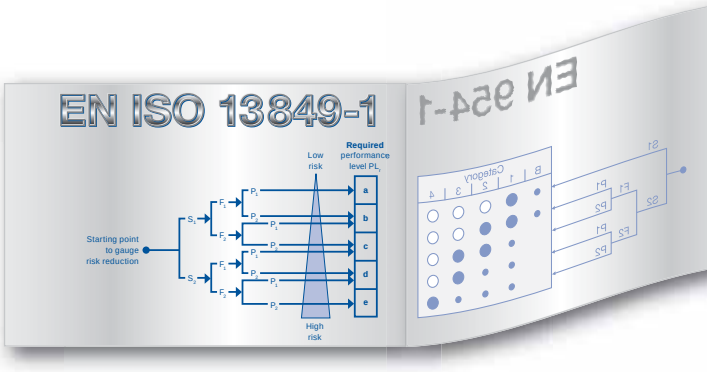
2) EN ISO 13849-1:2006: Safety of machine safety-related parts of control systems – Part 1: General design guidelines.

3) IEC EN 62061:2005-10: Safety of machines – functional safety of safety-related electrical, electronic and programmable electronic control systems

4) IEC EN 61508:2002-11: Functional safety of safety-related electrical/electronic/programmable electronic systems

- Part 1: General requirements
- Part 2: Requirements of safety-related electrical/electronic/programmable electronic systems
- Part 3: Requirements of software
- Part 4: Terms and abbreviations
- Part 5: Examples to calculate the safety integrity level
- Part 6: Application guidelines for IEC 61508-2 and IEC 61508-3
- Part 7: Application details of procedures and measures

Source: Beuth Verlag GmbH, 10772 Berlin; www.beuth.de



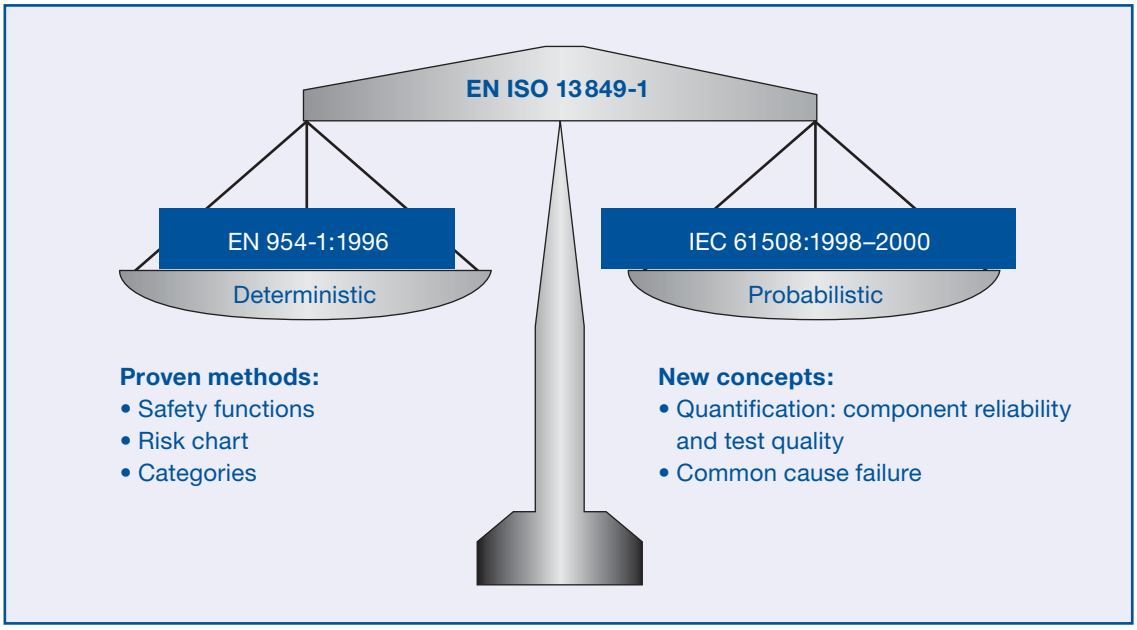


Figure 1: Balance between deterministic and probabilistic

Even without offending the EN ISO 13849-1:2006 standard-setter we might suggest that this standard is a “light” version of IEC EN 61508. It is “light” because the particular feature of EN ISO 13849-1:2006 is its attempt to take account of the interests of the majority of clients addressed, i.e. the medium sized engineering and control systems companies, by permitting appropriate and justifiable safety-relevant simplifications and generalisations geared to this target group. This is clearly combined with the objective to constrain additional effort involved in the probabilistic view.

For example, if we look at the development of complex microprocessor-based electronics with safety functions, whether the safety stored program controllers, safety field bus systems or laser scanners, the EN ISO 13849-1:2006 is of little help. Here it might be better to use the IEC EN 61508.

Background to the removal of EN 954-1

If we ask ourselves whether the removal of EN 954-1 makes sense, and whether it is induced by machine accident occurrence, i.e. whether industrial accidents can be ascribed to shortcomings and gaps in EN 954-1, then the answer is an emphatic “no”.

At least this is the answer given from a German point of view, even if this “no” does not mean that there is no potential for improvement or that EN 954-1 is above criticism. Rather, it is much more concerned with asking whether a complete replacement which is not automatically downward compatible is necessary.

On the other hand, for many years there has been an extremely controversial discussion about how accurate the perspectives and rules in EN 954-1 are, particularly in other Member States of the European Union but also within German circles.

- From a theoretical viewpoint the criticism is essentially based on the fact that EN 954-1 "only" provides measures designed to reduce risk across a range of risk levels, producing a single residual risk level for all categories[1]. This means the risk to the machine operator is theoretically always constant, irrespective of whether an SRP/CS[2] is being executed in accordance with category 1, 2, 3 or 4 and unaffected by, for example, the risk posed by a slight (reversible) compared to a serious (irreversible) injury. Moreover, this approach additionally results from EN 954-1 having no facility for a common category.

  Critics demand that increased risk levels attract more stringent measures which serve to reduce residual risk.

- Furthermore, as mentioned in the second criticism, the requirements of EN 954-1 inadequately reflect the increasing complexity of factory automation, i.e. with regard to analysing the number of "links in a chain" and diverse depths of interconnections it takes too little account of whether an SRP/CS is realised at an individual machine, a complex linked device or an integrated production system. One could also say: **the higher the complexity –> greater the level of residual risk –> greater the measures required to control the residual risk!**

  The factor of inadequate regard for the complexity of an SRP/CS is surely not to be dismissed.

- On the other hand the objection that EN 954-1 no longer reflects the state-of-the-art is undisputed, especially because, while it does not explicitly exclude programmable microprocessor-based technologies with safety functions, it also fails to define any requirements in respect of them.

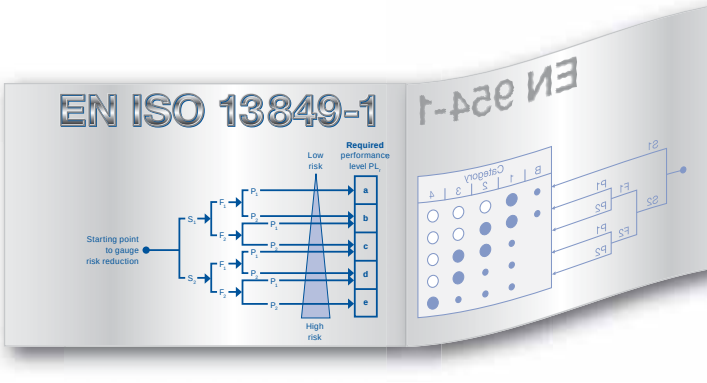
The above representation of criticisms (while not claiming to be complete) serve simply to improve background understanding, without having to go into the subject further here (refer also to Figure 2).

Criticism:

- Despite being applicable to programmable systems and complex electronics, there are no detailed requirements
- Inadequate requirements for consideration of reliability values
- Fault exclusion in category 1 leads to an absent hierarchy when determining the dimensions of risk reduction
- Risk chart: there is no direct connection between risk reduction and category, and complexityis not considered

Figure 2: Some criticism of the present EN 954-1

1) Here also compare with CR 954-100 – Guidelines for the use and application of EN 954-1.
2) **PLEASE NOTE!** Safety-related parts of machine controls will hereafter also be termed SRP/CS, which stands for the "safety-related part of a control system".



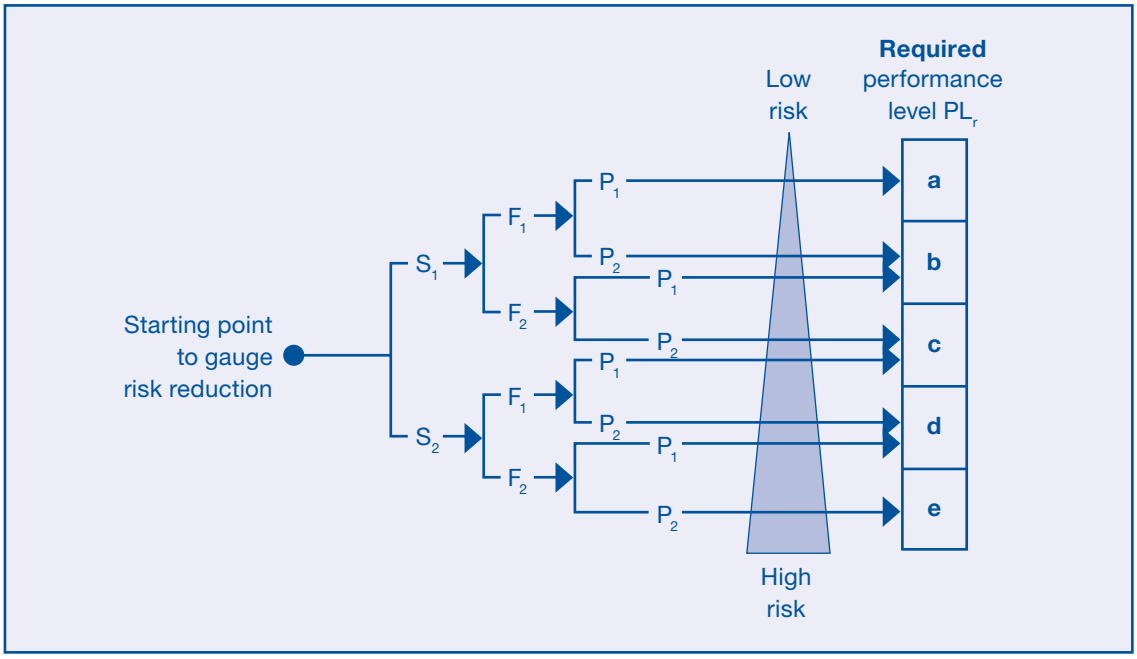


Figure 3: Requisite risk reduction and Performance Level: S = severity of injury; F = frequency and/or duration of exposure to hazard; P = potential to reduce the hazard.

New risk chart

Background
EN ISO 13849-1:2006 also makes use of a risk chart (see Figure 3); however, consideration of the risk parameters no longer results in control categories as in EN 954-1, but in so-called performance levels (PL).

PL designates the ability of a safety-related part of a control system (SRP/CS) to realise a safety function in order to achieve the expected risk reduction, a view which includes both quantitative and qualitative aspects.

The individual risk parameters in prEN ISO 13849-1 (the severity of injury, frequency and duration of stay etc.) are unchanged when compared to EN 954-1.

Execution
The relevant performance level (subdivided into PL “a” … PL “e”) reflects differing residual risks – expressed as the probability of dangerous failure per hour or PFHd (refer also to Figure 4).

Thus the approach of the new standard takes the residual probability into consideration, i.e. the inclusion of reliability engineering or a combination of deterministic and probabilistic.

The PL grades are selected so that they comply with the so-called safety integrity levels (SILs) from IEC EN 61 508 and also allow reference back to the control categories from EN 954-1 – with the exception of finer points (as cited) – i.e. Cat. 1 corresponds to (but is not identical with) PL “b”, Cat. 2 with PL “c” etc.

1) PFH = Probability of Failure per Hour

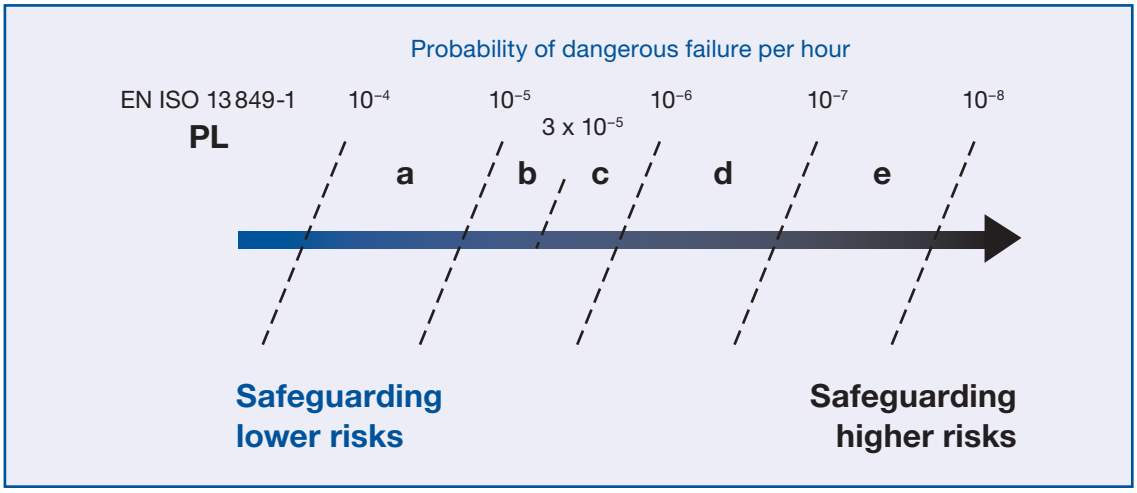


Figure 4: Definition of the PL as safety-related reliability

Application

- Every single safety function of a machine arising from a hazard analysis must be considered and analysed, for example the shut down in an emergency (emergency stop), the interlocking of moving protective devices etc. The so-called PL_r is then the product of the risk graph consideration ("r" for required or necessary Performance Level).
- The PL consideration is an overall consideration and always refers to the "sensor" chain (detect), "logic" (process) and "actor" (switch).

New aspects for consideration

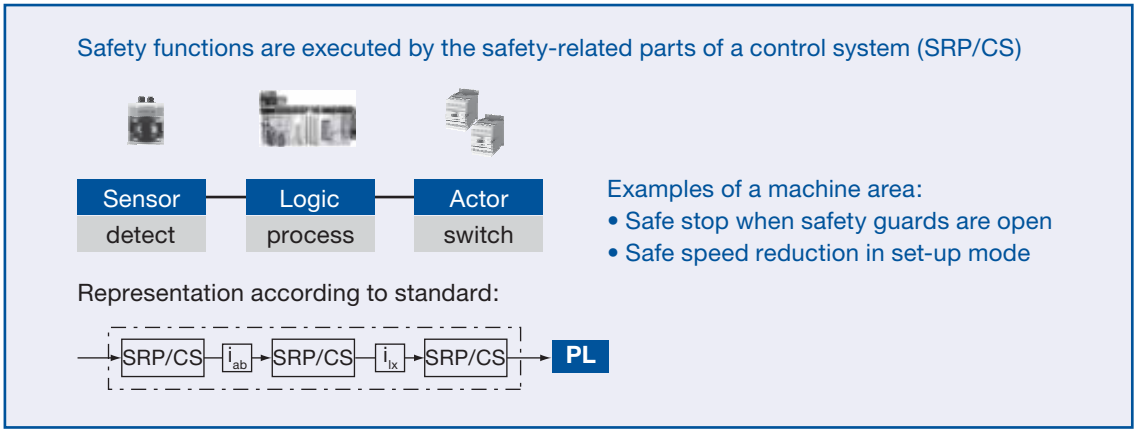


Figure 5: Safety function and SRP/CS

1) The systematics of the standard differentiate between PL_r and PL. PL_r stands for the performance level deemed necessary following consideration of risk (in effect an identification of target value). PL is the analysed result (in effect an identification of the actual value).

The result of the combination between deterministic and probabilistic approaches (the balancing act referred to above) is that the following aspects requiring consideration flow into the PL (refer also to Figure 6):

1. The control category (more or less, as discussed) contained in the standard predominantly represented by “designated architectures”;

2. The “$MTTF_d$” (which stands for the mean time to dangerous failure);

3. The “diagnostic coverage” (DC);

4. The so-called “common cause failure management” (CCF).

There are also measures to counteract system faults, a prerequisite already present in EN ISO 13849-1:2006 and which is listed in Annex G. The background to this is the failure theory in reliability engineering, which differentiates between coincident (refer to $MTTF_d$) and systematic failures, among others (refer also to Figure 7).

Systematic failures have deterministic, not coincident causes and can only be eliminated through changes in design, production, operation sequences or similar factors.

Annex G suggests the following measures:

- Selection from EN ISO 13849-2
- Strengthening of environmentally-related influences
- Typical computer measures (programme monitoring, reviews etc.)
- Data communication protection

Figure 7: Avoidance and control of system faults

Application

- Every single safety function of a machine arising from a hazard analysis must be considered and analysed, for example the shut down in an emergency (emergency stop), the interlocking of moving protective devices etc. The so-called PL_r is then the product of the risk graph consideration (“r” for required or necessary performance level).

- The PL examination is an overall consideration and always refers to the “sensor” chain (detect), “logic” (process) and “actor” (switch) (refer also to Figure 5).

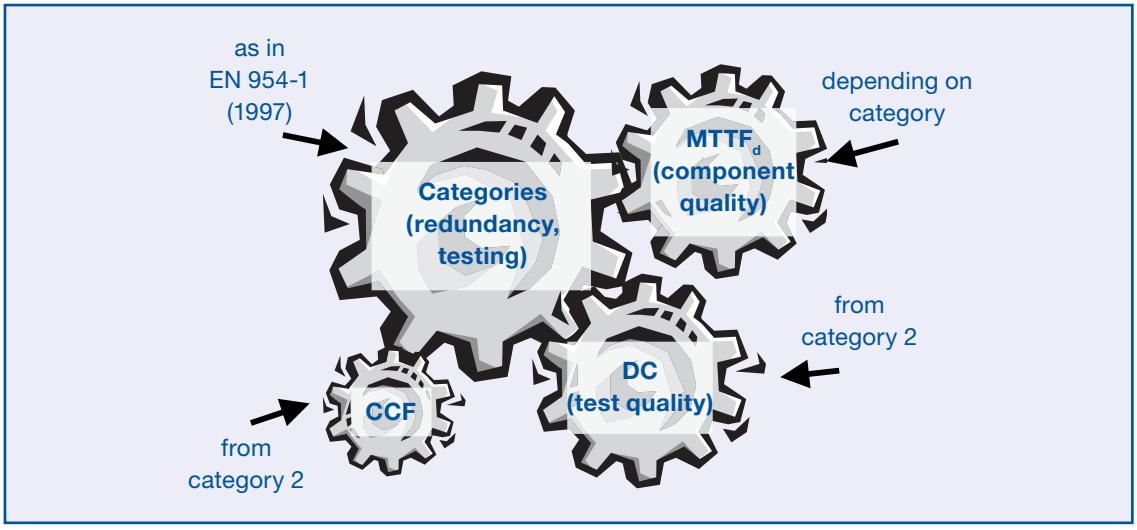


Figure 6: Extension of category terms

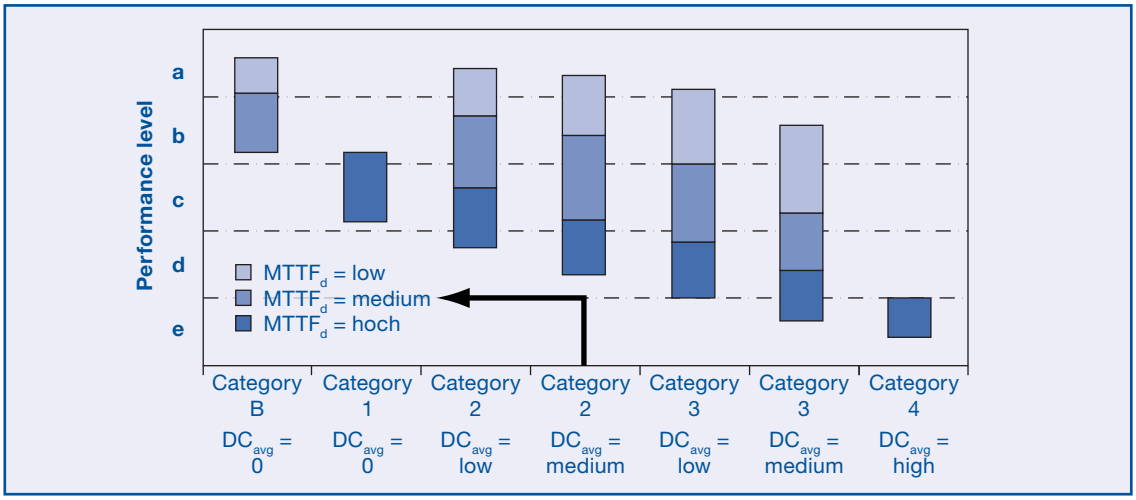


Figure 8: Simplified determination of the Performance Level PL

Performance level
instead of control category

The results of the analysis of 1 to 4 (i.e. the analysis of designated architecture, channel $MTTF_d$, DC and CCF) are then entered onto a block diagram, from which the performance level attained can be read off (refer to Figure 8).

This means that a PL “e” requires a structure corresponding to category 4, a channel $MTTF_d$ value of “high” and an equally “high” DC (for information on the DC_{avg} concept as cited).

If, on the other hand, the objective is for the requisite risk reduction to achieve a PL “c” or “d”, several design possibilities may be selected; for example for a PL “d” a structure in accordance with category 2, a channel $MTTF_d$ of “high” and a DC of “medium”. The CCF factor must always be considered from category 2 onwards.

Due to blurring at the borders of various PL’s in the above block diagram, a simplification is also permitted (in the standard there is a table for this rather than chart): refer to Figure 9.

This concludes the short or rough description of EN ISO 13849-1:2006.

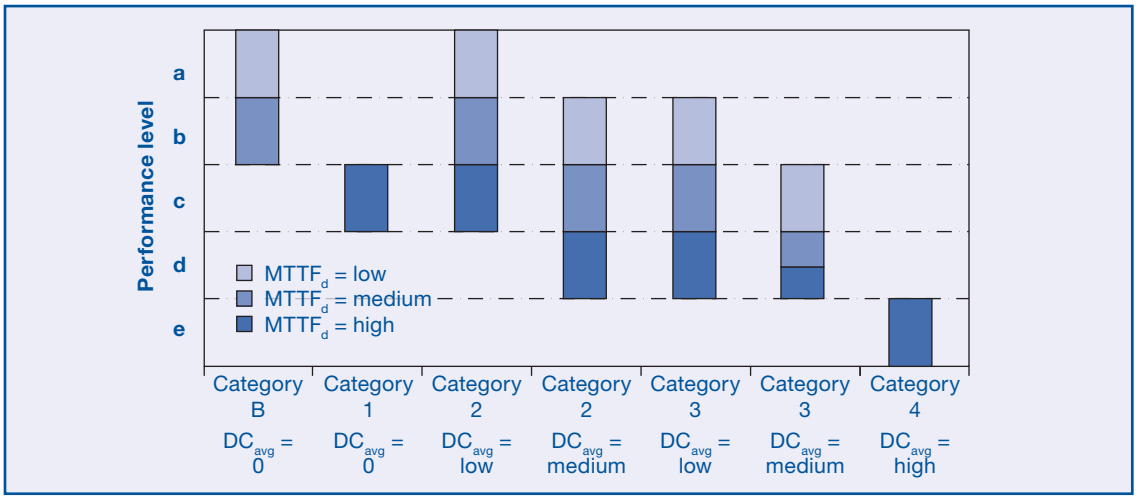
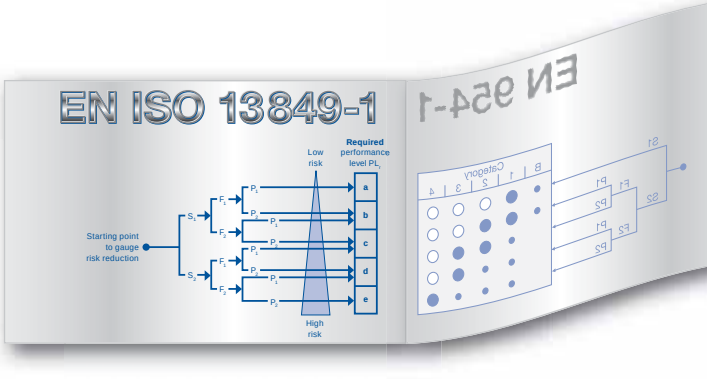


Figure 9: Performance level (PL): alternative determination using table



Designated Architectures

Background
The familiar control categories are taken into account in EN ISO 13849-1:2006 via the so-called designated architectures, which can also be described as the advance calculation of SRP/CS structures. Advance calculation means that the contribution to risk reduction that these structures effect within the framework of the Markov modelling as seen in IEC EN 61 508 has been previously tested, i.e. the user of EN ISO 13849-1:2006 no longer needs to be concerned with these complex mathematical calculations.

Consideration of the designated architecture of an SRP/CS updates the earlier deterministic approach in EN 954-1. However, as already described, it deals solely in the future with one aspect among many which make up the performance level.

If the designated architectures appear familiar you are quite right. They basically deal with nothing other than the familiar, established tried and tested SRP/CS structures for the various control categories which apply to the application of EN 954-1. An exception to this is, however, category 2 (as cited).

Execution
EN ISO 13849-1:2006 thus recognises the designated architectures contained in Figure 10.

Application
The setting up of designated architectures contributes to a positive development towards simplification in EN ISO 13849-1:2006; however, some questions go unanswered (questions which also remain unanswered when it comes to the interpretation of EN 954-1).

These include, for example, the question of how the 2-channel function is to be executed at the sensor and actor level in categories 3 and 4. This means the sensor or actor functions must physically be present twice, for example in the form of two switches on the position monitor of a moving protective device and what action is necessary if one wishes to deviate from the designated architectures.

Many alternatives may be considered:

Option 1 is based on the relevant C standard (product standard) where there are precise design suggestions. For example with a printing and paper machine a single, but electrical 2-channel executed safety switch for the position monitoring of a moving protective device suffices.

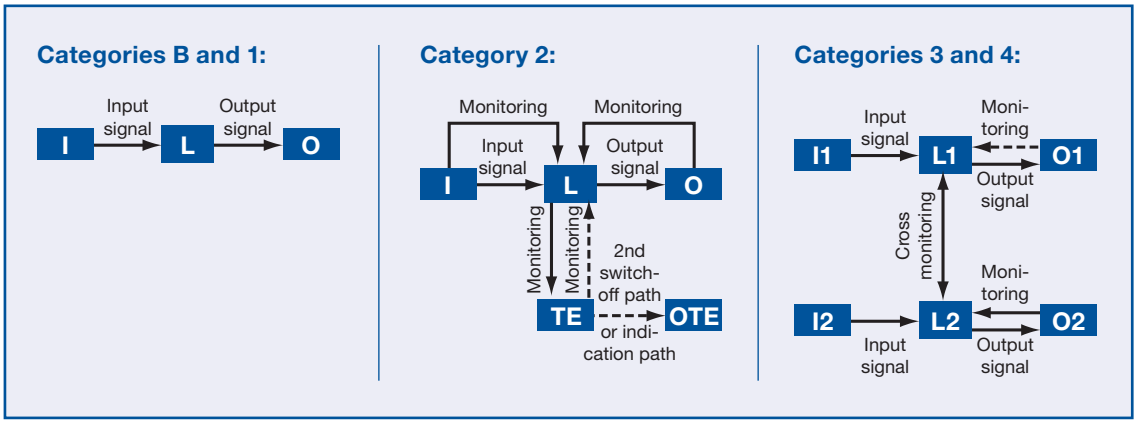


Figure 10: Introduction to Designated Architectures

Option 2 operates using fault exclusion (refer also to Figure 11), whereby as much attention should be paid to the practice of fault exclusion as given to EN 954-1 until now. One can either employ the fault exclusion lists in accordance with Annexes A to D of EN ISO 13849-2 (formerly EN 954-2) or conduct one's own analyses while adhering strictly to Section 3.3 of EN ISO 13849-2.

When can I conduct a fault exclusion?

It is not always possible to evaluate a SRP/Cs without assuming the exclusion of certain faults. For detailed information on fault exclusion refer to EN ISO 13849-2. …

Fault exclusions may be based on:

- The technical improbability of the incidence of certain faults
- The generally accepted technical experience, independent of application
- The technical demands regarding the application and special hazards

When faults are excluded, a detailed explanation must be provided in the documentation.

Figure 11: Fault exclusions

Option 3 is to put aside the simplifications in EN ISO 13849-1:2006 and instead perform mathematical calculations using the Markov modelling, Petri Nets or similar (or have them performed) (refer also to Figure 12).

Is it absolutely essential that I use designated architectures, or is it possible without them?

4.5.1 … There are several methods to make an estimation of the quantifiable aspects of the PL for any type of system (e.g. a complex structure). Methods are e.g. Markov Modelling, Generalised Stochastic Petri Nets (GSPN), Reliability Block Diagrams [see e.g. EN 61508 (IEC 61508) series].

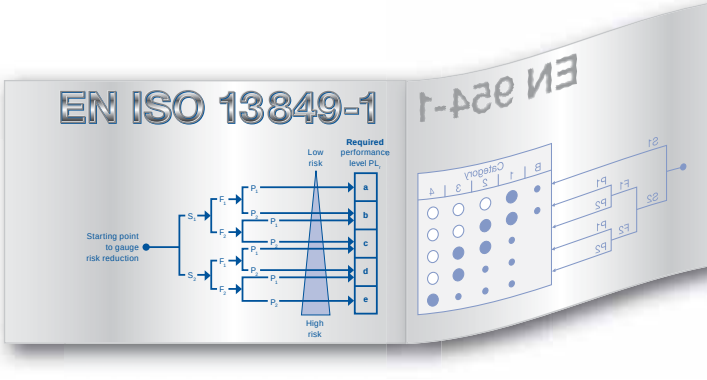
To make easier the assessment of the quantifiable aspects of this PL, this standard provides a simplified method based on the definition of five designated architectures that fulfil specific design criteria and behaviour under fault condition.

Figure 12: "No rules without exceptions"

CAUTION when using the designated architecture for category 2!

Although the description above states that the so-called designated architectures are well-known, there is here a serious exception, and this is the recommended structure for control category 2.

Here a considerable change will occur: where control category 2 has up to now defined a 1-channel structure which must involuntarily be tested at suitable intervals by the machine controls, this will in future when used with designated architecture require a test frequency 100 times higher than the foreseeable demand of the safety function and a second output must be provided (refer also to Figure 13 on Page 15).



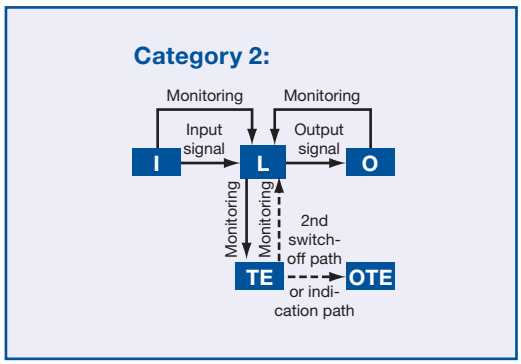


Figure 13: New requirements of control category 2

Basically this designated architecture is like a "light" control category 3 and when, at the end of this report we attempt to summarise which types of changes arise in practice following the process of introducing EN ISO 13849-1:2006, then this summary should include an urgent recommendation to test SRP/CS with control category 2 in respect of the future altered requirements.

$MTTF_d$ values

Background

Firstly in connection with the $MTTF_d$ considerations of EN ISO 13849-1:2006, and despite often suppressing the thought, one must first be aware that SRP/CS also always still have a residual safety-critical failure potential (namely the failure potential of coincident hazardous failures), thus the aim must be to control this residual risk, i.e. to depress this to an acceptable degree of residual risk.

For example, a switching contact cannot be opened or closed. Generally not being able to open with reference to a machine leads to a hazardous state, if there is no redundancy or timely fault identification. But switching contacts are not all the same. There are variances, design differences, material differences etc.

One could also say quality differences exist which can influence the probability of such coincident failures.

This means that $MTTF_d$ is a quality statement about the safety-related reliability of the safety components deployed and the safety-oriented devices in an SRP/CS.

By definition $MTTF_d$ is a statistical mean representing the expected working time without down time per annum (= MTTF), whereby in EN ISO 13849-1:2006 down times are only considered when they indicate a hazardous direction. This is the reason for the terminology $MTTF_d$ (not every failure is a safety-critical failure). Therefore the $MTTF_d$ value is always > an MTTF value. The value is expressed in years (= y).

An $MTTF_d$ value is thereby always the mirror image (the reciprocal value) of the PFH_d value and vice versa. This means a $MTTF_d$ value of 10y, for example, equates to a PFH_d value of 1.14×10^{-5} (1/10 x 8,760), however only with reference to one channel[1].

With considerations of MTTF or $MTTF_d$ an exponential distribution of coincident failure is assumed, i.e. after the MTTF or $MTTF_d$ sequence 63% of all (hazardous) units have already failed and the probability of survival of the relevant units considered after the MTTF or $MTTF_d$ sequence only constitutes 37% (refer to Figures 14 and 15).

1) PFH values, which were calculated in accordance with IEC EN 61508, may be included in calculations in accordance with EN ISO 13849-1:2006 as long as the SIL details are taken into account. This produces a simplified view – in particular for 2-channel structures – but there is less risk of calculating methods which "paint a rosy picture".

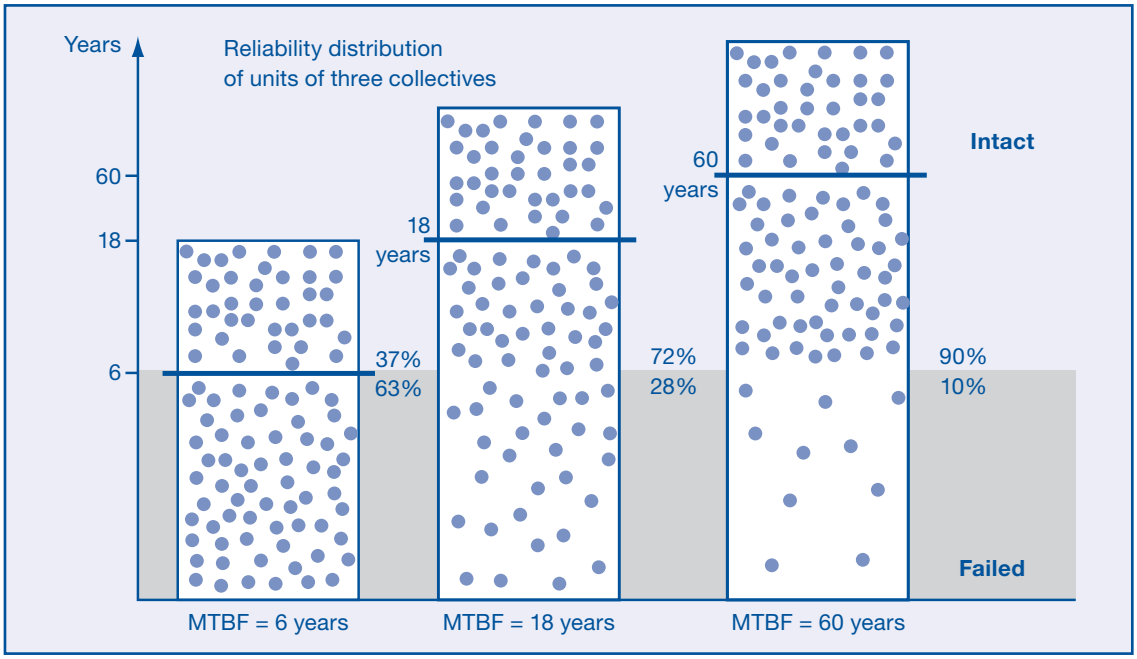


Figure 14: Illustration of mean service life: three collectives with differing reliability levels are represented. Their units (illustrated by the dots) fail at coincidental times. The vertical coordinates indicate their failure time. The failure times are spread over long time spans, e.g. in the case of the first collective some individual units last for 18 years while others have already failed after one year. 63% have already failed after 6 years. (Source: introduction to the methods of reliability analysis, SIEMENS AG, 1&S IS ICS IT2)

In other words:

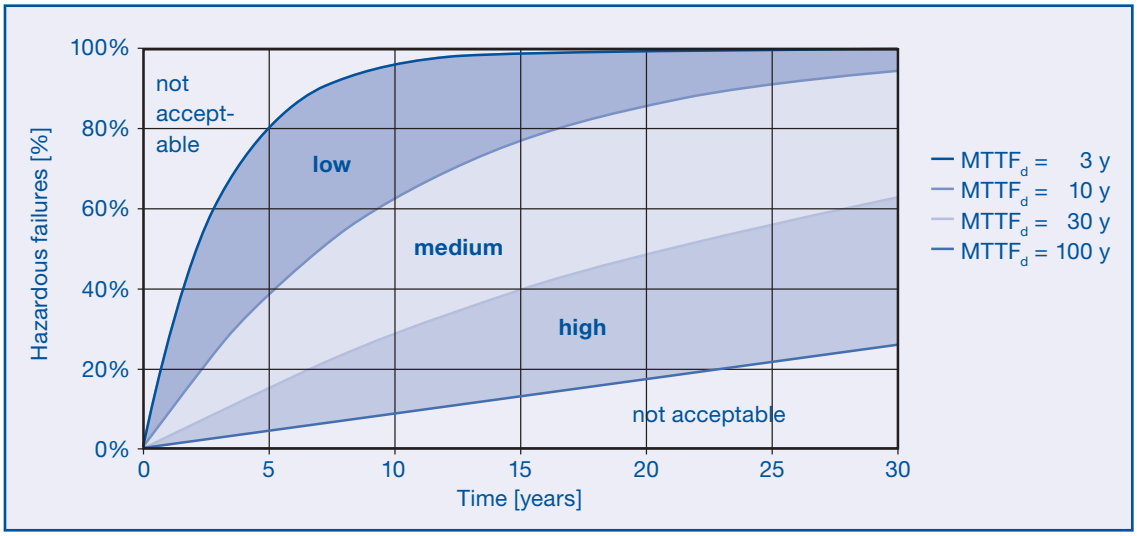
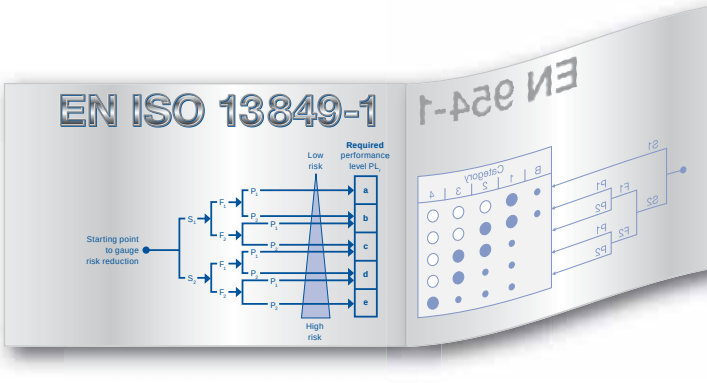


Figure 15: What does MTTF$_d$ exactly mean?



CAUTION: Exceptions to this assumed exponential distribution which is typical of electronics are components affected by wear and tear which have a different lifetime distribution. This factor applies to EN ISO 13849-1:2006 via the intermediate size of the so-called B_{10d} value calculation (as cited).

Execution
In terms of EN ISO 13849-1:2006, considerations of $MTTF_d$ and PFH are to be differentiated according to whether they are utilised

- for a single safety component
  or
- for a single channel of an SRP/CS
  or
- for a complete SRP/CS.

The above mentioned differentiation makes sense only when considering the fact that a large section of the clientele using EN ISO 13849-1:2006 safety components and other devices do not manufacture these themselves, rather they purchase them and integrate them into an SRP/CS.

In the future it will be easiest for this section of EN ISO 13849-1:2006 users, i.e. those who purchase ready to use safety components, for example from the product range of a company in the Schmersal Group, because it is assumed that all well-known manufacturers will include values in line with EN ISO 13849-1:2006 in their data sheets.

The purchaser of safety components can justifiably expect from his supplier that he has these values ready on time, before EN ISO 13849-1:2006 takes effect, i.e. with regard to time this may not be here and now, but should at least be expedient (refer here also to the section “Enactment of EN ISO 13849-1:2006”.

But others using components/devices can also expect to be provided with figures from suppliers, which within the strict terms of the EC machine directive (MRL) are not necessarily safety components but rather dual-use products, i.e. components/devices which can be deployed in both safety-relevant and operational tasks.

CAUTION! If a fault exclusion is formulated for a component, the $MTTF_d$ value in the relevant formula is taken to be ∞ (as cited).

Application:
$MTTF_d$ for a single channel
In this case with reference to the formula in Figure 16 the user needs only to add together the individual $MTTF_d$ values of components of an SRP/CS using the so-called parts count method. Refer also to the calculation example on Page 18.

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

Figure 16: $MTTF_d$ per channel (parts count method)

The sum is then compared with the values of the following tables (refer to Figure 17) to indicate the safety-related quality of a single channel of an SRP/CS.

Description of quality	Value range $MTTF_d$
low	3 years ≤ $MTTF_d$ < 10 years
medium	10 years ≤ $MTTF_d$ < 30 years
high	30 years ≤ $MTTF_d$ ≤ 100 years

$MTTF_d$ is a statistical mean value and does not guarantee lifetime!

Figure 17: $MTTF_d$ is a statistical mean value of operational time without dangerous failure in a single control channel

Calculation example

j	Component	Units (n_j)	$MTTF_{d,j}$ worst case [y]	$1/MTTF_{d,j}$ worst case [1/y]	$nj/MTTF_{d,j}$ worst case [1/y]
1	Transistors, Bipolar, low power	2	1142	0.000876	0.001752
2	Resistor, Carbon film	5	11416	0.000088	0.000438
3	Capacitor, Standard, no power	4	5708	0.000175	0.000701
4	Relay (data from manufacturer)	4	1256	0.000796	0.003185
5	Contactor	1	32	0.031250	0.031250
$\Sigma(n_j/MTTF_{d,j})$					0.037325
$MTTF_d = 1/\Sigma(n_j/MTTF_{d,j})$ [y]		**26.79**			

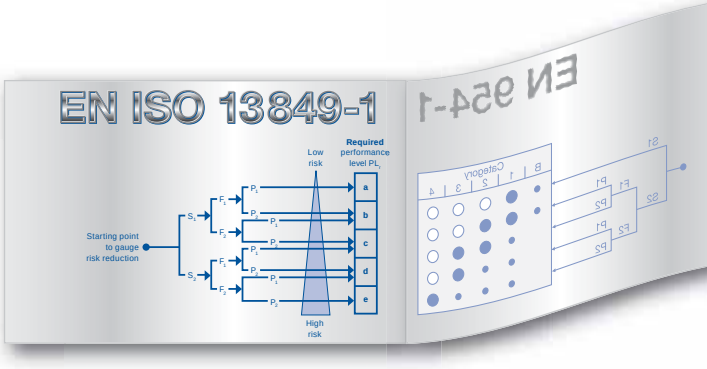
This example gives a $MTTF_d$ of 26.8 years, which is "medium" according to figure 17.
In this example the main influence comes from the contactor. In general the result will be much better, that is, a higher $MTTF_d$.

In addition the following “rules” apply:

- $MTTF_d$ values always apply to one channel, i.e. it is of no relevance whether we are dealing with a 1 or 2-channel structure (designated architecture), unless the channels have been differently (diversely) structured. In this case a so-called symmetrisation formula applies (refer to Figure 18).

- The manufacturer (or person distributing the machine) is responsible for calculating (or having somebody calculate) the $MTTF_d$ value of a channel within the terms of the EC machine directive.

- **CAUTION!** If the calculation produces several $MTTF_d$ values for a channel which are > 100 y, the excessive value is “cut off”, i.e. a single SRP/CS channel may only have one maximum $MTTF_d$ value of 100 y (in contrast to a [safety] component which, looked at in isolation, may well be higher). With this restriction of 100 y, the standard-setter aims to prevent the “painting of a rosy picture” with regard to $MTTF_d$ values in order to attain a higher performance level or enable calculation methods to be used to substitute 1-channel structures when 2-channel structures are required.



- **The designated architectures assume the same $MTTF_d$ for both channels.**
- **Symmetrisation formulae for differing $MTTF_d$ values:**

$$MTTF_d = \frac{2}{3}\left[MTTF_{d\,C1} + MTTF_{d\,C2} - \frac{1}{\frac{1}{MTTF_{d\,C1}} + \frac{1}{MTTF_{d\,C2}}}\right]$$

- **Example: $MTTF_{d\,C1}$ = 3 years, $MTTF_{d\,C3}$ = 100 years leading to $MTTF_d$ = 66 years**

Figure 18: Differing $MTTF_d$ per channel –> symmetrisation

- CAUTION! The merging of the single safety-oriented devices to one SPP/CS is conditional upon the following:
  - that the application takes place under strict consideration of any information in the relevant user instructions and
  - additional fault exclusions are guaranteed– particularly with reference to electrical wiring – in accordance with ISO 13849-2 (as cited).
- Where software is involved, the additional requirements of EN ISO 13849-1:2006 apply (refer to Section 4.6).
- The so-called symmetrising formula takes effect if two channels of an SRP/CS have been differently structured (refer to Figure 18).

Remarks

- If individual components or devices which are designed for an SRP/CS lend themselves to IEC EN 61508 (or IEC EN 62061) oriented manufacturers, then in general a so-called Lambda value (λ) is given. This value in terms of prEN IO 13849-1 can be equated with a PFH_d value.

  If, however, one wants or has to roam between the "worlds" of EN ISO 13849-1:2006 and IEC EN 61508 (or IEC EN 62061) for safety components and safety-oriented devices (refer here also to Page 44), then we recommend that this is done via the performance or SIL level.
- If only one MTTF value is available (i.e. no $MTTF_d$ value), the MTTF value may be doubled (under the assumption that dangerous and harmless failures are roughly evenly balanced) in order to arrive at an $MTTF_d$ value. EN ISO 13849-1:2006 furthermore recommends that when in doubt let only one part (suggestion is 10%) flow into the calculation, in order to err on the side of caution.
- If only one MTBF value is available, to simplify matters one can usually treat it as an MTTF value.

Application: $MTTF_d$ calculation for a single safety-oriented device

This applies to those building safety-oriented devices, control systems as well as dual-use products for their own use. For them the rule is to break down relevant safety-oriented equipment into its functional components and – again likewise – to calculate the $MTTF_d$ value using the so-called parts count method (as cited).

Here, too, EN ISO 13849-1:2006 offers help in the event that no MTTF or $MTTF_d$ value of one's own is available, by providing typical values in the standard in the tables in annex C for individual electrical and electronic components (refer to Figure 19). Further works of reference are, for example, the SN 29500 standard or MIL hand books.

Tables C.2 to C.7 name typical $MTTF_d$ values for electric components from SN 29500, e.g.:

Component	Example	MTTF [y] component	$MTTF_d$ [y] typical	$MTTF_d$ [y] worst case	Dangerous failures
Bipolar transistor	TO18, TO92, SOT23	34,247	68,493	6,849	50%
Suppressor diode		15,981	31,963	3,196	50%
Capacitator	KS, KP, MKT, MKC …	57,078	114,155	11,416	50%
Carbon film resistor		114,155	228,311	22,831	50%
Optocoupler with bipolar output	SFH 610	7,648	14,840	1,484	50%

Figure 19: $MTTF_d$ for electrical components (extract/examples)

Components/devices affected by wear and tear in an SRP/CS receive especial consideration in EN ISO 13849-1:2006, because here the demand (namely the demand mode) has a substantial bearing on the $MTTF_d$ value.

Only electronic components and safety-relevant devices have a direct $MTTF_d$ value, because here the so-called bath curve can be referred to as an indicator of failures which are independent of wear and tear. Both the left part (keyword: early failures) and the right part of the bath curve are disregarded. The left part is disregarded because any early failures will have been addressed through appropriate measures by the manufacturer, such as artificial aging. The right part is excluded because it is assumed that it lies far beyond the actual duration of use.

B_{10d} values
There are intermediate sizes for an $MTTF_d$ conversion, the first of which being the B_{10d} value, used with components affected by wear and tear, such as for example electromechanical or fluidic devices as well as mechanical components. This value is equivalent to a kind of operating cycle capacity, whereby safety-related function is deemed tolerable when considered using the Weibull approach.

The B_{10d} value is converted bearing in mind the application conditions, i.e. considering the duration of use and the mean demand mode of the safety function of the relevant component in an $MTTF_d$ value (refer to Figure 20).

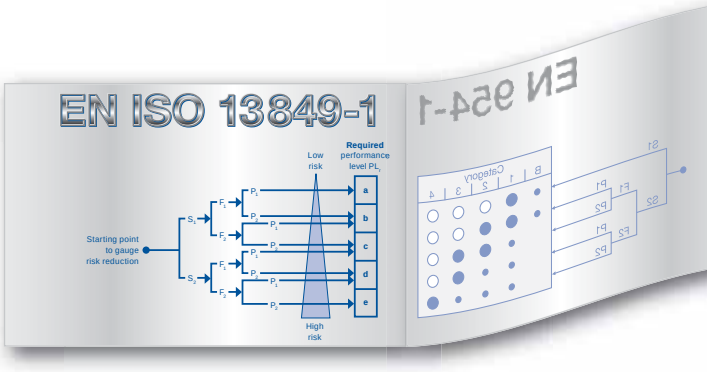
- **The manufacturer supplies the B_{10d} value for the component** (value in operating cycles, whereby statistically 10% of the samples tested are dangerous failures).
- **The mean switching frequency of application must be determined e.g. 0.2 Hz => interval t_{cycle} = 5 s.**
- **Conversion of B_{10d} (operating cycle) to $MTTF_d$ (years):**

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

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

d_{op} = average number of operating days per annum
h_{op} = average number of operating hours per day
n_{op} = mean number of operating cycles annually
t_{cycle} = average demand of the safety function in s (for example 4 x per hour = 1 x per 15 min. = 900 s)

Figure 20: Calculation of $MTTF_d$ for components with wear and tear



Mechanical components	$MTTF_d$ = 150 years
Hydraulic components	$MTTF_d$ = 150 years
Pneumatic components	B_{10d} = 20,000,000
Relays/contactors (with small load)	B_{10d} = 20,000,000
Relays/contactors (with maximum load)	B_{10d} = 400,000
Main contactor (small load)	B_{10d} = 20,000,000
Main contactor (maximum load)	B_{10d} = 2,000,000
Emergency stop device	B_{10d} = 10,000
Control device (push button)	B_{10d} = 100,000

Factor of 50

Figure 21: B_{10d} values (extract) in accordance with standard

In addition (refer to Figure 21) prEN ISO 13849-1 offers recommendations for deciding which B_{10d} values to adopt for typical devices affected by wear and tear should no indications be given by the manufacturer.

These are differentiated according to whether the respective device is operated at "full load" or lower (for example in respect of contactors and relays). Here "full load" is not only meant in the electrical sense, but also for example in the sense of particularly unfavourable environmental operating conditions, i.e. marginal operating conditions in general.

The scale for small load is defined in the standard as 20%, however the representation of intermediate values – although not linear – may be "allowed", for example (at 20.0 million operating cycles and 20%) 7.5 million operating cycles at 40%, 2.5 million operating cycles at 60% and 1.0 million operating cycles at 80%.

t_{cycle} =	24 h	1 h	1 min.	1 sec.
Pneumatic components	547,945	22,831	380	6.3
Relay/contactors (small load)	547,945	22,831	380	6.3
Relay/contactors (maximum load)	10,960	457	7.6	0.1
Main contactor (with small load)	547,945	22,831	380	6.3
Main contactor (with maximum load)	54,794	2,283	38	0.6
Emergency stop device	274	11	0.2	0.003
Control device (push button)	2,739	114	1.9	0.032

$MTTF_d$ > 100 years

Figure 22: Converted $MTTF_d$ for pneumatic and electromechanical components depending on the demand mode (t_{cycle})

There is an exception for mechanical and hydraulic components that deviate from the calculation loop. Here the standard-setter has determined $MTTF_d$ values of 150 y unaffected by demand mode on the base of empirical tests[1].

Figure 22 shows a conversion example of B_{10d} values into $MTTF_d$ values based on diverse demand modes (1 x per 24 hours, 1 x per hour etc) (whereby this assumes a 24 hour operation on 365 days of the year).

T_{10d} values

CAUTION! The so-called T_{10d} value, which is derived from consideration of the B_{10d} value, is also in the EN ISO 13849-1:2006, and this corresponds to 10% of the calculated $MTTF_d$ value. In connection with this comes the recommendation that safety-oriented devices and other safety-relevant devices should be replaced when they reach the T_{10d} value as a precautionary measure.

Good engineering practices

When calculating $MTTF_d$ values, EN ISO 13849-1:2006 prefers to use manufacturer's specifications and only then resort to the abovementioned simplified methods, i.e. the use of the tables which enable missing $MTTF_d$ values to be sought where necessary.

However, at the same time general conditions are stipulated, particularly with regard to the use of the tables which – as indicated in Figure 24 – must additionally be considered.

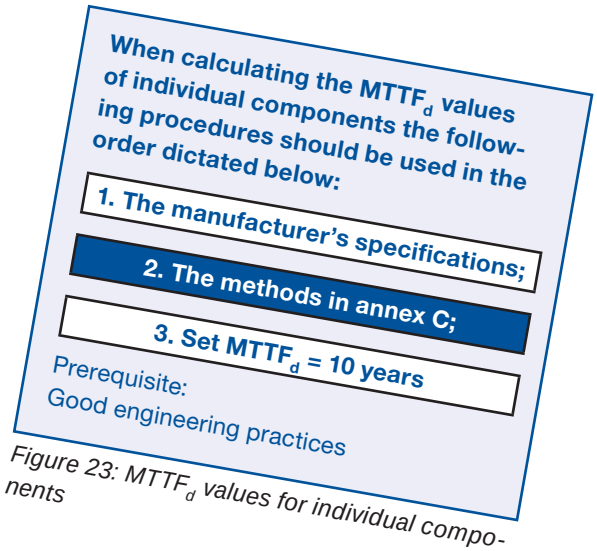


Figure 23: $MTTF_d$ values for individual components

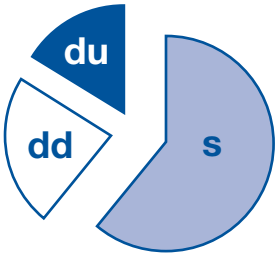
- **Basic, tried and tested safety principles (EN ISO 13849-2) considered when designed;**
- **Specification by the manufacturer of appropriate applications and permitted operating conditions;**
- **Basic, tried and tested safety principles considered during the installation and operation of the component**

➥ **Bearing these conditions in mind, the failure modes stipulated in the standard apply.**

➥ **The manufacturer, installer and operator are obliged to abide by these conditions.**

Figure 24: Good engineering practices

1) BIA Report 6/04, examination of the aging processes of hydraulic valves, www.hvbg.de/bgia. Web code: 1006447



$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \lambda_{du}}$$

Failure mode of detected dangerous failures
Failure mode of all dangerous failures

Figure 25: Diagnostic coverage DC

Diagnostic coverage

Background
While the requirements in EN ISO 13849-1:2006 in respect of $MTTF_d$ calculations remain, in spite of everything, relatively easy to understand and straightforward (once the mental hurdle of the probability consideration and the search for the values has carefully and successfully been completed), some allowances must be made when examining the so-called diagnostic coverage (DC).

This is concerned with the ratio of detected dangerous failures to the failure mode of all dangerous failures and the quantification of the efficacy of measures to uncover failures in an SRP/CS.

This assumes that (a) failures can occur (see $MTTF_d$) and (b) that mechanisms for detecting such failures – also when accounting for the timeline – are not equally effective and that there is even a proportion of undetected failures.

This too is apparent, particularly because not every failure in an SRP/CS can be immediately detected, but sometimes is only noticed when the safety function is next demanded; for example, when opening a moving protective device one thinks of a bridged electromechanical safety contact or a welded relay.

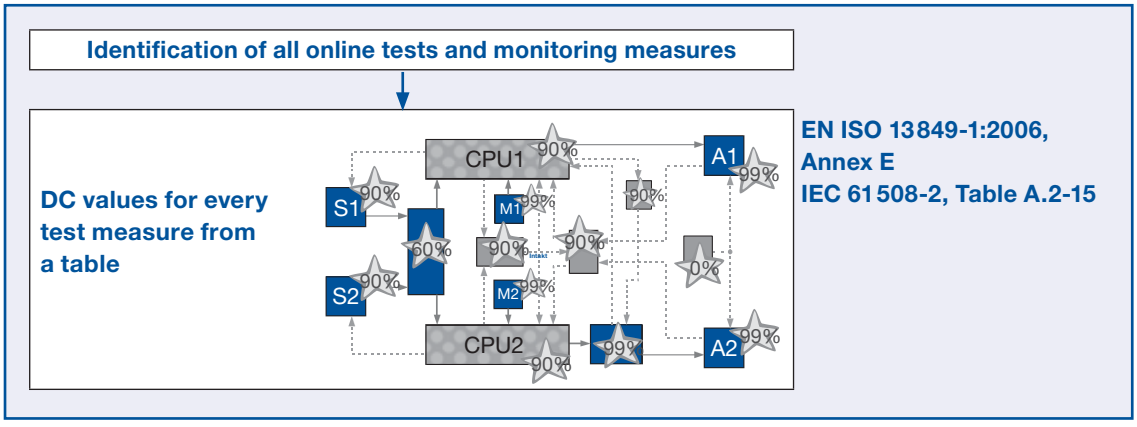


Figure 26: Determination of the average DC for the total system, Part 1

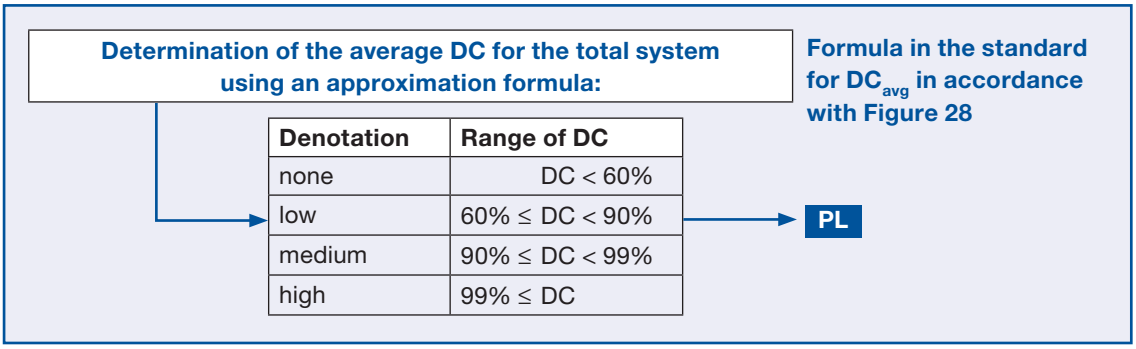


Figure 27: Determination of the average DC for the total system, Part 2

The subject of "failure recognition" is of particular significance from a safety-relevant point of view, notably to avoid so-called fault accumulation. This means avoiding a situation whereby one remaining undetected fault in an SRP/CS is joined by a second fault (a so-called second fault) which would make the safety function obsolete.

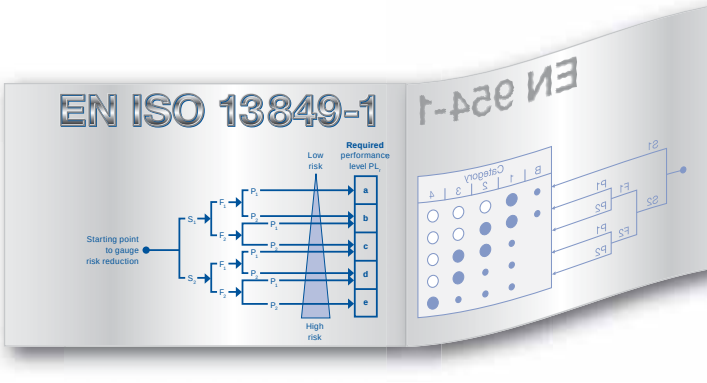
When one considers empirical examinations which show that a simple redundant system with fault detection has a better safety performance than a multiply redundant system without fault detection, this plainly illustrates the particular importance of the quality of fault detection – apart from the fact that they are cost effective.

Execution
In the interests of simplicity, EN ISO 13849-1:2006 also divides the quality of fault detection (the so-called diagnostic coverage) into steps (refer to Figure 27).

With annex E, EN ISO 13849-1:2006 offers further simplification still (refer to Page 25).

	Measure	DC
Relay/ contactor	Plausibility test, e.g. application of positively driven NO and NC contacts	99%
Actor	Monitoring of outputs via 2-channels without dynamic tests	0–99% depending on the signal changes in the application
Sensor	Monitoring of certain properties (reaction time, area of analogue signals, e.g. electric resistors, capacity)	60%
Logic	Self-testing using software	60–90%

Figure 29: Examples for coverage



- **Only an average value for DC_{avg} enters the PL, which must be weighted across all tests.**
- **Weighting factor is the $MTTF_d$ of the *tested* parts:**

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

- **Untested parts are entered as DC = 0. All parts which cannot demonstrate a fault exclusion enter the sum (fault exclusion => $MTTF_d = \infty$).**

Figure 28: Average diagnostic coverage DC_{avg}

Application

An average value DC_{avg} is calculated which reflects the fault detection quality of all parts of each channel.

The $MTTF_d$ values of the safety-oriented components/devices which go to make an SRP/CS channel flow into the consideration in so far as a combination of a “bad” $MTTF_d$ and a “bad” single DC are more heavily weighted, thus the DC_{avg} is forced down (and vice versa).

This inductive approach when calculating the fault detection mode DC_{avg} may make sense. Nevertheless it does not exactly serve the interests of simplification, even if there is a comprehensive look-up table in annex E of EN ISO 13849-1:2006.

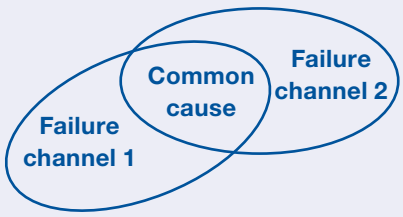
A multitude of diverse tried and tested measures for fault detection with a DC evaluations as a percentage are listed in annex E, but there are some occasions where the evaluation of a measure in the table is given as “0 … 99% depending on …” which leaves a great deal of leeway – something which EN ISO 13849-1:2006 actually seeks to avoid and which seriously requires greater analysis, as has been the case with IEC EN 61508.

Common cause failure management (CCF)

Background
In addition to the designated architectures, the $MTTF_d$ calculation and the DC analysis, the performance level of an SRP/CS is determined by considering the so-called common cause failure management (CCF) parameter 4.

This is the case (is only required) for 2-channel structures from category 2 onwards, because here measures apply which are designed to combat failures in an SRP/CS with a common cause and effect.

The effect of such failures is that they can bring both channels into a safety-related critical failure mode at the same time, e.g. through lightening (a surge effect), thus affecting redundant semi-conductor outputs with the result that both channels are simultaneously "robbed" of their capability to switch on or off.



Measures to protect against CCF are required for multiple channel structures (cat. 2, 3, 4) which, in accordance with IEC 61508-6 annex D, correspond to a β factor of 2% or lower.

Figure 30: Common cause failures (CCF)

Execution
The easiest way in prEN 13849-1 to analyse the methods used to combat CCF failures is the application of a points table in which the individual methods are listed and evaluated with a points system.

Due to the motivation behind CCF examinations, measures such as clear separation of the signal path, diversity or special EMC hardening naturally gain "many" points (the same applies to measures to protect against power surges or overpressure, as well as filter measures in the case of fluidic technology).

A maximum of 100 points can be gained; at least 65 points must be attained to fulfil the requirements of prEN 13849-1 in respect of this feature.

This is equivalent to the so-called β-factor of 2% correspondingly to IEC EN 61508.

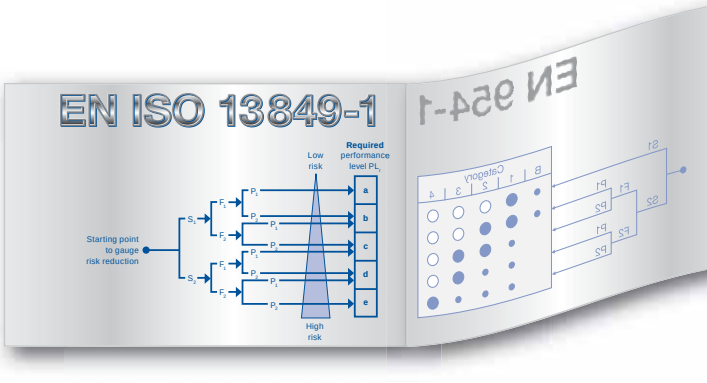
CCF: Failures of diverse parts through common parts

List of measures with points system (maximum sum: 100 points)

• Separation of the signal path	15 points
• Diversity	20 points
• Protection against e.g. surge/overpressure	15 points
• Tried and tested components	5 points
• FMEA	5 points
• Competence/training of developer	5 points
• EMC or filtering of pressure medium and protection against contamination	25 points
• Temperature, dampness, shock, vibration etc.	10 points

Objective: at least 65 points

Figure 31: Measures to combat common cause failures (CCF)



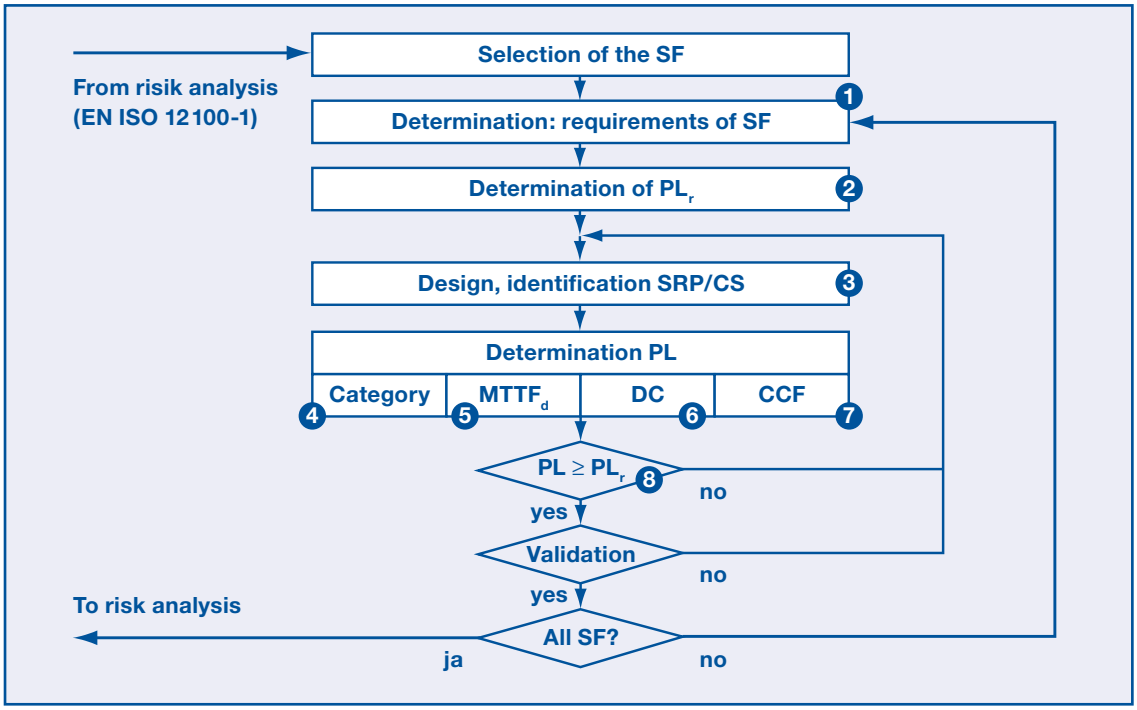


Figure 32: Iterative design and development process in accordance with prEN 13849-1

Example

Firstly, the iterative design and development process in EN ISO 13849-1:2006 is also present in a suitable version as is the case with EN ISO 12100-1, i.e. here too it is theoretically divided into 8 steps, beginning with the selection of a safety function (1) then on via steps (2) … (7) to the decision whether the requisite PL_r has been attained (8).

The above example (refer to Figure 33) relates to the interlocking of moving guards, i.e. a hazardous movement is stopped when the protective device is opened, with no re-engaging possible while open etc. (refer also to EN 1088: safety of machines – interlocking devices associated with guards – principles for design and selection).

❶

Example:

- Interlocking of a guard

Safety function

- Hazardous movement is stopped when the guard door is opened

Figure 33: Selection and determination of safety function requirements

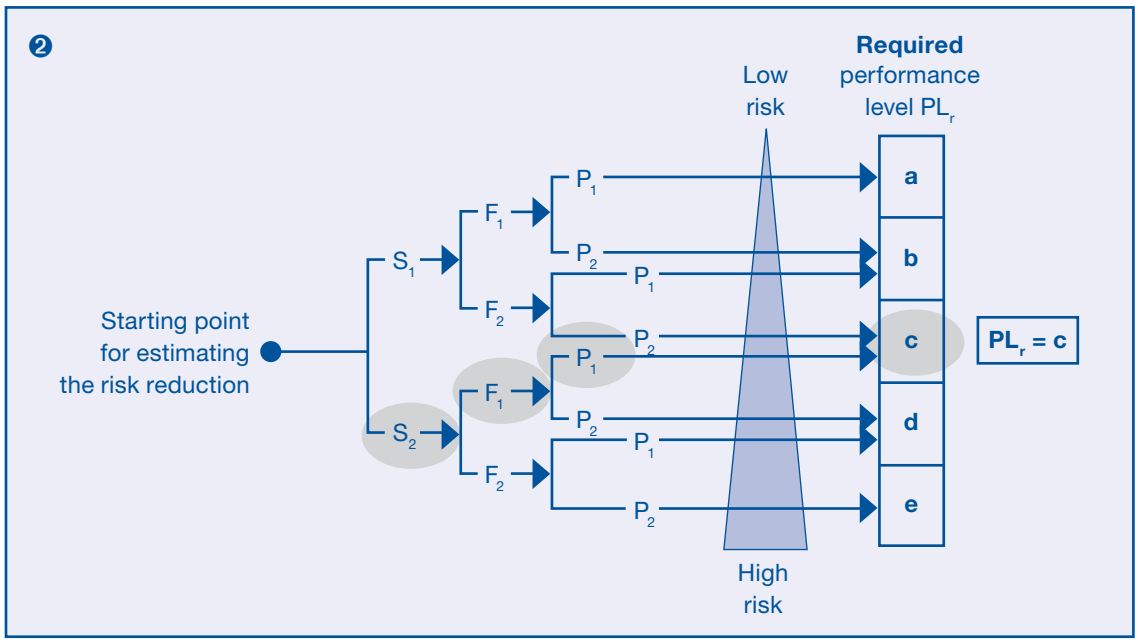


Figure 34: Determining the PL_r

To determine the requisite performance level, i.e. the risk graph consideration in the new version of prEN 13849-1, should result in a PL_r of "c" (refer to Figure 34).

Refer to Figure 35 for discussion of an SRP/CS structure (designated architecture).

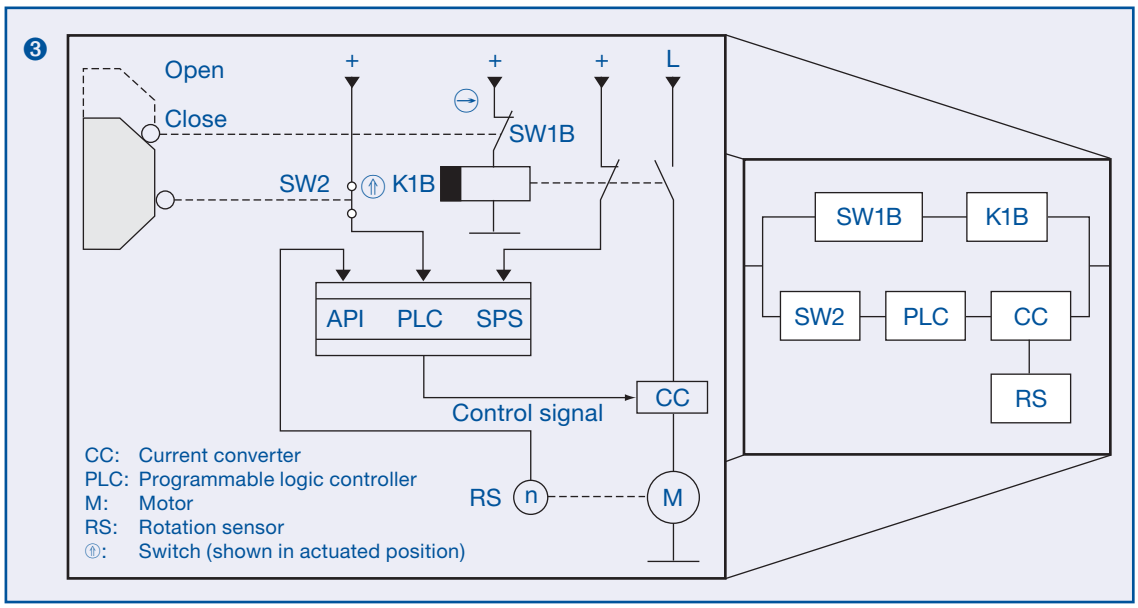
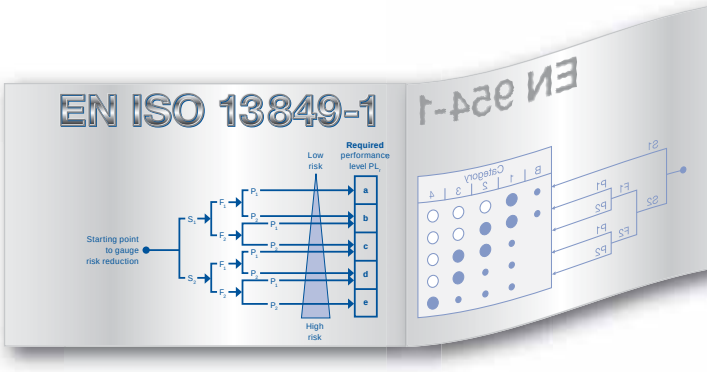


Figure 35: Design and identification of an SPS/CS



Based on the designated architecture in accordance with Figure 35 this means:

❹

- Fulfills the requirements of category B ✔
- Single failure do not lead to loss of SF? ✔
- Partial fault detection ✔
- An accumulation of undetected faults does not lead to loss of the SF? (1st SPS fails without being detected, 2nd channel A fails) ✔

–> Category 3 can be achieved

Figure 36: Determination of the PL category

Because both channels in the example are constructed differently (refer to the SRP/CS structure), differing $MTTF_d$ values for the two channels A and B must first be determined and symmetrised with each other.

❺

- **SW1B: positive opening contact:** Fault exclusion for non-opening of the contacts, non-activation of the switches due to mechanical failure (e.g. plunger break, wear and tear of actuating lever, misalignment)
- **K1B: $MTTF_d$ = 30 y (manufacturer's specification)**

$$\frac{1}{MTTF_{d\,C1}} = \frac{1}{MTTF_{d\,K1B}} = \frac{1}{30\ y}$$

Channel 1: $MTTF_d$ = 30 y

Figure 37: Determination of the PL: $MTTF_d$ for channel A

❺

- **SW2, SPS, CC: $MTTF_d$ = 20 y each (manufacturer's specification)**

$$\frac{1}{MTTF_{d\,C2}} = \frac{1}{MTTF_{SW2}} + \frac{1}{MTTF_{PLC}} + \frac{1}{MTTF_{CC}} = \frac{3}{20\ y}$$

Channel 2: $MTTF_d$ = 6.7 y

- **$MTTF_d$ symmetrised for both channels:**

$$MTTF_d = \frac{2}{3}\left[MTTF_{d\,C1} + MTTF_{d\,C2} - \frac{1}{\frac{1}{MTTF_{d\,C1}} + \frac{1}{MTTF_{d\,C2}}}\right]$$

$MTTF_d$ = 20 y (medium)

Figure 38: Determination of the PL: $MTTF_d$ for channel B and total $MTTF_d$

Below is an analysis of the diagnostic coverage (DC):

❻

- DC_{K1B} = 99%, "high" due to the positively driven electric contacts from the table in annex E.1
- DC_{SW2} = 60%, "low" due to the monitoring of the entry signals without dynamic tests
- DC_{PLC} = 30%, "none" due to the low effectiveness of the self-tests
- DC_{CC} = 90%, "medium" due to the reduced switch off distance with actor monitoring by the controller, refer to table in E.1 from table in annex E.1

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

DC_{avg} = 67% (low)

Figure 39: Determination of the PL: DC_{avg}

Below is the determination of the CCF management:

❼

CCF: Failures of various parts through common causes

• Separation of the signal paths	15 points
• Diversity	20 points
• Protection against e.g. surge/overpressure	0 points
• Tried and tested components	5 points
• FMEA	5 points
• Competence/training of the developer	0 points
• EMC or filtering of the pressure medium and protection against contamination	25 points
• Temperature, dampness, shock, vibration etc.	10 points

Σ = 80 points > 65 points

Figure 40: Determination of the PL: CCF

… and – finally – the arrangement in the block diagram, i.e. the verification whether PL => PL_r (refer to Figure 41).

Remarks: Remarks: naturally the meticulous breakdown in the individual stages of the above example has been somewhat exaggerated. Furthermore the example illustrates two differing constructed channels on both the sensor side and logic side, and it thus looks rather more complex than those frequently used in practice.

Nevertheless: this demonstrates the thoughts behind the new requirements of EN ISO 13849-1:2006, although in the example no B_{10d} value consideration was employed for the interlocking device (as an electromechanical device) – which would actually be (more) accurate.

❽

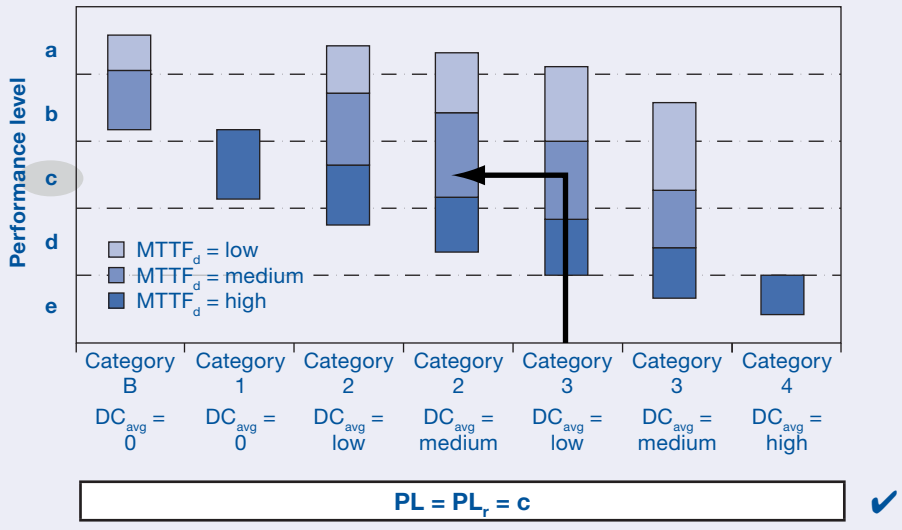
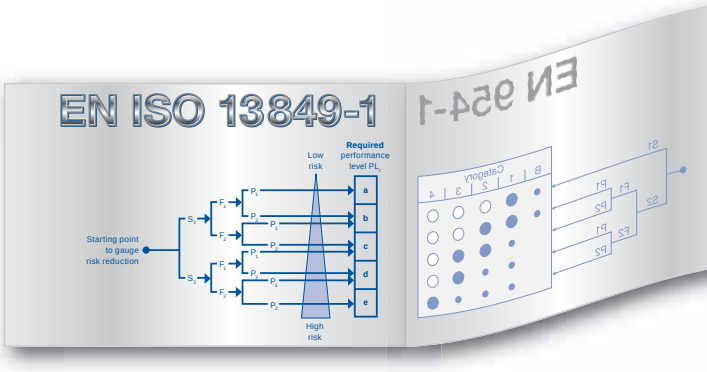
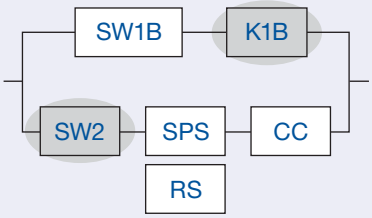


Figure 41: Verification of whether PL ≥ PL_r has been achieved



Have you noticed anything?

Safety-oriented block diagram:



$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}$$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3.600 \frac{s}{h}}{t_{cycle}}$$

n_{op} = medium number of operating cycles per annum

Figure 42: Electromechanical components do have a B_{10d} value

The B_{10d} value would then prompt a new calculation of $MTTF_d$ for K_{1B} and SW2 as follows, if we assume a protective device is operated 240 days per year for 16 hours a day, with an average demand mode of 20 s:

Assumption: 240 days / 16 hours / access every 20 s

$$n_{op} = \frac{240 \cdot 16 \cdot 3{,}600}{20} = 691{,}200 \frac{\text{switching cycles}}{\text{year}}$$

$$MTTF_d = \frac{20{,}000{,}000}{0.1 \cdot 691{,}200} = 289 \text{ years}$$

The maximum operating time intended according to the standard:
$T_{10d} = B_{10d}/n_{op} = 28.9$ years

Figure 43: Calculation of $MTTF_d$ for K_{1B} and SW2

In the example the risk graph assumption F1 would however no longer hold (see above: exposition of hazards seldom to more often and/or short exposition duration). Rather F2 should be assumed, and with it the required performance level “d”. Thanks to the corrected and “good” $MTTF_d$ value however this too poses no problem.

Editorial remark:
The necessary correction loop in the above example shows that the setting of standards is also an iterative process, for the example actually stems from the standard although it was created at a point in time when B_{10d} value considerations had not yet been included. But B_{10d} value considerations are the very ones which for the user constitute a fundamentally significant part of the standard. Without them prEN 13849-1 would have problems justifying its specific requirements with regard to actual practicability.

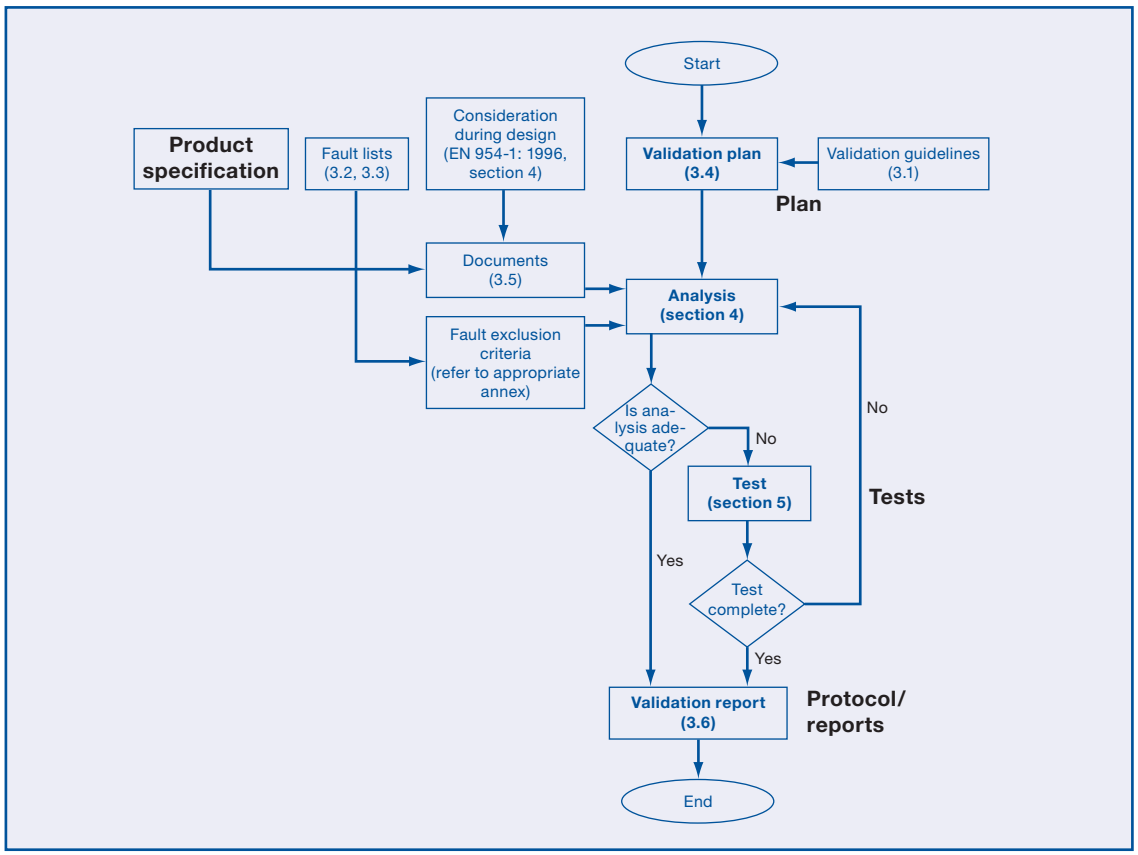


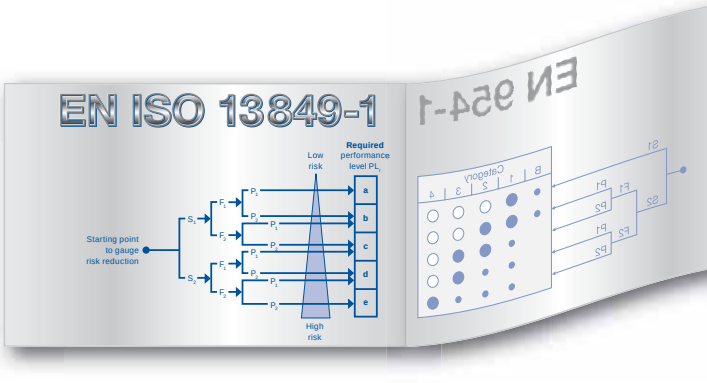
Figure 44: Validation plan in accordance with EN ISO 13849-2

Validation[1]

Subsequently, the validation follows in accordance with EN ISO 13849-2, but this will not be examined in detail here as the considerations to be followed must already be observed today.

EN ISO 13849-2 is concerned with content originally planned for the EN 954-2 standard which – once passed – was, however directly transferred to the ISO level. But a revision is expected here sooner or later in order to align editing as of 1998/1999 and references to EN 954-1 with the current state of affairs – in other words EN ISO 13849-1:2006.

1) There is no detailed examination here of measures to combat systematic failure because these too already form part of the total requirements of SRP/CS. A detailed representation can be found in annex G of EN ISO 13849-1:2006.



Nevertheless: when one considers that the majority of machine accidents cannot be attributed to coincident failures, but can be linked to specification faults and subsequent alignments and alterations, then the subject of validation is the very one that is of major significance to the safety of a machine.

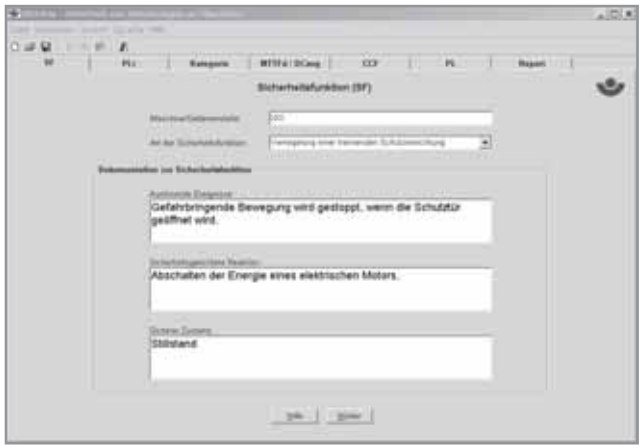
In addition the informative annexes from EN ISO 13849-2 play an important role in connection with EN ISO 13849-1:2006. The annexes – which are split into the technologies of mechanics (annex A), pneumatics (Annex B), hydraulics (Annex C) and electrics (Annex D) – consist of the following lists:

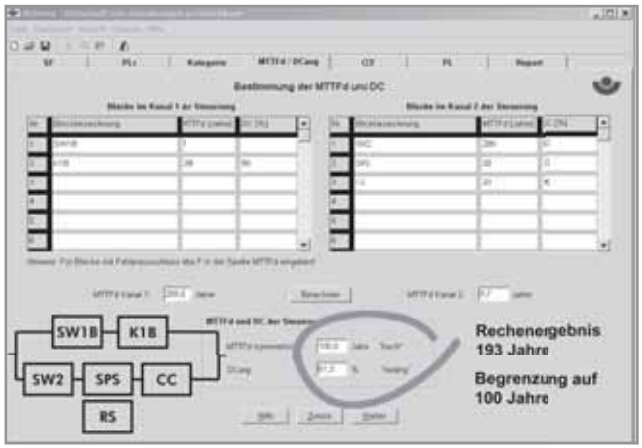
- Fundamental safety principles (important for EN 954-1 control category B and PL “a”);
- Tried and tested safety principles (important for EN 954-1 control category 1 et seq. and PL “b” … PL “e”);
- Safety-related tried and tested components (important for EN 954-1 control category 1 and PL “b”);
- And lists of applicable faults and permissible fault exclusions (important for EN 954-1 control categories 2, 3 and 4 and PL “c” … PL “e”).

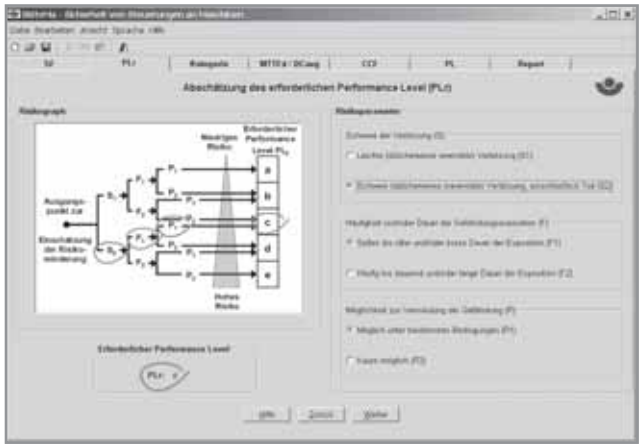
SiSteMa

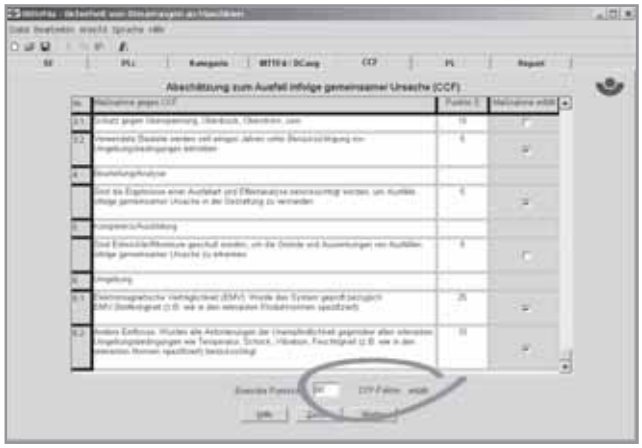
The answer to the obvious question which arises at this juncture, i.e. whether the exemplary procedures introduced above could not be enormously simplified through the use of software, is that this is now surely only a question of time.

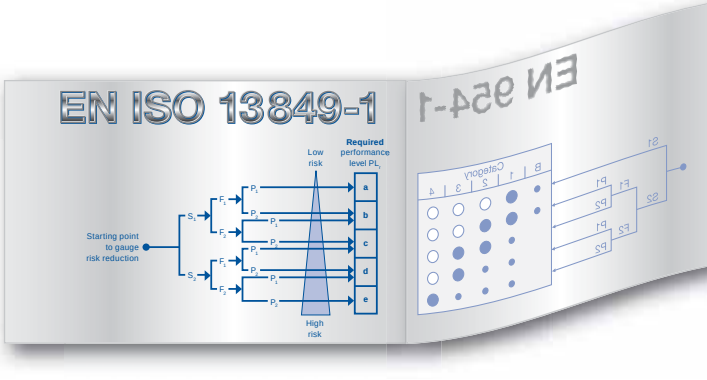
The BGIA for example is working on software called SiSteMa (safety of machine controls) which at will be available as freeware in due course.

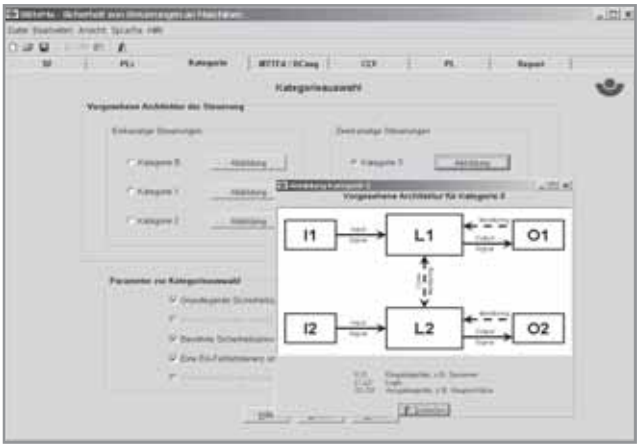


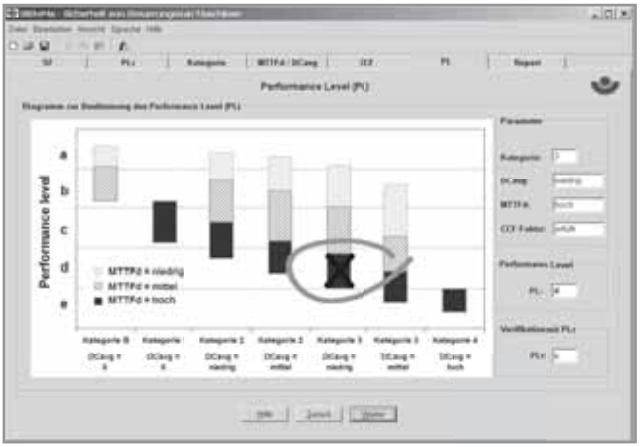


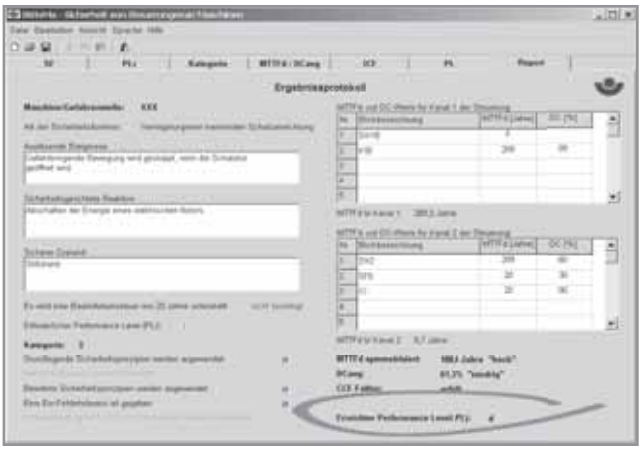












Although SiSteMa is not yet available (availability is planned from the middle of 2006), support with regard to dealing with EN ISO 13849-1:2006 is already being provided by the employer's liability insurance association. This is in the form of a so-called PLC disc which facilitates the simple determination of the performance level, and which has been developed with the support of the Zentralverband Elektrotechnik- und Elektroindustrie (ZVEI) – Fachverband Automation (the German central association for electrotechnology and the electrical industry – professional association for automation) and the Verband Deutscher Maschinen- und Anlagenbau VDMA (the German mechanical engineering/capital goods manufacturers' association).

The methods of prEN 13849-1 are made comprehensible through the use of two discs which rotate against one another. The performance level (PL) is determined simply by twisting one disc until the desired value of $MTTF_d$ (mean time to dangerous failure) appears in the lower window.

Then the desired category and diagnostic coverage (DC) must merely be selected in the upper window and the numerical value which appears in the window next to it read off. The mean time to dangerous failure of the safety-related control system is produced by multiplying this by a factor represented in the key (order of magnitude). The colour code serves the selection of the factor and simultaneously indicates which PL has been achieved.

PLC reference source:
www.hvbg.de/e/bia/pra/drehscheibe.html

EN ISO 13849-1:2006 and straightforward SRP/CS

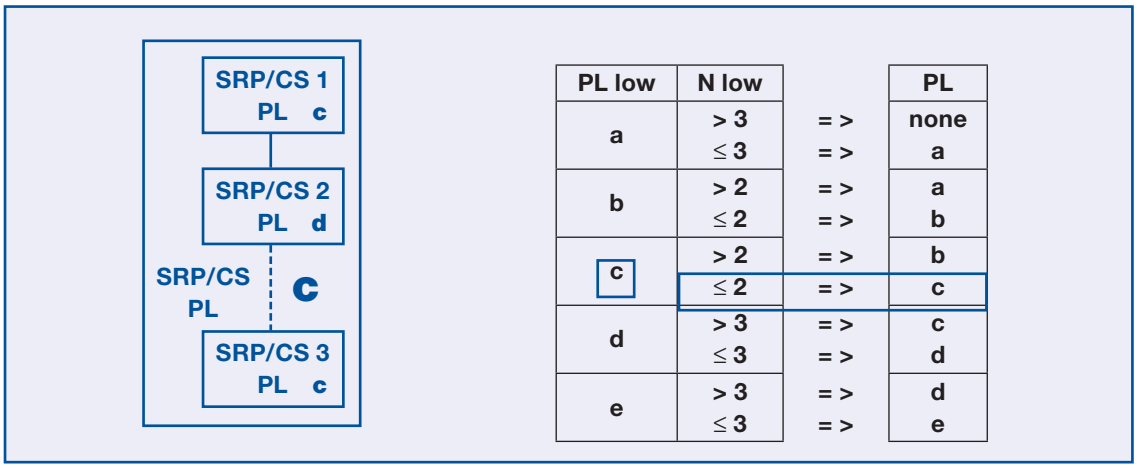
Background
When we know the relevant performance levels for the safety-oriented devices implemented we are able to discern the manageable complexity in EN ISO 13849-1:2006 for SRP/CS, arising from its singular concept of simplification.

At the same time this procedure also reflects the fact that the linking of a greater number of safety components and other safety-oriented devices can affect the overall PL, i.e. that the overall PL of a complete control system (consisting of several series connected SRP/CS) can very well turn out to be lower than individual PL's and the "chain links" involved. The idea behind this thought, and one which is also evident, is that in this case the probability of so "many" residual failures adds up, so that the overall PL can very well be lowered by one step.

Design
The above mentioned consideration in favour of simplification is rediscovered in the table seen in Figure 45 (which is also known as the combination table), in which the number of individual PL's in a control system can be read off on the left-hand section, whereby the lowest PL's should be added together here, and then the overall PL read off on the right-hand side.

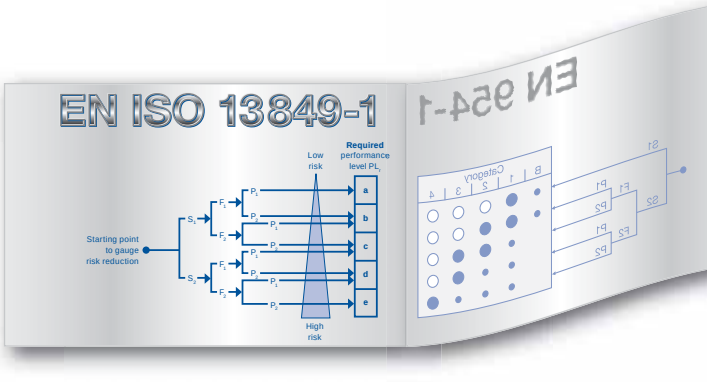
As a rule (when dealing with "more simple" structures") more than three identical single PL's and more than four identical single PL's (when it comes to fully-fledged 2-channel structures) sink the overall PL by one step, i.e. 3 x one single PL "c" produce an overall PL of "b", or 4 x one single PL of the type "e" an overall PL of "d".

The following example (refer to Figure 45) shows that this means the two lowest single PL's are to be added together (2 x PL "c", whereas the one higher PL "d" is not included in the calculation (PL "d" is viewed as an order of magnitude better than PL "c" with regard to the PFH value). 2 x PL "c" therefore remain as PL "c". If, however, a PL "c" could be accounted for here (instead of the 1 x PL "d"), this would (only) produce an overall PL of "b".



PL low	N low		PL
a	> 3	= >	none
	≤ 3	= >	a
b	> 2	= >	a
	≤ 2	= >	b
c	> 2	= >	b
	≤ 2	= >	c
d	> 3	= >	c
	≤ 3	= >	d
e	> 3	= >	d
	≤ 3	= >	e

Figure 45: Linear combination of multiple SRP/CS



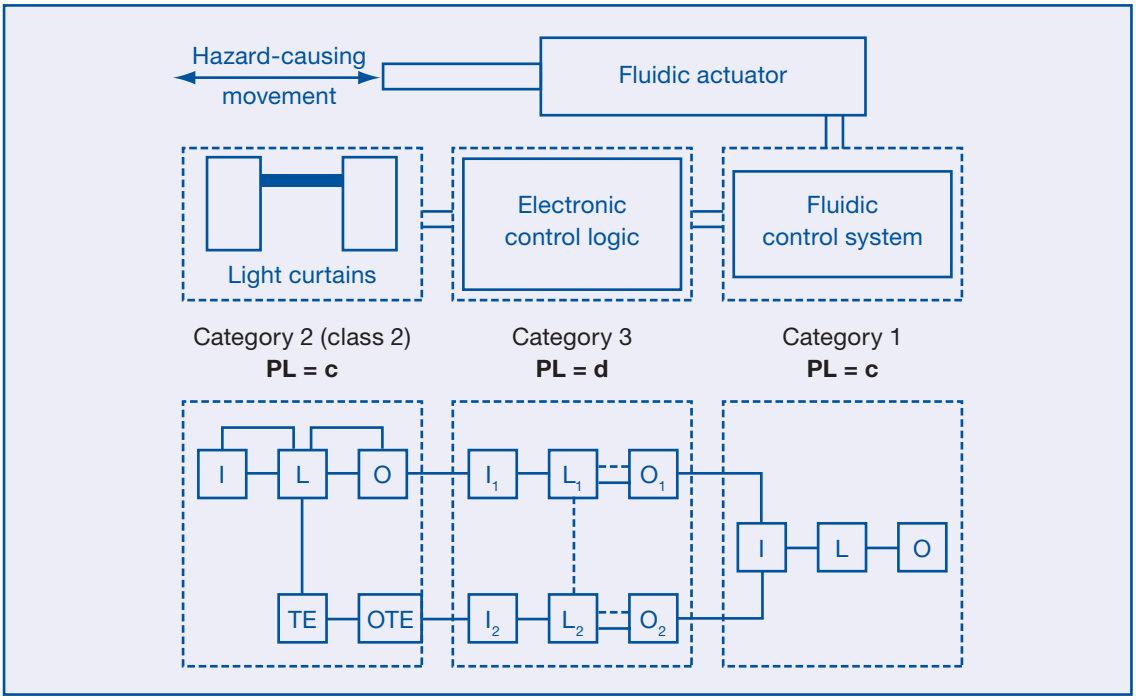


Figure 46: Combination of SRP/CS (example)

Application
The application shown in the above table doubtless has its appeal to the extent that the examination, which arises from the preceding risk analysis for the appropriate safety function, produces the desired PL_r outcome. One must furthermore consider that fault exclusions can be included in the assessment while not being connumerated.

However if the linking leads to an overall PL which does not equate with the PL_r, a more detailed analysis is required. Nonachievement in this sense is not the end of the matter; rather it is initially due to the generalisation of the analysis.

Here too EN ISO 13849-1:2006 offers assistance (refer to the following section on “series alignment”).

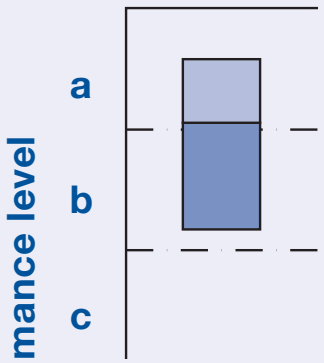
EN ISO 13849-1:2006 with series alignment

Background
Within the philosophy of EN ISO 13849-1:2006 a series alignment should be thought of as a summation of the probabilities of residual failure.

This feature may also be discerned today when interpreting EN 954-1, for example in the documents of the employer's liability insurance associations as well as in our documentation, when a series alignment of electromechanical safety switching devices (each one for example having category 4) is "only" classified by an overall category 3. But not all manufacturers make people aware of this and there are also multiple "false" interpretations on the part of the customer.

Design
The table in Figure 47 can be used to gain a deeper understanding of the safety-related quality of a more complex series alignment in EN ISO 13849-1:2006 (under the heading: addition of the probabilities of residual failure).

The table in annex K of EN ISO 13849-1:2006 depicts a detailed representation of the central block diagram (refer to figure 8) for the determination of the PL's achieved. It is possible to determine a more accurate PFH_d if a more exact $MTTF_d$ for the channel is known. The values achieved for individual SRP/CS should then be added together, and the sum compared with the maximum permissible overall PFH for the relevant PL (refer to Figure 4). The rule is that the better the PFH_d value, the lower the "crash hazard" will be.

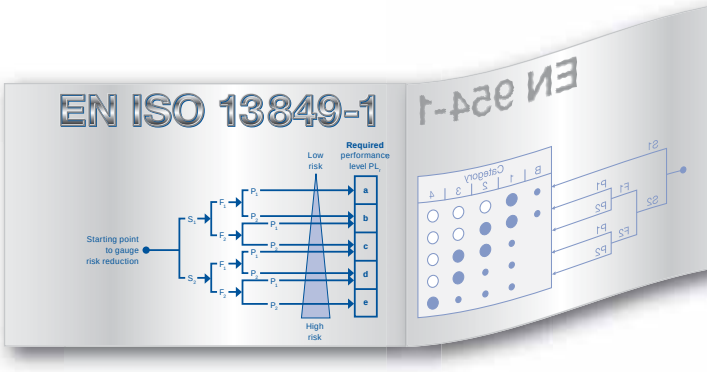


$MTTF_d$ [years]	PFH_d [1/h]	PL
3	$3.80 \cdot 10^{-5}$	a
3.3	$3.46 \cdot 10^{-5}$	a
3.6	$3.17 \cdot 10^{-5}$	a
3.9	$2.93 \cdot 10^{-5}$	a
4.3	$2.65 \cdot 10^{-5}$	a
4.7	$2.43 \cdot 10^{-5}$	a
5.1	$2.24 \cdot 10^{-5}$	a
5.6	$2.04 \cdot 10^{-5}$	a
6.2	$1.84 \cdot 10^{-5}$	a
6.8	$1.68 \cdot 10^{-5}$	a
7.5	$1.52 \cdot 10^{-5}$	a
8.2	$1.39 \cdot 10^{-5}$	a
9.1	$1.25 \cdot 10^{-5}$	a
10	$1.14 \cdot 10^{-5}$	a
11	$1.04 \cdot 10^{-5}$	a
12	$9.51 \cdot 10^{-6}$	b
13	...	

+

$MTTF_d$ [years]	PFH_d [1/h]	PL
3	$3.80 \cdot 10^{-5}$	a
3.3	$3.46 \cdot 10^{-5}$	a
3.6	$3.17 \cdot 10^{-5}$	a
3.9	$2.93 \cdot 10^{-5}$	a
4.3	$2.65 \cdot 10^{-5}$	a
4.7	$2.43 \cdot 10^{-5}$	a
5.1	$2.24 \cdot 10^{-5}$	a
5.6	$2.04 \cdot 10^{-5}$	a
6.2	$1.84 \cdot 10^{-5}$	a
6.8	$1.68 \cdot 10^{-5}$	a
7.5	$1.52 \cdot 10^{-5}$	a
8.2	$1.39 \cdot 10^{-5}$	a
9.1	$1.25 \cdot 10^{-5}$	a
10	$1.14 \cdot 10^{-5}$	a
11	$1.04 \cdot 10^{-5}$	a
12	$9.51 \cdot 10^{-6}$	b
13	...	

Figure 47: Alternative addition of the PFH_d with complex series alignments



Series alignment without loss of control category

- installed electronics monitor the switch function (self-monitoring)
- all faults will also be detected within a series alignment (… 31 devices)
- series alignment of switches (CSS 180 **and/or** AZM 200) **without** loss of control category possible

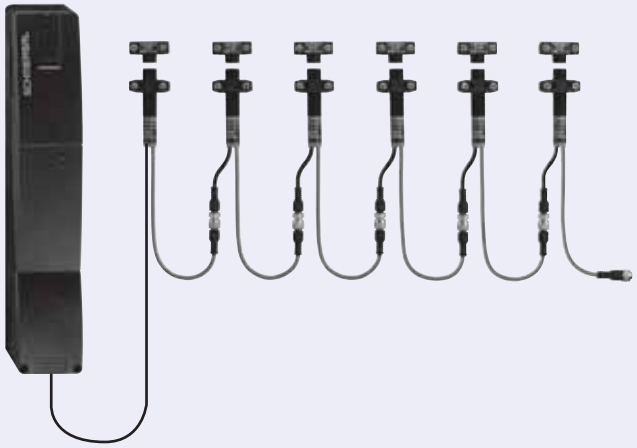


Figure 48: Non-contact interlocking devices with and without latching

Complex series alignments: yet still PL “e”!
The problem that complex series alignments can affect the overall PL of an SRP/CS is particularly manifest with regarded to electromechanical safety components among others.

Microprocessor-based switching technologies with safety functions offer new possibilities in this respect because the technology permits a continuous dynamic testing of the device, i.e. the control category or the performance level is maintained even where there are multiple safety components which are aligned in series.

The safety sensors CSS 180 among others are available from the SCHMERSAL product range, as well as the non-contact latches of the AZM 200 range, which can also be mixed and linked to a series alignment (Figure 48).

Further information under
www.schmersal.com

Electronic safety sensors and latches

The electronic safety sensors and latching serve to monitor moving guards. When these are opened the machine is stopped; at all events the hazardous re-engaging of the machine is prevented. Its fundamental advantage lies in the non-contact detection of the door position. This means they are completely free of wear and tear and unsusceptible to misalignment through sensors and actuators.

EN ISO 13849-1:2006 and software

Background
While EN 954-1 is currently not involved with the subject of "microprocessor-based switching technology with safety function" (= PES systems) and thus also not with the matter of software, this is the case and in all the more detail with EN ISO 13849-1:2006. Nevertheless the requirements have not completely replaced IEC EN 61508 (e.g. for applications in PL "e"), but this is only of interest to developers of PES systems and will not be discussed further here.

The basic idea behind EN ISO 13849-1:2006 is depicted in Figure 49.

Design
The software requirements in prEN the programming ISO 13849-1 are divided into general requirements (as cited) as well as requirements pertaining to safety-relevant embedded software and requirements for safety-relevant application software, whereby there are also additional divisions according to language used (LVL[1] or FVL[2]) and PL's (refer to Figures 50 and 51).

- For all PL and SRESW + SRASW
- basically measures to **avoid faults and provide defensive programming**
- consideration of the fact that faults will be introduced during the specification and design of software
- taking the fundamental safety standard of IEC 61508-3 as a basis
- … however not to a high scientific level
- principally without links to IEC 61508
- comprehensible, practice oriented and easy to use

Figure 49: Basic idea behind the SW requirements in accordance with EN ISO 13849-1

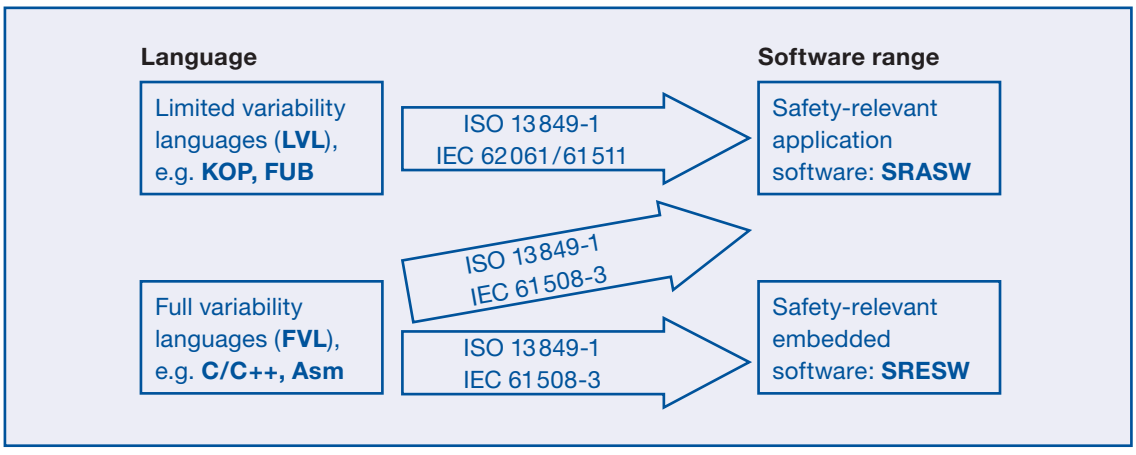
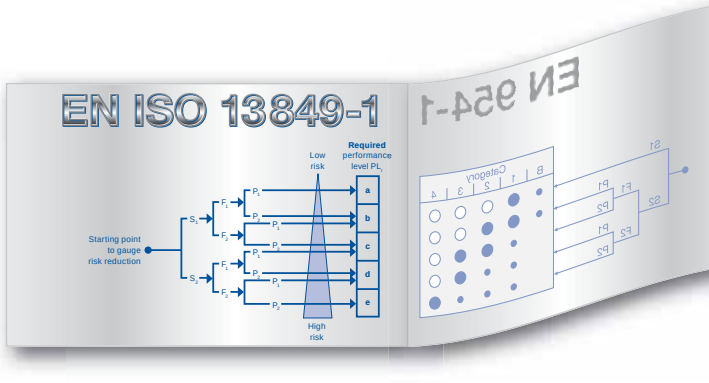


Figure 50: "Networking" of safety-oriented software

1) LVL (limited variability language) – programming language with limited language range: language type that provides the capability to implement predefined application-specific and library functions in combination in order to execute the safety requirement specifications.

2) FVL (full variability language) – programming language with unlimited language range: language type that provides the capability to implement a wide variety of functions and applications.



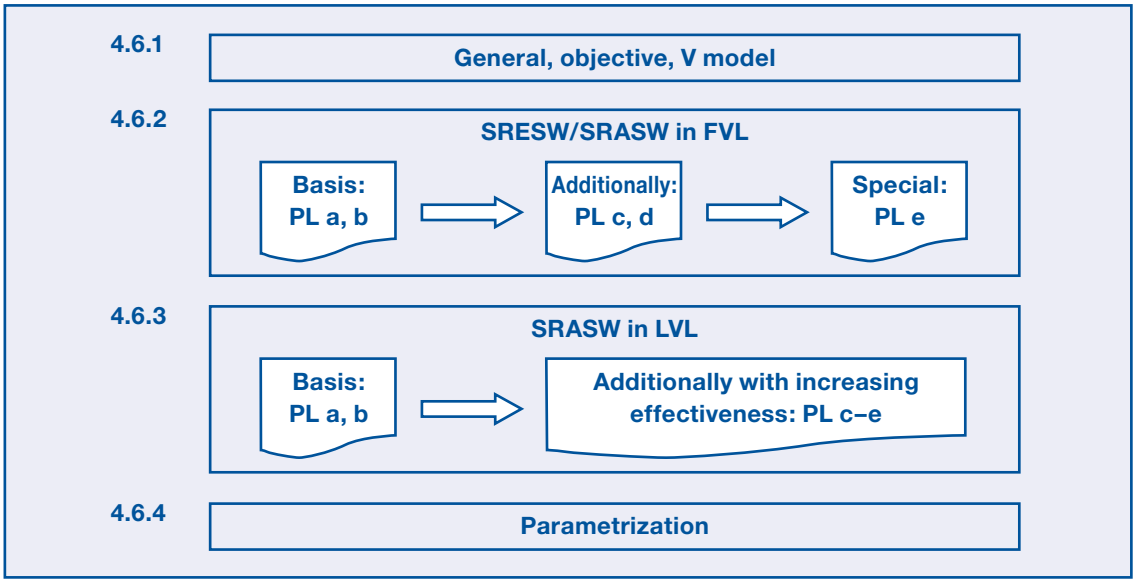


Figure 51: The structure of the SW requirements in accordance with paragraph 4.6 of EN ISO 13849-1:2006

Application

We will not go into details of safety-relevant embedded software as this only affects EN ISO 13849-1:2006 clientele in exceptional cases. Increasingly what is more typical is, however, the use of application software in SRP/CS, whether this is in connection with safety SPS's, safety bus systems or safety-oriented drive controls.

EN ISO 13849-1:2006 recommends taking the so-called V model as a basis for application software (and also for embedded software), as it is already very familiar in the software branch, if only in a simplified form.

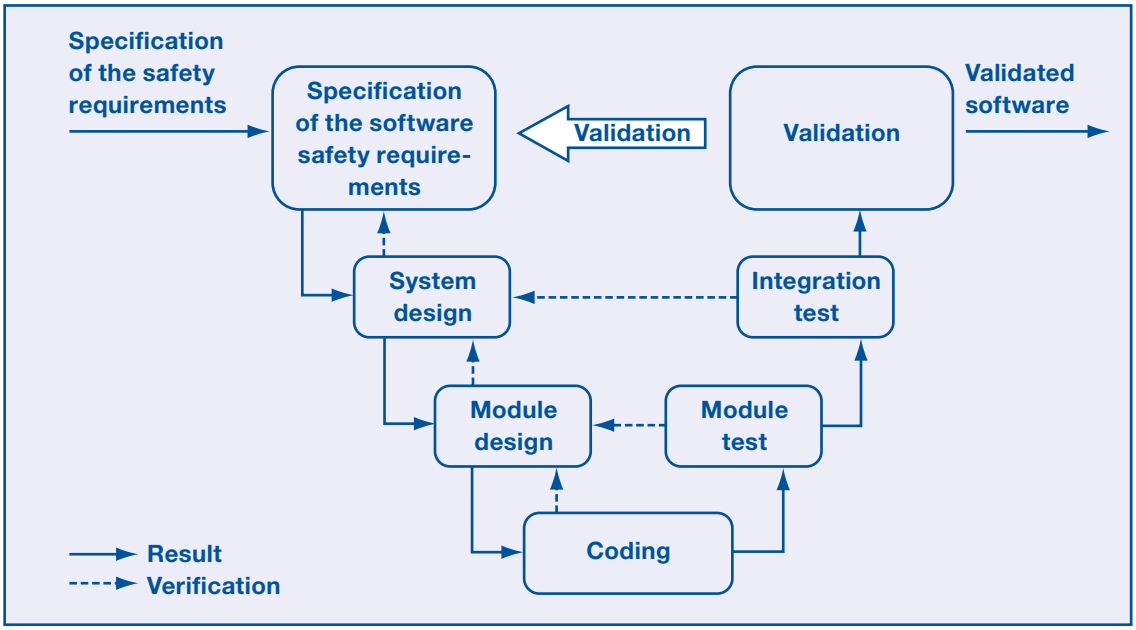
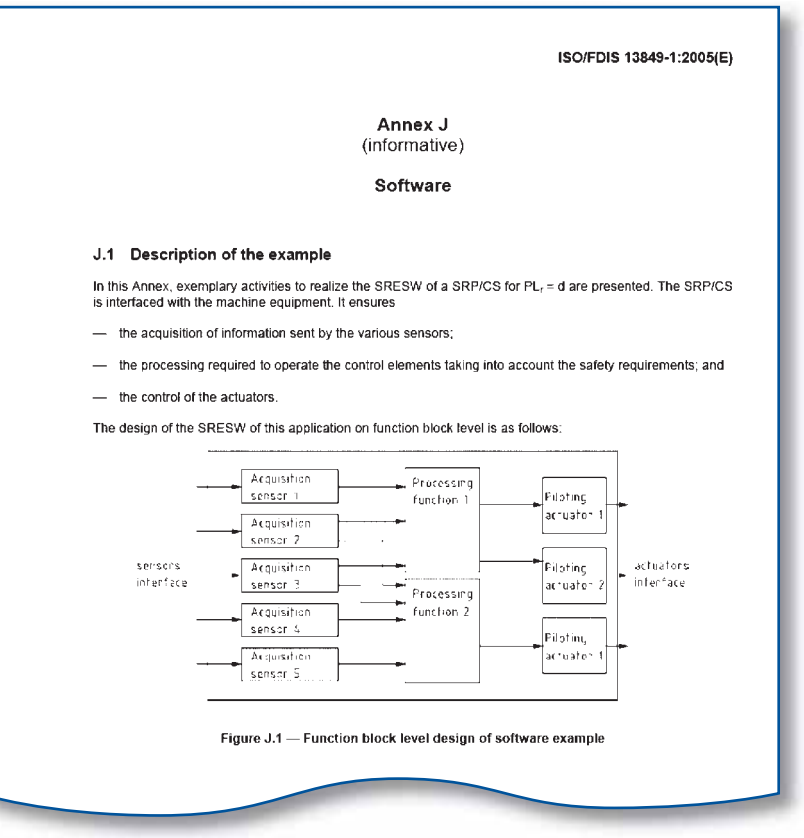


Figure 52: Simplified V model for SRESW and SRASW in EN ISO 13849-1:2006

If on the other hand the application software consists of just one parametrisation, as is typical in the case of safety laser scanners for example, further simplifications apply because here in principle one must be able to rely on the preparatory work of the supplier.

Further software requirements are contained in annex J of EN ISO 13849-1:2006 (refer to Figure 53).



ISO/FDIS 13849-1:2005(E)

Annex J
(informative)

Software

J.1 Description of the example

In this Annex, exemplary activities to realize the SRESW of a SRP/CS for PL_r = d are presented. The SRP/CS is interfaced with the machine equipment. It ensures

— the acquisition of information sent by the various sensors;

— the processing required to operate the control elements taking into account the safety requirements; and

— the control of the actuators.

The design of the SRESW of this application on function block level is as follows:

Figure J.1 — Function block level design of software example

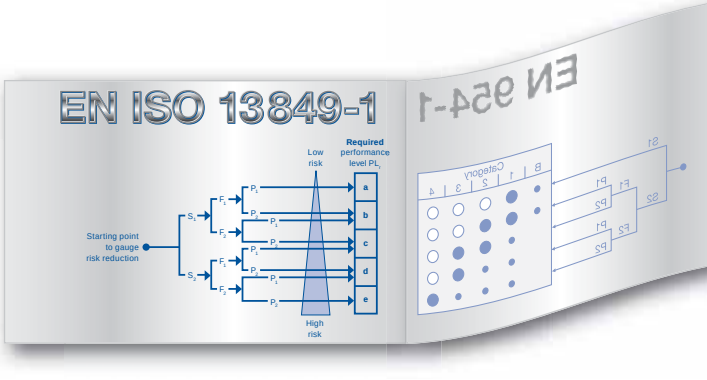
Figure 53: Annex J in EN 13849-1

Requirements of the parameter-assigning software

Most important requirements for parameterization

- special tool from the manufacturer
- protection against unauthorised access (e.g. password)
- plausibility controls of the parameters
- securing of the integrity of the parameter data during the parameterization process
- secure data transfer (with diversity of representation)

Figure 54: Requirements of parameter-assignment software



EN ISO 13849-1:2006 vs. IEC EN 62061

Background

As discussed at the beginning, the IEC EN 62061 standard is competing against EN ISO 13849-1:2006 to be the successor to EN 954-1, even if the term “competing” is slightly exaggerated in this context. Still, it is no longer possible to speak of “co-existence” as had once been envisaged.

In contrast to IEC 61508 one can furthermore take it that both IEC EN 62061 and EN ISO 13849-1 will also be harmonised under the EC machinery directive. This means that both standards will have the advantage of the so-called supposed impact on their side.

IEC EN 62061 is the sector specific derivate of IEC EN 61508 for mechanical engineering. Apart from this there is, for example, the IEC EN 61511[1] standard for the processing industry (for chemical and process engineering).

Originally IEC EN 61508 was intended exclusively to close a gap, namely the failure of EN 954-1 to recognise any requirements for complex SRP/CS, especially with regard to programmable electronic, i.e. microprocessor-based systems with safety functions (PES); however the IEC 61508 standards committee has widened the application range of the standard in the course of its work to include discrete electrical and electronic systems (E/E/PES).

Since as a result of this IEC EN 61508 has developed into a fundamental and comprehensive standard for almost all types of safety-related problems and become correspondingly complex (with over 350 pages divided into 8 sections), it has generated so-called sector-specific standards for individual branches, among others in the form of IEC 62061[2] for mechanical engineering.

The typical requirements of the branch are determined here while requirements that apply to other branches and design scenarios are being left out.

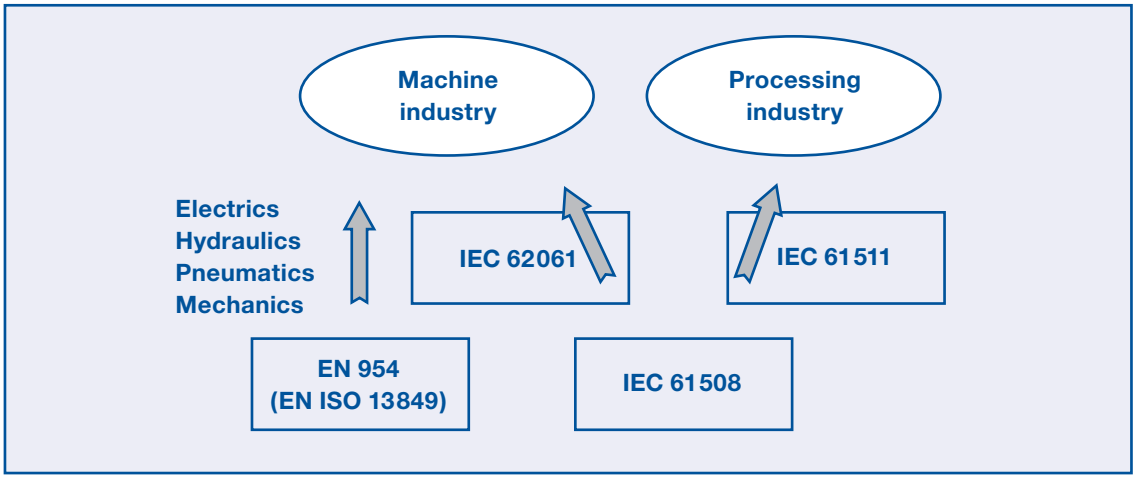


Figure 55: Situation with competing standards

1) IEC EN 61511-1 (VDE 0810-1:2005-05): functional safety – safety-related systems for the processing industry – part 1: general, terms, system requirements, software and hardware

2) IEC EN 62061-1 (VDE 0113-50): safety of machines – functional safety of safety-oriented electrical, electronic and programmable electronic control systems

4 safety integrity levels and 2 operational modes

Safety integrity level	Low request rate Medium probability of a dangerous failure on demand PFD	High request rate or continuous request Medium probability of a dangerous failure per hour PFH
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

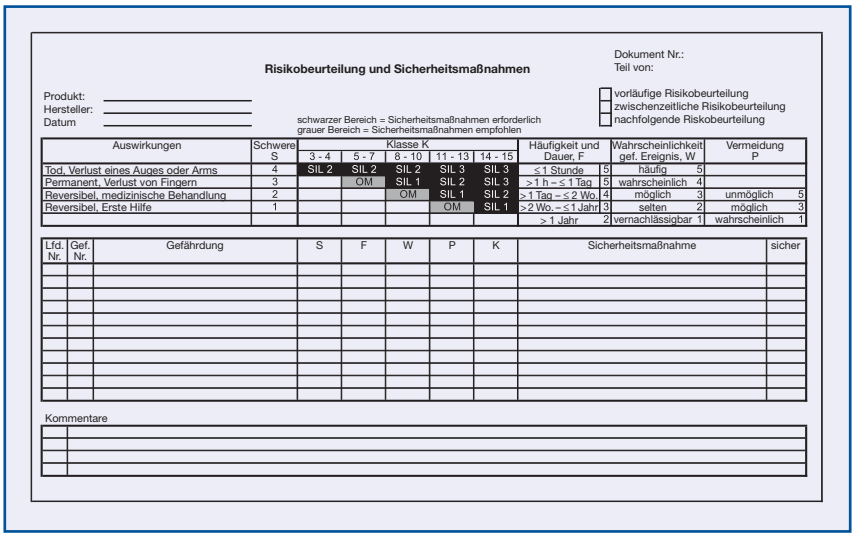
Relevant to the machine area?

Figure 56: Safety integrity level: IEC 61508 (universal applications) and IEC 62061 (mechanical engineering application)

With respect to mechanical engineering this means being limited to the safety-related requirements of so-called higher demand mode or for continuous demand mode (as expressed in a PFH value) (a lower demand mode with less than one safety function demand per year is disregarded). In addition the safety integrity level 4 (risk parameter: death of several people at least, catastrophic effects) is also excluded.

Application
IEC EN 62061 is not to be dealt with in detail here. However, critics remark that it has become more difficult to handle compared to EN ISO 13849-1:2006 as far as “clearer” safety-related issues are concerned as frequently typical of the construction of machines and control systems and that, conversely there is no way around IEC EN 61508 for more complex issues. Another difference is the incorporation of mechanics, pneumatics and hydraulics in EN ISO 13849-1:2006 which IEC EN 62061 does not cover due to its origin.

Figure 57: Example form for the process of determining the SIL



Risikobeurteilung und Sicherheitsmaßnahmen

Dokument Nr.:
Teil von:

Produkt:
Hersteller:
Datum

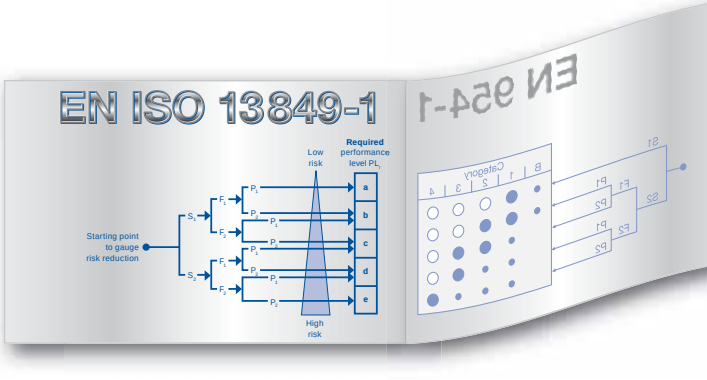
☐ vorläufige Risikobeurteilung
☐ zwischenzeitliche Risikobeurteilung
☐ nachfolgende Riskobeurteilung

schwarzer Bereich = Sicherheitsmaßnahmen erforderlich
grauer Bereich = Sicherheitsmaßnahmen empfohlen

Auswirkungen	Schwere S	Klasse K 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Häufigkeit und Dauer, F		Wahrscheinlichkeit gef. Ereignis, W		Vermeidung P	
Tod, Verlust eines Auges oder Arms	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 Stunde	5	häufig	5		
Permanent, Verlust von Fingern	3		OM	SIL 1	SIL 2	SIL 3	> 1 h – ≤ 1 Tag	5	wahrscheinlich	4		
Reversibel, medizinische Behandlung	2			OM	SIL 1	SIL 2	> 1 Tag – ≤ 2 Wo.	4	möglich	3	unmöglich	5
Reversibel, Erste Hilfe	1				OM	SIL 1	> 2 Wo. – ≤ 1 Jahr	3	selten	2	möglich	3
							> 1 Jahr	2	vernachlässigbar	1	wahrscheinlich	1

Lfd. Nr.	Gef. Nr.	Gefährdung	S	F	W	P	K	Sicherheitsmaßnahme	sicher

Kommentare



Planned compatibility of EN ISO 13849-1:2006 and IEC EN 62061 (IEC EN 61508)

In spite of all this, both standard-setters, i.e. both the committees of IEC EN 62061 and EN ISO 13849-1:2006 – have made efforts to create compatibility between the two standards, by co-ordinating the safety integrity level and performance level requirements. Thus SIL 1 corresponds for example to the PL's "b" or "c" etc. (refer to Figure 58).

Furthermore both standards provide similar sounding recommendations concerning which standard should be applied for which questions. However there is still room for criticism as the EN ISO 13849-1:2006 standard-setter has departed from this compromise through the implementation of subsequent alterations, even if the application table continues to be included in EN ISO 13849-1:2006 (refer to Figure 59).

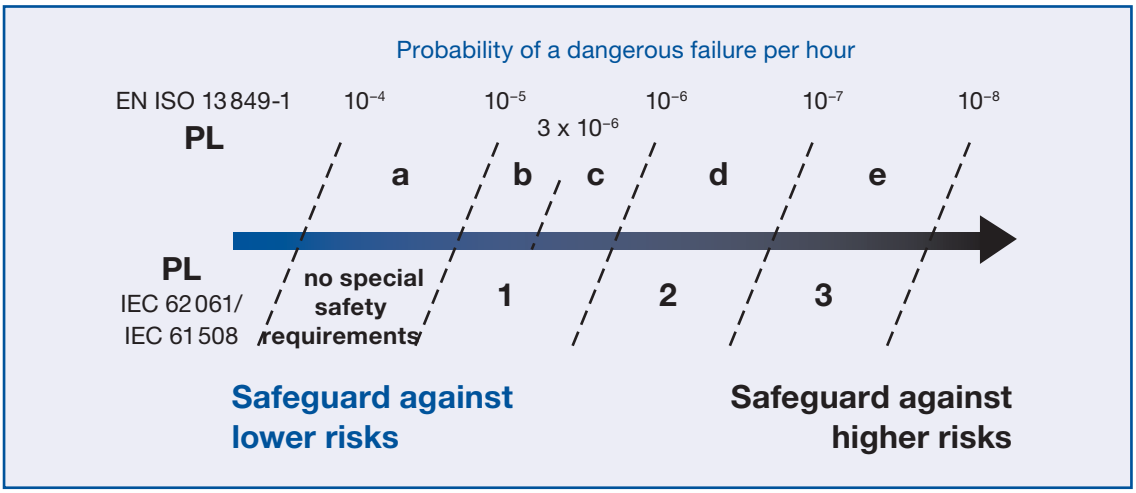


Figure 58: Relationship between SIL and PL

	Technology	ISO 13849-1 (in revision)	IEC 62061
A	Non-electrics, e.g. hydraulics	X	Disregarded
B	Electromechanics, e.g. relay or simple	Designated architectures[1] and up to PL = e	All architectures and up to SIL 3
C	Complex electronics, e.g. programmable	Designated architectures[1] and up to PL = d	All architectures and up to SIL 3
D	A combined with B	Designated architectures[1] and up to PL = e	X (EN ISO 13849-1 for A)
E	C combined with B	Designated architectures[1] and up to PL = d	All architectures and up to SIL 3
F	C combined with A, or C combined with A and B	X[2]	X[3]

"X" means that this point is covered by the standard in the column heading.

1) Designated architectures are defined in annex B of the EN ISO 13849-1 (rev.), in order to provide a simplified quantification of the performance level.

2) For complex electronics: use of the designated architectures in agreement with EN ISO 13849-1 (rev.) up to PL = d or every architecture to IEC 62061.

3) For non-electrical technology: use of parts in accordance with EN ISO 13849-1 (rev.) as a partial system.

Figure 59: Recommended application of IEC 62061 and ISO 13849-1 (in revision)

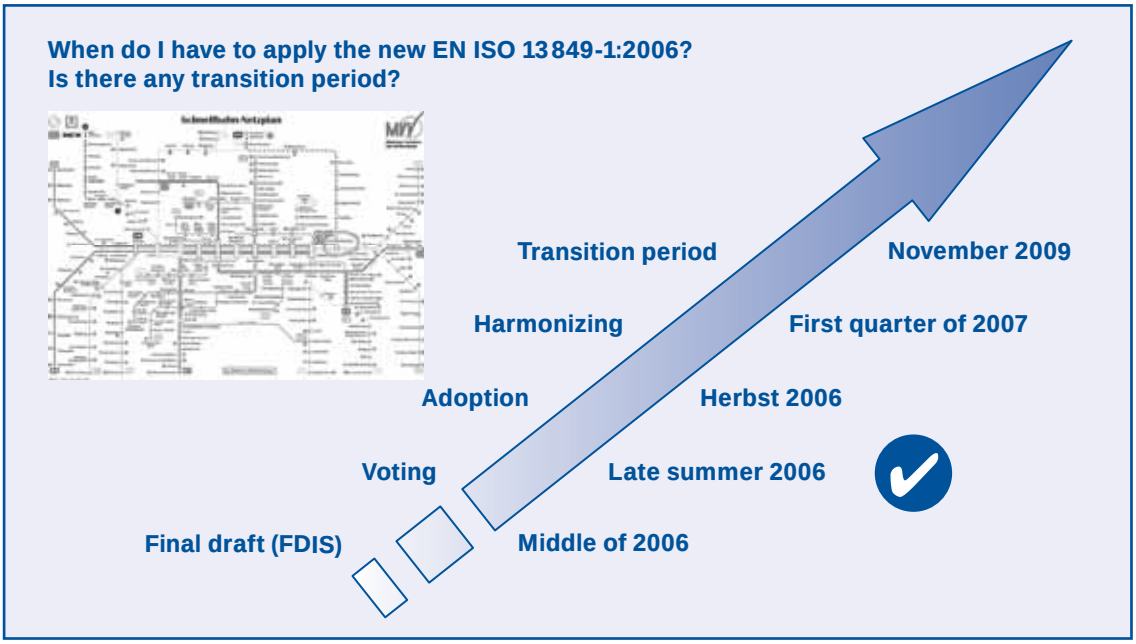


Figure 60: Up-dated time table (May 2007): According to the latest decisions the now concluded standard has a transition period until November 2009 (which means the new provisions can be already applied from now on, but here is not yet a must to do so), but in November 2009 all conflicting standards (in practical terms ISO 13849-1:1999 respectively EN 954-1:1996) have to be recalled. Than the "old" standard finally will be replaced by EN ISO 13849-1:2006.

The coming into force of EN ISO 13849-1:2006

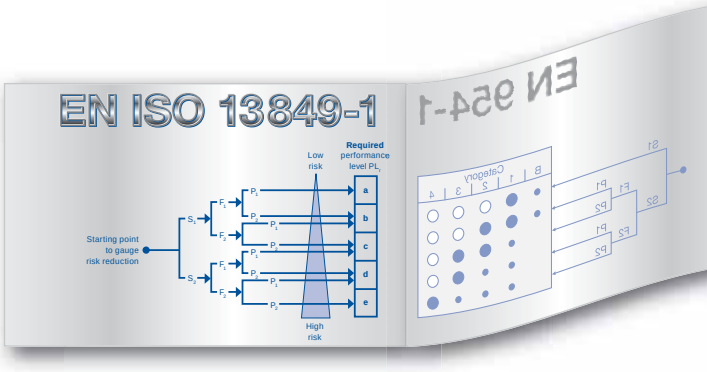
Current "timetable"
While IEC EN 62061 has already been formally passed, EN ISO 13849:2006 finds itself still at the final ballot stage (FDIS) and it runs the real risk of a further editorial round. This is why only a draft standard is available in German at the present time (as of June 2007), while 62061 can already be bought in perfect form as IEC EN 62061 from Beuth publishers (www.beuth.de).

see page 2

However if the current "timetable" remains, EN ISO 13849-1 will come into force in 2006 and, after a 3 year transition period, replace EN 954-1 completely.

Comparison with the state of the draft in June 2004
In comparison with the state of the draft in June 2004, EN ISO 13849-1:2006 demonstrates a few important amendments in the final version, among others with respect of the application range (see above) and the risk graphs. Furthermore one could – albeit with limitations – also realise PES systems under EN ISO 13849-1:2006.

With regard to risk graphs, there are now unambiguous specifications of which risks lead to which performance level, i.e. there are no longer any "double entries" (e.g. optionally PL x or PL y). What is more, the risk parameter F1 (frequency and/or duration of the hazardous exposition) is clarified so that generally "seldom" is taken to mean > 1 x per hour.



FAQs

Where do the essential differences lie between the current draft and the published status of prEN ISO 13849-1:2004?

- alignment with the risk graph
- concrete values for safety-related reliability (PFH_d)
- concrete $MTTF_d$ and B_{10d} values for hydraulics, pneumatics and electromechanics
- software requirements
- amendment to the application range
  - no limits to designated architectures
  - only for embedded software with PL_e referral to IEC 61 508

Figure 61: Selected questions

A further difference occurs through the amendment in the interpretation of control category 4 by which the consideration of fault accumulation must generally be limited to two faults.

How many faults do I have to combine in category 4?

1. Single faults do not lead to the loss of the safety function.
2. These initial faults are … uncovered. If detection is not possible, an accumulation of faults must not lead to the loss of safety function.

Remark: In practice the consideration of the combination of two faults may be adequate.

New: no longer dependent on the technology of the application or the failure rates of components.

Figure 62: Selected questions

EN ISO 13849-1:2006 vs. C standards
The question of compatibility arises when one considers that there are now a few hundred C standards, i.e. product standards, for example for machine tools, machining centres among others, because all current C standards only recognise a requirement for one control category.

Thus in the coming years the C standard-setters will have to do something, whereby they have two options when it comes to adapting to EN ISO 13849-1:2006.

Either the C standard-setters confine themselves to requiring exclusively a performance level for "their" machines in the future in order to be able to offer their "clientele" greater design flexibility, particularly in the "medium" performance level.

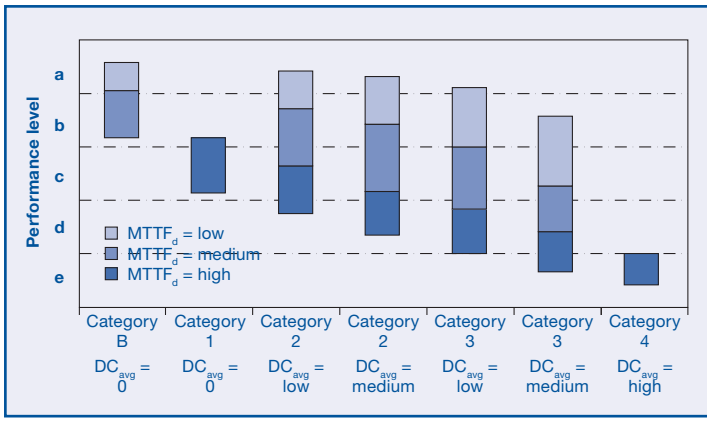


Figure 63: Multiplicity of realisation possibilities

The other option is that the C standard-setters determine a control category – in addition to the performance level – if one wishes to have greater influence on the structure.

My C standard demands a category to control the machine. Will a performance level be adequate in the future?

- In principle the declaration of a performance level will suffice for classification in the future. However EN ISO 13849-1 plans the following specification for each SRP/CS in the user information:

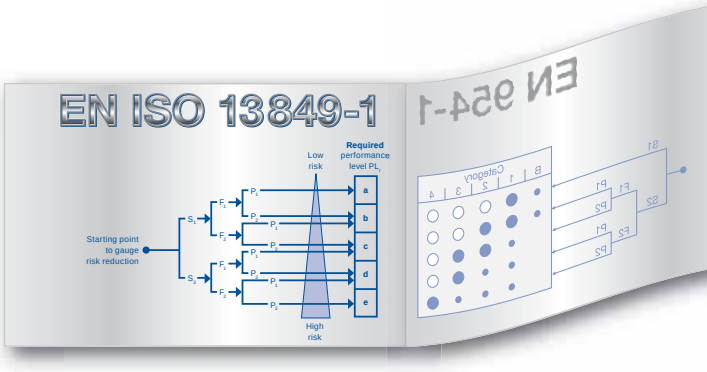
  EN ISO 13849-1:200x
  Category X PL Y

Figure 64: Selected questions

In the meantime we should all be best served by using the following table (caution when realising control category 2 with the designated architecture specified! Refer to the place already cited).

	B	1	2	3	4
Design in accordance with relevant standards, to withstand expected influences	X	X	X	X	X
Tried and tested safety principles		X	X	X	X
Tried and tested components		X			
Mean time to dangerous failure – $MTTF_d$	low – medium	high	low – medium	low – high	high
Fault detection (tests)			X	X	X
Single fault safety				X	X
Consideration of fault accumulation					X
Diagnostic coverage – DC_{avg}			low – medium	low – medium	high
Measures to combat CCF			X	X	X
Principally characterised by	Component selection		Structure		

Figure 65: Control categories and additional requirements



Outlook

Without doubt a series of questions remains with regard to prEN 13849-1. We will therefore keep you informed within the framework of the MRL News of further future clarifications as they emerge.

If one attempts to summarise the effects of prEN ISO 13849-1, these can be divided roughly into two groups.

The first is the group of those who must merely revise the quantification ($MTTF_d$, DC, CCF). Here we can assume that a machine with SRP/CSS's will "pass" the new safety standard if safety-related factors have been well thought-out and executed with appropriate quality, and that no substantial amendments will be necessary as a result.

By contrast, however, amendments may be required where complex series alignments are realised (heading: "crash hazard" in the PL through the summation of residual risks) and when the designated architecture for category 2 is used.

Notes

K.A. Schmersal GmbH
Industrielle Sicherheitsschaltsysteme

Möddinghofe 30
D-42279 Wuppertal
Postbox 24 02 63
D-42232 Wuppertal

Tel. +49 (0)202 6474-0
Fax +49 (0)202 6474-100
E-Mail info@schmersal.com
Internet www.schmersal.com

Elan Schaltelemente GmbH & Co. KG

Im Ostpark 2
D-35435 Wettenberg
Postbox 1109
D-35429 Wettenberg

Tel. +49 (0)641 9848-0
Tel. +49 (0)641 9848-420
E-Mail info@elan.schmersal.de
Internet www.elan.de

05/06 V