

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

### Autor:

Frank Schmidt,  
Manager of Marketing  
K.A. Schmersal GmbH, 42279 Wuppertal



The "category principle" for **Safety-Related Parts of Control Systems (SRP/CS)** of machinery belongs in the past: The familiar control categories of EN 954-1:1996 have been replaced by the performance levels of EN ISO 13849-1:2005 and must be applied by the end of 2009. What now changes for the designers and safety engineers?

Why a new standard for the control unit categories is needed? Many of the designers and planners of machines and machine systems will ask this question. Is the present safety level so low that it must be replaced by new standards? This question can safely be answered in the negative. There are other reasons that demanded a revision of EN 954-1.

### Adaptation to international standards

A rather formal aspect is the fact that – after the European harmonization – an adaptation of the standards on an international level, i.e. IEC 61508 in this case, is desired step by step. In addition, the EC standards committees have communicated to adjust the standards continuously to the technical progress. This was logical for the EN 954-1, because it only insufficiently included programmable electronic systems with safety functions. Although there was a comparable "new standard" that relates to the IEC 61508. However, the IEC 62061 is completely concentrated on electronics. A "real" technology comprehensive replacement for the EN 954-1 that is compatible with the IEC 61508 was therefore necessary.

In addition, there always appeared criticism regarding the EN 954-1. A central point of criticism was the fact that this standard pursues a deterministic approach. This means: The safety systems were considered to be "static" and constant. A probabilistic approach that also considers the failure probability of the individual com-

ponents and therefore the overall system (Fig. 1) is more practical.

All of this resulted in the decision by the standards committees to replace the EN 954-1 by a new standard – the EN ISO 13849-1. Speaking realistically, it can be said that there have been some changes for the designer of machines and systems.

### First step: Calculate potential risks

When designing a SRP/CS, he must first – as before – calculate the potential risk based on a modified risk graph. However, then the changes arrive: The risk analysis does not result in one of the old familiar control categories, but one of five "performance levels" (from "a" to "e"), which reflect various residual risks (Fig. 2). This residual risk is quantified as PFHd value, which indicates the average **Probability of a dangerous Failure per Hour**. The probabilistic theory therefore comes into play here.

The performance level calculated by this method is also described as PLr – the "r" stands for "required", i.e. it is the required performance level. Thus, the designer now knows which PL he must reach to arrange a SRP/CS in conformity with the legal and normative requirements.

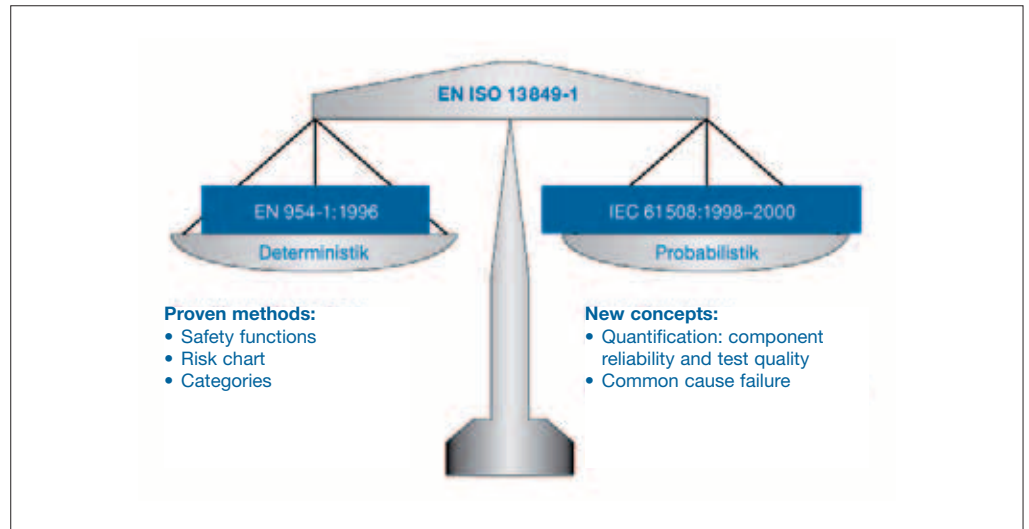
The fact that the PLs contain many more characteristics than the previous control system categories is also new. The values MTTFd (average **Mean Time To dangerous Failure**), **Diagnostic Coverage (DC)** and measures against **Common Cause Failures (CCF)** are therefore defined for each PL – the probabilistic factors are included in the calculation of the performance level by this method.

The designer knows up to this point only, which performance level he must pursue. How does he

## Sicherheit im System. Schutz für Mensch und Maschine.

K. A. Schmersal GmbH  
Industrielle Sicherheitsschaltssysteme  
Postfach 24 02 63, 42232 Wuppertal  
Möddinghofe 30, 42279 Wuppertal

Telefon: +49-(0) 2 02-64 74-0  
Telefax: +49-(0) 2 02-64 74-1 00  
E-Mail: info@schmersal.com  
Internet: http://www.schmersal.com



**Fig. 1: The new EN ISO 13849-1 also includes the probabilistic theory. A frequent point of criticism of the EN 954-1, which occurred purely deterministic, is therefore eliminated.**

convert this knowledge into the design usage? In order to answer this question, the procedure must be viewed from another angle. The manufacturers of safety components and safety-related control systems have already oriented themselves to the new standard situation and included IEC 61508 in the design, which defines the so-called safety integrity levels (SIL). These SILs deliver technical data from which the performance levels can be calculated. In addition, the compatibility of the new standard system is shown here, because the safety integrity levels are always assigned to performance levels. SIL 2 always corresponds with the PL "d".

#### **Risk observation for the entire safety chain**

These values are specified in product documents of the safety devices, so that the designer can select the appropriate components. Since a safety chain always consists of several components (sensor technology, control system, actuating elements), he must combine the values to a total PL. This is the "real" PL, which now has to be compared with the required PLr. If the calculated PL is greater or equal to the PLr, the safety circuit is constructed according to standard.

#### **Including validation**

The aspect of the validation is also new. A validation plan is listed in EN ISO 13849-2, which must be followed in the calculation of the performance levels. The procedure of the component selection and the configuration of the safety chain becomes therefore more objective. The procedure must also be documented - this is also specified by EN ISO 13849-2.

#### **Helpful: Designated Architectures**

The so-called "designated architectures", which must be applied according to the new standard, are also helpful in the construction of the safety circuit. These are previously calculated structures of the safety-related parts of control systems, which are already known from the application of EN 954-1. However, these preliminary

calculations do not release the designer from the task to include the mentioned parameter values MTTFd, DC and CCF in the calculation of the performance level.

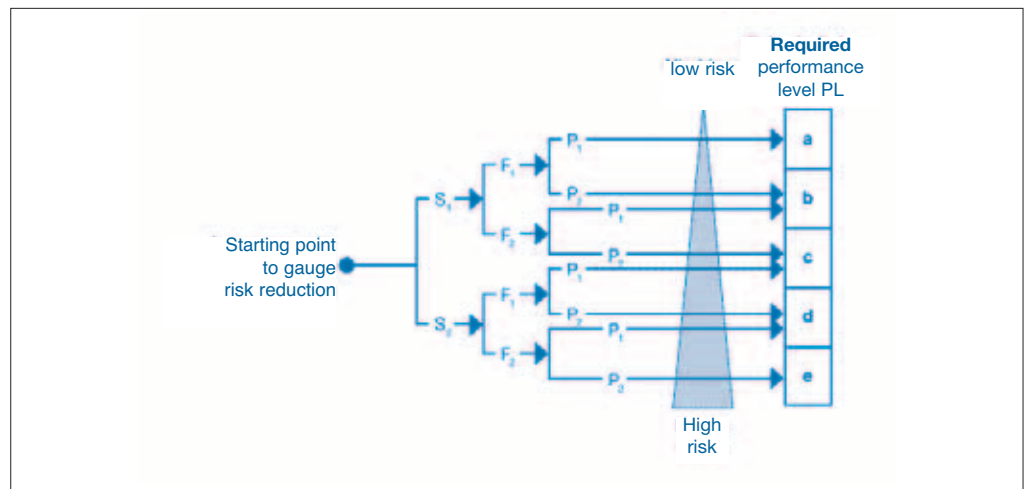
#### **The standard is more complex**

This means: The designer in mechanical engineering must grapple with this standard. He must plan some time for this, because the EN 13849 is clearly more complex than the EN 954-1. If it is an improved step in the right direction to expand the standards for machine safety at the high safety level at which today's machines are will surely be discussed at a later point.

#### **Transitional problems cannot be ruled out**

Furthermore, problems can be anticipated in the initial application of the new standard, since some manufacturers of safety components have not yet calculated the required information, which his customers, the designers of machines and systems, require. The more complex steps, which are now required for the selection of the standard-compliant safety device, could also create difficulties. However, there is support: The BGIA (professional cooperative institute for job safety) has created free software (SISTEMA: <http://www.dguv.de/bgia/de/pra/softwa/sistema/index.jsp>), which provides guidance through the steps of the EN 13849-1 as "assistant".

## **Sicherheit im System. Schutz für Mensch und Maschine.**



**Fig. 2: Schematic illustration of the modified risk graph.**

**S** = stands for the seriousness of the violation,  
**F** = for the frequency and / or duration of Gefährungsexposition,  
**P** = ways to avoid the risk.

Regardless of the somewhat more complicated procedure that the new standard presents, it is not an option that the standards had to be adjusted to the technical progress. Especially from the view of German mechanical engineering as world champion in exports, it is also extremely logical that the standards were now also standardized at an international level. In addition, the designer that familiarizes himself with the not so easy material of EN 13849, can take comfort that many tasks that the new standard system brings - the calculation of the values, for example, for the failure probability, errors of a joint origin, etc. - must be provided by the manufacturer for safety switching systems. The manufacturers have adjusted to this early: New device generations have already been developed according to the conditions of IEC 61508 and EN ISO 13849

**Images:**

**K.A. Schmersal GmbH, Wuppertal**

**Autor:**

**Autor: Frank Schmidt, Manager of Marketing  
 K.A. Schmersal GmbH, 42279 Wuppertal**

**Sicherheit im System. Schutz für Mensch und Maschine.**

K. A. Schmersal GmbH  
 Industrielle Sicherheitssysteme  
 Postfach 24 02 63, 42232 Wuppertal  
 Möddinghofe 30, 42279 Wuppertal

Telefon: +49-(0) 2 02-64 74-0  
 Telefax: +49-(0) 2 02-64 74-1 00  
 E-Mail: info@schmersal.com  
 Internet: http://www.schmersal.com