

Pepperl+Fuchs GmbH – Lilienthalstrasse 200 – 68307 Mannheim – Germany

Please quote the following contact information when publishing:

Tel.: +49 621 776-2222, Fax: +49 621 776-27-2222, www.pepperl-fuchs.com, pa-info@de.pepperl-fuchs.com

Editorial contact: Christa Blas (extension: -1420, fax: -1108), cblas@de.pepperl-fuchs.com

IEC 62061 and ISO 13849-1 – complementary or in competition

The publication of the IEC/EN 61508 series, which was originally intended as a tool for the development and validation of complex electrical, electronic and programmable electronic systems, was a milestone in the standardization of safety-relevant technologies.

The IEC 61508 is *the* standard to use for functional safety (Safety Integrity Level, SIL) of complex systems. There are already a number of derived standards, but what is in store for machine constructors?

Background

Traditionally, machines with moving parts have been identified as dangerous. Many efforts are made by professional associations, machine manufacturers, safety component manufacturers and legislative bodies to keep the risk of injury as low as possible.

In Europe, a new approach directive for the machine sector was published (89/392/EC and subsequent). This new approach provides a complete harmonization of the technical regulations of all member states.

For several years, standards were written as part of an agreement between parties. One of the most well-known standards with regard to safety in the machine sector is EN 954-1, which was published at the end of 1996 and harmonized in the Machinery Directive. This standard is a **B1 standard**, which describes principles for the design of safety related control systems.

Previous approach in machine construction

EN 954-1: Machine safety: safety-related control systems components

The EN 954-1 is based on the results of risk analysis and describes methods for reducing the risk of safety-related control system components. The measures are divided into categories B, 1, 2, 3 and 4.

EN 954-1 clearly establishes that programmable systems cannot be used in a single-channel configuration for safety-relevant applications. The (at the time of EN 954 publication) IEC 1508 was already cited as a reference for such systems.

The focus of this standard, therefore, lies in structure requirements as well as “proven” components and principles. Safety integrity is achieved via fault recognition (diagnosis) and redundancy (multi-channel structure).

The **requirements for safety management** are relatively ambiguous and vaguely formulated: “The developers must guarantee that the safety-relevant function meets all requirements that are specified in the result of the risk analysis” ...

The derived **application standards**, also called C Standards, contain all safety requirements for a single machine or group of machines. An example is EN 693, which describes the safety requirements for hydraulic presses.

Hundreds of C Standards have already been published, which refer to EN 954-1, so the EN 954-1 standard is the standard of reference for machine construction.

The new approach

IEC 61508: functional safety of safety-related electrical/electronic/programmable electronic systems

As the use of complex and/or programmable electronic systems increased in the 1970s and 1980s and corresponding specific problems arose, it quickly became clear that basic guidelines were lacking. Particularly in the area of software development, the probability of implementing a systematic fault in the design phase was (and still is) completely underestimated. The analysis of accidents shows with shocking consistency that around 40% of all faults are generated during the specification phase.

Unfortunately, these systematic faults cannot be completely controlled: they must be avoided as far as possible. A detailed quality management system based on the "four-eyes" principle is a traditional approach, which is the basis for the IEC/EN 61508. This comprehensive document deals with functional safety and was originally written for

- manufacturers and users of programmable safety-related systems
- and authors of sector-oriented, safety-relevant standards, including:
 - Process industry (IEC/EN 61511)
 - Railways (EN 50128 series)
 - Medicine (IEC/EN 60601 series)
 - Machines (IEC/EN 62061)
 - Burner control (EN 50156)

However, IEC 61508 can be applied for every safety-relevant system, regardless of the technology.

In addition to the management requirements addressed above, failure rates are also required. The integrity of a safety function depends on two aspects:

- Structure (as before)
- Failure probability (new)

Structure

The structure of a safety function must fulfill two requirements:

- Fault prevention or detection, described by the proportion of dangerous faults.
- Fault control, achieved by increasing the number of channels, i.e., by increased fault tolerance of the hardware.

The following table shows the relationship between the two requirements for complex components (type B):

Proportion of non-dangerous failures	Hardware fault tolerance		
	0	1	2
< 60%	-	SIL1	SIL2
60% - ≤ 90%	SIL1	SIL2	SIL3
90% - ≤ 99%	SIL2	SIL3	SIL4
> 99%	SIL3	SIL4	SIL4

In order to classify the diagnostic capability of a system, IEC/EN 61508 has introduced a new concept: the “Safe Failure Fraction“ (SFF).

Failure probability

Components do not last forever. That is obvious. But it requires a great deal of effort to describe it. The problem is that the failure rates depend strongly on the particular technology used and ambient conditions and that every component technology has its own failure

modes, sometime depending from the actuation frequency: an electromechanical contact will no longer open (contacts welded) if it has been actuated too often. It will no longer close if the actuation frequency is too low (contact material corroded). This fact leads to 2 operation modes:

- **Operation in the low demand mode** (PFD_{avg}) up to one safety-relevant function demand per year, typically used in the process industry.
- **Operating mode in the high or continuous demand mode** (PFH_D) more than one safety-relevant demand per year, typically used in the machine sector.

Several tools are available for the calculations, for example SISTEMA from BGIA,. For particular structures (1oo1, 1oo2, 1oo2D etc.), some formulas are available in Part 6 of IEC 61508. However, these formulas assume that the failure rates are constant. But this is not always true (for example, with mechanical components or if electronic systems are at the end of their service life).

Derived sector standards for machine safety

The **IEC/EN 62061 standard** makes recommendations for the design, integration and validation of safety-relevant electrical, electronical and programmable machine control systems (SRECS). The technical requirements of the IEC/EN 61508 have been tailored accordingly and the failure rates (PFH_D) are specified. Non-electrical components are not explicitly mentioned, but the framework and quality management can also be used here. In addition, in this standard and in ISO 13849-1, users will find a table with the relationship between SIL and the previous categories from EN 954. General requirements for quality management are part of the IEC/EN 61508 standard. IEC/EN 62061 references the corresponding parts.

<Fig. 1>

One reason for writing **ISO 13849-1** was to avoid that the C Standards would not suddenly be obsolete ... In this standard, a link between the old categories and the “new” world was created, the approach of IEC 61508 (quality management, structure and reliability requirements) was taken into consideration and Performance Levels were born. On the one hand, it is based on the old categories and on the other, it refers to failure rates as further evaluation criteria. As a parameter for reliability, the “Mean-Time-To-Dangerous Failure“ ($MTTF_d$) was introduced instead of failure rates, which makes the formulas somehow cluttered. Also, the “Safe Failure Fraction” has been replaced by “Diagnostic Coverage“ (DC)“ (ISO assumes that there are no safe failures ...).

<Fig. 2>

Competition or supplementary?

It cannot be denied that both standards focuses on the same field of application. However, the approaches differ:

IEC 62061 has the full flexibility and variability of IEC 61508. It is well suited for complex systems.

ISO 13849-1 describes systems with limited degrees of freedom and based upon the categories of EN 954. The advantage here is that the transition between categories and modern state of the art can easily be accomplished. Another positive effect is that the C Standards can still be used.

Therefore, both standards have their uses. A report titled *Guidance on the application of ISO 13849-1 & IEC 62061 in the design of safety-related control systems for machinery* is available to help determine which standard is appropriate for a particular application. This recommendation is also found in both standards.

Manufacturers of safety-related components and systems support both approaches and provide the relevant data.

<Fig. 3>

Key words: Functional safety, SIL, sector standards, safety technology, IEC62061, ISO 13849, EN 954, machinery directive, safety aspect, machine construction, PL, Performance Level

Author: Dipl.-Ing. Patrick Lerévérénd,
Trainer for explosion protection and functional safety
Division Process Automation

Co-Author: Dipl.-Techn.-Red. Xenia Döbling
Technical Editor
Division Process Automation

Characters: 7,439, without space characters

Characters short text: 445 without space characters

Pictures: No. MC7522_090116_01, No. MC7522_081031_07, No. MC7522_090917_20

October 2009



Fig. 1: Elevator: safety function according to SIL



Fig. 2: Wind power plants: safety function according to ISO 13849-1 (standard proposal)



Fig. 3: Rotary encoders: suitable for SIL 3 and PL_e