Series of articles Functional Safety, Part 1

FUNCTIONALE SAFETY

Product lifecycle management – but how!?

Light in the jungle of standards

Motivation

The topic of functional safety in industrial automation has grown in importance in recent years owing to the increased cooperation, or collaboration, between man and machine. Component manufacturers are therefore having to address the issue now more than ever before.

While large, highly process-driven companies may find it easier to adjust their processes to the strict requirements of IEC 61508, smaller, more customer- and solution-oriented manufacturers of sensors and actuators, with their lean and efficient processes, find their flexibility significantly impacted.

This two-part technical article serves to provide assistance to SMEs who are dealing with functional safety for the first time, offering as a starting point a brief overview of the complex topic.

The first part explains the principles of functional safety, the relevant standards and the safety lifecycle of a product.

The second part describes the steps a company should take in order to integrate this both practically and pragmatically.

The basics

Firstly, it should be noted that functional safety forms only part of the overall safety of a system. Other topics, such as electrical safety, must be considered separately.

Generally speaking, the term ‘functional safety’ is used when the safety of a system at least partially depends on the correct implementation of a safety function. Functional safety must therefore always be considered from the perspective of real applications and real dangers. Dangers are divided into four safety integrity levels (SILs), from SIL 1 (low) to SIL 4 (high). In industrial automation, only SIL 1 to SIL 3 are considered. Categorisation takes place by means of a two-part risk assessment process.

When it comes to functional safety, it is essential that dangerous failures be avoided or kept under control. These faults are always associated with the failure of a safety function.

It is widely accepted that a dangerous failure exists when a defined safety function is not available upon request. An example of this can be seen during the monitoring of a safety door. If the door is opened, the safety function should ensure that no danger is posed to those who enter

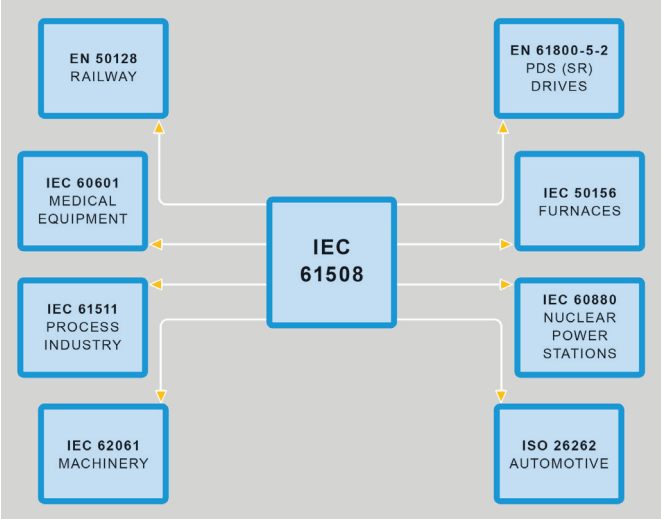

Figure 1: Functional safety standards

the safety area. In its simplest form, this may mean that the machine is intentionally shut down. In this case, anything that leads to the shutdown not taking place or not being able to take place is considered as ‘dangerous’. This may, for instance, be an issue embedded in the system caused by an error during assembly or by a random hardware failure in the logic control.

By analysing their root causes, one finds that failures can be divided into two main categories: systematic and random.

Random failures occur only in electrical/electronic components and normally cannot be avoided. IEC 61508 Part 2 addresses this, noting that for defined technical elements, defined component faults, such as short circuits or interruptions to electrical resistance, must be identified if they can lead to a dangerous fault. Faults are detected by means of additional diagnostics in the product itself or on a higher system level, for example by means of test pulses from a PLC. This recognition then triggers an error response, as a result of which the recognised dangerous fault is no longer relevant from the point of view of functional safety. In industrial automation, the most common error response is to switch off the machine. The diagnostics increase the proportion of safe failure fractions (SFFs) that are viewed as positive when it comes to functional safety.

The IEC 61508 standard makes clear specifications between the SFF – the so-called hardware fault tolerance (HFT) –

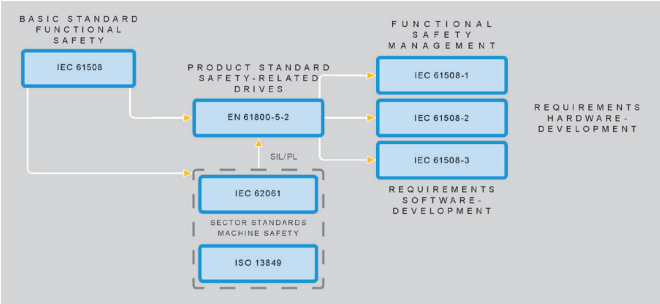

Figure 2: Overview of the relationships between standards

and the maximum achievable SIL. A single-channel system has an HFT of 0, as a single failure would result in the loss of the safety function. A dual-channel system therefore has an HFT of 1, as at least two errors would be required for the safety function to fail.

As the SIL goes up, so too do the requirements on HFT and SFF. For example, when complex electronic components are used, a SIL 2 device is possible in a single-channel system with an SFF of at least 90% and in a dual-channel system with an SFF of at least 60%. The system architect can therefore work with the parameters of redundancy and diagnostics.

Systematic errors can occur throughout the entire product lifecycle, from faulty specifications and design errors during product development to installation and operational faults.

In addition to higher-level functional safety management, IEC 61508 Part 1 also requires specific quality assurance measures for individual phases of the entire product lifecycle in Parts 2 and 3.

Standards

Figure 1 illustrates the relationships between the various applicable standards. The focus here is on standards that are related to functional safety. Other standards, such as those that stipulate compliance with the EMC Directive or Low Voltage Directive, are not shown here.

For new industry players, it can prove particularly challenging to navigate these standards and get to grips with the relationships between them. Figure 2 helps to make this easier to understand.

The starting point is IEC 61508, the basic standard for functional safety, which serves as the basis for several other sector-specific standards. However, it is important to note that IEC 61508 is not a harmonised standard. As such, users must first select the harmonised standard that applies to them.

For safety-related electrical drive systems, EN 61800-5-2 specifies an applicable product standard.

This product standard, however, refers back to IEC 61508 Part 1, which covers functional safety management, and to IEC 61508 Part 3, provided the device's software affects the safety function.

These relationships are somewhat complicated by the fact that there are two equal standards for system integration in mechanical engineering (IEC 62061 and ISO 13849) and that the system integrator can decide between them. The reasons for this lie in historical developments, when electronics and software entered the domain of functional safety in the 1990s. Component manufacturers are now keen to make their products universally applicable to both standards. Since IEC 62061 is a sector-specific derivative of IEC 61508, this does not pose any major problems. However, ISO 13849 has several additional requirements in terms of product development, most notably in that it defines performance levels from a to e, instead of using SIL.

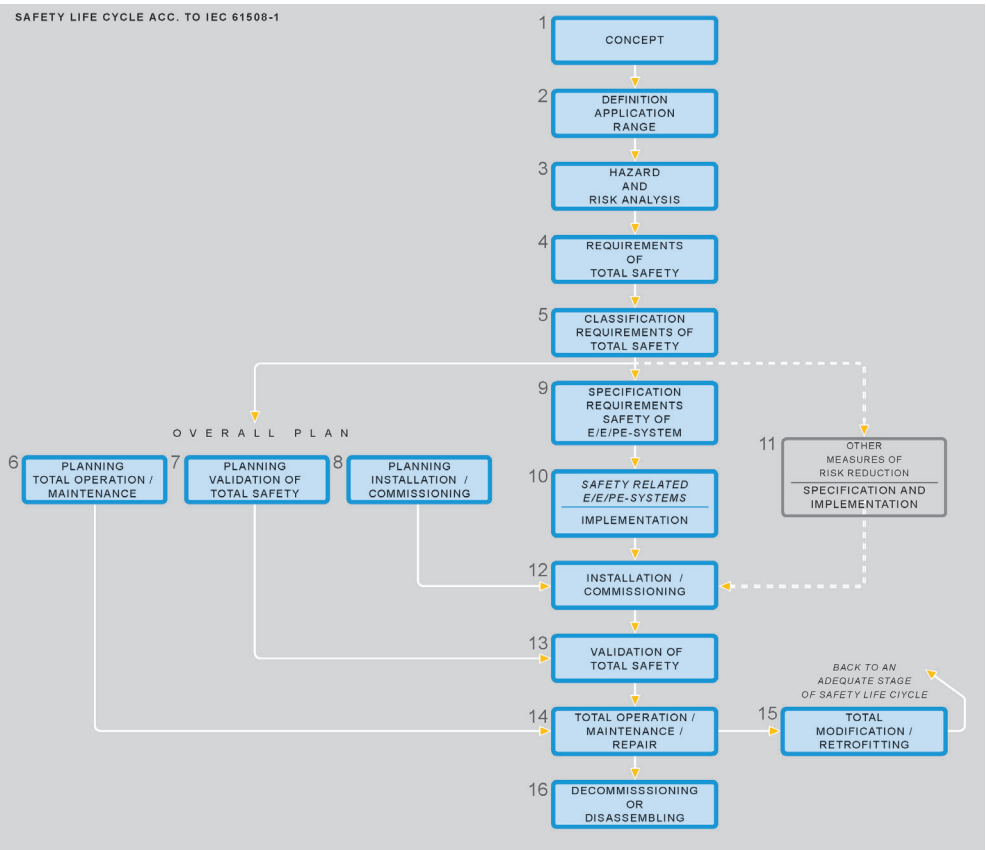

Figure 3: Overview of the safety lifecycle

Product lifecycle

To examine product lifecycles more closely, we must first refer to the safety lifecycle detailed in IEC 61508 Part 1, as shown in Figure 3. To help identify the phases relevant to component manufacturers, the system here is depicted as a whole. From the point of view of industrial automation, the lifecycles of system operators, mechanical engineers and manufacturers of safety components are nested.

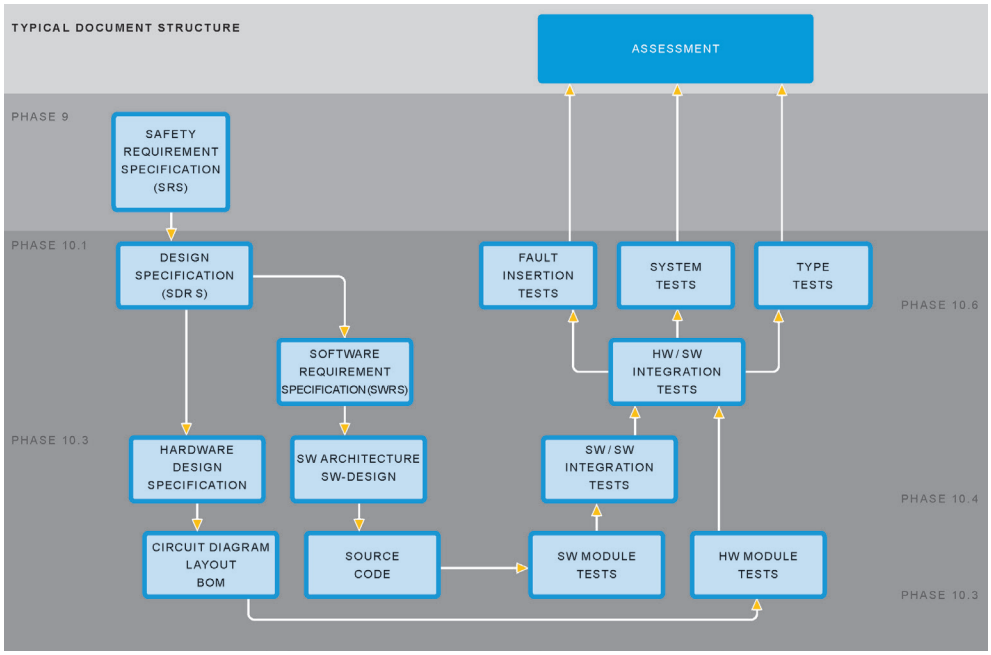

Figure 4: Typical document structure for a safety-related component

Note: Each phase, or rather each document, is checked and approved via a pre-defined means of verification (e.g. a review). The documentation and verification serve, among other things, to prove that the safety requirements described in the documents, including the SRS and SDRS documents, can be found and tested in the architecture, design, technical documentation, circuit diagrams and source code. This is known technically as "traceability". However, test specifications are also created in parallel. Tests, running through the right branch of the V from bottom to top, are carried out in accordance with these test specifications and reports.

For a component manufacturer, the situation is as follows: The primary phases relevant to manufacturers are phase 9 (defining requirements) and phase 10 (implementation, i.e. product development and testing).

Secondary phases include phases 12, 13, 14 and 16, during which the manufacturer informs the system integrator/ operator about the safety manual. Interestingly, the most important phase for a component manufacturer is phase 10, and in Part 2 and Part 3, this phase is further subdivided into phases 10.1 to 10.6.

Often, the standard is misinterpreted in that it is perceived that business processes have to correspond to these phases exactly. This is not the case. In most cases, it makes more sense to maintain the processes in place and selectively deviate from the standard. However, one thing that the standard makes clear is the basic procedure, which is namely to plan and proceed in clearly defined steps.

In practice, the development of a safety-related component results in a V-shaped document structure, as shown in Figure 4.

Planning is usually done in Functional Safety Management Plans and Verification and Validation (V&V) Plans. In a typical project, SRS and SRRS documentation and design specifications for hardware and software gradually emerge along the left branch, and only at the end does classic technical documentation appear, such as circuit diagrams and source code.

In component development, there are usually three levels of testing: module tests for hardware and software, integration tests, and system tests, including the compulsory assessment.

We strongly advise involving the assessor as soon as possible to guarantee the project's "safety strategy". While this may seem like extra effort at the start of a project, it pays off down the line, helping the project to progress more swiftly.

Summary

Neither starting out with the topic of functional safety, nor its practical application are easy. Experience plays an important role here. To save time and money in the long run, we recommend getting external support. This helps you complete the learning curve faster and allows you to benefit from the experience of others. A combination of basic training, workshops, advanced training and consultation accompanying the project is advised. As an expert in product development and consulting, MESCO supports component manufacturers and helps them from the very first step meet the various requirements during a product's lifecycle.

Autor: Dr. Johann Pohany
Managing Director
Medidtcine Consultants
www.medidtcine.com

Autor: Armin Götzmann
Managing Director
MESCO Systems GmbH
www.mesco.de