FUNCTIONAL SAFETY

Functional Safety Management according to IEC 61508-1

Series of articles Functional Safety, Part 8

This is the last, i.e. the eighth article on the topic Functional Safety for KMU. With this, we are ending the series with a résumé. The following short summary of the contents of the interrelated articles gives the relevant gist once again.

Light in the jungle of standards

Part 1 of the series of articles illuminated the world of standards, described the individual standards, their correlations and the formal needs required by the standard.

The standards of functional safety that have differentiated into various sector-specific/product-specific types over time mainly help to avoid damages to persons and material assets. The effect can be seen by means of statistics, optimally via drastically reduced values.

However, there are inconsistencies in this process: Thus, there are two equal standards for mechanical engineering with the IEC 62061 and ISO 13849. The system integrator can opt for one of the two standards. However, both the standards are quasi mandatory for the component manufacturer for marketing reasons.

The ISO 13849 leads to some additional requirements for product development. The most evident is that ISO 13849 defines a so-called *Performance Level* (PL a to e) instead of SIL.

The most basic uplift resistance function *Safe Torque Off* (STO) can principally be implemented as purely hardware-based. EN 61800-5-2 provides good support for the same. On the other hand, it becomes interesting when more complex uplift resistance functions are required.

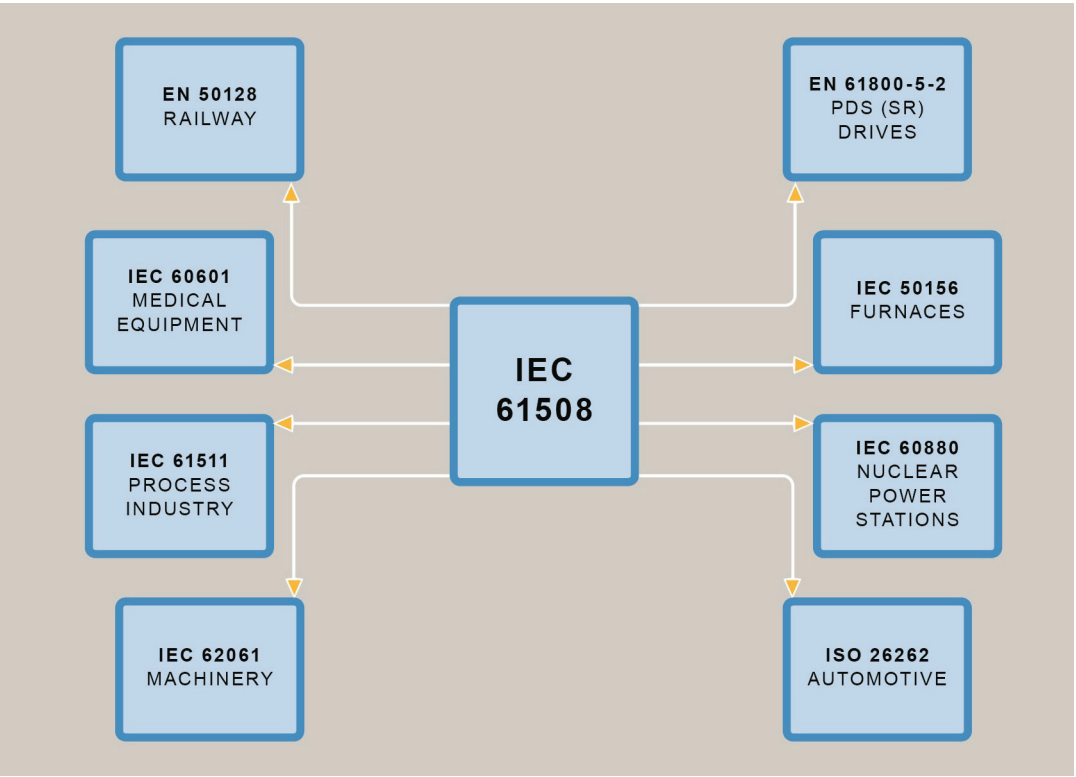

Figure 1: Standards of Functional Safety

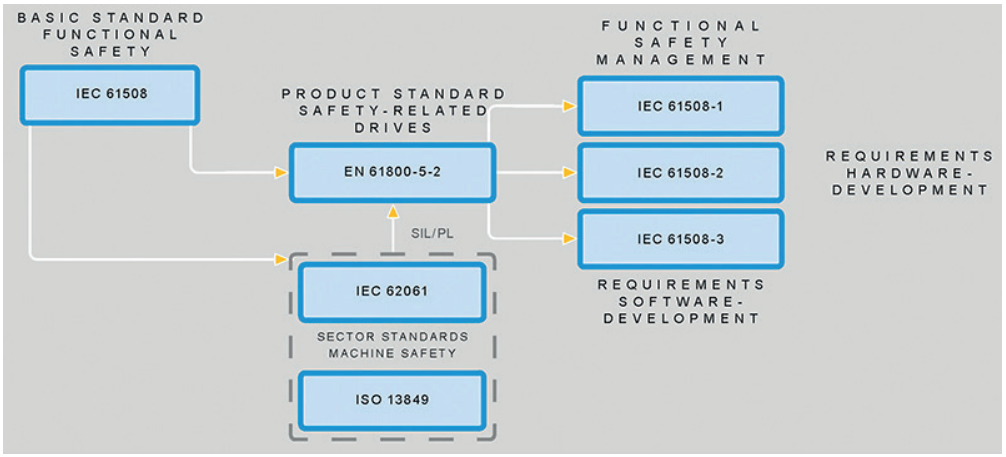

Figure 2: Correlation of the standards in industrial automation

In practice, such functions are implemented in the software. For software, the drive standard refers to IEC 61508-3. Increasing *Safety Integrity Level* (SIL) leads to high requirements for software development – such as the methods used and the verifications to be carried out, including the tools used. This requires documentation, as shown in Figure 3.

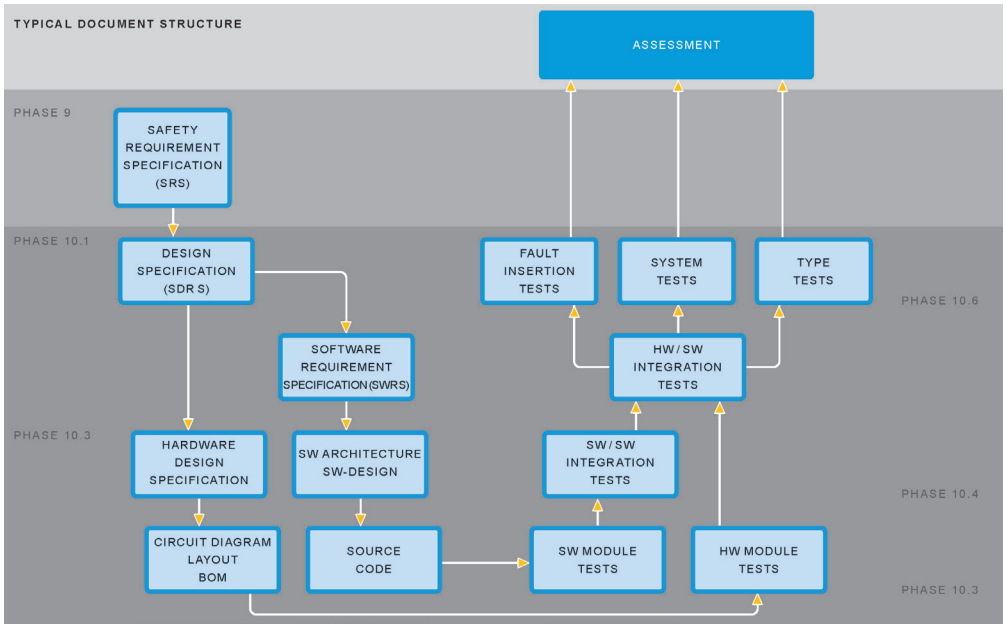

Figure 3: Typical structure of documents in the development of a safety product

The safe way

Part 2 provided support for former SRS-project phases and dealt with the development and the correct contents of a Safety Requirement Specification (SRS).

An important phase of every development in the field of functional safety is Requirement Engineering, i.e. the phase of creating the requirements. Planning is usually carried out in the superimposed Functional Safety Management Plan and in the *Verification and Validation Plan* (V&V-Plan).

The typical documents SRS, SDRS, Design Specifications for the hardware and software and only at the end, the classic technical documents such as circuit diagrams and source code then emerge gradually in the project along the left branch.

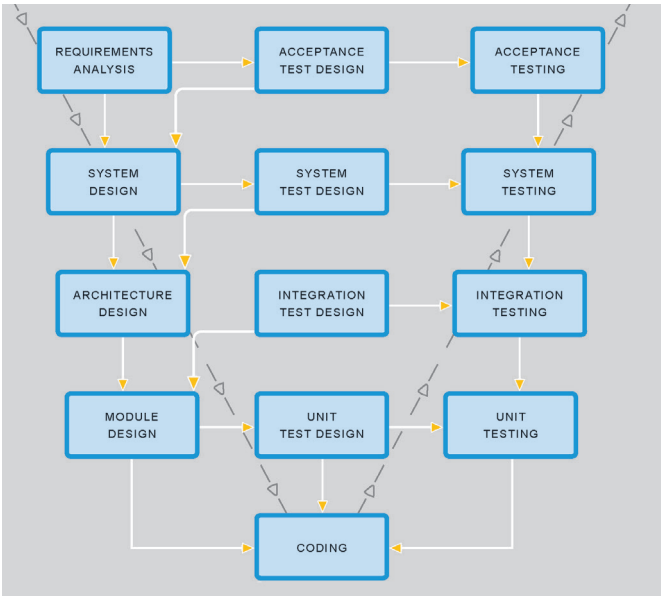

Figure 4: V-model

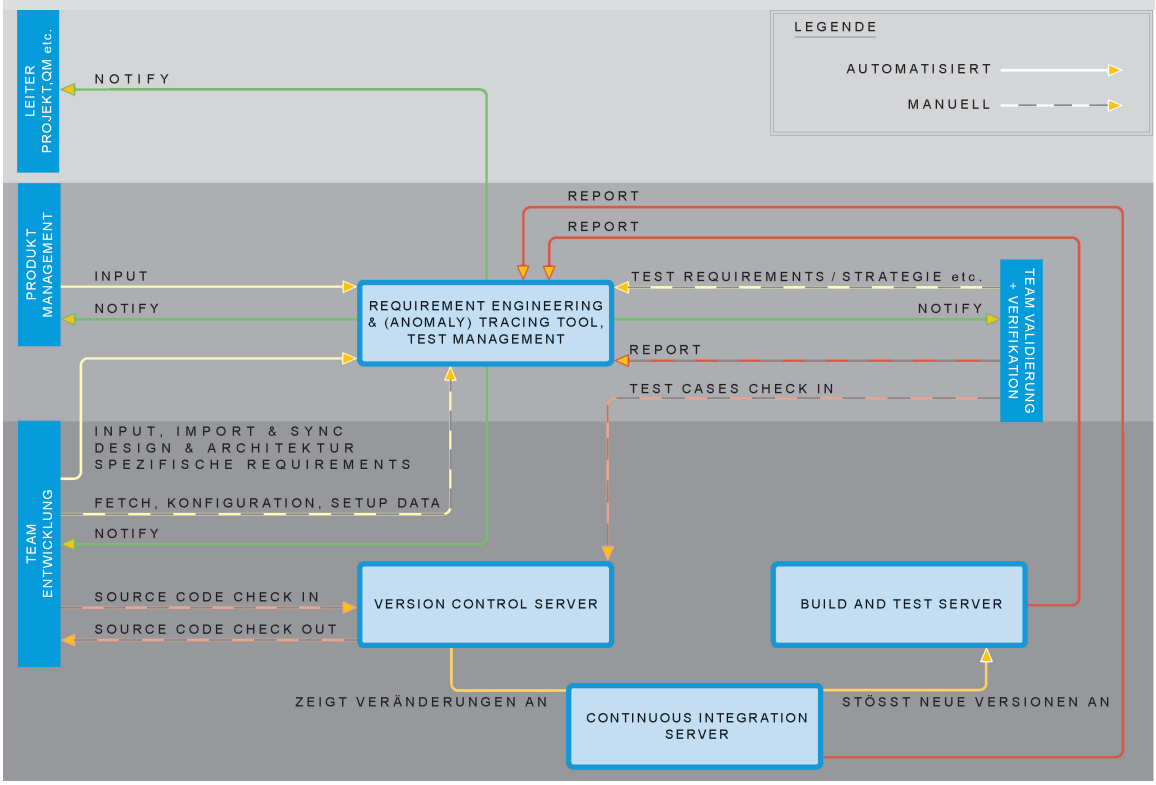

Figure 5: Complete overview of the Software Development Toolchain

Toolchain – from Requirement to Test Case

Part 3 of the series discussed the (software-) development process and the Product Lifecycle Management Environment, the Documentation and Development Environment, wherein a traceable and auditable product that is certifiable according to the rules of IEC 61508 should emerge from the requirements.

The traceability of the requirement till the performed test and the verifiable statistical statements arise due to the integration of the Tools. The Toolchain is a combination of the processes with these tools. Only the processes can generate the evidence and traceability with great difficulty and with a lot of efforts. Even the ToolChain cannot afford this without integration and the defined processes. An intelligent integration of individual tools combined with intelligent processes, which are adjusted to the required Safety Integrity Level (from Standard Development without SIL requirement up to SIL3 requirement) is the tool of choice. Figure 5 demonstrates this.

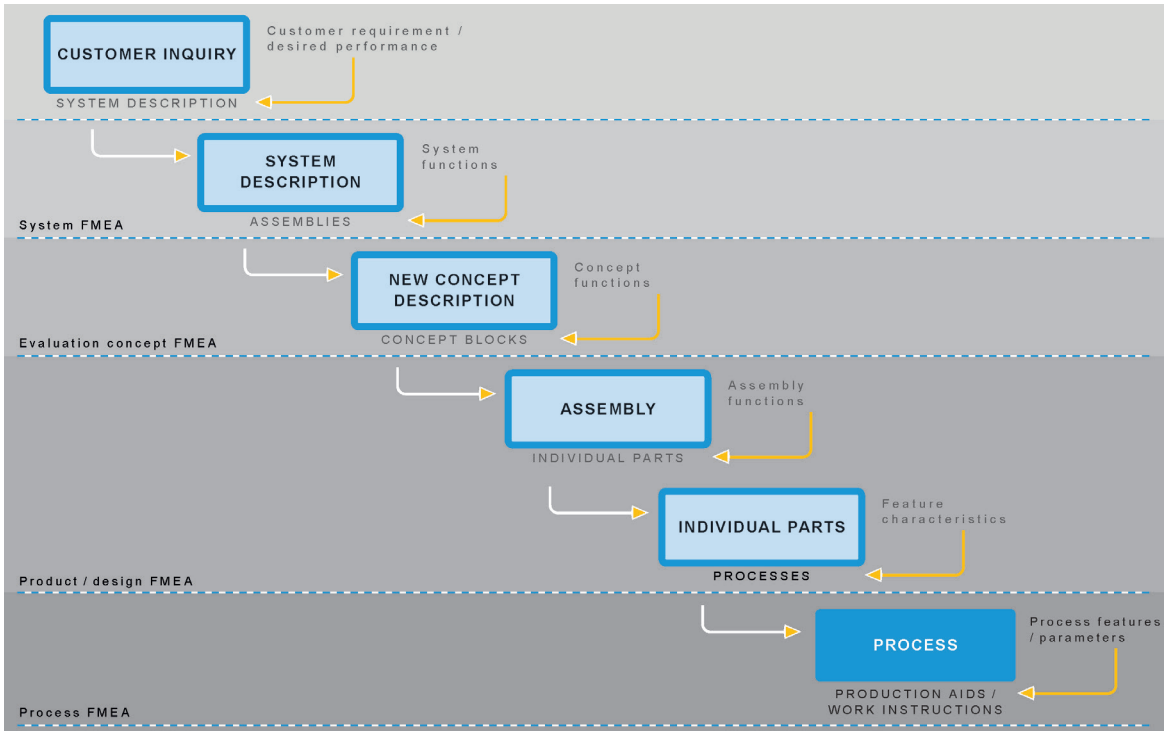

Figure 6: Different FMEA in the Product Development Process

FMEA – Failure mode and Effects analysis

We dealt with quality planning and system-FMEA in the safety project in two articles (Part 4 + 5). Their application in practice is often a time-consuming task with some obstacles.

The aim of investigating the *Failure mode and Effects analysis* (FMEA) on one hand is the preventive detection of the links to potential errors, causes and consequences as well as the prioritisation of the Cause and Effect chains in terms of their risk. On the other hand, the aim is preventive introduction of corrective actions for the Cause and Effect chains with high risk. Figure 6 shows different FMEA in the Product Development Process.

	HARDWARE FAULT TOLERANCE FOR SAFETY-RELATED ELEMENTS					
	HFT=0		HFT=1		HFT=2	
SHARE SFF	**TYP A**	TYP B	**TYP A**	TYP B	**TYP A**	TYP B
< 60%	**SIL 1**	—	**SIL 2**	SIL 1	**SIL 3**	SIL 2
60% – < 90%	**SIL 2**	SIL 1	**SIL 3**	SIL 2	**SIL 4**	SIL 3
90% – < 99%	**SIL 3**	SIL 2	**SIL 4**	SIL 3	**SIL 4**	SIL 4
≥ 99%	**SIL 3**	SIL 3	**SIL 4**	SIL 4	**SIL 4**	SIL 4

Figure 7: Correlation between HFT and SFF

System FMEA in safety project

Part 5 argued the use of the FMEA tool in the development of functionally safe components. It described the step from normative requirements to practical application and used the typical requirements of factory automation: SIL3, Requirement Rate High Demand.

Depending on the safety integrity level to be achieved, the standard sets concrete specifications as regards the *Hardware Fault Tolerance* (HFT) and *Safe Failure Fraction* (SFF) to be achieved. In addition to failsafe design principles, diagnostic measures of keys contribute to a high SFF. The table in Figure 7 demonstrates this correlation.

The variety and the interdependence of the influencing factors complicate the application, especially in case of newcomers and often lead to sub-optimal results if used incorrectly. The typical negative consequences in practice are the need for adjustment-developments, which can be detected only later during the development cycle. But it is also Over-Engineering of safety measures that are at the expense of the availability of the product and unnecessarily increase the price of the product. Design Packages for safe propulsion technology on the basis of EN 61800-2 minimise such risks.

In addition to highly product-specific blocks such as the power unit and the control unit, function blocks such as Diagnostic Functions as well as Communication & IO-Block are suited to the standardisation as a generic function block, which ultimately saves time, effort and personnel and can be reused. In the form of:

- requirements
- accepted documentation
- specific FMEA
- specific Test design and Test protocols

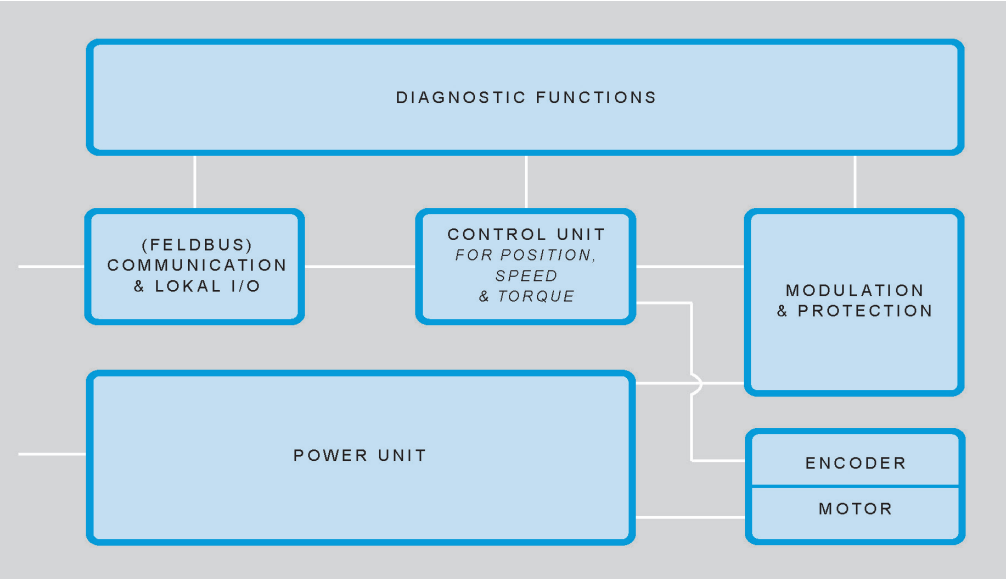

Figure 8: Block diagram of safety drive - PDS(SR)

FSM according to IEC 61508-1 – FSM as part of QM

In Part 6, we have dealt with the question of which topics or requirements arise from the IEC 61508-1 for the component manufacturer and which departments are influenced by the same.

Functional safety does not work without the support of the top management. The IEC 61508 is not just another standard that must be adhered to by the Development Department. It concerns the whole company. IEC 61508 provides a detailed definition of the *Management of Functional Safety* (FSM) as an extension of an ISO 9001-Quality Management-System. In practice, a combination of adjustments is mostly made at multiple places:

Figure 9: Correlation of QM / FSM

- Introduction of additional processes
- Introduction of additional /new tools
- Adjustment of milestone-checklists
- Adjustment or recreation of templates
- Introduction and description of new methods (e.g. for carrying out a FMEDA)

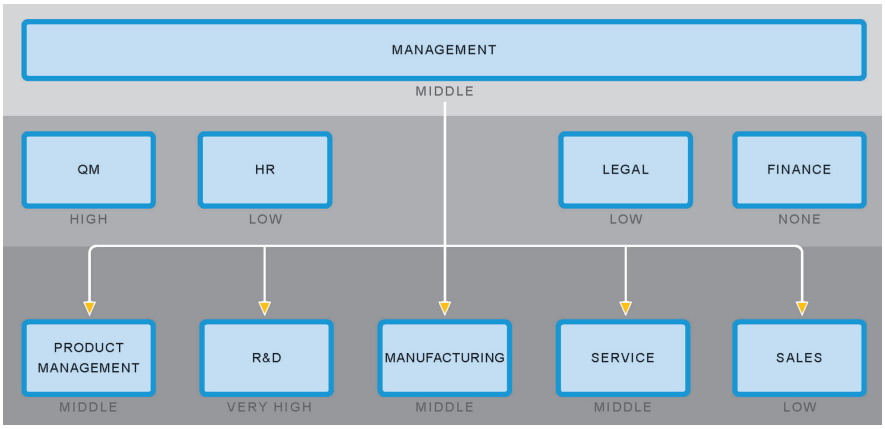

Figure 10: Affected departments. The extent of the effects of Functional Safety can be quite astonishing. The following chart shows an overview of the affected typical departments.

A résumé

This information, these charts and presentations illustrate why the introduction of a FSM system and the structure of a Functional Safety Development make sense. However, they also indicate that this is time-consuming, goes far beyond development, has pitfalls in all respects and is best tackled as a project.

The greatest motivation to take up this challenge is often the increasing demand for safety products and the risk of falling behind in competition without safety products in the portfolio. Customers prefer buying from a single source.

For a technical pre-project to set up a Functional Safety Management System, three to six months should be estimated. However, the duration of the lead time of a development project depends greatly on the company, the inventory processes and the available resources.

The management of functional safety overlaps quite a lot with quality management. Therefore, it does not make sense to separate the disciplines. It has proven useful to regard the FSM as a subset of QM. If the ISO 9001 and a long-standing management exists in the company, then there's already a stable basis for introducing a Functional Safety Management.

Process orientation while developing the product contributes significantly to avoid development risks, to improve the product quality, to reduce Product LifeCycle Costs, to meet the external auditing and certification criteria and lastly to reduce the time-to-market.

It takes experience, expertise and pragmatism to build (or adapt) the required structures and to avoid a typical over-interpretation of the requirements.

The series of articles has shown that processes and structures should not hamper, but in fact help to create intellectual freedom from which true innovations emerge.

Authors:
Dr. Johann Pohany, Managing Director
Medidtcine Consultants / www.medidtcine.com

Armin Götzmann, Managing Director
MESCO Systems GmbH / www.mesco.de