FUNCTIONAL SAFETY

Functional Safety Management according to IEC 61508-1

Series of articles Functional Safety, Part 7

Introduction and background

In the previous article, we presented the system FMEA as a method for identification of diagnostic measures to detect and control errors during operation in the context of functionally safe production development. This primarily concerns the random hardware failures. If we now consider the real failures in the field, then we would see that they can often be traced back to systematic causes. Consequently, Part 1 of IEC 61508 comprehensively defines Functional Safety Management (FSM) as an extension of the ISO 9001 quality management system.

This article in the series also focuses on the perspective of the manufacturer of a safe component. This primarily restricts the part of the safety lifecycle to be considered to phases 9 and 10.

As already emphasised: The standard is generic and is supposed to be applicable for a wide range of market segments. This hampers the readability, and a relevant and practical interpretation for the respective areas of application must be ensured.

Topics

The first question is – What are the topics and/or requirements that IEC 61508-1 defines for the component manufacturer in the first place?

A range of extremely important topics:

- Appointment of the responsible persons for management of functional safety
- Definition of activities to be carried out by these persons
- Specification of the information necessary for the execution of the (relevant) phases of the safety lifecycle
- Specification of information to be communicated between the relevant parties

Other requested processes / procedures:

- Assessment of functional safety
- Verification and validation activities
- Configuration management
- Execution of regular audits
- Implementation of modifications
- Ensuring appropriate qualifications of the persons concerned

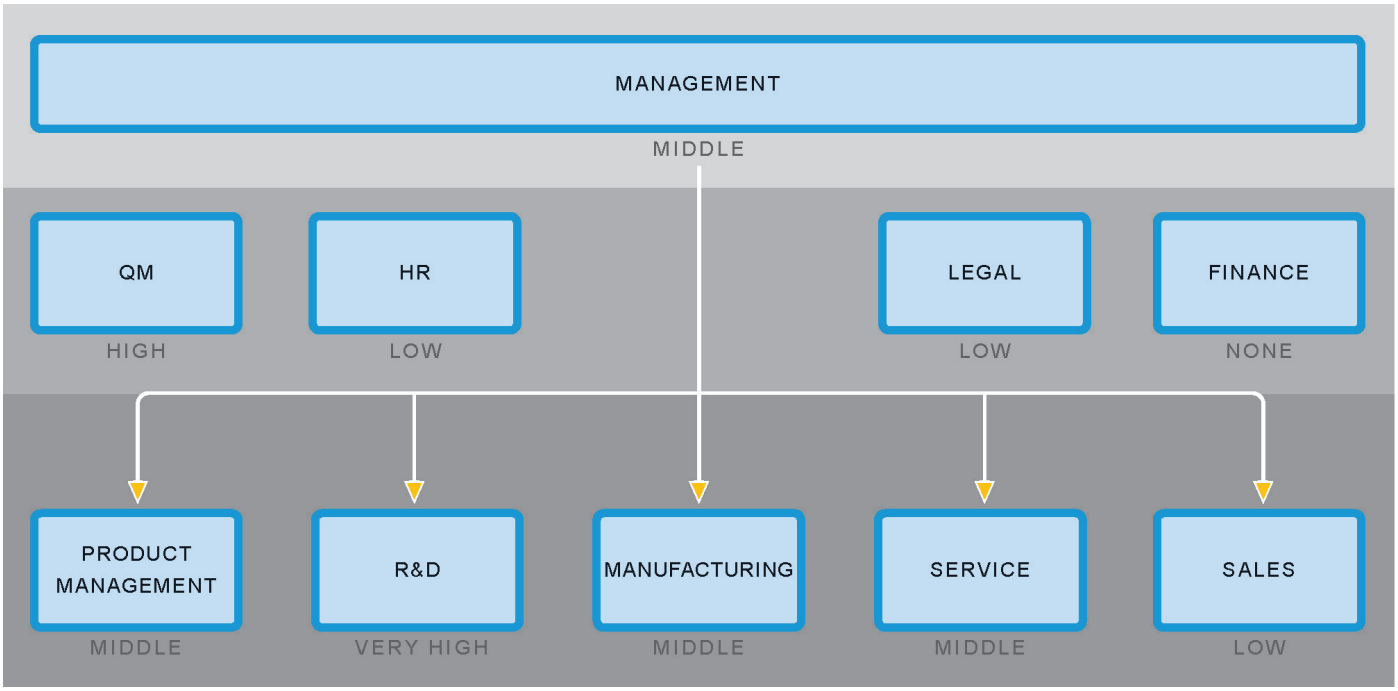

Figure 1: Company departments that can be affected

It will be clear from the first point itself that functional safety cannot work without the support of the top management. The IEC 61508 is not just another standard to be complied with by the development department. It affects the entire company. The extent to which functional safety can affect a company can be surprising. The following diagram shows an overview of the typical company departments that can be affected by this.

In the following, we will go into greater detail about a few individual topics and present possible interpretations of the often abstract standard requirements as well as ways to implement them for the component manufacturer.

Responsible persons

The list above shows a close link to the quality management department and to the person who bears the responsibility to set up and maintain the FS management. The overall responsibility for the management of functional safety is generally assigned to the Head of the Quality Management department and a new role of the Functional Safety Manager may often be additionally assigned to the QM Head.

In bigger organisations where many safety development projects or safety projects are simultaneously in the active marketing stage, it may be practical to delegate a part of the responsibility, e.g. the responsibility for the operative FS supervision of a product family. In practice, the term Functional Safety Coordinator (FSC) is frequently used for this role.

The position(s) can be held by different people, e.g. employees from the Q department, the responsible product manager or a production supervisor. From the point of view of the standard however, clear regulation of the responsibility beforehand is more important than whom the responsibility lies with.

In order to prevent misunderstandings: More people should undertake a part of the responsibility, especially before and during the product development phase since the technical requirements as per IEC 61508-2 and IEC 61508-3 can generally be implemented only by the R&D employees. It would be possible to appoint the project head together with the deputy project head for hardware (for IEC 61508-2) and the deputy project head for software (for IEC 61508-3).

It is unusual to define explicitly new roles in the company. Instead, additional qualification requirements can be defined for the development engineers assisting in the safety project. The relevant people are mostly appointed as part of a (project-)specific safety plan.

Specification of necessary information

The standard requirement aims at defining the (additional) activities that must be executed and documented during the safety project in order to be able to conduct the obligatory final assessment of the functional safety for each project/product, before the start of the development project itself.

Since an FS development project is usually started during a development process according to the V-model, the conceptual run of V helps in identifying the additional activities systematically. The detailed requirements for phase 10 resulting from IEC 61508-2 and 3 also should be fulfilled now.

The scope of additional activities depends, inherently and greatly, on the process maturity level of the organisation. If, for instance, dedicated test levels – module test – validation test are defined for the right branch of the V-model, the standardised requirements are already fulfilled. In this case, the Fault Insertion Tests to prove the efficiency of the diagnostic measures are an activity to be additionally specified.

Furthermore, the left side of the V primarily includes safety-typical activities such as safety plan, V&V plan, FMEA/FMEDA, derating analysis, (SW) tool chain validation and forward/backward traceability.

In principle, all the additional measures can be defined in the safety plan. This is primarily practical if this concerns a one-time safety development and the expenses incurred for direct process expansions can be avoided.

In practice, a combination of adaptations is implemented at several positions:

- Introduction of additional processes
- Adaptation of milestone checklists
- Adaptation or creation of templates
- Introduction and description of new methods (e.g. to conduct an FMEDA)

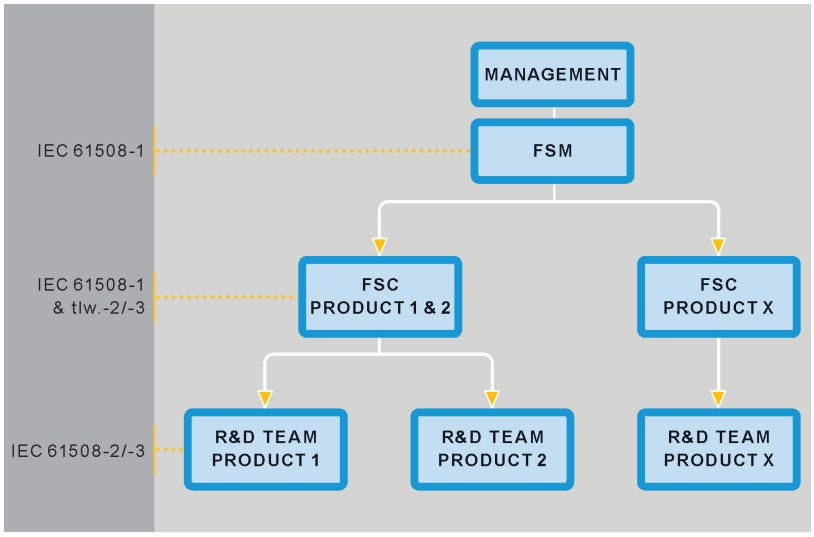

Figure 2: FSM organisation

Timetable for introducing an FSM system

The description above shows that the introduction of an FSM system is quite time-consuming and should ideally be considered a project in itself.

Since customers prefer to buy from a single source, the motivation for this is often an increasing demand for safety products and the risk of lagging behind competitors, without any safety products in the portfolio.

Ideally, the company management should already have the basic knowledge of functional safety and should assign the most suitable company department with this task.

The duration of the lead time for a development project largely depends on the company, the existing processes and the available resources. A reference value here is three to six months.

The existing processes are compared with the (relevant) requirements of IEC 61508 by means of Gap analysis. Here, it is practical to take into account three perspectives: the perspective of the existing processes, the company departments and the IEC 61508, which is used as a checklist so to say. This ensures that nothing is overlooked during the subsequent implementation of the necessary adaptations.

Existing processes or possible loopholes can be pointed out while working through the standard. This is helpful in a subsequent assessment as well, since the assessor bases his assessment on the standard.

The existing processes and company departments are first divided into relevant and not relevant processes. For example, the product development process as well as the development department are “clearly safety-relevant”, whereas departments such as finance and IT are not.

The next step is to check the relevant processes for their conformity to the standard. If ISO 9001 has already been introduced, it is possible that some existing processes already meet the standard requirements (e.g. document management, configuration management, version management), whereas some others need to be supplemented (e.g. development processes) or new processes need to be defined (e.g. audits and assessment of functional safety).

If existing processes need to supplemented or new processes need to be created, changes are drafted and the costs for introducing them is roughly estimated. The involvement of the process owners concerned as well as the definition of a sequence for implementation is recommended by this stage at the latest.

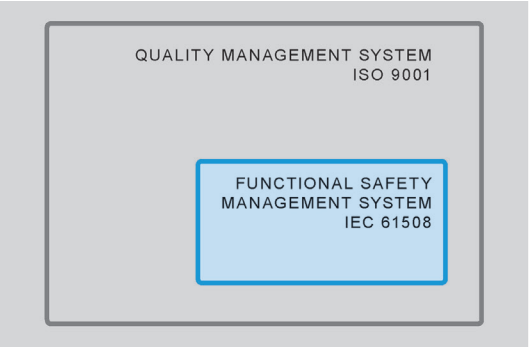

Figure 3: Correlation of QM / FSM

The Gap analysis is thus concluded with a definite timetable for the implementation of the necessary measures. The reference value for the time requirement of the entire analysis is 1 to 1.5 months.

The implementation takes place in multiple steps. The focus should first be on the creation of fundamental structures such as the advanced training of the employees involved. Only then will it be practical to focus on the development processes in order to then start with the generally long product development phase. The production-relevant processes and finally the processes for the sales and marketing can be adapted in parallel to this.

Summary

Functional safety management has many overlaps with quality management. A differentiation between the disciplines is thus not practical. It has been proven that FSM can be considered a subset of QM. If ISO 9001 is truly followed in the company and the process management is mature (towards CMMI Level 3), a stable foundation for the introduction of the Functional Safety Management has already been laid. However, if the manner of work greatly leans towards on demand, then this could mean major changes to the process structure in the company.

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

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