

Experience with Functional Safety Management Certification in the scope of IEC 61508 and 61511

Thomas Huber
TÜV Industrial Services GmbH
Automation, Software and Information Technology ASI

Abstract

IEC61508, Part 7 defines two possibilities, how to meet the QM-requirements for a safety related project:

1. “The establishment of regulations and measures for the creation and validation of safety related systems in cross project and project specific guidelines”
2. “The creation of an organizational model, especially for quality assurance (see standards such as the series ISO 9000-1 to ISO 9004-1 or similar) which is set down in a quality assurance handbook”

TÜV-ASI meets both possibilities with project related Functional Safety Assessment Activities (**FSAA**) and company specific Functional Safety Management Certification (**FSMC**).

The FSMC activities combine the approval and certification of Management of Functional Safety (**MFS**) measures according to IEC 61508 and/or IEC 61511 with focus on the Quality Management System of the audited company. It is an objective to create an applicable and manageable Functional Safety Management System (**FSMS**) to integrate a “Safety Culture” in the audited company.

The FSAA are usually integrated in the Type Approval Activities (**TAA**) of TÜV-ASI, which result for example in the certification of a new product. FSAA imply two different objectives, one are the basic MFS procedures and the other achieving the project specific safety requirements, for example the safety concept.

Over the last three years the Business Sector ASI of TÜV Industrial Services GmbH has cumulated experiences with FSAA and FSMC and the application of the related QM-Documents and QM-Procedures in numerous different projects.

The target group of these FSMC and FSAA are in general System Manufacturers (**SM**), System Integrators (**SI**) and Operators (**OP**).

1. Introduction

The following experience report gives an actual overview of interpretations and relations of IEC61508 and IEC61511 requirements which appear during FSMC and FSAA of TÜV-ASI.

Furthermore this report addresses the necessary organizational requirements of IEC61508 and IEC61511 for SM, SI and OP.

Recurring focal points discussed during FSMC and FSAA as represented in this presentation were:

- Basic requirements concerning the Quality Management of a company
- Allocation of Safety Lifecycle Phases (**SLCP**)

- Responsibilities in view of the applied SLCP
- Service Provider and Sub-Contractor
- Importance of Functional Safety Assessment
- Independencies of project members
- Information Feedback
- Procedure of Corrective Actions

2. Basic requirements concerning the Quality Management of a company

Both in the IEC61508 and IEC61511 there are basic requirements listed which should be covered by a company's Quality Management System (**QMS**). But it is not required that there must be an existing Quality Management System, for example according to ISO 9000 ff, to project E/E/PE Safety Related Systems or equivalent.

IEC61508, Part 7 gives a description of the measure "Project Management" (e.g. Part 2, Annex B) which includes two possibilities:

1. "The establishment of regulations and measures for the creation and validation of safety related systems in cross project and project specific guidelines"
2. "The creation of an organizational model, especially for quality assurance (see standards such as the series ISO 9000-1 to ISO 9004-1 or similar) which is set down in a quality assurance handbook"

To understand the importance of a QMS regarding safety it is necessary to ask for the meaning of a QMS for example concerning the development of an E/E/PE - Safety Related Systems or Safety Instrumented Systems (**SIS**).

On the one hand the purpose is to make work more efficient or effective. On the other hand, an applicable and manageable QMS is highly effective to avoid systematic faults during the SLC of a safety related project.

TÜV-ASI works with both possibilities. Possibility 1 is part of the project specific FSAA during a TAA, possibility 2 is the subject of the company specific FSMC. Please refer to the chapters before.

TÜV-ASI represents the opinion that it is also possible to create an applicable and manageable MFS on the basis of the "good engineering praxis" of a company. For this purpose a Management Handbook which covers the necessary requirements and MFS – procedures has to be produced which includes or refers to work procedures, work instructions and templates.

Nevertheless a basic quality management like ISO 9000 ff is a good basis for the implementation of a MFS-System. The greatest benefit is given by the existing experience of the company in quality management systems and the already existing procedures and instructions which can be reused for the MFS.

Of course the creation and the certification of a MFS-System based on "good engineering praxis" needs more time effort than a MFS-System based on, for example, ISO 9000 ff. Due to the reference of existing QM-procedures the FSMC can be focused on the additional FSM related requirements.

It is the company's decision if the "new" MFS – System is an integral part of an existing QMS or vice versa. It is typical for a company business to integrate the MFS-System in the existing QMS.

3. FSMC and FSAA Basic Procedures

To give a better understanding of the FSMC procedure and FSAA of TÜV-ASI a short review follows:

3.1 TÜV-ASI Functional Safety Certification Procedure

The following abstract of the Functional Safety Certification Procedure (BCP) is part of the Certification Regulation which is an important part of the Certification Contract between the company to be audited and TÜV – ASI.

Until today there are already four MFS certified companies and three further companies (D and SI) with certification activities in progress.

3.1.1 Step 1 – Kick-Off Meeting

The BCP starts with an informative Kick-Off Meeting (**KOM**) in which one or two auditors of the certified body and the representative of the customer participate.

The objective of the KOM is to define the audit scope and to agree upon and define the certification sequence according to the company's present conditions.

The definition is necessary for example in case not all SLC or SLCP, which are necessary for the development or manufacturing of a product, are covered by the company to be audited.

In the framework of the certification procedures, special attention has to be paid to these points of intersection towards other manufacturers.

Furthermore, the SLCP, which are relevant for the company's process to be audited, are identified and determined.

The certification procedure of FSMS is divided into the following steps.

3.1.2 Step 2 - Pre-Audit

At the beginning of a Pre-Audit (**PA**), the customer receives an audit plan which has been agreed upon with him.

The objective of a PA is to state deviations of the implemented Functional Safety Management System (**FSMS**) and the related management documents. At the same time, the company process to the relevant phases of IEC 61508 – Safety Life Cycle will be reflected.

The results of the PA will be summarized during the audit day in an Open Item List (**OIL**) which has to be used continuously.

The results of the PA together with the following described step are the informal basis of the Certification Audit (**CA**).

3.1.3 Step 3: Assessment of the Submitted Management Documents

During the Assessment of the Submitted Management Documents (**ASMD**) the identified management documents (e.g. management hand book, procedures and work instructions) will be proved and evaluated by the audit team.

The results of the documentation proof will be summarized in the continuously used OIL and the customer will be informed accordingly.

Should the management documentation not fulfill the fundamental requirements of the guideline, an additional discussion for clarification can be agreed upon.

After all open points have been concluded and all supplementary activities have been completed, the certification audit can start.

3.1.4 Step 4: Certification Audit

Step 4 starts when the customer receives an audit plan which has been agreed upon with him.

During the CA at the company's site, the effectiveness of the implemented FSMS will be examined.

Basis for the assessment is the application area to which the FMS refers to as well as the requirements of standard IEC 61508 or IEC61511. The audit questionnaire and the information obtained from the above mentioned audit steps serve as guideline for the assessment.

The company's responsibility is to demonstrate the practical application of its documented procedure in the audit.

For this purpose an actual FSM-Project will be reviewed.

After the conclusion of the audit, the customer will be informed of the audit result in the final meeting. Furthermore deviations as well as recommendations will be documented in the continuously used OIL.

After clarification of all deviations, the result of the certification will be documented in an audit report. Recommendations for the improvement of the FSMS will be given with the audit report.

3.1.5 Step 5: Granting of Certificate, Surveillance and Re-Certification

After positive examination of documentation relating to the certification procedure, the certificate will be granted by the Head of the Certified Body.

The certificate will only be granted if all mentioned deviations have been clarified and correction measures determined in writing.

The validity duration of the certificate is three years if a surveillance audit will be carried out at least once a year in the company.

Surveillance Audit:

For the maintenance of validity of the certificate, an annual or semi-annual (according to agreement) one day Surveillance Audit (**SA**) is necessary.

The topics of the SA are primarily all relevant amendments and/or innovations which have been undertaken by the customer in the meantime.

Besides, the proper use of the certificate as well as the effectiveness of correction measures to the deviations from the previous audit will be assessed.

After each SA, the client receives a report.

Re-Certification Audit:

Before the expiry of the validity duration, a Re-Certification Audit (**RA**) concerning the extension of the certificate for a further period of three years has to be carried out in the company.

The effectiveness of the complete FSMS will be examined in the RA.

The sequence of the audit will be carried out according to Step 4.

3.1.6 Basic MFS organizational measures and procedures

The following list gives an example of basic topics discussed and reviewed during the BCP:

- MFS organization
- Documentation requirements
- FSAA
- Safety Lifecycle Planning – SLCP relation
- Verification and Validation Processes
- Selection of fault avoiding measures
- Responsibilities and competences
- Integration of Service Providers
- QM-Procedures: Modification Management, Configuration Management, Tool Management, Change Management (Procedure of corrective actions)

Not included in the FSMC is the approval of the correct solutions for a safety concept, safety calculation or other non organizational project related specifications. This is part of the FSAA during the TAA, which is explained in the following chapter.

3.2. TÜV-ASI Functional Safety Assessment Activities

The FSAA and the relating requirements are defined in IEC61508, Chapter 8 or in IEC 61511, Chapter 5.2.6.1 which form the basis of the TÜV-ASI FSAA.

The FSAA concentrate on all organizational and project specific safety measures, for example during the development of an E/E/PE - System, which result in the certification of a new product. The FSAA is usually integrated in the TAA.

Considering the FSAA requirement of IEC61508 for SIL3-projects an organizational grade of independency has to be obtained. Consequently the customers of TÜV-ASI benefit from: on the one hand carrying out the type approval and on the other hand fulfilling the FSAA requirements of independency.

Therefore FSAA carried out by TÜV-ASI imply two different objectives: one is the achievement of basic MFS organizational measures and procedures and the other is the achievement of the project specific safety requirements, e.g. safety concept.

In general there is a project specific FSM-Meeting at the beginning of a project to define and review the basic MFS organizational measures, to clarify the role of the Assessment Team and its responsibilities and to plan the further assessment activities. Also the verification and validation activities have to be planned and documented, e.g. in the Verification and Validation plan (V&V-Plan).

Usually the FSAA are successfully carried out mainly for SM. For SI and OP the FSAA should be carried out according to IEC61511 which contains in principle the same requirements as the FSAA according to IEC61508. However for this target group a different perception is prevalent. (To be discussed subsequently.). In general the FSAA of TÜV-ASI can also be applied to these target groups.

It is often intended by the company under consideration to carry out one or more safety relevant projects intending to “learn” and to understand the MFS requirements and their means for the company’s Quality Management in a first step. In a second step it is intended to integrate and to certify the Quality Management.

Companies, which have a MFS will have the benefit that the FSAA for the MFS organizational measures are not necessary, which result in cost reduction for the type approval. Otherwise the validity of MFS organizational measures has to be re-assessed for each project.

4. Allocation of IEC61508-SLCP and related responsibilities for SI, SM, OP

The IEC61508 is a basic safety standard which applies to all possible safety related applications and users.

This chapter explains which typical allocations of SLCP should be considered by SM, SI and OP with focus on the IEC61508, Part 1 - Overall Safety Lifecycle (**OSLC**).

In general the OSLC addresses the SM, SI, and the OP. Also the basic requirements of the chapters 5 - Documentation, 6 - MFS and 8 – Functional Safety Assessment (**FSA**) have to be regarded by SM, SI and OP, and have to apply to all relevant phases of the OSLC.

To allocate the different phases to SM, SI and OP the SLCP scope descriptions (see IEC61508, Table 1) helps in a first step.

Of course, OP are seldom involved in the development of an E/E/PE Safety Related System. Also SM do not operate a plant or process. SI are more or less in the position between the OP and SM in view of the OSLC.

Because of this there are necessarily phases of intersections between the direct applicable phases OP, SM and SI are responsible for. The typical allocation and responsibility of phases to these three groups are shown in the following overview:

OP	Phase of responsibility	Phase of intersections
	Phases 1 to 5 Overall Concept, Scope Definition, Hazard and Risk, Safety Requirements and Allocation	Phase 5 and 9: To define functional and safety requirements necessary for an E/E/PES development (SM) or system application (SI)
	Phase 9 Not usually applied	Responsible for FSAA if SM, SI are subcontractors in a safety related project
	Phases 6 to 8 Overall planning for phases 12 to 13	Provide information to SM, SI for the completion of the (safety) requirement specification
	Phases 12 to 16 Overall Installation, Commissioning, Validation, Operation, Maintenance, Repair, Modification, Retrofit, Decommissioning	Operators have the overall responsibility, SM and SI could be subcontractors, for example for Factory Acceptance Test (FAT), Side Acceptance Test (SAT), Modification and other Services

SM	Phase of responsibility		Phase of intersections
	Phases 1 to 5	Not usually applied	Phase 3: Hazard Analysis of the E/E/PES to be developed (recommended) Phase 5: To define functional and safety requirements: Inputs provided by OP, Product marketing, Product Care (Services, Statistics)
	Phase 9	E/EPES – Realization	Within the E/EPES-SLC: Additional Subcontractors, e.g. for SW development or component suppliers. SM is responsible for the required safety integrity level of delivered components or subsystems. This can be controlled for example due to FSAA.
	Phases 6 to 8	Not usually applied	Provide sufficient information to End-user, e.g. OP or SI, that the consecutive SLCP could be carried out correctly
	Phases 12 to 16	Not usually applied	Operators have the overall responsibility, SM could be subcontractor, for example for Factory Acceptance Test (FAT), Side Acceptance Test (SAT), Modification and other Services

SI	Phase of responsibility		Phase of intersections
	Phases 1 to 5	Not usually applied	Not usually applied
	Phase 9	E/EPES – System integration (only a subset of requirements have to be covered by the SI)	Sub phase 9.1 of E/E/PES-SLC: The customer of the SI (usually OP) has to provide all relevant functional requirements and safety requirements. Further inputs also provided by Product Care, Services: FAT, SAT, Modification, Repair (Statistics) SI is responsible for the required safety integrity level of delivered components or subsystems. This can be controlled for example due to FSAA.
	Phases 6 to 8	Not usually applied	See SM
	Phases 12 to 16	Not usually applied	See SM

The overview above shows that the allocation of related OSLC-Phases for SI is nearly the same as for SM. There are two slight differences: the intersection phase is a part of the E/E/PE System Integration Lifecycle (Phase 9.1) because the allocation of the functional requirements and safety requirements are (more or less) already done by the customer (OP). Second, the Safety Lifecycle requirements have to be interpreted on the basis of IEC61508, Part 1 and 2, because SI already use and apply existing and validated HW and SW components.

5. Allocation of IEC61511-SLP and related responsibilities for SI, SM, OP

The IEC61511 is an application specific standard and addresses the application of SIS for the Process Industries.

This means the standard is not directly relevant for SM. Nevertheless SM are addressed to support information for their safety systems, as explained in the chapter above, or they are also addressed to provide information to enable SI for example to fulfill the requirements for the HW-selection according to the “Prior use requirements” determined in the Standard.

In general the SIS - SLC applies for SI and OP. In the same way as the IEC61508 does, the IEC61511 defines basic requirements for MFS and FSA (Clause 5), Safety Lifecycle Structure and Planning (Clause 6.2) , as well as for Verification (Clause 7 ff) which apply to all phases of the SIS - SLC.

OP	Phase of responsibility		Phase of intersections
	Phases 1 to 3	Hazard and Risk assessment; Allocation of safety functions to protection layers; safety requirement specification for the safety instrumented system	Phase 3: To define functional and safety requirements necessary for the System Integration process done e.g. by SI
	Phase 4	No detailed experience until today	Responsible for FSAA
	Phases 5 to 8	Installation, Commissioning, Validation, Operation, Maintenance, Modification, Decommissioning	Operators have the overall responsibility e.g. SI could be a subcontractor, for example for Factory Acceptance Test (FAT), Side Acceptance Test (SAT), Modification and other Services

SI	Phase of responsibility		Phase of intersections
	Phases 1 to 3	Not usually applied	Phase 3 To determine all functional and safety requirements necessary to achieve the specified safety integrity
	Phase 4	E/EPES – System integration	Within the SLCP: Additional Subcontractors, e.g. for SW development Provide sufficient information to End-user, e.g. OP that the consecutive SLCP could be carried out correctly
	Phases 5 to 8	Not usually applied	Operators have the overall responsibility; e.g. SI could be a subcontractors, for example for Factory Acceptance Test (FAT), Side Acceptance Test (SAT), Modification and other Services

The overview above shows a similar structure as the overview presented for the IEC61508. There are also nearly the same phases of intersections whereas the meaning and characteristic of the intersection phases differs according to the requirements determined in the standards IEC61508 or IEC61511.

The IEC61508 refers to the IEC61511 in case of “Developing new HW devices”, “Developing embedded (system) SW”, and “Developing application SW using full variability languages”.

Furthermore the IEC61508 refers to the Modeling Methods of Part 6 for the use of the SIF probability failure calculation.

TÜV-ASI also recommends to consider the tables in IEC61508 Part 2 and 3 regarding the Measures for Fault Avoidance, which are not included in the IEC61511. The tables can be used as an easy checklist for planning or checking a safety relevant organization or project.

6. Recurring focal points discussed

The following chapters discuss selected topics which repeatedly give reason for extended and recurring discussions during FSMC and FSAA.

6.1 Service Provider and Sub - Contractors

Both the IEC61508 and IEC61511 define requirements for Service Provider or Sub-Contractors.

The standards determine: "Any supplier, providing products or services to an organization, having overall responsibility for one or more phases of the safety lifecycle shall deliver products or services as specified by that organization and shall have a Quality Management System."

This means for "that organization", procedures in place to handle and to control this MFS-intersection phase have to exist. Depending on the complexity and safety relevance the supplied object (HW and / or SW) has to be specified, designed, developed and tested in the same detail as it would be done by the ordering organization. To ensure this, Safety Audits or FSAA can be planned and carried out by that organization.

Additionally the SI have to be very sensitive to the following items:

- SI are responsible for the correct application of the used HW and SW components which are already validated, for instance according to IEC61508, by an other manufacturer
- SI are responsible for the required safety integrity level of used but not pre-validated HW and SW components (refer also to "Prior Use of HW" and "SW selection")

6.2 Functional Safety Assessment

The role of the Functional Safety Assessment during a safety related project has not always been understood correctly by the project partners of TÜV-ASI.

Mostly it was combined with the requirements of verification and validation activities. But this is incorrect, as the FSA additionally has to keep a defined grade of independency according to both standards the IEC61508 (Part 1, chapter 8) and IEC61511 (Clause 5.2.6.1).

As shown in the a.m. overviews, the FSA also has a special meaning for the relationship between a purchaser and the contractor, e.g. for the Operator and the Safety Integrator. (See next chapter which determines the relating requirements.)

This means the purchaser (the operator) has the responsibility to apply a FSA on the SLCP which will be carried out by the contractor, the SI. Consequently the operator has to apply at least two FSA: in the beginning and in the end of the lifecycle phases. Typically this is the intersection phase, in which all necessary functional and safety requirements (Phase 3) are agreed upon and the FAT at the end of Phase 4 takes place. It is recommended to plan a

third assessment after all design documents have been finished and the engineering of the safety application starts.

Actually the operators do not understand correctly, what their responsibilities to fulfill the FSA requirements are.

In chapter 2.2 the FSAA of TÜV-ASI, according to the IEC61508 requirements, have been described. This shows exemplarily, how these activities can also be carried out by independent organizations or independent business units of companies.

Generally the FSAA in safety related projects according to IEC61508 are very well known, accepted and applied, especially because of the TÜV support.

6.3 Independencies of Person

The independence of person which are carrying out for example verification and validation activities is not clearly defined in IEC61508 and IEC61511. It is of common understanding that persons in charge for the verification process should also be competent members of the project team which are not involved in the development of the verification object. The validation activities should be effected independently from the development team, for instance by the internal quality department or also by the customer (FAT).

Members of the FSAA-Team have to be independent from the development team. Both standards have this in common. IEC61508 furthermore specifies a graduated level of independency.

6.4 Information Feedback

A fundamental characteristic of a QMS is to integrate procedures for information feedback and the control of related information. A typical example is the complaint management.

In the scope of IEC61508 and IEC61511 there must be a similar procedure which processes feed back information from different sources like: Marketing Services, Customers, Development Experiences, Test Experiences, Maintenance Activities, Field Returns, Repair etc..

The intention should be to collect and evaluate this amount of information, to feed back information in order to improve on the one hand the MFS organization and on the other hand to reveal systematic faults, which possibly appear in the design of a E/E/PE System or SIF.

Due to the resulting increase of Field Experiences there is also the possibility to recognize impacts of Common Cause Effects which have the same fault characteristic of systematic faults for safety related systems or functions.

6.5 Procedures of Corrective Actions

The “procedure of corrective actions”, according to IEC61511, is a MFS procedure which should be used whenever corrective actions during the SLCP are necessary.

Corrective actions are necessary, for example, if a deviation from the specification or plan during the verification of a SLCP has been determined or test criteria have not been met for example during FAT or SW testing, and so on.

If corrective actions have to be carried out the first measure is to execute a Safety Analysis which should clarify and document the reason for the failure or deviation and should be documented, whether safety functions or safety requirements are concerned by the impact.

Based on this Safety Analysis the Corrective Actions should be determined, decided and planned with an according step back in the SLCP.

The IEC61508 defines the same procedure as part of the Modification requirements. The Safety Analysis is called accordingly Impact Analysis which comprises the same corrective actions. It is also the common understanding that the Impact Analysis has to be carried out because of the same reasons as the Safety Analysis, like faults during tests etc..

7. Conclusion

This experience report gives an overview concerning several practice-related requirements of the Functional Safety Management according to IEC61508 and IEC61511. It focusses on System Manufacturers, System Integrators and Operators.

The practice-experience has been made by the TÜV-ASI project teams over the last three years which were involved in various Functional Safety Management Certification Procedures (**FSMC**) and Functional Safety Assessment Activities (**FSAA**).

The following statements mark the topics of the experience report:

- TÜV-ASI meets the IEC61508 requirements for “Project Management” twofold: in assessing the company’s QM-System during FSAA on a project level, e.g. as a part of the Type Approval, and on a company’s level by carrying out the FSMC procedure.
- It is an objective of the Functional Safety Management Certification to create an applicable and manageable Functional Safety Management System in order to integrate a “Safety Culture” in the audited company.
- It is often intended by a company to carry out one or more safety relevant projects to “learn” and to understand the MFS requirements and their meaning for the company’s Quality Management in a first step. In a second step it is intended to integrate and to certify it.
- Every lifecycle phase can be certified under consideration of the adjacent lifecycle phases and the necessary information relation.
- TÜV-ASI represent the opinion that it is also possible to create an applicable and manageable MFS on the basis of the “good engineering praxis” of a company.
- It is important for System Manufacturers, System Integrators and Operators to identify the Safety Lifecycle Phase for which they are responsible. Furthermore they have to define the phases of intersection to provide the correct and complete information for the consecutive Safety Lifecycle Phases.
- The relations of IEC61508 and IEC61511 should always be considered for the completeness and correct interpretation of safety related requirements.
- It is a fundamental characteristic of a QMS to integrate procedures for information feedback and the control of related information. In a Safety Management System this information should be used to reveal Systematic faults and Common Cause Effects.
- A “Procedure of corrective actions” is an essential part of a Safety Management System to document, analyze, track and solve for instance safety relevant faults.
- The role of Functional Safety Assessment is not always understood correctly by companies.
- Products of Service Provider or Sub-Contractors must be under the quality control of the ordering company. It must be shown that the required Safety Integrity Level is met

by the ordered product. Also Functional Assessment can be carried out to control this.

- To qualify HW components according to the requirements of IEC61511 - "Prior Use of HW" is difficult and costly and requires a extensive competence. Additionally the department performing the qualification, for example a System Integrator, is responsible for qualified results, while mostly depending on insufficient information of a manufacturer.