The Design & Engineering of Safety Instrumented Systems

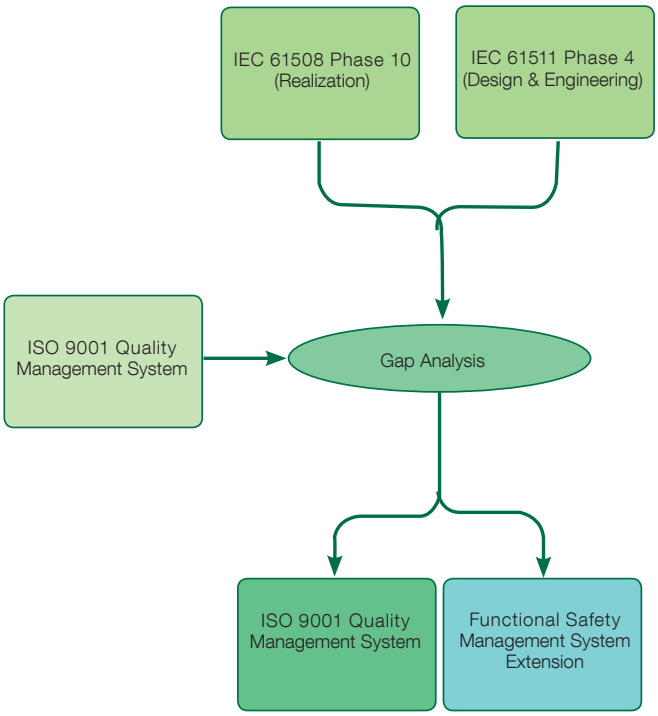
Experiences and Benefits of Using an Accredited and Certified Functional Safety Management System

The introduction of any new procedure is a challenge, when ABB rolled out its new Functional Safety Management System (FSMS) to its global Safety Execution Centers in over 20 countries; it needed to ensure that the transition was as smooth as possible.

The problem was a common one; how can you convince your engineers to use a new set of processes and how can you ensure that they are being used correctly? Both were essential in obtaining Accredited TÜV certification of the Safety Execution Centers 'Functional Safety Management Systems'. This was compounded further for the need to utilize a common suite of ABB FSMS procedures that could also incorporate any specific in-country additional requirements.

Process Development

Development of the Functional Safety Management System resulted from a gap analysis performed against the existing ISO9001 Quality Management System (QMS), and the requirements of the relevant clauses of the IEC61508 and IEC61511 (herein called 'the standards'). Having the QMS baseline was essential, as the process of gap analysis identified that many of the recommended techniques and measures required by the standards are generally accepted as good practice, and are therefore already part of the QMS.



Once the standards had been interpreted, terminology understood, and how they related to the existing QMS process, the additional Functional Safety Management System procedures could be identified, and the existing QMS extended.

An important tool from getting an early buy in from key SEC personnel was to ensure that they were involved in the gap analysis and subsequent FSMS process development. This not only increased confidence within the SEC that the new FSMS was necessary, but also drew on real life project experiences and documentation when developing the new processes. This approach not only reduced the cost of development, but also reduced cost in relation to roll out, training and long-term use.

Before using the FSMS, it was essential to gain pre-approval from the chosen certification body (TÜV). This 'affirmation of content' was not in itself certification of the FSMS, but instead a confirmation that it was fit for purpose. It was well understood that retrospectively changing the common FSMS procedures because they are fundamentally wrong is an expensive business particularly on a global scale thereby impacting all projects that had used the processes both in terms of functional safety and cost:

– In order to demonstrate compliance with the standards in terms of functional safety management, both the existing Quality Management System and the additional Functional Safety Management System Extension have to be used.

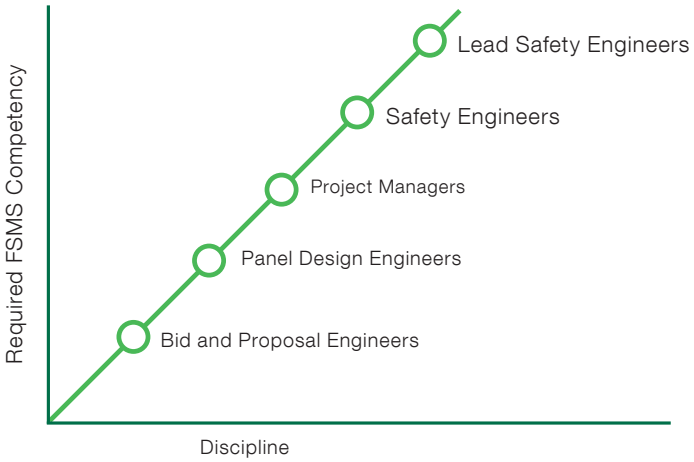
– In development of the FSMS use the experience of the project teams, and wherever possible, existing project documentation and processes.
– Ensure that the FSMS is fit for purpose before rolling out to projects.

Preparation and Training

Once the FSMS had received its pre-approval from TÜV it was necessary to prepare and deliver the training material which would be used to ensure that the SEC understood the purpose of the FSMS and how to use it.

Those requiring training were identified from the typical project lifecycle, from the initial bid and proposal through to delivery, installation and site acceptance of the safety system. This typical lifecycle involved the following people:
– Bid and Proposal Engineers
– Project Managers
– Lead Safety Engineers
– Safety Engineers
– Panel Design Engineers

Each of these different disciplines had different competency requirements, and so training had to be tailored to meet their specific needs.



Three training courses were developed to address these different competency requirements:
– Functional Safety Management Overview
– Functional Safety Management
– SIL Achievement

The Overview course was developed to provide an appreciation of the standards, functional safety management, and ABB's FSMS later identified and developed as ABB T140 and T141). The target audience was Bid and Proposal Engineers, Panel Design Engineers, and Project Managers. Specific emphasis was put on the individual responsibilities of these disciplines, for example, the need for independent, competent verification of hardware design drawings and schedules produced by Panel Design Engineers.

Detailed training in Functional Safety Management, SIL Achievement AND Functional Safety Assessment was provided to Safety Engineers and Lead Safety Engineers.

The course provided comprehensive training in the use of ABB's FSMS, working from project conception through to delivery and the requirements for the provision of an 'approved pool' of independent FS Assessors operating within the global FSMS programme.

As each stage of the project lifecycle was addressed, examples of how the new FSMS procedures should be used and example deliverable documents where presented. The aim of this detailed training was to ultimately prepare the prospective project teams for future safety projects, providing them with the tools required to execute those projects in accordance with ABB's FSMS, and subsequently the relevant phases of the IEC 61508 and IEC 61511 safety lifecycle.

An important deliverable of the training was to provide the evidence that team members had received training in Functional Safety Management and Functional Safety Assessment, in the form of ABB T140, T141 and SLCC FSA certificates and updated training databases. This evidence was later used as part of the competency assessments carried out on future safety projects.
– Ensure training is targeted and tailored to individual needs.
– Ensure evidence of completed training is documented and available.

Roll Out

Once pre-approval had been achieved, and training delivered, the FSMS required deploying within the SEC's.

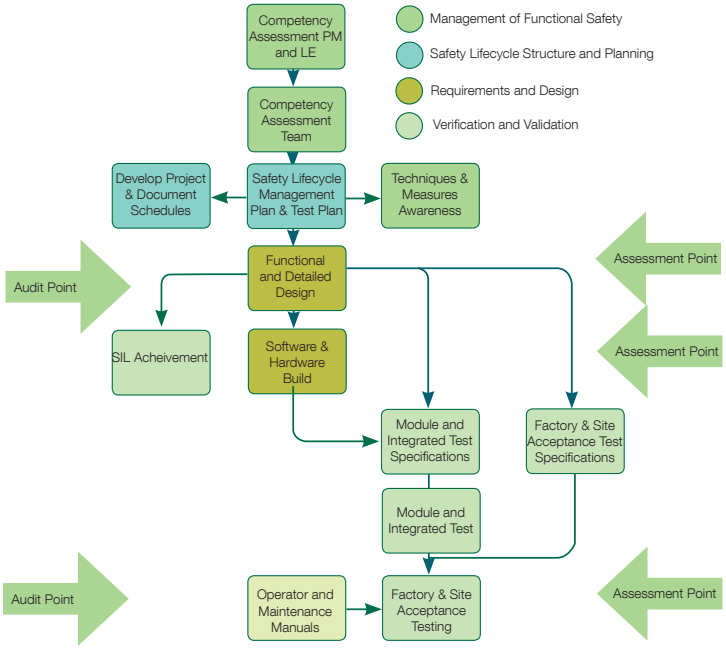
Deployment of the FSMS was a critical phase, after the date of issue, it was mandatory that every safety project from that date on must follow the new FSMS and critical as any of these safety projects could be the subject scrutiny by ABB's certification body, TÜV, as part of their annual surveillance or triennial certification audits.

Projects currently being executed at the time of deployment, were not required to re-engineer to meet the full requirements of the FSMS, however, where good practice could be adopted at specific stages of these existing projects, appropriate elements of the FSMS were adopted.

Design & Engineering Project Execution

The effectiveness of the FSMS could only be measured when adopted by safety projects and for the first safety project (called the 'pilot project'), it was crucial that the FSMS was used correctly, as this would form the basis of the TÜV certification audit.

For any project, having a high level plan of how it should be executed is essential, especially when starting to use a new management system. For the pilot safety project, the ideal time to develop this high level plan was during the internal project kick off meeting. This process set out the key tasks in order, and made sure that the project did not have to retrospectively complete any activities, which may have led to queries and observations being raised unnecessarily during project audits and functional safety assessments.



Competency Assessment

From the high level plan, it was clear that the first activity to be completed was ensuring that the project team members had been assessed for their competency as retrospective assessment would not be acceptable. The Lead Engineer, responsible for maintaining functional safety for the project, performed the competency assessments of all team members, including the Project Manager. (Note that the Lead Engineer was assessed by the Safety Execution Center Manager).

Competency assessment within ABB's FSMS is performed against a checklist, with acceptance criteria based on knowledge, experience, training and qualifications. (Note there are even more rigourous competency requirements and training to undertake for those colleagues wishing to be developed into functional safety assessors).

Each of these criteria is reviewed against the product selected for the project, the industry into which the project would be delivered, and the standards themselves. Any shortcomings in competency are mitigated by peer review or additional training. What was clear from the assessment process of the pilot project was that a person's role and responsibility must be clearly defined prior to their assessment, for example, someone that is assigned to the project as a test engineer, does not need extensive knowledge of transposing safety requirements to design, but they will require competency in specifying, witnessing and performing tests. It was also important to understand that if a person's role on the project changed, they must be re-assessed for their competency in the new role.

- Competency Assessment must be one of the first activities of a project.
- Competency should be assessed for the proposed job role.
- Changes in role may require competency to be re-assessed.

Safety Lifecycle Planning and Scheduling

Planning the lifecycle of a safety project is provided by a Safety Lifecycle Management Plan (SLMP) and Test Plan (TP), both key documents which set out the detailed strategy for how the project will be executed. ABB's FSMS contains a framework SLMP and TP, which can be tuned to a specific requirement. As framework documents, all of the essential information relating to safety lifecycle management and test planning are already embedded, and is pre-validated by the certification body (as part of the pre-approval process). For safety projects, the framework SLMP and TP are copied and modified to reflect the individual project requirements. For example, the pilot project did not have Site Acceptance within its scope of supply; as such this was removed from the scope of the project TP and SLMP, together with a justification statement.

The concept of framework documents introduces a cost saving in pre-prepared documentation, and also flexibility within the FSMS:

- Projects with no deviations from the standard FSMS can adopt the frameworks in their entirety, reducing the cost of document production.
- Projects with deviations from the standard FSMS can declare the deviations within the SLMP and TP, advising on their use and suitability, without the need to write project specific procedures. This may be required where a client has specific needs in terms of revision control, or how to handle errors found during testing. Functional safety, in respect of these changes will be checked during the verification process of the document, and also through Functional Safety Assessment (FSA).

One of the outputs of the detailed planning activities of the SLMP and TP is to produce the project, document, software and hardware schedules which identify all quantifiable elements (documents, software and hardware modules). Early identification of these project building blocks ensures that the scope and content of the project is clearly visible and that individual module progress can be tracked, helping to reduce systematic errors due to the incorrect sequencing of these activities.

- Use the SLMP and TP to identify changes in use of the FSMS and its procedures (Though do not compromise functional safety).
- Plan the project through the SLMP and TP to the project, document, software and hardware schedules.
- Ensure progress and status is tracked, and schedules updated on a regular basis.

Functional and Detailed Design

The technical design of a safety project is specified in the Functional Design Specification (FDS) and Detailed Design Specification (DDS), documents which define the solution for the Safety Instrumented System, addressing each of the requirements identified in the clients Safety Requirements Specification (SRS). Production of FDS and DDS documents is a well defined QMS process that was already established for the development of safety as well as non-safety projects. The fundamental difference with the design documentation for ABB's FSMS is that they are required to encompass key design features to ensure functional safety:

- The FDS includes a definition of each of the safety functions identified in the SRS. This traceability followed through to detailed design and test activities, allowing the project team, end user and assessors to trace individual Safety

Instrumented Functions from their conceptual design in the SRS through functional design in the FDS, detailed design in the DDS and on to Module, Integrated and Factory Acceptance Tests.

– Ensuring that the certification of hardware elements (for example Barrier, IO Module, Safety Controller) used in the design of the SIS remain valid, all restrictions on the use of these elements must be addressed and compliance demonstrated. The FDS provides the means by which each of these restrictions, extracted from the elements Safety Manual, are addressed – referencing the appropriate document, schedule or drawing providing which provided the necessary evidence of compliance.
– In the absence of a good SRS (as identified in IEC 61511 part 1 clause 10.3.1), the FDS can provide a mechanism to record any assumptions made regarding the design of the Safety Instrumented System.

ABB's FSMS contains a skeleton FDS and SDS, which can be tuned to a specific requirement. As skeleton documents, basic information required in these design documents are embedded (including product safety manual and SRS checklists), and is pre-validated by the certification body (as part of the pre-approval process).

– Ensure traceability between the SRS and Functional and Detailed Design Specifications.
– In the absence of a good SRS, use the FDS to define any assumptions made during the design of the SIS.
– Ensure that compliance to element Safety Manuals is documented in the FDS.

Build, Verification, Validation and Change Management

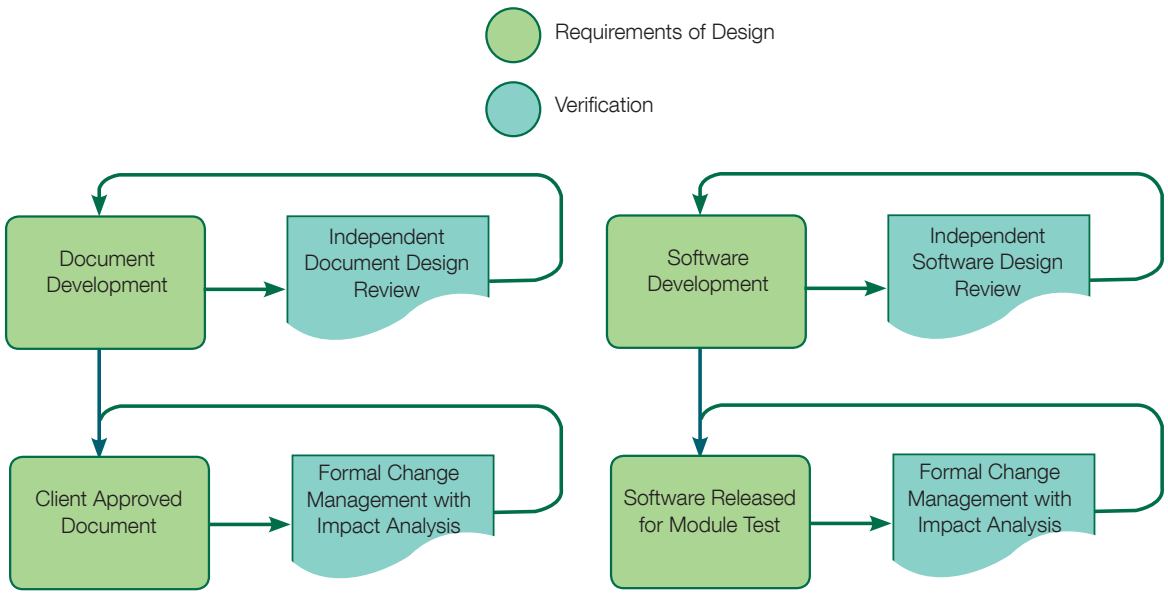
Build activities on safety projects continue as part of the normal project execution cycle, however more rigorous verification is introduced for both documentation and applications software during the design and build phase of the project. Formal independent review of both project documentation (including hardware design) and applications software is required. The outcome of independent reviews is recorded on design review forms, providing evidence that the activity had been performed, documenting review comments and the responses to these comments. Of course the reviewers themselves must be competent to perform this review activity.

Once documents have been approved by the client, and applications software released for module test, formal change control is introduced, necessitating a documented impact analysis for each proposed change. It is important to note however that prior to client approval of documentation and release of software to module test, the design and development process can continue, unhindered by the restraints of formal change management and as with all projects, there is always some fluidity in the design and build process until the design and software solutions can be fixed.

Modification to approved documentation and software released for module test is managed using a Change Management Tool (CMT) implemented as a Lotus Notes Database. The CMT enforces impact analysis of each change, ensuring that the engineer completing the proposed solution assesses the change for its impact on other modules (including documentation) of the SIS. The CMT generates a unique reference number for each change which is used as a reference point in the revision histories of both documents and application code. This methodology ensures that full traceability can be maintained for project deliverables. During execution of the pilot project, close monitoring was required during the test phases (Module, Integrated, Factory Acceptance and Site Acceptance), as project teams were used to recording errors and observations using a paper based 'punch-list' system – this process could not be used for the FSMS because of the need for formal impact analysis.

Document and software review records, verification and validation testing, together with formal change control with impact analysis provide some of the necessary techniques and tools identified in IEC 51508 to combat systematic errors.

– All project deliverables, including application software, require independent competent review.
– Formal change control need not start until first approval of documentation, or release of application software to module test.
– Impact analysis is required for all changes, including errors or observations found during verification and validation test phases.



SIL Achievement

Traditionally safety projects would produce a reliability report, demonstrating that the system met the target failure measure of the required SIL, whilst this was considered an onerous task, it was essentially a number crunching exercise, adding all component Pfd (or Pfh) figures to derive to average Pfd for the system.

Demonstration of achieved SIL for each safety project is not just about the target failure measure, it is a far more complex analysis, requiring that each safety function (not safety system) meets the requirements of the target SIL in terms of the following parameters:

- Architectural Constraints, in terms of:
  - Safe Failure Fraction (SFF) and
  - Hardware Fault Tolerance (HFT)
- Target Failure Measure, expressed as either:
  - Pfd, or
  - Dangerous Failure Rate (Pfh)
- Systematic Capability, in terms of:
  - Each element that carries out the safety function.
  - The method by which the safety instrumented function was designed and implemented.

Only when a safety instrumented function meets the criteria set by IEC 61508 in terms of architectural constraint, target failure measure and systematic capability, can the target SIL be said to be achieved. It was because of this increased complexity that the training courses where given in SIL Achievement as part of the FSMS development and roll out process.

What became evident during the SIL Achievement demonstration of the pilot project was that it was absolutely essential to have selected the correct elements (Barrier, Relay, Safety Controller) for each safety function. Whilst each element may be technically suitable for use, in order to demonstrate its suitability in terms of functional safety, the manufacturer would also be required to provide data regarding architectural constraint, target failure measure and systematic capability. Preliminary selection of the correct equipment had to be performed during the conceptual design performed during the bid and proposal process, even before the order had been awarded. Without this awareness during the bid preparation, demonstrating SIL Achievement during the project would become extremely difficult.

ABB's FSMS includes a 'Bid and Proposal Checklist', which provides guidance during the sales pursuit of a safety project. The checklist provides a set of prompts when assessing client requirements, and allows assumptions regarding the proposed design to be documented in the absence of a safety requirements specification. Through the analysis of the client requirements during the bid and proposal process, suitable equipment can be specified, and through dialogue with suppliers, it is ensured that the data required to demonstrate SIL Achievement was available.

- SIL Achievement is not just about Pfd.
- SIL Achievement is required to be demonstrated for each SIF.
- Ensure equipment is specified that has all necessary data required to demonstrate the achievement of the target SIL.

Audit and Assessment

Audit and assessment are an integral part of demonstrating functional safety, and these activities must be clearly identified and scheduled during the planning phase of the project. Both activities should be seen as beneficial to the project, ensuring that compliance to the FSMS and to the standard is monitored throughout the project. Care should be taken to ensure that any actions resulting from audit and assessment are acted on quickly, reducing the risk of propagating errors through the project lifecycle.

To ensure correct use of the FSMS, two audits are executed for safety projects. The first audit performed after FDS completion, and the second after FAT. The purpose of the two stage audit is to identify any non conformity early, ensuring that any retrospective corrections are kept to a minimum. The two stage audit can be reduced to a single audit when the FSMS is well understood and used correctly by project teams.

The purpose of the Functional Safety Assessment (FSA) is to review the pilot project in terms of its achievement of functional safety, ensuring its compliance to the relevant clauses of IEC 61508 and IEC 61511. The process of assessment is controlled using a Functional Safety Assessment procedure, which is part of the FSMS.

Using the procedure, and a framework report template, assessment is carried out on the pilot project. The assessment process is divided into three phases:

- Preliminary FSA - Post planning
- Design FSA – Post design
- Final FSA – Post validation

As with the audit, the purpose of the three stage assessment is to identify any non conformity early, ensuring that any retrospective corrections where kept to a minimum.

- Ensure Audit and Assessment Activities are clearly identified on the project plan.
- Ensure audit and assessment actions are completed in good time.

Feedback and Periodic Review

An important part of any quality management system is ensuring its effectiveness; the FSMS requires periodic review and update, based on project experience. This provides another opportunity for involvement of project teams, promoting a collective ownership, which ensures that the procedures and processes are more effectively used on future safety projects.

An example of the effectiveness of this feedback and review process was evident during execution of the pilot project. Early in the project, it was identified that the Techniques and Measures framework document did not need to be updated when the project specific version was created. This was due to the generic nature of the original document, and its reference out to all elements of the standard FSMS. Through the review process it was decided that this document would be converted into a procedure, as such would not need to be re-created for each safety project. This had the effect of reducing documentation hours required on future safety projects.

It should be considered that any change to the FSMS may require re-training in the use of the updated processes. In the case of the Techniques and Measures specification mentioned above, this was essential. As the document was no longer project specific (i.e. it did not need to be created for each safety project), further training had to be given on its purpose and role, ensuring that the safety team where aware that even though they did not need to produce the document, that it was still a key component of the overall FSMS.

– Ensure periodic review of the FSMS, involve project teams.
– Assess any changes for the need to re-train project teams.

FSMS Extension

Based on the significant legacy of FSMS implementation on a global basis and over several years, it has been relatively straightforward for ABB to develop FSMS extensions to cover additional safety standard lifecycle requirements. Today, ABB has a FSMS extension in place that is certified by TuV for the operations and maintenance phases of the IEC 61508/61511 lifecycle i.e. phases 14 & 15 and 6 & 7 respectively.

Again the requirements for preventative, corrective maintenance repair and modification are in alignment with the content and principals of this paper.

Conclusions

Implementation of a FSMS does not need to be an onerous task. If an organization already has a well established and well understood QMS, the additional work required for functional safety is relatively small. Ensuring that project teams are involved early in the development of the FSMS is essential, as is ensuring that the reason for the new processes is as clearly understood as how to use them. If project teams can understand the benefits of a FSMS, they will be more likely to adopt them in practice, and using a common approach for implementation ensures expertise grows quickly. Those responsible for the development and maintenance of a FSMS must ensure that:

– There is no ambiguity in what needs to be delivered, ensure procedures and processes have a clearly defined function.
– Ensure project teams have a clear definition of how the project should be executed.
– Ensure project teams understand the flexibility of the FSMS.
– Ensure that later projects benefit from project documentation already produced, for example Operator and Maintenance Manuals can easily be re-used.
– Audit and Assessment become second nature.

Together with the extensive hazard and risk services and world leading expertise, as found within the front-end functional safety lifecycle phase requirements provided by the ABB Consultancy Group, then ABB is the partner of choice for our clients for best in class functional safety management compliance services and SIL 3 capable solutions and products.

Stuart Nunns, Managing Consultant ABB Safety Lead Competency Center

John Walkington, Manager, Safety Lead Competency Center

Assured and certified products, services, delivery and execution.

For further information please contact:
ABB Safety Lead Competency Centre
Howard Road, Eaton Socon, St Neots
Cambridgeshire, PE19 8EU
Phone: +44 (0)1480 475321
E-Mail: oilandgas@gb.abb.com
www.abb.com/oilandgas